Dhanya Thakkar

Preventing Digital Extortion

Mitigate ransomware, DDoS, and other cyber-extortion attacks

Packt

Preventing Digital Extortion

Mitigate ransomware, DDoS, and other cyber-extortion attacks

Dhanya Thakkar

BIRMINGHAM - MUMBAI

Preventing Digital Extortion

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: May 2017

Production reference: 1240517

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.
ISBN 978-1-78712-036-5

www.packtpub.com

Credits

Author
Dhanya Thakkar

Reviewer
Abhijit Mohanta

Acquisition Editor
Prachi Bisht

Content Development Editor
Sweeny Dias

Technical Editor
Mohit Hassija

Copy Editor
Safis Editing

Project Coordinator
Virginia Dias

Proofreader
Safis Editing

Indexer
Aishwarya Gangawane

Graphics
Kirk D'Penha

Production Coordinator
Deepika Naik

About the Author

A transformation specialist with over 20 years' experience as a business leader focused on the next generation of enterprise companies including security, **Dhanya Thakkar** understands how to help organizations drive innovation, compliance, and business efficiency while managing risk without compromising security. With a strong track record in leadership roles in top-tier technology firms and in various start-ups, he is recognized as an industry thought leader and is regularly quoted by the press on issues surrounding information security, cybercrime, and the future of technology by trade, national, and international media.

A highly dynamic and extremely skilled executive who successfully blends technological acumen and business skills, he has a proven track record in demonstrating to organizations how to operationalize their cyber security policies with effective tools, processes, and people.

He is the co-inventor of two patented technologies and has published articles on software technology. He earned his bachelor's degree in computer science from Maharaja Sayajirao University in India. He completed the Executive Program at Queen’s School of Business. He has helped create and grow multiple technology businesses and product lines to market-leading positions and is also a frequent speaker at conferences and forums around the world.

To my father, who in 1984 wrote a book titled "On the structuring of Sanskrit drama: structure of drama in Bharata and Aristotle." I could not understand most of his book. I decided that someday I would return the favor to him.

About the Reviewer

Abhijit Mohanta has a decade of experience in cyber security. He has worked as a security researcher for malware labs in Symantec, Mcafee, and Cyphort and has a rich experience in dealing with various kinds of cyber attacks involving web application vulnerabilities, operating system vulnerabilities, and malware. His expertise includes malware reverse engineering, vulnerability research, and Windows programming. He has published several blogs related to malware research and is passionate about exploring new technologies such as machine learning and big data. He is an active member in security communities such as Cysinfo.

Beyond computers, he is a fitness freak and a foodie. He loves to hit the gym daily, go swimming, and practice yoga.

> *I would like to thank my family and friends, who inspire and encourage me to explore new things in life.*

Customer Feedback

Thanks for purchasing this Packt book. At Packt, quality is at the heart of our editorial process. To help us improve, please leave us an honest review on this book's Amazon page at `https://www.amazon.com/dp/1787120368`.

If you'd like to join our team of regular reviewers, you can e-mail us at `customerreviews@packtpub.com`. We award our regular reviewers with free eBooks and videos in exchange for their valuable feedback. Help us be relentless in improving our products!

Table of Contents

Preface

In today’s digital age, hacking into data, encrypting it, and making it inaccessible is becoming more and more commonplace. Irrespective of the scale of your business, such an attack can prove very costly. If you want to save yourself from such cyber extortion, it is important to gain insights into various attacks and their impact on your business. This book gives you a brief overview of the process and will also teach you to mitigate or eliminate such attacks. It will not only teach you about cyber attacks, but will also equip you to mitigate them. Be it computers, smartphones, servers, or IoT devices this step by step practical guide will teach you to secure any environment. Apart from this, we will also teach you to leverage various security tools available.

What this book covers

`Chapter 1`, *Introduction to Cyber Extortion*, is an overview of the concept of cyber crime and how cyber extortion fits into overall cyber crime.

`Chapter 2`, *DDoS Extortion*, covers all DDoS attacks, which hold companies ransom by threatening to shut down services, servers, or websites.

`Chapter 3`, *Avoiding Data Theft Extortion*, gives insight into attacks where attackers take sensitive data hostage and extort the users and the corporations.

`Chapter 4`, *Mitigating Locker Ransomware*, dives deep into the world of locker ransomware and teaches you about the different approaches to defending against locker ransomware.

`Chapter 5`, *Crypto Ransomware Prevention Techniques*, teaches you about crypto ransomware and its different stages.

`Chapter 6`, *Exploring Mobile Extortions*, covers mobile ransomware extortion with practical examples.

`Chapter 7`, *Follow the Money*, details the cybercriminal world and digital currency in detail and how money flows in various types of extortion.

`Chapter 8`, Held Hostage – What Now?, tells you about the different options you have if your system has been compromised, along with details about the world of cyber insurance.

`Chapter 9`, *Extortion of the Future*, finishes the book with final thoughts, with an eye toward the future, especially mobile and Internet of Things (IOT) technology, and discusses the attacks of the future on servers as well as how machine learning will play a big role in attacks as well as defense.

What you need for this book

You don't need programming experience to understand this book--just an appetite for and interest in the digital extortion scene.

Who this book is for

This book targets IT security managers, IT security engineers, security analysts, and professionals who are eager to avoid digital extortion for themselves or their organizations. They may have heard of such attacks, but are not aware of their various types, techniques, and business impact.

Conventions

In this book, you will find a number of text styles that distinguish between different kinds of information. Here are some examples of these styles and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "Risky files belong to the family of executable files. Users should particularly avoid e-mails containing attachments with phishing-prone extensions, such as `.exe`, `.js`, `.vbs`, and `.ps` files, or document files that can support macros, such as `.doc`, `.xls`, or `.xlm`."

Any command-line input or output is written as follows:

```
%USERPROFILE%\Start Menu\Programs\Startup\[reveton_filename].dll.lnk
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\
[reveton_filename]dll.lnk
```

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book-what you liked or disliked. Reader feedback is important for us as it helps us develop titles that you will really get the most out of.

To send us general feedback, simply e-mail feedback@packtpub.com, and mention the book's title in the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide at www.packtpub.com/authors.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books-maybe a mistake in the text or the code-we would be grateful if you could report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting http://www.packtpub.com/submit-errata, selecting your book, clicking on the **Errata Submission Form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded to our website or added to any list of existing errata under the Errata section of that title.

To view the previously submitted errata, go to https://www.packtpub.com/books/content/supportand enter the name of the book in the search field. The required information will appear under the **Errata** section.

Piracy

Piracy of copyrighted material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works in any form on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors and our ability to bring you valuable content.

Questions

If you have a problem with any aspect of this book, you can contact us at `questions@packtpub.com`, and we will do our best to address the problem.

1
Introduction to Cyber Extortion

A huge and fundamental shift is taking place.

We often make the mistake of relying on the past for predicting the future, and nowhere is this more relevant than in the sphere of the Internet and smart technology. People, processes, data, and things are tightly and increasingly connected, creating new, intelligent networks unlike anything else we have seen before. The growth is exponential and the consequences are far reaching for individuals, and progressively so for businesses. We are creating the Internet of Things and the Internet of Everything.

It has become unimaginable to run a business without using the Internet. It is not only an essential tool for current products and services, but an unfathomable well for innovation and fresh commercial breakthroughs. The transformative revolution is spilling into the public sector, affecting companies like vanguards and diffusing to consumers, who are in a feedback loop with suppliers, constantly obtaining and demanding new goods.

Advanced technologies that apply not only to machine-to-machine communication but also to smart sensors generate complex networks to which theoretically anything that can carry a sensor can be connected. Cloud computing and cloud-based applications provide immense yet affordable storage capacity for people and organizations and facilitate the spread of data in more ways than one.

Keeping in mind the Internet's nature, the physical boundaries of business become blurred, and virtual data protection must incorporate a new characteristic of security: encryption.

In the middle of the storm of the IoT, major opportunities arise, and equally so, unprecedented risks lurk. People often think that what they put on the Internet is protected and closed information. It is hardly so. Sending an e-mail is not like sending a letter in a closed envelope. It is more like sending a postcard, where anyone who gets their hands on it can read what's written on it.

Along with people who want to utilize the Internet as an open business platform, there are people who want to find ways of circumventing legal practices and misusing the wealth of data on computer networks by unlawfully gaining financial profits, assets, or authority that can be monetized.

Being connected is now critical. As cyberspace is growing, so are attempts to violate vulnerable information gaining global scale. This newly discovered business dynamic is under persistent threat of criminals. *Cyberspace*, *cybercrime*, and *cybersecurity* are perceptibly being found in the same sentence.

Let's get back to the purpose of this book. We will learn about:

- Cybercrime
- Digital extortion
- Ransomware

Cybercrime - underdefined and underregulated

A massive problem encouraging the perseverance and evolution of cybercrime is the lack of an adequate unanimous definition and the underregulation on a national, regional, and global level. Nothing is criminal unless stipulated by the law. Global law enforcement agencies, academia, and state policies have studied the constant development of the phenomenon since its first appearance in 1989, in the shape of the AIDS Trojan virus transferred from an infected floppy disk.

Regardless of the bizarre beginnings, there is nothing entertaining about cybercrime. It is serious. It is dangerous.

Significant efforts are made to define cybercrime on a conceptual level in academic research and in national and regional cybersecurity strategies. Still, as the nature of the phenomenon evolves, so must the definition. Research reports are still at a descriptive level, and underreporting is a major issue. On the other hand, businesses are more exposed due to ignorance of the fact that modern-day criminals increasingly rely on the Internet to enhance their criminal operations.

Case in point: Aaushi Shah and Srinidhi Ravi from the Asian School of Cyber Laws have created a cybercrime list by compiling a set of 74 distinctive and creatively named actions emerging in the last three decades that can be interpreted as cybercrime. These actions target anything from e-mails to smartphones, personal computers, and business intranets: *piggybacking*, *joe jobs*, and *easter eggs* may sound like cartoons, but their true nature resembles a crime thriller.

The concept of cybercrime

Cyberspace is a giant community made out of connected computer users and data on a global level. As a concept, cybercrime involves any criminal act dealing with computers and networks, including traditional crimes in which the illegal activities are committed through the use of a computer and the Internet.

As businesses become more open and widespread, the boundary between data freedom and restriction becomes more porous. Countless e-shopping transactions are made, hospitals keep record of patient histories, students pass exams, and around-the-clock payments are increasingly processed online. It is no wonder that criminals are relentlessly invading cyberspace trying to find a slipping crack.

There are no recognizable border controls on the Internet, but a business that wants to evade harm needs to understand cybercrime's nature and apply means to restrict access to certain information.

Instead of identifying it as a single phenomenon, Majid Jar proposes a **common denominator** approach for all ICT-related criminal activities. In his book *Cybercrime and Society*, Jar refers to Thomas and Loader's working concept of cybercrime as follows:

> *"Computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic network."*

Jar elaborates the important distinction of this definition by emphasizing the difference between **crime** and **deviance**. Criminal activities are explicitly prohibited by formal regulations and bear sanctions, while deviances breach informal social norms. This is a key note to keep in mind. It encompasses the evolving definition of cybercrime, which keeps transforming after resourceful criminals who constantly think of new ways to gain illegal advantages.

Law enforcement agencies on a global level make an essential distinction between two subcategories of cybercrime:

- Advanced cybercrime or high-tech crime
- Cyber-enabled crime

The first subcategory, according to Interpol, includes newly emerged sophisticated attacks against computer hardware and software.

On the other hand, the second category contains **traditional** crimes in modern clothes: for example, crimes against children, such as exposing children to illegal content; financial crimes, such as payment card frauds, money laundering, and counterfeiting currency and security documents; social engineering frauds; and even terrorism.

We are much beyond the limited impact of the 1989 cybercrime embryo. Intricate networks are created daily. They present new criminal opportunities, causing greater damage to businesses and individuals, and require a global response. Cybercrime is conceptualized as a service embracing a commercial component. Cybercriminals work as businessmen who look to sell a product or a service to the highest bidder.

Critical attributes of cybercrime

An abridged version of the cybercrime concept provides answers to three vital questions:

- Where are criminal activities committed and what technologies are used?
- What is the reason behind the violation?
- Who is the perpetrator of the activities?

Where and how - realm

Cybercrime can be an online, digitally committed, traditional offense. Even if the component of an online, digital, or virtual existence were not included in its nature, it would still have been considered crime in the traditional, real-world sense of the word. In this sense, as the nature of cybercrime advances, so must the spearheads of law enforcement rely on laws written for the non-digital world to solve problems encountered online. Otherwise, the combat becomes stagnant and futile.

Why - motivation

The prefix "cyber" sometimes creates additional misperception when applied to the digital world. It is critical to differentiate cybercrime from other malevolent acts in the digital world by considering the reasoning behind the action. This is not only imperative for clarification purposes, but also for extending the definition of cybercrime over time to include previously indeterminate activities.

Offenders commit a wide range of dishonest acts for selfish motives such as monetary gain, popularity, or gratification. When the intent behind the behavior is misinterpreted, confusion may arise and actions that should not have been classified as cybercrime could be charged with criminal prosecution.

Who - the criminal deed component

The action must be attributed to a perpetrator. Depending on the source, certain threats can be translated to the criminal domain only or expanded to endanger potential larger targets, representing an attack to national security or a terrorist attack.

Undoubtedly, the concept of cybercrime needs additional refinement, and a comprehensive global definition is in progress. Along with global cybercrime initiatives, national regulators are continually working on implementing laws, policies, and strategies to exemplify cybercrime behaviors and thus strengthen combating efforts.

Types of common cyber threats

In their endeavors to raise cybercrime awareness, the United Kingdom's **National Crime Agency** (**NCA**) divided common and popular cybercrime activities by affiliating them with the target under threat. While both individuals and organizations are targets of cyber criminals, it is the business-consumer networks that suffer irreparable damages due to the magnitude of harmful actions.

Cybercrime targeting consumers

Some forms of cybercrime target individual consumers. The following are some examples:

- **Phishing:** The term encompasses behavior where illegitimate e-mails are sent to the receiver to collect security information and personal details

- **Webcam manager:** A webcam manager is an instance of gross violating behavior in which criminals take over a person's webcam
- **File hijacker:** Criminals hijack files and hold them "hostage" until the victim pays the demanded ransom
- **Keylogging:** With keylogging, criminals have the means to record what the text behind the keys you press on your keyboard is
- **Screenshot manager:** A screenshot manager enables criminals to take screenshots of an individual's computers screen
- **Ad clicker:** Annoying but dangerous ad clickers direct victims' computer to click on a specific harmful link

Cybercrime targeting businesses

On the other hand, there is cybercrime that targets businesses as well:

- **Hacking:** Hacking is basically unauthorized access to computer data. Hackers inject specialist software with which they try to take administrative control of a computerized network or system. If the attack is successful, the stolen data can be sold on the dark web and compromise people's integrity and safety by intruding and abusing the privacy of products as well as sensitive personal and business information. Hacking is particularly dangerous when it compromises the operation of systems that manage physical infrastructure: for example, public transportation.
- **Distributed denial of service (DDoS) attacks:** When an online service is targeted by a DDoS attack, the communication links overflow with data from messages sent simultaneously by **botnets**. Botnets are a bunch of controlled computers that stop legitimate access to online services for users. The system is unable to provide normal access as it cannot handle the huge volume of incoming traffic.

Cybercrime in relation to overall computer crime

Many moons have passed since 2001, when the first international treaty that targeted Internet and computer crime-the Budapest Convention on Cybercrime-was adopted. The Convention's intention was to harmonize national laws, improve investigative techniques, and increase cooperation among nations. It was drafted with the active participation of the Council of Europe's observer states, Canada, Japan, South Africa, and the United States and drawn up by the Council of Europe in Strasbourg, France. Brazil and Russia, on the other hand, refused to sign the document on the basis of not being involved in the Convention's preparation.

In *The Understanding Cybercrime: A Guide to Developing Countries* (Gercke, 2011), Marco Gercke makes an excellent final point:

> *"Not all computer-related crimes come under the scope of cybercrime. Cybercrime is a narrower notion than all computer-related crime because it has to include a computer network. On the other hand, computer-related crime in general can also affect stand-alone computer systems."*

Although progress has been made, consensus over the definition of cybercrime is not final. Keeping history in mind, a fluid and developing approach must be kept in mind when applying working and legal interpretations. In the end, international noncompliance must be overcome to establish a common and safe ground to tackle persistent threats.

Cybercrime localized - what is the risk in your region?

Europol's heat map for the period between 2014 and 2015 reports on the geographical distribution of cybercrime on the basis of the United Nations geoscheme. The data in the report encompassed cyber-dependent crime and cyber-enabled fraud, but it did not include investigations into online child sexual abuse.

North and South America

Due to its overwhelming presence, it is not a great surprise that the North American region occupies several lead positions concerning cybercrime, both in terms of enabling malicious content and providing residency to victims in the regions that participate in the global cybercrime numbers.

The United States hosted between 20% and nearly 40% of the total world's command-and-control servers during 2014. Additionally, the US currently hosts over 45% of the world's phishing domains and is in the pack of world-leading spam producers. Between 16% and 20% percent of all global bots are located in the United States, while almost a third of point-of-sale malware and over 40% of all ransomware incidents were detected there. Twenty EU member states have initiated criminal procedures in which the parties under suspicion were located in the United States. In addition, over 70 percent of the countries located in the Single European Payment Area have been subject to losses from skimmed payment cards because of the distinct way in which the US, under certain circumstances, processes card payments without chip-and-PIN technology.

There are instances of cybercrime in South America, but the scope of participation by the southern continent is way smaller than that of its northern neighbor, both in industry reporting and in criminal investigations. Ecuador, Guatemala, Bolivia, Peru, and Brazil are constantly rated high on the malware infection scale, and the situation is not changing, while Argentina and Colombia remain among the top 10 spammer countries. Brazil has a critical role in point-of-sale malware, ATM malware, and skimming devices.

Europe

The key aspect making Europe a region with excellent cybercrime potential is the fast, modern, and reliable ICT infrastructure. According to *The Internet Organized Crime Threat Assessment (IOCTA) 2015*, ckybercriminals abuse Western European countries to host malicious content and launch attacks inside and outside the continent. EU countries host approximately 13 percent of the global malicious URLs, out of which Netherlands is the leading country, while Germany, the UK, and Portugal come second, third, and fourth respectively. Germany, the UK, the Netherlands, France, and Russia are important hosts for bot C&C infrastructure and phishing domains, while Italy, Germany, the Netherlands, Russia, and Spain are among the top sources of global spam. Scandinavian countries and Finland are famous for having the lowest malware infection rates.

France, Germany, Italy, and to some extent the UK have the highest malware infection rates and the highest proportion of bots found within the EU. However, the findings are presumably the result of the high population of the aforementioned EU countries. A half of the EU member states identified criminal infrastructure or suspects in the Netherlands, Germany, Russia, or the United Kingdom. One third of the European law enforcement agencies confirmed connections to Austria, Belgium, Bulgaria, the Czech Republic, France, Hungary, Italy, Latvia, Poland, Romania, Spain, or Ukraine.

Asia

China is the United States' counterpart in Asia in terms of the top position concerning reported threats to Internet security. Fifty percent of the EU member states' investigations on cybercrime include offenders based in China. Moreover, certain authorities quote China as the source of one third of all global network attacks. In the company of India and South Korea, China is third among the top-10 countries hosting botnet C&C infrastructure, and it has one of the highest global malware infection rates. India, Indonesia, Malaysia, Taiwan, and Japan host serious bot numbers, too.

Japan takes on a significant part both as a source country and as a victim of cybercrime. Apart from being an abundant spam source, Japan is included in the top three Asian countries where EU law enforcement agencies have identified cybercriminals. On the other hand, Japan, along with South Korea and the Philippines, is the most popular country in the East and Southeast region of Asia where organized crime groups run sextortion campaigns.

Vietnam, India, and China are the top Asian countries featuring spamming sources. Alternatively, China and Hong Kong are the most prominent locations for hosting phishing domains. From another point of view, the **country code top-level domains** (**ccTLDs**) for Thailand and Pakistan are commonly used in phishing attacks. In this region, most SEPA members reported losses from the use of skimmed cards. In fact, five (Indonesia, Philippines, South Korea, Vietnam, and Malaysia) out of the top six countries are from this region.

Africa

Africa remains renowned for combined and sophisticated cybercrime practices. Data from the Europol heat map report indicates that the African region holds a ransomware-as-a-service presence equivalent to the one of the European black market. Cybercriminals from Africa make profits from the same products. Nigeria is on the list of the top 10 countries compiled by the EU law enforcement agents featuring identified cybercrime perpetrators and related infrastructure. In addition, four out of the top five top-level domains used for phishing are of African origin: `.cf`, `.za`, `.ga`, and `.ml`.

Australia and Oceania

Australia has two critical cybercrime claims on a global level:

- First, the country is present in several top-10 charts in the cybersecurity industry, including bot populations, ransomware detection, and network attack originators.
- Second, the country-code top-level domain for the Palau Islands in Micronesia is massively used by Chinese attackers as the TLD with the second highest proportion of domains used for phishing.

Cybercrime in numbers

Experts agree that the past couple of years have seen digital extortion flourishing. In 2015 and 2016, cybercrime reached epic proportions. Although there is agreement about the serious rise of the threat, putting each ransomware aspect into numbers is a complex issue. Underreporting is not an issue only in academic research but also in practical case scenarios. The threat to businesses around the world is growing, because businesses keep it quiet. The scope of extortion is obscured because companies avoid reporting and pay the ransom in order to settle the issue in a conducive way. As far as this goes for corporations, it is even more relevant for public enterprises or organizations that provide a public service of any kind. Government bodies, hospitals, transportation companies, and educational institutions are increasingly targeted with digital extortion. Cybercriminals estimate that these targets are likely to pay in order to protect drops in reputation and to enable uninterrupted execution of public services.

When CEOs and CIOs keep their mouths shut, relying on reported cybercrime numbers can be a tricky question. The real picture is not only what is visible in the media or via professional networking, but also what remains hidden and is dealt with discreetly by the security experts.

In the second quarter of 2015, Intel Security reported an increase in ransomware attacks by 58%. Just in the first 3 months of 2016, cybercriminals amassed $209 million from digital extortion.
By making businesses and authorities pay the relatively small average ransom amount of $10,000 per incident, extortionists turn out to make smart business moves. Companies are not shaken to the core by this amount. Furthermore, they choose to pay and get back to business as usual, thus eliminating further financial damages that may arise due to being out of business and losing customers.

Extortionists understand the nature of ransom payment and what it means for businesses and institutions. As sound entrepreneurs, they know their market. Instead of setting unreasonable skyrocketing prices that may cause major panic and draw severe law enforcement action, they keep it low profile. In this way, they maintain the dark business in flow, moving from one victim to the next and evading legal measures.

A peculiar perspective - cybercrime in absolute and normalized numbers

> *"To get an accurate picture of the security of cyberspace, cybercrime statistics need to be expressed as a proportion of the growing size of the Internet similar to the routine practice of expressing crime as a proportion of a population, i.e., 15 murders per 1,000 people per year."*

This statement by Eric Jardine from the *Global Commission on Internet Governance* (Jardine, 2015) launched a new perspective of cybercrime statistics, one that accounts for the changing nature and size of cyberspace.

The approach assumes that viewing cybercrime findings isolated from the rest of the changes in cyberspace provides a distorted view of reality. The report aimed at normalizing crime statistics and thus avoiding negative, realistic cybercrime scenarios that emerge when drawing conclusions from the limited reliability of absolute numbers.

In general, there are three ways in which absolute numbers can be misinterpreted:

- Absolute numbers can negatively distort the real picture, while normalized numbers show whether the situation is getting better
- Both numbers can show that things are getting better, but normalized numbers will show that the situation is improving more quickly
- Both numbers can indicate that things are deteriorating, but normalized numbers will indicate that the situation is deteriorating at a slower rate than absolute numbers

Additionally, the **Global Commission on Internet Governance (GCIG)** report includes some excellent reasoning about the nature of empirical research undertaken in the age of the Internet. While almost everyone and anything is connected to the network and data can be easily collected, most of the information is fragmented across numerous private parties. Normally, this entangles the clarity of the findings of cybercrime presence in the digital world. When data is borrowed from multiple resources and missing slots are modified with hypothetical numbers, the end result can be skewed.

Keeping in mind this observation, it is crucial to emphasize that the GCIG report measured the size of cyberspace by accounting for eight key aspects:

- The number of active mobile broadband subscriptions
- The number of smartphones sold to end users
- The number of domains and websites
- The volume of total data flow
- The volume of mobile data flow
- The annual number of Google searches
- The Internet's contribution to GDP

It has been illustrated several times during this introduction that as cyberspace grows, so does cybercrime. To fight the menace, businesses and individuals enhance security measures and put more money into their security budgets.

A recent **Centre for International Governance Innovation - Ipsos** (**CIGI-Ipsos**) survey collected data from 23,376 Internet users in 24 countries, including Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, South Africa, South Korea, Sweden, Tunisia, Turkey, and the United States.

Survey results showed that 64% of users were more concerned about their online privacy compared to the previous year, whereas 78% were concerned about having their banking credentials hacked. Additionally, 77% of users were worried about cyber criminals stealing private images and messages. These perceptions led to behavioral changes: 43% of users started avoiding certain sites and applications, some 39% regularly updated passwords, while about 10% used the Internet less (CIGI-Ipsos, 2014).

GCIC report results are indicative of a heterogeneous cybersecurity picture. Although many cybersecurity aspects are deteriorating over time, there are some that are staying constant, and a surprising number are actually improving. Jardine compares cyberspace security to trends in crime rates in a specific country operationalizing cyber attacks via 13 measures presented in the following table, as seen in Table 2 of *Summary Statistics for the Security of Cyberspace* (E. Jardine, *GCIC Report*, p. 6):

	Minimum	Maximum	Mean	Standard Deviation
New vulnerabilities	4,814	6,787	5,749	781.880
Malicious web domains	29,927	74,000	53,317	13,769.99
Zero-day vulnerabilities	8	24	14.85714	6.336

New browser vulnerabilities	232	891	513	240.570
Mobile Vulnerabilities	115	416	217.35	120.85
Botnets	1,900,000	9,437,536	4,485,843	2,724,254
Web-based attacks	23,680,646	1,432,660,467	907,597,833	702,817,362
Average per capita cost	188	214	202.5	8.893818078
Organizational cost	5,403,644	7,240,000	6,233,941	753,057
Detection and escalation costs	264,280	455,304	372,272	83,331
Response costs	1,294,702	1,738,761	1,511,804	152,502.2526
Lost business costs	3,010,000	4,592,214	3,827,732	782,084
Victim notification costs	497,758	565,020	565,020	30,342

While reading the table results, an essential argument must be kept in mind. Statistics for cybercrime costs are not available worldwide. The author worked with the assumption that data about US costs of cybercrime indicate costs on a global level. For obvious reasons, however, this assumption may not be true, and many countries will have had significantly lower costs than the US. To mitigate the assumption's flaws, the author provides comparative levels of those measures. The organizational cost of data breaches in 2013 in the United States was a little less than six million US dollars, while the average number on the global level, which was drawn from the *Ponemon Institute's Annual Cost of Data Breach Study* (from 2011, 2013, and 2014 via Jardine, p.7) measured the overall cost of data breaches, including the US ones, as US$2,282,095.

The conclusion is that US numbers will distort global cost findings by expanding the real costs and will work against the paper's suggestion, which is that normalized numbers paint a rosier picture than the one provided by absolute numbers.

Digital extortion

Sharma and Thakur (2007) define digital extortion as follows:

> *"Illegally penetrating through the system of an enterprise and then compelling it to pay substantial amounts in lieu of their secret data or to save their system from being wiped out by the hackers."*

The first major issue concerning the understanding of digital extortion is that it can be executed by a person of any age-even a child can be a hacker. The second issue refers to its cross-border quality, which makes it difficult for law enforcement agents to tackle the crime at its roots. It is impossible to get to the bottom of the far-reaching consequences of digital extortion without discerning the prominent methods of digital extortion now and the way its methods have advanced over the past three decades.

Jay Becker in his article *Computer crime: career of the future?,* states the following:

"In a nutshell, there are several good reasons why you might consider a career in computer crime. First of all, no one will ever know if you commit one. Second, no one will ever tell if you do. Third, no one will ever punish you. Fourth, you don't really have to know an awful lot about computers to commit this crime. Fifth, the opportunities for advancement are phenomenal. And, finally, there's no time like the present."

The odd beginnings of digital extortion

Extortion is not new. Criminals have always demanded ransom from people in exchange for something of value. The first ransom incident in the digital era, conveniently titled **ransomware**, happened in 1989 and is a strange, screenplay-worthy story of a computer virus related to a real-life virus.

The incident took place at the height of the AIDS epidemic. Dr. Josef Popp, an evolutionary biologist who was later proclaimed mentally unfit, mailed a set of 20,000 floppy disks to groups providing care for AIDS patients and research into the disease, having identified them as subscribers of journals and AIDS conference delegates. The package was delivered to victims abroad, not in the US, and carried the stamp of the nonexistent **PC Cyborg Corporation**.

Although the content was marked as AIDS education software, it also contained the harbinger of today's ransomware, known as the AIDS Trojan, a virus that encrypted the files on the computers of the victims when they tried rebooting the hard disk.

The ransomware message demanded that either $189 or $378 be mailed to a PO box in Panama. Luckily, doctor Popp's malware was not perfect and untraceable, and it had a shortcoming: it used symmetric cryptography. When the experts found out about the encryption method, it was not difficult to identify and capture the offender.

Dr. Popp actually had a peculiar ethical idea that he was accomplishing a benevolent goal by collecting the money from the ransom for AIDS research.

The days of floppy disks are long gone, and data is now transferred in incredibly creative and various ways. Digital communication, social interaction, and online financial transactions multiply in spades. Key aspects of connectivity, such as digital data, computing devices, and the Internet, evolve.

Ransomware has spread and became a major concern of public and private organizations. The insidious ways by which the malicious software works can instigate major panic among victims. When the victim clicks on ransomware code disguised as a legitimate e-mail, website, link for application download, or advertisement, critical data is lost forever unless the victim pays the ransom to obtain the unlocking code.

Early experiments in extortion

After the quirky initiation of digital extortion instigated by the AIDS Trojan in 1989, there was a silent period in ransomware in which malware criminal activity was performed by acclaim-hungry amateurs whose main purpose was not criminal, but mainly a way to prove computer dexterity and expertise.

Hampton, Zubair, and Baig (2015) point out that it was the early noughties when malware started to be colored by financial motive. That was the time when ransomware business was born and entered the digital world with a confident step. Profits were collected from first-wave ransomware activity such as direct information theft by breaching sensitive passwords or important information, such as banking credentials and advertising revenue.

Malicious software was also taking the shape of botnets-for-hire. Botnets were incredibly successful for attacking businesses due to their social proliferation component. By amassing a system of compromised computers and compiling a bot network, cybercriminals targeted large organizations. Botnet networks were leased to the highest bidder and used to extort money from companies. The value of botnet malware was large scale as it aimed at corporate profits by applying multiple malware propagation methods. It could be used to run a phishing campaign to steal sensitive data or activate further infected software that could compromise user hard drives and steal valuable data. Botnets work underhand-they lay low and look legitimate while quietly stealing information in the background.

Extortion-based malware

The current nature of ransomware led by financial gain emerged around 2012. Until then, criminals did not have sophisticated means to attack and monetize end users. Direct end-user extortion started in 2011 by introducing fake antivirus software.

Fake antivirus (AV) malware

Although fake AV is considered the earliest malware variants, it keeps cropping up in modern versions, especially on mobile phones. Almost no one has been spared from seeing an annoying ad selling antivirus software for a nonexistent virus. In reality, the ad is the malware, and once the victim falls prey, the device gets infected and starts exploring and stealing valuable data. Antivirus scams used social engineering techniques to lure non-knowledgeable users into installing the fake anti-malware tool by warning about some already existing malicious software. When they show up nowadays, fake antivirus tools mainly target individuals and avoid large businesses because companies usually arrange professional protective anti-malware software and are less likely to take the bait. Most of these scams were successfully eradicated by repressing the credit card payment feature. This is why they withered almost instantly and left the throne to the next generation of evolved and more complex lockers that used denial-of-service tactics.

Early denial-of-service lockers hacked the machine boot operations and blocked access until the demanded ransom was paid. The weakness of the malware was quickly overcome by implementing a recovery anti-virus software.

PGPCoder/GPCode and strong encryption

Implementing strong encryption to create **reversible denial-of-service attacks** did not gain popularity until the middle of the noughties. The early variants of GPCode had many bugs, and the infected deleted content could easily be recovered. Over time, however, GPCode advanced, surpassed its initial failings, and strengthened its deletion capacity. Instead of code with poorly implemented encryption routines and insecure encryption keys, it became incomparably stronger with complex encryption schemes and improved key lengths.

Introduction of the third-party payment gateway

The malware's inherent characteristics did evolve, but the method of obtaining the ransom money from the attacked end-user was still very risky and entangled. Encryption lockers needed support from a third-party payment gateway to process payments. This was still impossible. Criminals used numerous contact points in the sequence to get to the end user, making the process lengthy, dangerous, and complex. While direct communication between the attacker and the victim was necessary in order to complete the ransom and recover the data stolen, an independent payment gateway was crucial to complete the process. This is why even with sophisticated encryption lockers, the extortion could not actually proceed to completion. Under such circumstances, malicious software collected profits via information and resource theft.

Fully functional ransomware is based on three critical technologies:

- A strong and reversible encryption locker
- An anonymous system for exchanging keys and decryption tools
- A concealed ransom payment method-one that cannot be detected and connected with the source of the digital extortion

CTB-Locker

CTB-Locker was the primary episode of triple-technology ransomware. CTB (**Curve, Tor, and Bitcoin**)-Locker combined the three components necessary to process the ransom. It was based on elliptic curve cryptography, which provided fast and secure encryption of file content. The anonymous communication was enabled by the **onion routing protocol** (**Tor**), while Bitcoin gave secure and untraceable crypto-cash transactions.

Recent versions of CTB-Locker can take over multiple platforms, target network shares and removable media, and develop far-reaching technological strategies, thus reducing network effectiveness and the success of hard-disk backups. These fresh threats may not be the main source of security irritation for larger corporate organizations as they usually apply complex anti-malware security solutions, but they can endanger smaller business systems, which do not usually invest significant resources into strong backup and protection systems.

Some authors (Kharraz et al, 2015, via Hampton, Zubair, and Baig) comfortably suggest that digital extortion is not the scarecrow it is usually presented and covered in the media as. Most ransomware types have flaws that can be stopped by anti-malware efforts of professionals. Then again, it is not recommended to undervalue ransomware as something of an impermanent value. Case history and research have shown that ransomware develops along its polarity-security-and quickly adapts to defensive strategies. What may work as a protective measure at the moment may be inefficient in due course.

Cybercriminals diligently work toward developing ransomware strategies for substantially large corporations, where the financial profits obtained from a ransom can undermine a business to the root. Security specialists must analyze trends to predict future development and preempt ransomware threats before they arise and attack vulnerable end-users.

Over the past decade, diversified variants of ransomware have spread from Russia to the rest of Europe and North America and are increasingly overtaking the global scene. The worth of examining practical history lessons to accelerate current anti-malware trends is self evident.

Types of digital extortion

To state that the creative ways of digital extortion have been rewarding and profitable for cybercriminals severely distorts the truth. The persistent and innovative methods of finding flaws in individuals' and businesses' security used by offenders are a great incarnation of the good old saying "*Where there is a will, there is a way*"-or, in this case, ways. In this section, we'll explore the leading types of digital extortion that are becoming significantly vital for business organizations.

Distributed denial of service (DDoS) attacks

Unlike a **denial of service** (**DoS**) attack, which uses one computer and one Internet connection to flood a targeted server, a distributed denial of service (DDoS) attack is launched from different computer locations and using many Internet connections in a synchronized manner. DDoS attacks flood a targeted server or network resource with requests or packets of information. In this way, the server becomes unusable, and the attack can even crash the network.

In a DDoS attack, cybercriminals act by searching for weak spots in a chosen computer system and turning the computer into the DDoS master. By using this master computer, the hacker searches for other compromised systems to spread the infection. There are several ways in which a hacker can perform a DDoS attack. One way to launch a DDoS is by flooding the network in order to obstruct legitimate traffic. Other variants are performed by way of disrupting system connections to prevent service access or by disrupting the state of information.

The first victim with a compromised computer is not the only target. Instead, all compromised systems are victims of a DDoS attack. The initial targeted compromised computer system is called a **zombie** or **bot**. The additional set of compromised computers is named a zombie army or a botnet. Attackers work by loading a number of cracking tools on the compromised computer network, which can occasionally include thousands of computer units, and by sending a single command, the botnets load flood attacks toward the target and cause a denial of service.

Although there are no absolutely bulletproof ways to guard against targeted DDoS attacks, there are certain actions that can reduce the tendency of a computer to become the initial compromised system and thus target and collect a zombie army across the network. Normally, you need regular maintenance of antivirus software and firewall installations and you need to keep up with good spam-reduction e-mail practices.

It is not always as straightforward and as smooth-sailing to identify a DDoS attack. Disruption to services can often be a result of technical problems or system maintenance, but there are specific DDoS indicators (McDowell, 2016) including:

- Unusually poor network performance
- Unavailability of a specific website
- Inability to view any website
- Dramatic growth in spam amount

The usual response to a DDoS attack is a tough job and needs to be executed by skilled security experts.

Taxonomy of DDoS attacks

Patrikakis, Masikos, and Zouraraki (2004) state that a DDoS attack takes place *"when many compromised machines infected by the malicious code act simultaneously and are coordinated under the control of a single attacker in order to break into the victim's system, exhaust its resources, and force it to deny service to its customers."*

The authors classify DDoS attacks into two main categories:

- Typical DDoS attacks
- Distributed reflector DoS (DRDoS) attacks

Typical DDoS attacks

When the DDoS attack is classified as typical, the attacking army consists of master zombies and slave zombies. Both zombie types are located on the compromised computers that have been identified as vulnerable during the scanning attack and infected with malicious code.

There is a hierarchy of commands: while the hacker controls the master zombies, they take command of their own slave zombies. Master zombies sneakily wait in hibernation for the command from the attacker to arrive. Once it is there, they give instructions to the slave zombies, who do the actual legwork and send large packets of useless data to the victim, blocking and exhausting the victim resources, sometimes even to a point where the system crashes.

In typical DDoS attacks, the hacker uses false IP addresses. The effect of the counterfeited addresses is twofold: it hides the zombies' identity and prevents tracing the attacker, and it prevents filtration of the malicious traffic.

DRDoS attacks

There is an additional player included in DRDoS attacks. Apart from master zombies and slave zombies, the attacker also employs a third army: reflectors. Reflectors are part of the system as non-compromised machines, which work without being aware that they're performing the attack.

The process of launching a DRDoS attack is the same as that of launching a DDoS attack to an extent. The hacker commands the army of master zombies, who then go on to command their armies of slave zombies.

The difference between the processes is that the slave zombies are directed by the army of masters to send a number of packets with the victim's IP address as the source IP address to other uninfected machines-reflectors. Reflectors connect with the victim and send a larger amount of traffic because they were upset to see that the victim was the host that asked for it.

DRDoS attacks way more harmful than typical DDoS attacks. They coordinate a larger network of machines and create a greater traffic volume, which results in a more distributed attack.

Notable DDoS attacks

In the same article, Patrikakis, Masikos, and Zouraraki (2004) not only identify and classify the types of DDoS attacks, but also refer to the most prominent DDoS attacks in the short history of their existence in cyberspace as a means of digital extortion:

- **Apache2:** This is the scenario in which a client asks for a service by sending a request with many HTTP headers to an Apache web server. The server cannot handle the large number of requests and subsequently crashes.
- **Address Resolution Protocol (ARP) poisoning:** Getting access to the end-user's LAN, the hacker provides fake MAC addresses for already familiar IP addresses, diverting the host of the concrete LAN.
- **Back:** Again, the back attack is executed when an Apache web server receives an extensive number of requests containing forward slash characters in the URL and therefore becomes incapable of processing the normal volume of standard requests, resulting in denial of service.
- **Land:** In this scenario, the attacker sends a TCP SYN packet with identical source and destination IP addresses to the victim and, consequently, completely locks up the victim's system.

- **Mailbomb:** The mailbomb attack has a conveniently chosen name. The compromised mail server is flooded by a bounty of messages, which causes a system crash.
- **SYN flood:** A SYN flood attack happens at the onset of a TCP connection, during the process of the three-way handshake, which consists of three separately initiated connections working in a circular system. A normal TCP connection functions without an additional load of useless information.

  First, the client sends a TCP SYN packet to a server, requesting a new connection. Then, the server responds by sending a SYN/ACK packet back to the client and places the connection request in a queue. In the end, the client acknowledges the SYN/ACK packet.

  In the case of a flood attack, the situation is different: the attacker sends a number of TCP SYN packets to the victim, imposing a double process of both opening a lot of TCP connections and responding to them. Hence, when this occurs, the attacker does not complete the final step in the three-way handshake system. The result is a victim's queue overburdened with half-open TCP connections, making it incapable of accepting any new incoming connections.
- **Ping of death:** The ping of death attacks by way of creating an oversized packet data. A packet that contains more than 65,536 bytes is created by the attacker, which is over the limit defined by the Internet Protocol. This overflowing packet can harm the machine under attack in several ways, out of which crashing and rebooting are most common.
- **Process table:** In the moment of establishing a new TCP/IP connection, the process table attack generates a new process each time, by abusing the features of some networks services. The attacker tries to generate a massive number of uncompleted connections to coerce the victim's system into generating a long series of processes. The victim's machine fails to serve additional requests, since the number of processes running on the system cannot be limitless.
- S**murf attack:** A "smurf" attack is based on **Internet Control Message Protocol (ICMP)** echo-reply packets. Similar to ping floods, it is carried out by launching a large number of ICMP packets that have the victim's IP address as the source address.
- **SSH process table:** By using a similar technique as in the standard process table attacks, the SSH process table attack makes a number of connections to the victim using the **Secure SHell** (**SSH**) protocol without completing the login process. Hence, the daemon contacted by SSH on the victim's system starts as many SSH processes, becoming exhausted to a crashing point.

- **Syslogd:** The syslogd attack is connected to Solaris 2.5 server. It works by crashing the syslogd program on the server via a message sent from an invalid source IP address.
- **TCP reset:** In this attack, the malicious action starts by monitoring the `TCPconnection` requests to the victim. The attacker looks for a `TCPconnection` request sent to the victim, and then sends a false TCP RESET packet, so the victim must stop the TCP connection.
- **Teardrop:** The teardrop attack works through a process of fragmentation. On its way from the source to the destination machine, the packet gets broken into smaller pieces. In this way, a stream of offset field-overloaded IP fragments so large is generated that in the end, it creates trouble for the destination host trying to figure out the puzzle and reassemble the fragments. The result of a teardrop attack is usually a system crash and reboot.
- **UDP storm:** The **User Datagram Protocol** (**UDP**) storm attack scrambles a network by creating a constant flow of useless loads via character generation. The **chargen** (**character generation**) service creates a series of characters every time it receives a UDP packet, while an echo service echoes the characters received. By abusing both services, the attacker sends a misleading packet to another machine, making it look as if it originated from the victim's machine. The process continues by the echo services of the previous machine and the victim's machine working constantly, with data being echoed back and forth between one victim's and the subsequent victim's machines, thus creating endless useless streaming.

Data theft extortion

Data theft extortion is nothing new. It utilizes the same unscrupulous ancient criminal tactics that relate to kidnapping people and asking for ransom money. The difference in this case is that there are no people involved, at least not directly.

In data theft extortion, cybercriminals tend to harm people indirectly by holding hostage data and files until a ransom is paid to obtain the data back.

Data theft has a large and convenient reach. It can aim at a small or medium-sized business to collect valuable data and prevent the enterprise from running normal business. It can target huge corporations as well as private and public companies that deal with a large volume of critical data, and wreak massive havoc on people's privacy. No one is spared. Police departments, hospitals, mobile operators, universities, and transport companies are among the victims, and the threat comes from the inside as well as from the outside.

According to `www.techopedia.com`, *"data theft is the illegal transfer or storage of any information that is confidential, personal, or financial in nature, including passwords, software code, or algorithms, proprietary process-oriented information, or technologies. Data theft extortion, on the other hand, retains the additional extortion component."*

While data by itself holds precious value for the victim and may be sold on the black market or held in the possession of the criminal without necessary force applied, the extortion perpetuates the element of force. For example, medical records can be stolen by application of an unauthorized malware attack. Medical records contain numerous sub-records, such as banking details, private medical histories, social security numbers, home addresses, and payment receipts.

Such records hold double value, both for the victims and for the hospitals, which can suffer additional financial shocks working in multiple ways, not only in terms of lost patients, but also by way of damage and insurance claims, lawsuits, and, regrettably, lives. Such instances are rare, though, as cybercriminals' primary target is financial gain and not major collective terror. Hackers abstain from drawing too much unnecessary attention to them because under increased visibility, attacks can go wrong and the extortion "deal" could go askew. Data theft extortion is a severe breach of security and privacy, with detrimental consequences for individuals and businesses.

The usual way cybercriminals perform data theft extortion is by malware attacks. By applying unauthorized malicious software, offenders steal or restrict data access in order to extort ransom payment. Once the payment is complete, the data is restored. It is essential to emphasize that malware is not the only intrusion technique used in data theft, but it is the critical one for data theft extortion. Alternatively, data theft can be performed by various other methods. USB drives and portable hard drives are convenient and cheap methods for the thumb-sucking technique. On the other hand, memory cards and personal digital assistants are the favorable means for pod slurping. E-mail transmission, printing, or remote sharing are also used for illegal data transfer.

Preventing data theft extortion

In the end, there is a system of measures that can be applied to guard against data theft, such as a secure data management system that prevents illegal access to files, periodic reviews of risky systems and devices, restricted network usage, laptop lockdown, and biometric security measures. The most effective way to prevent malware attacks and data theft extortion is by encryption of confidential, sensitive, or personal information and by the use of anti-malware software.

Mobile extortion

While initial cyberattacks were launched against computers using the Windows OSes, it is no wonder that Android and iOS users are becoming a progressively popular target. There are several factors that make mobile devices excellent points of attack: the constant reliance on them of users in personal and business life, the privacy and the individual ownership of such devices, and the widespread availability of numerous applications flourishing on the free software market.

Android

The largest percent of mobile cyber threats happens on mobile devices operating on Android software. This comes as no surprise, seeing that Android is the most popular software platform for mobile devices: 79 percent of the user mobile devices use Android. The fact that it works as an open-source Linux-based operating system on Google Play, where any mobile developer can submit an application, just adds to Android's susceptibility to attracting malware.

Highly sensitive data such as private SMS messages, private and business contacts, and calendar data can leak and endanger user privacy. Moreover, data from GPS sensors can be exploited to track and monitor the user. Mobile devices are also at great risk of malware attacks, such as viruses and Trojan worms.

> *Google Android Security Annual 2015 Report* states that the company implemented user protection by checking and scanning several hundred million devices per day and 6 billion installed applications each day. The report discovered a drop in malware threats from the previous year, which is presumably due to the monthly security updates undertaken by Google, completed by removing potential vulnerabilities in the system. The biggest threat for Android users, according to the report, is the installation of **potentially harmful applications** (**PHA**).

Threats to mobile safety often arise out of convenience. It is the classical catch of the "terms and conditions" scenario because a user rarely reads all that is stipulated under the T&A guidelines. In a similar way, users download various applications without checking credentials. Cybercriminals do not need an invitation to exploit users' oversight and cash it in creative ways. Another relevant convenience reason is the massive presence of third-party applications misguiding users into downloading malware loaded software.

Notable Android ransomware cases

Recent threats involve several fake versions of the ultra-popular Pokemon Go game. One of the fake versions worked by installing a remote-access Trojan on Android mobiles and the other featured a fake lockscreen application called Pokemon Go Ultimate. The app actually forces the user to reboot the device and then starts working in the background, clicking on pornography ads without the user's knowledge.

The rise of mobile malware to the level of ransomware goes in parallel with the increased popularity of digital extortion. The Android-based Trojan Marcher was first put on the market in 2013 as a phishing malware designed to target customers of major banks in the UK and steal banking credentials. At the start, the Trojan worked as malware-as-a-service by putting up a fake payment screen. Alternative variants for mobile device threats surfaced as spyware made to intercept and send messages and make phone calls without the user's knowledge.

Recent Trojan variants emerged via apparently legitimate apps, such as Adobe Flash Player, as malware capable of locking the device in a way similar to classic ransomware. Although initially launched in Russia, this Trojan quickly took over at least 40,000 Android mobiles from European countries. The malware monitors banking applications launched by the user, downloads a phishing form from its C&C server, and puts it on top of the running application. The stolen information is exploited by the cybercriminals to steal money from the user's bank account.

The larger the mobile market, the larger the threat, as a recent research paper report completed by Trend Micro (Gu, 2014) about the Chinese market demonstrated. Smartphones are an excellent means for criminal activities in the real world and in cyberspace, exploited both in overall cybercrime and in the world of digital extortion. Cybercriminals not only find ways to abuse mobile devices directly, but also indirectly: the appropriateness of the devices makes it super-efficient for the latest developments in extortion-sextortion, a toxic form of digital blackmail where cybercriminals attack user's sexual intimacy and privacy by threatening to expose private images or videos unless a ransom is paid in exchange for the sensitive material.

iOS

As ransomware is becoming an increasingly vilifying phenomenon for cybersecurity, no operating platform is spared. While classic ransomware scenarios include hacking the user account by encryption or screen locking until the ransom in demand is paid (usually via cryptocurrency such as Bitcoin), notable ransomware cases that have targeted iOS devices are considerably different.

The iOS platform is almost taken for granted in terms of security due to its "walled garden" attribute. This fact has given users the idea that Apple devices are safe from malware threats. While it is true that there are more threats concerning Android platform users, past incidents confirm that the iOS software is not 100% free from security and privacy risks. Kaspersky Labs (2014) reports an increase in the OS X malware threat since 2003, with a recent dramatic rise of 3,600%. It is not wrong to assume that this figure is partially affected by the growing number of iOS devices in use by individuals and businesses, which, though it may comprise a smaller proportion of the mobile device market's users, are still those more inclined to purchase new devices and related applications. This by default makes them a fortuitous target.

Notable iOS ransomware cases

iOS users manage their accounts via iCloud. Notable cases of iOS-based ransomware include cybercriminals hacking iCloud accounts and thus gaining access to the connected devices. The compromising attacks date back to February 2016, in which over 40 million devices were infected with the malicious software, locking the user out of the phone by taking over their iCloud accounts.

When hackers took over the account, they changed the existing password and immediately locked the iOS devices in the individual's possession via the "Find My iPhone" phone-lock feature. Additionally, they sent the ransom message through the same feature and, using the element of panic, tricked people into thinking that they must pay $50 to get access to the compromised devices.

In practice, attacked iPhone users saw a specific lock screen on their iOS-based devices, which, instead of the standard swipe-to-unlock slider, notified that the account had been compromised. The actual alert stated that the device had been locked and that it would be unlocked once the $50 ransom money was paid in return. The text was followed by a an e-mail address, *helpappledevice*@gmail.com. Although the threat could easily be overcome by unlocking the device with a passcode and indicating that the true owner is in possession of the device, some users fell prey to the scare tactics and paid the $50 amount.

Still, it is key to remember that the threat of having the data on the iPhone or iPad deleted is real, as hackers who are in administrative possession of the devices can always wipe the data. An additional protective measure that works in the scenario is changing the password on the iCloud account, thus blocking the hackers from access to the device.

Sextortion

When they want to make profit, cybercriminals work in cunning ways, and nothing can stop them in harming sensitive human values.

> Sexual extortion, or sextortion, is a crime in which the hackers steal private images or videos from a person's computer, phone, or webcam feed and threaten to distribute them online unless the victim pays the money requested.

Hackers can use various tactics to get to the digital media. For example, a person close to the victim, perhaps an ex-partner, shares the pics with a third party. In another scenario, the victim could be cajoled or pressured to deliver the photos personally. Alternatively, hackers could breach the victim's online account and steal personal photos or gain remote control over the victim's computer by infecting it with a remote access Trojan.

The impact of sextortion to victims is devastating. There are Interpol reports of severe consequences from around the world, with victims committing suicide or other types of serious self-harming behavior. Considering the nature of the crime, exact figures cannot be given as victims often choose to avoid reporting and tackle the matter on their own, normally by submitting to the will of the extortionists and paying the ransom. When minors are victims, the atrocious manipulation can be stronger and even more dangerous.

> Due to the tragic consequences and public coverage, the case of a 15-year-old Canadian, Amanda Todd, depicts the devastating impact of sextortion executed on minors, particularly when they belong to a vunerabale category. Following a shocking series of cyberbullying behavior that ended in her naked pictures being exposed online and the perpetrator sextorting her for sexual favors afterward, she took her life in 2012, when she was just fifteen. Amanda was later named *The Girl Who Woke Up the World* as her case raised spectacular public attention and outrage.

The cost for children may not be money, but something far more valuable. The US Department of Justice's National Strategy for Child Exploitation Prevention and Interdiction from 2016 presented survey results, claiming that 60 percent of the respondents indicated an increase in sextortion behavior. Children not only suffer the abuse of the attack when it happens, but also demonstrate later self-harming and depressive behavior, school dropouts, and lower grades as well as suicides and suicide attempts.

Undoubtedly, the easiest way to stay safe from such threats is to abstain from taking private pictures or videos as there is no surefire way to guard privacy. However, this advice bears fruit only occasionally. It is normal to anticipate that humans will not change their ways just overnight, and hence reasonable to explore encryption as a protective mechanism and work on raising awareness about the crime.

The perpetrators of this high-level blackmail frequently work in groups. Sextortion is an organized crime business where criminals work in networks to target multiple victims in one organized attack. The number of ways in which potential victims can be harmed is limitless. Sometimes, sextortionists work from business centers organized in a similar way to a call center and strike via websites, social media, dating applications, webcam hijacking, or adult pornography sites. When the attack is launched on many potential victims at once, the chances of making profits increase. It is worth noting that sextortion is not a new crime, showing up for the first time in the digital world. The high exposure of online distributed material and the ease of extortion conducted in the age of connectivity just helps it thrive in exceptional new ways.

Sextortion techniques

A sextortion attack may be performed in a handful of ways. Often, criminals enter the story as an attractive person who gains the victim's trust and creates videos or images of the victim containing sexual actions or nudity. In the aftermath, the blackmailer threatens to distribute the sensitive material either online or among the victim's close family and friends unless the required ransom is paid.

Another unscrupulous way of sextortion happens when a child appears in the sex scenario that has already occurred between the victim and the criminal. In this case, the victim gets a warning that looks as if it comes from a law enforcement agency and says that he or she must pay a certain amount of money or an investigation will be raised. Obviously, the police never works in this way, but in the moment of emotional turmoil and panic, the victim may succumb to the sextortinist's ways and pay the money to avoid embarrassment or prosecution. In certain situations, victims are located via memberships on adult sites where they have provided credit card information.

There is no one common method to target victims. The only thing that connects all methods is the existence of an organized crime group. They use the so-called **scatter-shot** photography technique, which enhances the range of victims that can be targeted. Interpol confirms that they often work in advanced ways by recruiting agents and providing bonuses for the best performers. Sextortion presents low-risk, high-gain business due to the victim's reluctance to report the crime. Criminals are aware of this and measure the ransom amount to a level that can be paid by an average victim without reporting the sextortion to the police. On the other hand, although the average ransom amount for sextortion is $500, there are cases with amounts as high as tens of millions of dollars.

The environment conducive for extortion of this kind is created upon communication and trust. Social networks pose a particular threat as they contribute to helping criminals imitate a genuine social networking contact. Interpol reports that organized crime groups working with sextortion mostly target countries where the victims' first language is English, such as the UK, USA, Australia, Singapore, Hong Kong, Indonesia, and Malaysia. The crime is also present in French-speaking Africa, targeting France. Cases of sextortion in the Far East target countries such as Japan, South Korea, and the Philippines, exploiting the weight of the humiliation that comes from the local cultural norms and values.

Bug poaching

To understand the nature of bug poaching, we borrowed a metaphor used by IBM Security that illustrates the distinct nature of bug poaching, a particular cybercrime scenario in which criminals attack the victim's sense of security. The metaphor describes bug poaching as similar to a home burglary, when criminals get into your home and steal nothing but only take pictures of your personal stuff and later send a notice in which they demand a payout to disclose the secret of how they got in your house in the first place. The notice does not include a threat of a future burglary, but only a notion of your home's vulnerabilities. Bug poaching happens when hackers do the same with your business-sensitive data, just not in your home but on your corporate data network. Bug poachers actually deliberately hunt for vulnerabilities in the data system and demand large sums of money to disclose the flaws to the victim.

Bug poachers claim to act with good intentions because they expose system vulnerabilities, but the argument is erroneous and it does not paint the real picture of the nature of bug poaching.

Cybercriminals start the process by finding flaws on the victim's website. IBM Security data postulates SQL injection as the key attack technique used in bug poaching. The assumption is that attackers use off-the-shelf penetration testing tools to find flaws. When they find and collect sensitive or personal data and information, they store it on a cloud storage service. Once this step is complete, the victim organization gets an e-mail with a link to the stored cloud data to prove that the corporation's network has been penetrated and that the data was stolen. Finally, the hackers ask for the ransom money to be sent via wire transfer in exchange for information about the flaws in the system that enabled the data theft. Although the attackers claim that the data is kept safe and do not threaten to disclose it to the public, the reasoning behind the tactics is dubious. The victim has no guarantee that the used cloud storage is safe or that the attacker will not leak the data after all.

Certain professionals argue that if the organization pays the ransom, it can still obtain the value of the discovered vulnerabilities. However, this is a foolish plan in several ways. First, the attacker may decide not to deliver the information about the vulnerabilities, regardless of the promise and the payment. In addition, there is no guarantee that the first bug-poaching attack will be the last one. By paying the ransom, the victim is actually encouraging cybercrime and creating convenient alleys for future extortion. Undoubtedly, the best way forward is the way backward, by applying strong intrusion-protection mechanisms such as regular vulnerability scans, penetration testing, and web firewalls. Although bug poaching seems less malevolent than the other data extortion attacks, businesses should certainly treat it as seriously and guard against it with strong defense strategies.

Corporate extortion

A specific variant of cybercrime involving ransomware is corporate extortion, targeting large businesses with threats of harming their reputation with negative online reviews, complaints to relevant business authorities, harassing telephone calls, or wrongful deliveries.

A notable case of this kind is the 2014 Domino's pizza data theft extortion, in which the hacker group Rex Mundi accessed 592,000 French customer records and 50,000 Belgian customer records, threatening to publish the data unless they got the Euros 30,000 ransom amount.

Unquestionably, if a case is classified as corporate extortion, it does not automatically exclude characteristics of other types of cybercrime. Hackers usually target customers' sensitive data, such as credit card details or social security numbers, and threaten to sell the records on the black market. Although certain cybercriminals contact customers directly, the primary target of the extortion attack in this case are large corporations or public and private organizations.

Ransomware

In 1996, Adam Young and Moti Yung became the pioneers of the first ransomware sprouts implemented on an academic level at Columbia University.

This first secure attack was based on the processes of **cryptoviral extortion, zeroization**, and **hybrid encryption,** and incorporated a lab demonstration emulating the basics of a real-life scenario that includes a pair of keys.

Almost a decade later, Young and Yung authored the book *Malicious Cryptography: Exposing Cryptovirology* (John Wiley & Sons, 2004) with the aim of illustrating how malicious code works once it enters a computer system. In the foreword, the authors point out that the book can serve in two ways, as a vade mecum for cybercriminals and as a critical warning for security professionals.

Their ominous words fall nothing short of the true nature and practice of ransomware:

"Ransomware actually works by encrypting your files. It holds your computer hostage and doesn't let you access anything else except for the channel of communication with the extortionists."

While many types of malware are just quietly sitting in the background while you are totally unaware that your computer or mobile device is infected, ransomware will not be so silent. Usually, you get a perfidious flashy message demanding that you pay a certain amount of money or Bitcoins in exchange for the unlocking code.

Ransom amounts are not exactly pocket money and can range from a few hundred to several thousand dollars. The snarky way extortion works is nothing different in the digital world than the real world. Once a blackmail attack is over, it does not mean that it will not happen again. Next time, the ransom may increase. Malware intrusion powers grow and can surpass antivirus protection levels on your computer.

New ransomware strides along and develops in sync with anti-malware software. Current popular versions are crypto ransomware and CryptoLocker.

Ransomware - crypto

Crypto ransomware locks files and data by injecting malware code into the user-end systems, usually searching for files and data with extensions such as FLV, PDF, RTF, MP3, MP4, PPT, CPP, ASM, CHM, TXT, DOC, XLS, JPG, CGI, KEY, MDB, and PGP.

Crypto ransomware or data lockers search silently in the background until they target a file, while the regular OS and applications work normally so that no suspicion is raised at the end of the oblivious receiver. The malware then encrypts the file and the end user data while completely choking system functionality. Until the demanded ransom is paid and a decryption key is obtained in exchange, there is no way for the user to get access to the files.

Ransomware - locker

Locker ransomware blocks access to computers or mobile devices by locking the keyboard or the mouse. By flashing a screen notice, the malware allows limited functionality of the mouse or the numerical keys, only to enable typing the ransom amount when the user gets normal access to the data restored. The "good" thing about lockerware is that unlike data locker malware, it keeps the system in its original operating mode and the files intact.

Ransomware propogation techniques

There are many ways in which a computer can become infected by ransomware. A device can get infected by clicking on a compromised website. CryptoLocker malware works using an infected e-mail attachment. Other types work as malvertising, by browsing a page or clicking on an ad with malicious content. Additionally, outdated software carries additional risks as many variants seek to target vulnerabilities in older software versions.

In their report, *Ransomware: A Rising Threat in a New Age Digital Extortion* (2015), Bhardwaj, Avasthi, Sastry, and Subrahmanyam pinpoint the key methods of ransomware propagation as well as protection techniques by describing the usual actions performed by the harmful software when injected by criminals.

Traffic redirection

Traffic redirection is a classic click-and-bait technique by which the user gets redirected to a malicious server. The attacker tricks the victim by offering free application upgrades or games to download that carry the infection. The malicious site then uses the downloaded applications or games to install itself while examining and attacking vulnerabilities in the operating system of the victim.

E-mail attachments

E-mail is undoubtedly the best known traditional method of trapping users to access malicious content. By clicking on a link from a website containing malware or opening an e-mail attachment sent from the adversary, the malware takes control of the user system, usually the installed e-mail server. Incoming malicious e-mails are disguised as authentic messages from relevant friends and public companies. A common occurrence is to receive an e-mail from a public authority, such as a tax or utility company, that contains malicious software in the e-mail attachment.

Botnets

Botnets work in two steps. They do not contain malicious code right from the start.

1. They sneak around in the user system. Botnets are downloaded as legitimate applications or games and function regularly.
2. Then, they download the malicious software.

Social engineering

Certain types of malware can spread and infect other user systems by targeting the user's Outlook address book or phone contact list and by sending an infected e-mail or SMS. Social engineering is dangerously contagious as the ransomware comes from a legitimate source well known for the end user, who usually accepts it without giving a second thought.

Ransomware-as-a-Service (RaaS)

The infamous Jigsaw and Stampado malware belong to the **Ransomware-as-a-Service** (**RaaS**) category. Talented, experienced, and knowledgeable coders become cyber criminals by selling malicious software on the dark web. In this way, literally anyone can buy a malware package and demand ransom from victims, thus proliferating the mafia aspect of cybercrime, where coders and amateurs work along to extort Bitcoins and earn illegal profits from victims.

Evolution of ransomware

Prominent ransomware occurrences are about a decade old and were first seen in Russia. In its earlier years, ransomware encrypted particular file types, such as DOC, XLS, JPG, ZIP, PDF, and other commonly used file extensions. The next milestone took place between 2008 and 2009, when cybercriminals started applying fake antivirus programs, a disruptive subcategory of misleading applications. In 2011 and 2012, perpetrators went from fake antivirus tools to increasingly intruding extortion involving police ransomware and crypto ransomware.

Statistics of ransomware evolution - misleading applications give way to cryptoware

The popularity of specific ransomware variants has fluctuated over the last decade, but nonetheless, all of them were more or less present as the years went by, Although in different proportions.

More than half of the malware in the initial years originated from misleading applications, while the remaining occasions were ruled by crypto-ransomware.

Over the next couple of years, misleading applications took almost the whole ransomware market, with an occasional case of crypto-ransomware as well as a few examples of the newly introduced fake antivirus software showing up here and there. The situation has dramatically changed over the last couple of years, when cryptoware quickly grew to rule the total number of ransomware cases.

SpySherriff

SpySheriff was a fake AV variant that was published via its own website and worked by reporting false malware infections as real. The desktop background was replaced by an image with the **blue screen of death** reporting the ransomware message. When end users tried to remove SpySheriff, they received a message that the fake malware will reinstall itself.

Gpcoder

Trojan.Gpcoder reared its ugly head in Russia in May 2005. It implemented poor custom-encryption techniques by applying symmetric encryption algorithms, which use the same encryption and decryption keys.

Cryzip

A specific case from the subsequent year involved a ransomware version named **TROJ_CRYZIP.A**. This malware zipped certain file types and overwrote the original files, creating a text file that was actually the ransom note and asking for $300 in exchange for retrieved files. Only password-protected ZIP files remained in the user's system.

Archiveus

Trojan.Archiveus accompanied Cryzip in 2006. Archiveus used password-protected archive files, but did not ask for monetary compensation. In certain weird scenarios, the victim had to buy medication from designated pharmacy URLs via the Internet and submit the order ID number to get the decryption key for the archived files.

Randsom.C

The first pure computer-locking malware pioneered as early as 2008, in the shape of **Trojan.Randsom.C**. It worked by locking the computer, sending an illegitimate security message, and asking the user to call a premium-rate telephone number in order to renew the security software license.

SMS ransomware

A 2011 variant of ransomware that used a premium telephone number as a means to extort money from the infected computer end users was **TROJ_RANSOM.QOWA**. End users could only see a repetitive ransomware page until they paid the ransom by dialing the designated telephone number.

MBR ransomware

Another popular case from Russia is the **master boot record** (**MBR**) ransomware, which attacked the MBR on an operating system and prevented its uploading. The malware works by copying the original MBR and injecting malicious code in its place. The infection then spreads by forced system restart, while a notification in Russian language is displayed on the screen.

The rise of ransomware

Ransomware's advantages turned it into a profitable business model. By March 2012, the infections started spreading across European countries and invaded North America.

The peculiarity of the new ransomware wave was that instead of a standard ransom message, it threatened the users by displaying a notification page allegedly sent by their respective law enforcement agency. The early variants of fraudulent law-enforcement malware were known as **Reveton** and police ransomware.

A notable case from this period referred to a popular online French confectionery business whose website, Laduree.fr, was compromised by **TROJ_RANSOM.BOV**. The fact that the famous cake and pastry shop was an unlikely target is an excellent reminder that anyone can become a victim of a cyberattack.
The malware used waterhole tactics to spread infections across France and Japan, where the company also had an online presence. The ransomware message displayed a notice supposedly sent by the French police, called Gendarmerie Nationale. The attack was performed by a blackhole exploit kit, a type of malware that belongs to the same family previously used to imitate other law enforcement agencies, such as the German BundesPolizei.

Police ransomware - Reveton

Reveton is an advanced police ransomware type that has the enhanced quality of imitating national law-enforcement agencies by tracking the geographical location of the victim. Police ransomware or Police Trojans are notorious for showing an alleged notification from the local police informing the victims that they were busted while performing an illegal online activity.

> An in-depth analysis completed by Sancho and Hacquebord (2012) discovered that Reveton identifies the applicable law enforcement agency using the geographical location. Findings pointed to affected users in Germany, Spain, France, Italy, Belgium, Great Britain, and Austria. In this way, the Trojan achieves global impact. While you may be "persecuted" by the FBI in the US, you will get a "notice" from the Gendarmerie Nationale while in France.

Another distinct advantage of Reveton is that it applies another payment method than the one used in earlier attacks. To retrieve and clean a system infected by Reveton, users must pay a ransom through UKash, PaySafeCard, or MoneyPak-payment vouchers that can only be purchased at newsstands, petrol stations, pharmacies, or special kiosks across Europe, thus limiting traceability.

Later in 2012, new Reveton variants emerged: one used an alternative audio recording technique made in the victim's mother tongue voicing the displayed extortion message, while another used a fake digital signature and fake digital certificate.

Patched malware

Patched malware is a legitimate file modified with malicious code, either via addition or injection. The advantage of legitimate file modification for cybercriminals stands in the file's frequency of use: the more the file is used, the greater are the chances of execution of the malicious code.

Reemergence of crypto-ransomware

As of 2013, crypto-ransomware retook center stage. Unlike low-level social engineering, crypto-ransomware is quote vocal about what it wants. Crypto-ransomware displays a clear extortion message demanding ransom payment in exchange for the stolen data. Variants from the new generation employed increased ransom amounts and promoted extortion to an advanced business level. Usual payments average around US$300 per computer. If you do the math for the impact of advanced-level crypto-ransomware in a business setting that utilizes a large computer network with multiple connected machines, it is crystal clear that perpetrators would love targeting large corporate businesses with crypto-ransomware.

CryptoLocker

The newest malware type from 2013 performed two malicious actions at the same time: it encrypted the files and locked the system. In this way, the attacked parties had to pay the ransom amount even when the malware was removed.

The ransomware variant, named CryptoLocker, displays a wallpaper warning to users. The message alerts that unless the ransom is paid by clicking on a nominated link in the advised time frame, CryptoLocker will destroy the decryption key. It was not only the access that was compromised, but also the files. The files might be permanently lost if the decryption key was not obtained in time. This perpetuated the sense of panic at the victim's end.

The CryptoLocker ransom notice specifies only RSA-2048 as the encryption method, but the ransomware actually uses a combination of AES and RSA encryption. RSA is asymmetric-key cryptography. By using a set of two keys-a public and a private key-RSA applies one key to encrypt data and the other to decrypt the data. The public key is available to any outside party, while the private is kept at the user's end. AES uses a system of symmetric keys: the same key to encrypt and decrypt information. CryptoLocker encrypts files by AES. Further, this key is encrypted with an RSA public key, and a private key is needed for decryption.

TROJ_UPATRE

CryptoLocker infections were spread by spammed messages that had malicious attachments of **TROJ_UPATRE**, a relatively small and simple malware family that downloads a ZBOT variant, which then downloads the CryptoLocker malware.

WORM_CRILOCK.A

WORM_CRILOCK.A emerged in 2013 and was characterized with improved proliferation attributes. This type propagated via removable drives, a new routine not applicable to previous CRILOCK variants, and impersonated a software activator present on peer-to-peer file sharing sites.

Cryptorbit

Cryptorbit, or CryptoDefense, detected as **TROJ_CRYPTRBIT.H**, not only encrypts non-binary files from the type database, such as web, MS Office, video, image, script, and text files, but it also deletes backup files.

Cryptocurrency theft

Cryptocurrency theft was implemented into ransomware in 2014 as a new malware called **BitCrypt**, which stole funds from cryptocurrency wallets.

There are two known variants of BitCrypt:

- **TROJ_CRIBIT.A**: This is ransomware that adds the `.bitcrypt` extension to encrypted files and displays a ransom note only in English.
- **TROJ_CRIBIT.B**: This adds the `.bitcrypt2` extension to the filename and displays a ransom note in 10 languages.

The Angler exploit kit

The Angler exploit kit was a 2015 hit, and remains so because of its easy integration. It was used in a series of malicious ad attacks committed through popular news and media websites. Angler was introduced in the famous hacking campaigns Hacking Team and Pawn Storm, and it remained functional by being constantly updated to include several Flash exploits.

Ransomware in 2016 and beyond

In 2016, ransomware continues to stride forward, implementing additional sophisticated features such as dynamic pricing, alternative payment gateways, and aggressive consequences for non-paying victims: countdown timers and infections that spread over networks and servers via new distribution methods. What follows are some of the ransomware types released in 2016.

Locky

Locky entered the ransomware scene in February 2016, becoming distinguished by its unique distribution methods and affinity for attacking healthcare facilities. It was behind the attack on the Methodist Hospital in Henderson, Kentucky, which was targeted in the very same month and forced to work under an "internal state of emergency."

The first instance of Locky emerged as a macro in a Word document. It got into user systems disguised as a legitimate invoice with an attachment that contained the malicious macros with an e-mail subject saying **ATTN: Invoice J-98223146.**

Locky is one of the most popular malware variants, steadily updated and showing up in distinct versions. It inflicts damage by deleting shadow copies of local files so that they cannot be used as backup. The other thing notable about Locky is that it renames key files, adding the extension `.locky`. Files get both scrambled and renamed and can be restored to the original version only when the perpetrators hand over the decryption key.

Petya

Petya followed in the footsteps of Locky in March 2016, making a detour from the typical e-mail attachment malware infection as it was delivered via legitimate cloud storage services, in this case, Dropbox. Attacked users received an e-mail that looked like a job application with a link to the applicant's Dropbox, supposedly to get access and download the applicant's resume. Petya works by overwriting the MBR with the purpose to lock users out.

Keeping in mind the exponential growth of cloud storage for commercial purposes, the Petya menace has excellent chances of staying alive as a lucrative business solution for cybercriminals.

Cerber

Cerber ransomware delivered a particularly irritating voice message stating "Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!" It was also known for its wide reach: it potentially endangered the computers of millions Microsoft Office 365 users.

This malware lets distributors modify its components, making it adequate for sale on the dark web. The only way to decrypt the encrypted files is by getting the Cerber Decryptor, a key worth 1.24 Bitcoin, or between US$500 and US$800. The payment must be paid via Tor within the first week; the amount doubles every week.

After encrypting the victim's files, Cerber ransomware creates TXT, HTML, and VBS files titled `Decrypt my Files`, which are then delivered in folders with encrypted files with instructions on how to pay the ransom.

Samsam

Rather than the typical way of installing via malicious URL links or spammed e-mail messages, Samsam ransomware gets to work when the unpatched server vulnerabilities are investigated and abused to compromise other machines.

Jigsaw

If you have seen the violent thriller Saw, then you know the psychological dread caused by Billy the Puppet and the popularity the franchise got to the horror-keen movie audience. Jigsaw ransomware adopted the pressure scare tactics from the movie, accompanying them with an innovative digital extortion technique.

The ransomware displays a screen message with an image of Billy the Puppet and a ransom notice that works incrementally. In addition to the image and the notice, the locked screen presents a countdown timer with a pressure tactic to frighten the victim by deleting certain portions of the encrypted data as long as the ransom amount remains unpaid. The eerie red clock counts down and can only be rebooted when the payment is complete. As time passes by, files are deleted hourly. The initial ransom amount increases by the hour, too, with the least possible sum to be paid being between $20 and $150 US.

Obviously, Jigsaw used a double-edged sword. Users had to avoid the potentially larger damage of having a greater number of files deleted and had to keep from paying a larger ransom amount. Jigsaw's specific feature was the inclusion of a chat support feature installed to enable victims to get in touch with the extortionists.

Is ransomware financially viable?

It is beyond any doubt that cybercriminals are no longer happy with recognition and glory, but diligently work to compensate their extortion gifts. Nowhere is this more evident than in organized cybercrime related to information obtained from digital extortion.

While it is obvious that cybercriminals work for profit, for someone who does not have a lot of contact with data value, the connection between a set of data and financial worth remains vague and on the level of general knowledge, obscure media coverage, or plain assumptions.

Although many ransomware instances are not made for the purpose of data resale, there are many whose primary aim is not only to extort ransom, but to sell the valuable personal and sensitive records for monetary compensation on the black market. In a way similar to standard markets, the black market has tailor-made prices for data obtained from cybercrime.

While the value from the AIDS Trojan in 1998 may have been intrinsic for the distorted ethics of Dr. Josef Popp, he still put a price tag to it. Recent ransomware incidents demand victims to pay between $21 and $700 US. The average amount calculated from this range would be about $300, which comes close to the 1989 Trojan price tag when inflation over the 3 decades had been taken into account. To make a straightforward call about why the price tag attached to single-user incidents has changed so little, we would have to dive deeper into the motives of the perpetrators.

An obvious assumption to make is that cybercriminals decide to levitate the ransom amounts within the scope of victim's capabilities. A key factor in play may be the type of the attack and the end user. The demand on businesses is undoubtedly more aggressive than ones on individuals. In the end, law enforcement is critical. Not all instances of cybercrime are reported, fewer are prosecuted, and fewer still are sentenced. When cybercriminals evaluate that the scope of the crime is not relevant enough to initiate a criminal prosecution, they expect that the victim will be left to his or her own devices to combat the threat. Under the circumstances, unless the attacked party is a computer security expert, there is not much left to do but pay the ransom price. When the price is assessed to match the victim's payment capacity, extortionists are in for a definite deal to earn some money.

Dynamic pricing of ransomware

Assailing many victims on a global level is much easier when the ransom price a user has to pay is adjusted to the individual budget. When the attacked person is actually in the position to collect the ransom amount in a simple way, the payment is way more viable. Why bother with reporting the crime when the actual payment costs less time, anxiety, and even money?

Across countries

It is evident that the $300 average price of ransomware will not be the same burden for a US citizen and for one coming from a less developed country. To be able to use the same ransomware sample worldwide, cybercriminals must adapt the currency value to the local purchasing power. This trait has been noted in Cryptowall or Trojan. Cryptodefense, which applies the dynamic geographical pricing model.

Across targeted victims

Attacks on businesses and public organizations are taking a vital part in the total ransomware incidents in 2016 and are growing in time.

It is not uncommon for attackers to demand another ransom amount from a business user than from an individual. Data is value; data is money. Cybercriminals know these facts. They are particularly aware of the data cost for businesses especially when sensitive data is concerned. The value here is not only monetary or material. Attacks on multiple sensitive personal or business records may potentially impact other factors such as business reputation and may undermine authority, costing the organization additional sums from lost contracts, lawsuits, or claims.

Reported cases of ransoms for business attacks range from several hundred to several thousand dollars. The ransom amount is only a portion of the cost. These sums do not include the auxiliary costs, which are second-level only by nature and almost never by size. Certain data encryption attacks targeting businesses demand ransoms as high as $50,000 US. The average amount rounds up to $10,000 as an optimal value, which is likely to be paid by businesses and not attract prosecution by law enforcement agencies.

History of payment methods

Payment methods evolved along with ransomware evolution, increased reliance on electronic payment, and the rise of modern electronic currencies.

The pioneering AIDS crypto-ransomware Trojan from 1989 demanded a check payment that needed to be sent to a post office box in Panama.

By 2009, and the emergence of the **Trojan.Ransomlock** ransomware variant, cybercriminals introduced money wire transfers, sending premium-number text messages and using premium-rate calls.

When payment vouchers came out, extortionists started using payment voucher systems issued locally on a national level, such as the international Paysafecard and MoneyPak, the United Kingdom-based UKash, CashU, which is available in the Middle East in Northern Africa, and the Ukrainian MoneXy.

Bitcoin - the ideal ransom method

The majority of attackers today demand payment by way of Bitcoin cryptocurrency. Some use alternative cryptocurrencies, such as **Litecoin** [**LTC**] and **Dogecoin** [**DOGE**] since they provide anonymity and thus make it simple for the cybercriminals to legitimize the illegal profits.

Bitcoins are increasingly available, both for the victims to purchase them as a means to pay the ransom and for offenders to convert them into cash later when the ransom amount has been delivered. Payments are made through sites hosted on the dark web accessed through Tor, which makes law enforcement agents' work close to impossible when they work on identifying the cybercriminals.

It seems logical that crypto-ransomware perpetrators would prefer to be paid by cryptocurrency, while attackers using locker ransomware would use payment voucher systems as the preferred method of payment. The rationale behind this distribution is the different functionality of the two types of ransomware.

Locker ransomware acts by disabling computer access. In this case, common sense is to assume that the victim would be left without means to actually go online and purchase cryptocurrency. It would be much easier for the attacked to go to a kiosk, get a payment voucher, and enter the payment code. On the other hand, crypto-ransomware does not usually block computer access, and the victim can use the Internet to find and purchase cryptocurrency. Moreover, threats that include crypto-ransomware help victims find Bitcoins by sending links to Bitcoin purchase sites, payment instructions, and educational videos about the nature of Bitcoin.

Industries and services affected - is your company under threat?

Leading security companies are tireless in their endeavors to stop cyber-attackers pass businesses security defenses. A significant amount of work and resources have been invested to analyze the market, learn lessons, and improve tactics as time goes by. The aim is not only to analyze the past, but also to map the future. Prediction is key, and history trends and statistics from real-life stories are invaluable to avoiding costly future mistakes.

In the *2015 IBM® X-Force® Cyber Security Intelligence Index Report,* security specialists estimated an average number of 16,856 attacks for a business per year. This means that each business is targeted by cybercriminals around 46 times a day, or almost twice hourly. In the avalanche, businesses usually get protected by the security defenses they have already put in place. However, an average of 1.7 attacks per week still strike the target.

Numbers obtained from clients serviced by IBM Security Services in 2015 measure an annual total number of 53 million security events. The definition of security events includes cases *"identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources - or the information itself."*

The wording of the interpretation refers to actions of wider scope than those related to digital extortion, a worthwhile fact that must be kept in mind when assessing the numbers, scope, and diversity of cybercrime incidents.

In addition, the company reports a significant drop in attacks as reported by an average client company-from 12,017 in 2014 to 1,157 in 2015. This does not mean that cybercriminals went on holiday. Instead, it means that companies diligently worked towards optimizing security policies by investing efforts into tackling security events that needed additional research and investigation. On the other hand, the average client company serviced by IBM was subject to 178 security incidents, which is 2.5 times more than the 109 experienced in 2014. The 64-percent rise involves cases worthy of further analysis by the corporation's security experts.

Top targeted industries

Although no business is spared, certain industries seem to rate high on cybercriminals' priority lists. Financial institutions are no longer top rated. It seems that criminals stopped milking the same cow as they envisaged additional value in service industries. IBM noted that the healthcare industry topped the attack chart in 2015. Yet, there was no need to rely on IBM's findings to get the picture: the media did not fail to give massive attention to attacks executed on public health institutions. Manufacturing came second, just after healthcare, while financial services, government, and transportation followed in order, taking the last three positions in the top five endangered industries in 2015.

Healthcare

As of 2010, the top five healthcare security breaches, with the largest impact of over one million compromised records took, place in the first half of 2015. A staggering number of over 100 million healthcare records were compromised. Nothing sells as good on the black market as private healthcare records. A hospital record contains not only the person's medical history, but offers a full buffet of sensitive data that can be exploited in more ways than one: credit card numbers, social security numbers, banking credentials, e-mail IDs, and employment history. It is a life's worth of information. Medical records do not lose value over time. Cybercriminals use this currency to spread infections by phishing attacks, data fraud, and theft of medical histories.

Manufacturing

The manufacturing industry is firmly set on the second place, encompassing automotive, electronics, textile, and pharmacy businesses. Although no large attacks took place in 2015, the second position of manufacturing companies remained solid. A new significant trend is the rise in attacks on automotive manufacturers, which accounted for 30 percent of the total number of attacks, while chemical manufacturers followed closely behind. Security experts disclosed that criminals can target smart vehicles using remote hacking. This exposed a new threat that pushes the automotive industry up the list, considering the rise of smart automotive vehicles and largely connected transportation systems. The nature of the chemical and automotive businesses makes certain aspects horrifying, keeping in mind the scope of human casualties that can be effected from a large-scale attack. However, cybercriminals' motivation is predominantly financial, as they attack corporations not with the intention of mass murder, but to obtain valuable data and lucrative sensitive information.

Financial services

When there is a tough new kid on the block, it is expected that the veteran drops a few places on the rating scale. Due to healthcare and manufacturing taking over the first two positions, financial services took position number three in 2015. Additional factors that contributed to the drop are advanced security mechanisms developed by security professionals for the industry as well as the industry's awareness, strain, and energy to improve security. The danger from being a prime target in the previous period made its impact, too.

The accessibility of payment methods and globally spread banking services whose main purpose is customer convenience will keep the financial industry high on the list. Consumers like to manage their assets in a quick and efficient way, and services such as ATMs, credit cards, and mobile applications increase vulnerability.

Businesses, on the other hand, were subject to ransomware attacks of the Dyre Trojan and Dridex Trojan types, which extorted millions of dollars from companies. Digital extortion in the financial services industry skyrocketed to a level 80 percent higher than the previous year.

Government agencies

IBM reports on several highly exposed security breaches targeting government bodies that happened across the globe, in the US, Turkey, and Japan. The US scenario revealed millions of employee records containing lifelong valuable data, such as social security numbers, home addresses, and digitized fingerprints. When the national identity information of over 50 million Turkish citizens was leaked from government records, they were exposed to the risk of identity theft, while the Japanese scenario involved a pension service that was attacked in the classical way of having the victim open a malicious e-mail attachment.

Transportation

There are two ways by which transportation is targeted in cybercrime, and extortion is one. All industry levels are under attack: airlines, buses, and subway and railway lines as well as freight lines and ships that transport goods all around the world. On occasion, the intention of the cybercriminals includes political reasons, when cyberattacks aim at blocking the transportation process by producing major chaos. As a rule, though, financial profit is the leading motivation behind malicious code and DoS attacks.

Ransomware statistics - malware variants and affected devices

Similar to related ransomware statistics, numbers about devices are relative. A full picture of ransomware impact by type and device would take in-depth investigation of computer and security companies on a global level, a task that requires prolonged effort over time and evaluation of longitudinal studies. However, as the research topic is new and distributed, in the absence of complete general statistics, we must rely on ardent research attempts made by isolated concerned parties. Generally, respectable security companies undertake efforts to explore the market in order to improve services and retain customers.

In the *McAfee Labs Threats* Report from March 2016, Intel Security investigated ransomware statistics for the cases reported to the company by generating comparison charts for the number of ransomware variants in the last two quarters of 2015. Intel security specialists compared malware samples, mobile malware, incidents of new macOS malware, rootkit malware, ransomware, macro malware, new suspect URLs, new phishing URLs, and new spam URLs as well as global spam and e-mail volume.

While it is important to keep in mind that these numbers reflect only a portion of the reality as they come from a limited source and for a short period and thus cannot be generalized, it is also worth mentioning that the security industry is still working on conceptualizing and measuring cybercrime, and any findings gathered on the way are relevant for statistical as well as heuristic purposes.

Total malware

After a trend of going down during the first three quarters, the number of total new malware samples started climbing again in the last quarter of 2015. This increase has been partially instigated by the number of new mobile threats, which has risen to 2.3 million, a million more than in Q3.

Mobile malware

A 72% increase in new mobile malware samples was noted in the last quarter of 2015. Intel Security assigned the rise to Google's monthly Android update from August 2015 and the subsequent action taken by malware creators to follow up the change with sophisticated malware variants. The increase was unevenly distributed across geographical locations, with Africa-based client companies measuring an increase of 13%, Asian-based clients following closely with 10%, whereas South and North American clients were on the third and fourth place, with an increase of 9% and 6% respectively. Europe and Australia were least affected, with an increase of just 4%. It is critical to read these findings in view of the parallel results measured by Intel Security reflecting the percentage of mobile customers reporting detections, which dropped from a quarter average of 16% in 2014 to a quarter average of 7% in 2015.

Rootkit malware

2015 marked a severe drop in the number of new rootkit malware samples. Intel Security reported the finding as a continuation to a similar trend, initiated by ongoing user adoption of 64-bit Intel processors and 64-bit Windows. The respective technologies have built-in features such as Kernel Patch Protection and Secure Boot, which work together to guard from rootkit malware.

The macOS malware

Intel analyzed new macOS malware samples, which were reportedly dominated by just a few malware families. The macOS malware had a significant average quarterly increase of around 18,000 new samples in 2015 compared to an average quarterly increase of just around 1,500 samples in 2014.

Ransomware

A 26% increase in new ransomware samples was marked in the last quarter of 2015. McAfee Labs justified the findings with the emergence of open source ransomware types, code such as Hidden Tear or EDA2, and Ransomware-as-a-Service variants such as Ransom32 and Encryptor as well as TeslaCrypt and CryptoWall 3. McAfee Labs concluded that ransomware campaigns grow on the basis of high money-making potential and low chances of arrest.

Malicious signed binaries

McAfee Labs affirmed that the continuous decrease in the number of new signed binaries might be due to two major arguments: businesses incorporating stronger hashing functions and expiring or revoked older certificates, popular in the dark web. In addition, Smart Screen technology was an extra trust test that complicated the signing of malicious binaries for malware creators.

Macro malware

On the other hand, the number of total macro malware samples increased from around 220,000 reported in the last quarter of 2014 to approximately 410,000 reported in the last quarter of 2015.

Worldwide botnet prevalence

In the same report, Intel Security proportioned global popular botnet types by disclosing data for eight principal botnets: Wapome with 34% prevalence, Muieblackcat with 14%, Sality with 9%, Darkness with 8%, Ramnit with 6%, China Chopper Webshell with 5%, Maazben with 4%, and H-Worm with 3%. The other 18 percent belongs to other botnet types.

Report results include the United States, Germany, Russia, the Netherlands, France, South Korea, the United Kingdom, and Ukraine as the top eight countries hosting botnet control servers. The US led the pack by hosting 32%, or almost a third, of the world's botnet servers. The next third is distributed among the rest of the pack, where each country participates in smaller chunks measuring from 3% to 5%, while the rest of the world makes up the remaining third.

Network attacks

McAfee Labs calculated top network attacks by measuring browser, brute force, denial of service, SSL, scan, DNS, and backdoor attacks and found out that browser attacks are securely positioned at first place with 36% of the total number, while brute force and denial of service attacks occupy the second and third positions, with 19% and 16% respectively. SSL attacks follow closely with 11%, while the remaining types of network attacks participate in relatively smaller amounts.

Summary

From today's perspective, it seems as if ransomware has always existed. This is certainly not the case, as we have seen in this introductory chapter. We started the introduction by exploring the birth and concept of cybercrime and the challenges law enforcement, academia, and security professionals face when combating its threatening behavior. We also explored the impact of cybercrime by numbers on varied geographical regions, industries, and devices.

We learned that the area of digital extortion is still vastly under regulated and thus highly appropriate for exploitation. It is certain that the evolution of ransomware we have discussed in numbers, malware variants, encryption techniques, and targeted victims, has no intention of stopping. We became familiar with the varied means used by cybercriminals who work in organized groups, their motives, and the financial gains behind digital extortion.

Additionally, we analyzed basic aspects of notable ransomware cases through history, thus getting an idea of current, pertinent threats, locker ransomware, and crypto-ransomware. Our vocabulary and general knowledge of cybersecurity was enriched by notions of modern extortion crimes such as sextortion, bug poaching, and corporate extortion. We confirmed the concern that mobile devices are not immune from the ransomware game.

In the end, we saw that businesses are severely targeted, and we looked at the idea of a proactive mitigating approach that needs to be at the forefront of an inquisitive chief information officer. The focus is on predictive intelligence.

In the next chapter, we will learn about DDoS extortion and its different attack groups.

2
DDoS Extortion

A **Distributed Denial of Service** (**DDoS**) attack happens when attackers use a large network of botnets to overpower another system's connection or processor, causing it to refute service to the real traffic it's receiving. DDoS extortion is one of the most revolutionizing extortion techniques that is becoming mainstream among cybercriminals. This chapter covers all DDoS attacks that hold companies ransom by threatening to shut down services, servers, or websites. This chapter will discuss who are targeted in these attacks and why it is so hard to defend against these attacks. It will also cover some of the recent scams and what trends we expect to see in 2017 and beyond.

In this chapter, we will learn about:

- DDoS extortion
- The science behind DDoS extortion attacks
- Defending against DDoS attacks and extortions
- Future trends

DDoS extortion - ransomware's older cousin

Cybercrimes, in general especially cyber extortion, in particular, is incrementing day by day across the multitude of businesses and institution, both public and private. Similar to a borderless organized crime, DoS, or DDoS, is a global phenomenon that is generally complex and resource intensive in nature.

Ransomware has been receiving a lot of attention lately, but at the same time, its older cousin - extortion by DDoS demands the attention due to a massive increase in its trend. DDoS is one of the most weaponized methods for extortion and vandalism in the cybercriminal's arsenal, causing damages worth millions of dollars to public and private industries.

These attacks can be previewed as the Achilles heel of an enterprise that is dependent on the Internet and the impact of which could affect its finances and brand reputation to the highest degree. Sometimes, it is also used as a cover for more menacing cybercrime activity as the industry has seen with multiple ransomware campaigns.

DDoS attacks are certainly not something new running aloof in the wild, but certainly there have been several new developments to it recently. For extortion, the use of Bitcoin as a method of payment is going mainstream. Multiple industries have been victims to crude extortion plots using DDoS attacks as punishment for not paying the ransom. Such attacks target business information systems such as business portals, servers, and infrastructure ecosystem and make it impossible for regular users to access them normally.

Usually, once an organization has resolved the issue in the phase of an attack, it doesn't face repeated attacks. With extortion, the difference being that the attack may not stop until the cybercriminals have been paid.

The impact of such attacks is getting complex and sophisticated every year with the attack in itself getting bigger and targeted. While such assaults are on the rise, many companies have been content to protect themselves with legacy perimeter security systems. Extortion along with an attack on the target organization magnifies both the seriousness of the situation and the potential for financial loss to the targeted organization.

As per the growing trends of DDoS extortion, it should be considered as one of the bigger threats that can be chosen over other threats due to:

- The type of target (industry or organization size, for example)
- The attackers' toolset
- Skill level (the depth of the criminal organization behind the attack), or the relative ease of execution

DDoS attacks are not only targeted towards certain web portal or perimeter devices, but they also frequently focus on exhausting the network itself. This includes all perimeter devices, including but not restricted to, routers, firewalls (web application and traditional firewalls), and servers have limited resources (in terms of overall throughput and capacity), which can fail under multiple DDoS circumstances and heavy load.

Targeted attacks towards DNS servers and network infrastructure are being notified round the clock 365 days a year across multiple **Security Operation Centers** (**SOC**).

DDoS extortions and attacks, even though they are a growing threat across sectors worldwide, they are also a weapon of mass destruction. Designed to evade detection by today's advanced security solutions, these attacks can quickly put a targeted business out of action, costing millions of dollars in lost productivity and revenue. Just by overwhelming servers, network links, perimeter devices, and web applications with bogus traffic from botnets across the globe, the attacks can paralyze the Internet systems.

Botnets today can be rented by the hour at a minimal cost, wherein even the cybercriminals targeting a victim don't have to spend any money at all to launch a successful DDoS attack. Open source tools such as **Low Orbit Ion Cannon** (**LOIC**) have been around for several years and are free of cost. The inclusion of the **Hivermind** feature (**Low Orbit Web Cannon** (**LOWC**)) expanded the popularity of this tool due to the fact that this capability allows for creating a hive of thousands of participants to be mobilized to target a particular victim. cybercriminals thus need only the URL of the target and they are a couple of clicks away from accomplishing their task. These blends of activities are followed by a not-so-friendly extortion e-mail that delivers an inexpensive DDoS extortion attack.

The trend of cybercriminals targeting small and large businesses to make their services unavailable and asking for the ransom to prevent them causing DDoS attacks is going mainstream. Since extorting organizations opens a major avenue to gain profit from DDoS attacks, multiple groups of cybercriminals are in the midst to use the opportunity. cybercriminals are also assisting multiple organizations to profit from DDoS attacks by targeting DDoS attacks against their competitors. Recent attacks also show multiple DDoS campaigns against crypto currency Bitcoin, eventually causing the exchange rates to drop by more than 50% allowing cybercriminals to buy Bitcoins cheaper and sell with a huge margin. Thus, the increase in usage and dependency on the Internet provides a rational for DDoS extortions and attacks against businesses of all sizes, across multiple sectors.

Specific sectors at risk

DDoS extortion attacks are being targeted towards all major industries, whether they are a **small or medium business** (**SMB**) or a large enterprise across sectors. DDoS extortion attacks began in the early 2000s. Small businesses were targeted primarily because their cyber security defense systems weren't as robust as that of larger enterprises.

Often when attackers target web startups, they keep their monetary demands low. Generally, DDoS attack victims weigh the extortion amount against what is usually the higher cost of defending against the attack and losing business, and often they decide to pay up.

Although DDoS extortion attacks have been a prime concern for small and medium businesses including gambling websites and virtual currency-based businesses, it's been seen that attackers are broadening their scope and diversifying their targets across different industry sectors, regions, and larger organizations.

> According to the reports by Symantec Corporation, the latest attack on the BBC, which saw its public facing website and associated services including iPlayer, which is the BBC's Internet catch up TV and radio service in the UK, taken down for several hours on New Year's Eve is one of the prime examples. It is also thought to be the biggest ever DDoS attack and according to New World Hacking, the anti-Islamic State organization claimed responsibility. The cybercriminals also claimed that the DDoS attack reached a peak of 602 Gbps.
> For more information, check out the following link:
> `http://www.bbc.com/news/technology-35204915`.

In May 2015, multiple banks in Hong Kong were also targeted with DDoS attacks followed by a note demanding ransom. These attacks were suspected to be the work of one of the leading extortionist hacker groups called **DDoS for Bitcoin** (**DD4BC**). There have also been cases wherein multiple online investment websites have been targeted.

Sometimes even for huge DDoS attacks, the cybercriminals often demand quite a small amount of ransom. For example, during an attack against social networking site `https://www.meetup.com` in 2014, the attacker demanded US$300. Instantaneously, Meetup.com's servers were attacked with massive levels of traffic that brought its networking services down, which had ripple effects for the company's 16 million users. DDoS attacks are so prevalent today that many businesses and websites are always under some form of traffic attack, 365 days a year.

Recently in June 2016, one of the anti-DDoS solution providers mitigated one of the largest confirmed DDoS attacks routed in their network, which peaked at 363 **Gigabits per second** (**Gbps**) and 57 **Million packets per second** (**Mpps**). The attack was targeted towards a European media organization and compromised of a hybrid attack methodology.

The attack consisted of more than five varied attack vectors:

- Syn
- UDP fragment
- push
- TCP
- DNS
- UDP DDoS floods

The attack analysis by the provider identified a DNS reflection technique that abused a **Domain Name System Security Extension** (**DNSSEC**) configured domain. This attack technique generated a bigger response size, due to the requirements of the DNSSEC. As per the provider, the attack techniques and duration of the attack pointed to the use of booter services, which are easily available for lease in the underground marketplace (for DDoS).

Prevailing DDoS attacks against industries are primarily driven by financial benefits and the urge to take services down due to various motives. With the attack techniques getting more sophisticated and flexible in terms of ease of launching an attack, the overall security equation is getting more vicious in nature.

Why is it hard to defend against these attacks?

The current threat of DDoS trends makes it quite clear that existing strategy across enterprises is no longer defensible. Large-scale hybrid attacks are growing in size, requiring increased network capacity in order to keep up. In addition to this, more sophisticated DDoS varieties are emerging across platforms that require organizations to be highly flexible and focus on fixing application flaws exposed to the Internet.

Furthermore, these days little or no technical skill is required to mount a DDoS attack. Typically attacks are launched through resource amplification or botnets and with such botnets containing thousands of infected hosts, it can be instructed to launch a devastating coordinated attack on their target instantly.

One of the other crucial developments across enterprises of all sizes is the dissolution of the network perimeter. As businesses are embracing cloud and investing heavily in migrating their solutions to a public or private cloud, they are developing and deploying applications in the cloud. This transition renders traditional defenses inadequate against the potential DDoS attacks.

A DDoS attack potentially is quite difficult to deflect without specialized DDoS mitigation in place. Responding to a DDoS attack as required poses a significant challenge for all Internet-dependent companies. Traditional defenses with network devices and perimeter security technologies, although they are an important facet of an overall security strategy for an enterprise, they don't by themselves provide thorough DDoS protection. Instead of defending against the current DDoS threats, enterprises require a purpose built secure ecosystem that consists of the ability to specifically detect and defeat increasingly complex and deceptive attack vectors.

New technology evolutions such as IoT are also being used to launch DDoS attacks. Currently, there is widespread adoption of smart devices across sectors, especially consumer sector in the form of wearables and home appliances enabling basic comforts of life.

As per the *Verizon IoT Report of 2016*, home monitoring solutions have seen a growth of 50% from 2014 to 2015 and 43% annual growth for smart cities technologies and networks.

The growth and adoption of smart devices is incremental and getting mainstream. As per Gartner, there will be approximately 20.8 billion connected devices by 2020. If you consider the potential quantities associated with IoT products and associate their computing power towards DDoS, it can be envisaged how possibly strong a DDoS attack would be.

These types of attacks have already commenced. A researcher at Sucuri had released a report that noted the compromise and use of over 2,5000 **Closed Circuit Television** (**CCTV**) devices towards a DDoS attack. The researchers pointed to a **remote code execution** (**RCE**) flaw exposed by some vendors in the market. This example showcases again the potential impact of such usage of technologies from cybercriminals. From an IoT perspective, compromising IoT products does not have to be as complex as identifying an unpatched vulnerability and exploiting that loophole to procreate a botnet. Lots of IoT products ship with no password protection and a lot of them use vendor default passwords for local access.

For more information, check out the following link: `http://securityaffairs.co/wordpress/48807/iot/cctv-devices-ddos.html`

cybercriminals who can identify these low hanging fruit can victimize large populations of the product quickly and employ them for their malicious purposes. A real-world example of this is the Lizardstresser DDoS botnet. Security firm Arbor Networks noted that the actors running this botnet have already begun targeting IoT devices that share default passwords across device classes.

Thus, organizations with a multifaceted approach will be better equipped to defend against different types and categories of DDoS attacks. Organizations should develop a plan that is both proactive and responsive. The alternative in an extortion DDoS incident is to negotiate with the attackers and pay up, which potentially opens the door to future extortion.

The science behind DDoS attacks

DDoS attacks are classified in different ways following different criteria. The following subsections present DDoS attack types and corresponding technical details based on the attack approaches, volume of traffic generated, and based on attack rate dynamics.

Evolution of DDoS attacks types

As discussed in an earlier section, DDoS extortion and attacks pose an immense threat to all organization worldwide. On the other hand, constantly many defense mechanisms have been proposed and evolved to combat them. Attackers continuously modify the tools to circumvent these defense mechanisms and on the other side, security researchers modify their strategy to approach new attack vectors.

The DDoS disaster is largely due to the ease with which anybody can launch an attack in addition to the weak defense mechanisms and DDoS protection frameworks deployed by the organizations. Detailed tutorials are also available for inexperienced users on how to carry out comprehensive DDoS attacks including how to rent botnets and from where via a pay-for-hire DDoS service.

cybercriminals change their attack strategies so not to miss any of their targets. Modern attacks utilize multi-level attack vectors in a single DDoS campaign targeting multiple components of an organization's network infrastructure and their applications. These attacks not only exhaust bandwidth and network resources, but in the majority of cases take down business sensitive servers and application resources.

Inside DDoS attacks

DDoS attacks essentially exploit Internet protocols and the behavior of packets that get delivered from nearly any source to any destination. Either there are multiple network assets (devices and servers) that are incompetent to serve access to the users or they cannot recognize the illegitimate packets from the legitimate packets making detection complex in nature. Signature-based identification performed by **Next Generation Firewall** (**NGFWs**) and **Intrusion Detection and Prevention Systems** (**IDS/IPS**), do not work these days. Most of the attacks today are hybrid in nature and use spoofed source IP addresses, which helps to escape monitoring tools using heuristic-based analysis.

Operation Sony is a classic example, wherein cyber attacks on the Sony Playstation Network hit Sony on multiple fronts especially reputation and financial damage. It was an ultimate case in which a DDoS attack campaign was launched by the intruders, to distract their target from their exact objective - data theft. It allowed for the cybercriminals to steal the account information of over 77 million users of Sony's PlayStation Network by implementing a well planned attack. Sony was unaware for a long time that any information had been stolen completely because they were focusing on handling the initial DDoS attack.

Traditionally, DDoS attacks usually were low-level protocol attacks with limited focus areas. Today DDoS attacks have multiple attack vectors segregated across different layers having a multi-faceted approach. In two major groups, DDoS attacks can be categorized based on their respective attack characteristics. Firstly, the types of attack include those that target bandwidth consumption (network and system resource exhaustion) and secondly those that exploit the vulnerability of application or Layer 7 resources. Both of the categories have their own distinctions and effect on the designated target.

Bandwidth attacks

In this category of attack, cybercriminals target to flood perimeter devices with more network bandwidth than they can withstand. The primary objective of this attack is to prevent legitimate traffic from reaching the target business services. This is one of the most common types of DDoS attack that targets to push more network traffic to the victim than the bandwidth can consume. If the intended victim has a 100 Mbps Internet connection, the cybercriminal only needs to direct 100 Mbps of DDoS traffic at it and any traffic above that would be dropped disrupting the services to legitimate users. A few dozen bot infected machine across the world is enough to take the victim down.

There are a certain group of attackers that target network resources by primarily attempting to exhaust system resources of the victim. As we are aware all services are provisioned on servers with certain resource limitations (both physically and programmatically as per the design). For example, a single application server may be able to cope with 5000 simultaneous HTTP-based user sessions or 1000 HTTPS-based user sessions. Once 5000 user sessions have been initialized no further sessions can be made to the corresponding servers until some of the earlier sessions expire.

It's one of the easiest attacks to launch wherein an attacker can manually pursue to exhaust the resources of the target intended system by generating multiple sessions from their systems or if botnets are used, an attacker can instruct tens or hundreds of bots to make thousands of simultaneous connections to the victims server and to keep those connections and sessions open for as long as possible. This would prevent legitimate users to connect to the server and receive the intended services.

According to *The DDoS Threat Spectrum* paper by *David Holmes*, within bandwidth attacks, the most common attacks in the DDoS landscape are network attacks called **floods**, which connect a multitude of nodes to send an overwhelming amount of Internet traffic to the victim server. With such an attack, either the victim server gives away or the perimeter device, which would be in front of the victim server.

By using multiple clients or bots (which can be rented), the attacker can amplify the volume of the attack having complete control of the traffic pattern. In the case of bots, security devices may not be able to track and block the malicious traffic or be able to analyze the intent of the traffic since that traffic may potentially seem to originate from all over the globe representing authentic users. SYN flood and Connection flood explains these simple forms of distributed attacks that focus on filling up the flow tables for stateful devices that monitor connections such as firewalls, or **intrusion prevention systems** (**IPS**).

Modern DDoS attacks do exceed the throughput capacity of the targets, but typical perimeter networks and security devices within the target data center naturally fail long before those limits get outdone.

The following Layer 3 and Layer 4 attacks are still in use today, often along with the most advanced techniques of application-based attacks:

DNS attacks

Name queries (such as `https://www.test.com`) are translated into the numerical address (for example, `192.168.1.2`) by the DNS. DNS is the most important and public of all services because almost all the systems count on DNS queries to get to their planned services. If the DNS or DNS services get disrupted, all the business services on the Internet provisioned by the victim's data center get affected. For all the businesses that are exposed to the Internet or are digital in nature, DNS is a potential target for attackers and architecturally becomes the single point of failure.

DNS attacks are one of the most common attacks that are easy to launch and complex to defend against. Even in a lot of cases, wherein a cybercriminal queries for the IP of the victim, prior to the attack getting initialized on the victim server, an indirect attack against the DNS servers gets carried upon.

The following are the specific modules of DNS attacks:

- **UDP floods:** *The DDoS Handbook* by *Radware* defines **User Datagram Protocol** (**UDP**) as a connectionless protocol that uses datagrams embedded in **Internet Protocol** (**IP**) packets for communication, without needing to create a session between two devices (in other words, it requires no handshake process)
- **NSQUERY and NXDOMAIN** are other type of attacks that emphasize on the request types crippling the DNS servers

Application attacks

DDoS attacks in this category are generally focused on application behavior and cybercriminals primarily focus on exploiting weakness within the applications being served by the hosting infrastructure. The attacks largely exploit the expected behavior and services of protocols such as TCP and HTTP to their advantage by binding computational resources and preventing them from handling and processing transactions or requests.

Application attacks can take multiple forms depending upon the target system features and intentions of the cybercriminal. A cybercriminal, for example, may deny victims the ability to log into an application server intentionally by supplying multiple incorrect passwords until the application locks the account out.

HTTP attacks

Most of the low-level DDoS attacks are HTTP floods. HTTP floods look like real HTTP web request unlike network attacks, wherein an attacker has to overwhelm resources with invalid packets.

Generally, to the conventional firewall technology, the HTTP requests are indistinguishable from standard regular traffic, so they are simply passed through to the web servers. Thus thousands or millions of attacking bots overwhelm the web server with a massive number of requests.

Largely there are two major variations of the HTTP flood attack. The most common are when a cybercriminal repeats the same request repeatedly. This kind of attack is easy to program and easy to detect and filter. The other advanced version of the HTTP flood is a recursive GET denial of service. Attackers that promote this attack request the main application page, parse the response, and then recursively request using HTTP GET every object present at the site. These attacks generally are very difficult to detect and filter since every connection request is targeted to a unique legitimate object within the site.

Low bandwidth HTTP denial of service attacks

One of the widely-seen application attacks is the low bandwidth attacks, which can be executed by multiple slowloris scripts. **Slowloris** works generally by initializing connections with a web server and sending just enough data in an HTTP header to keep the connections open - usually 5 bytes every 299 seconds. This fills up the web server's connection table.

Sometimes it can be a tricky attack since it would not get captured under the normal security monitoring solutions. Normally against a web server running Apache (in the earlier versions), Slowloris achieved denial of service with just 394 open connections.

Like Slowloris, the **Slowpost** attack is one of the other variants that uses a measured, low bandwidth approach. The difference is that instead of a `HTTP` header, it begins an `HTTP POST` command, which then feeds the payload of the `POST` header very slowly sometimes as slow as 1 byte per approximately two minutes. Due to the whole message being technically correct and complete the targeted server idle timeout will not be invoked and the server holds onto the connection alive until all the bytes of data specified in the content-length header were received by the server. Because the attack is so unpretentious, it could infect multiple applications, across multiple industries.

Another low bandwidth attack is the Hash Collision DoS attack. This attack has been exceptionally powerful, resource intensive, and is effective against all major web server platforms. In a **Hash Collision DoS** attack scenario, the cybercriminal sends a specially crafted POST message with a multitude of parameters. The parameters are essentially built in a way that causes hash collisions on the server side, slowing down the response processing dramatically.

> As per the F5 report on the DDoS Threat Spectrum, the security professionals exploring this attack demonstrated that a single client with a 30 Kbps connection (which literally could be a handset) could tie up an Intel i7 core for an hour. If we generalize this with a group of attackers with only a 1 Gbps connection, they could tie up 10,000 i7 cores indefinitely.

If a web server is terminating TLS connections, it can also be vulnerable to the SSL/TLS renegotiation attack. The attack, also called THC SSL DoS (THC stands for The Hackers Choice), works by initiating a regular SSL/TLS handshake, and then instantly requests for the renegotiation of the encryption key.

The attacker continuously repeats this renegotiation request up until all server resources have been exhausted. The server has more cryptographic computation than the SSL/TLS clients to establish the session. Thus, a single SSL/TLS client can attack and overwhelm a web server and thus has the potential to take down a complete farm of secure online services.

Attack	Target Vector	Description
Slowloris	Connection table	Slowly feeds HTTP headers to keep connections open
Slowpost	Connection table	Slowly POSTs data to keep connections open
HashDos	CPU	Overwhelms hash tables in backend platforms
SSL renegotiation	CPU	Exploits asymmetry of cryptographic operations

The preceding table shows low bandwidth HTTP attacks as per the *F5- DDoS Threat Spectrum Report*.

Modern web applications and servers have been a potentially vulnerable target for simple low bandwidth attacks. These "low and slow" attacks target specific application vulnerabilities, allowing a cybercriminal to stealthily cause a denial of service. Such attacks are precisely difficult to detect and mitigate, turning any weak points in an application into a new attack vector.

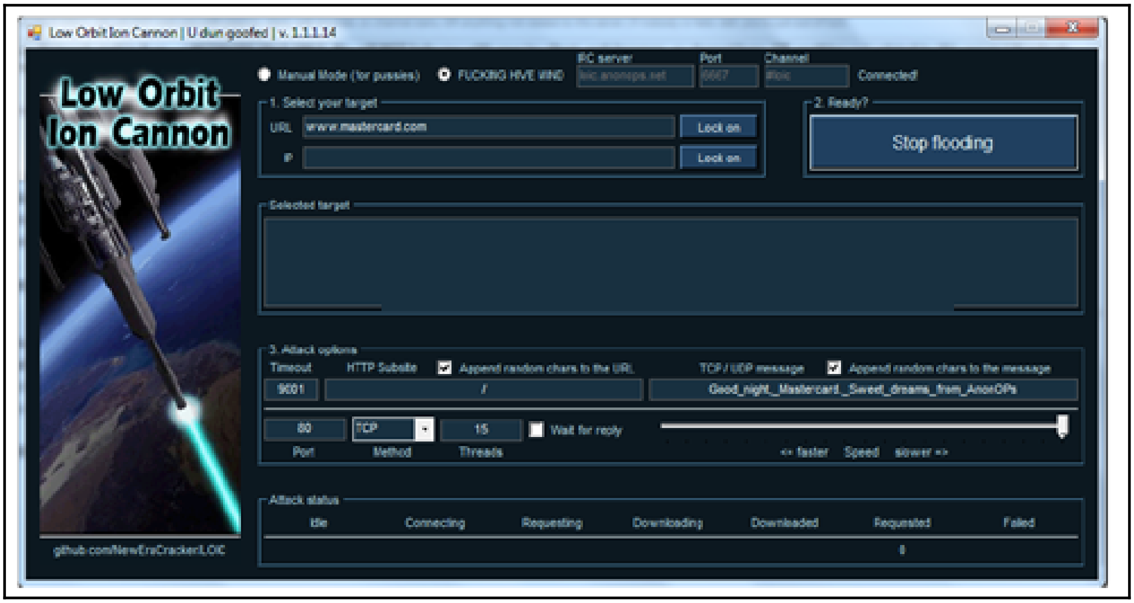
Attack tools

Until recent times, DDoS attack tools required a wealth of knowledge to execute, but now these tools have been transformed and are much easier and straightforward to use across platforms. Thus, it is more dangerous in the hands of any individual who wants to target businesses for causing disruption to its services.

Some of the most common tools include:

- **Low Orbit Ion Cannon** (**LOIC**)
- **High Orbit Ion Cannon** (**HOIC**)
- #RefRef
- HPing
- Slowloris
- RUDY
- TRUNO

LOIC was one of the simple and common tools used by Anonymous. The only challenge that Anonymous faced with this version of tool was that they weren't able to obscure the users IP address using this tool - which made them upgrade the tool to HOIC.


Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.14

○ Manual Mode (for pussies) ● FUCKING HIVE MIND

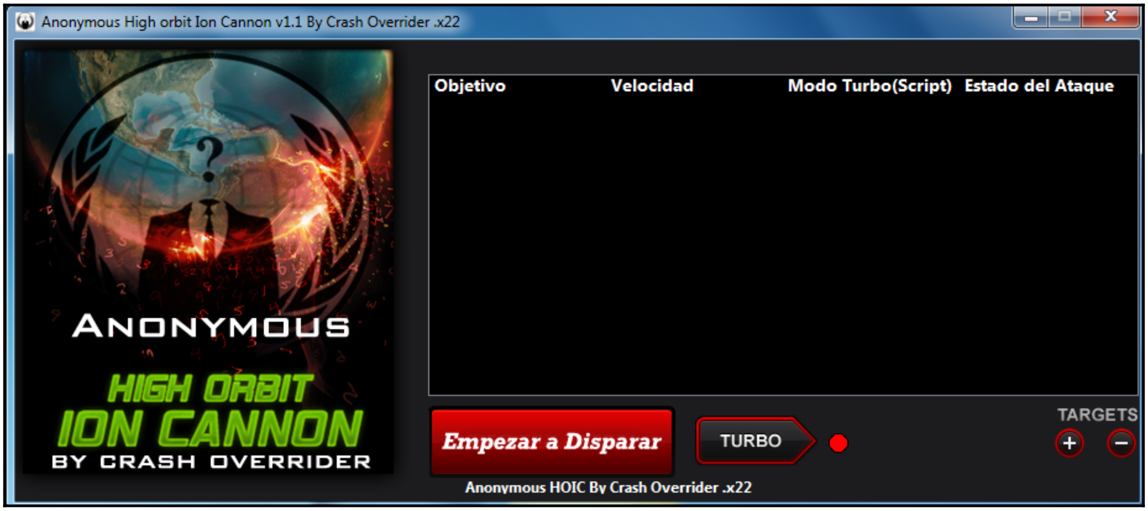
IRC server: loic.anonops.net
Port: 6667
Channel: #loic
Connected!

URL: www.mastercard.com

Timeout: 9001
HTTP Subsite: /
☑ Append random chars to the URL
TCP / UDP message: Good_night_Mastercard._Sweet_dreams_from_AnonOPs
☑ Append random chars to the message
Port: 80
Method: TCP
Threads: 15
□ Wait for reply

Low Orbit Ion Cannon (LOIC) tool

HOIC was used by Anonymous and had a wide impact on multiple public institutions.



High Orbit Ion Cannon

The botnet as a DDoS tool

Botnets are one of the most communal tools used by cybercriminals and they have the potential to execute attacks to multiple targets via bots provisioned by a Command and Control server. Multiple cybercriminals hosted "botnets" - which are fundamentally a collection of infected systems, provided to users to deface the targets with DDoS and multiple other attack vectors.

The price of renting such botnets varied from US$5 to USD$1,500 dependent on multiple factors from scale to impact of the attacks. Some of the potential famous botnets include:

Botnet	Estimated Size	DDoS Attack Types
Rustock	2.4 million	Connection flood
Cutwail	2.0 million	Fake SSL flood
akbo	1.3 million	General - unknown
TFN2K	Unknown	SYN flood, UDP flood, ICMP flood, Smurf attack
LOIC	15,000	HTTP flood, SYN flood, UDP flood
HOIC	Unknown	HTTP flood

Botnet	Estimated Size	DDoS Attack Types
RefRef	Unknown	DoS via SQL server vulnerability

The preceding table shows some of the high-profile botnets in the world as per the *F5-DDoS Threat Spectrum Report.*

Attack groups

This is a list of DDoS attack groups that have had some visibility:

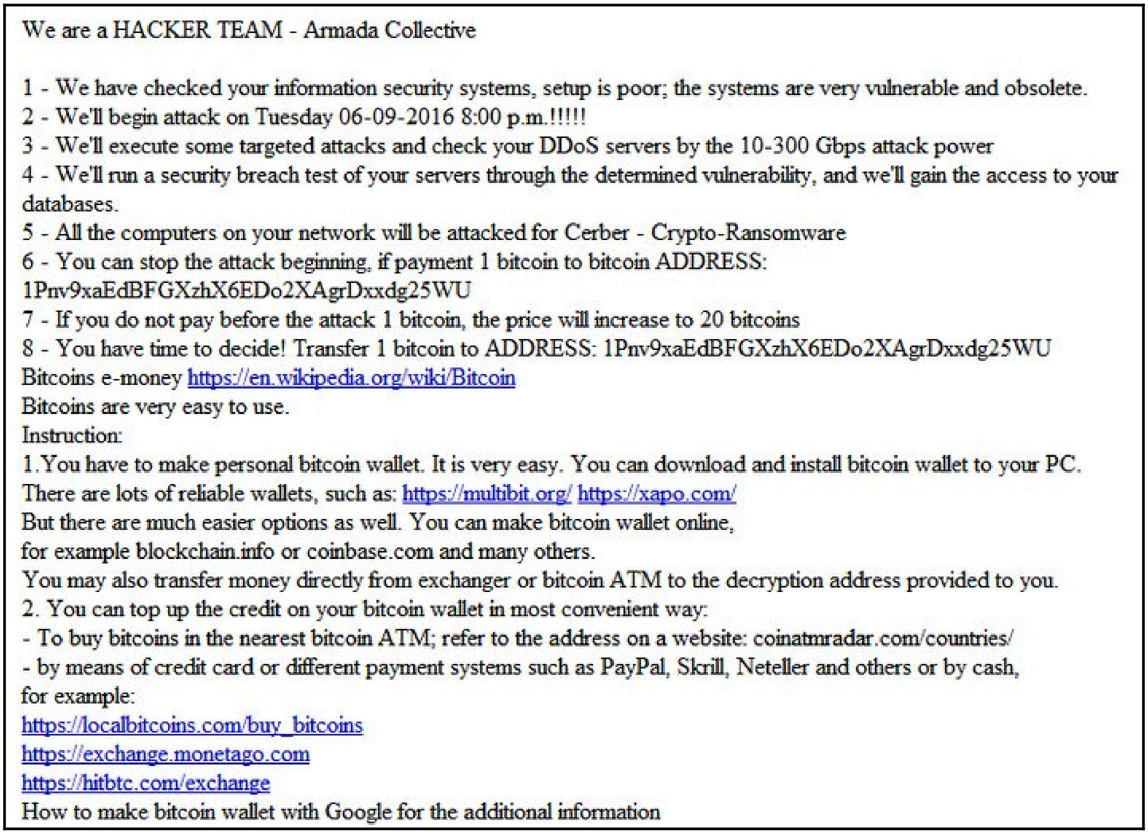
- The Armada Collective
- Lizard Squad
- DD4BC
- Imposters
- Recent Scams

The extortion method has become mainstream and very popular in the virtual space, especially in the form of DDoS attack threats. Indeed these work so profitably that multiple cybercriminals groups across the globe started DDoS extortion campaigns. Out of the total potential groups, some were very capable ones and multiple others were only impersonators of the original group. Armada Collective, DD4BC, Kadyrovtsy, ezBTC, Lizard Squad, and RedDoor are some of them. Most of the groups have shown their ability to launch DDoS attacks at various volumes. In most of the cases, they used to have a short demo attack potentially showing the seriousness of their threats followed by a ransom note. These threats were focused towards all size of businesses including small and medium-sized businesses that do not have as strong security defenses as larger enterprises.

The Armada Collective

The **Armada Collective** is a well-known DDoS extortion group that is currently unattributed. Its campaigns and mode of operation are exactly similar to those used by the extortion groups that go by the name DD4BC. They threaten the victims with extortion e-mails warning of an impending DDoS attack against their online businesses until a ransom is paid in Bitcoins.

One of the latest victims of this campaign is Etienne Delport from Port Elizabeth, South Africa, owner of Alpha Bookkeeping Services. On September 5, 2016, Delport published the e-mail that he had received from the group, showing a ransom note he received from the group. The group, this time, was threatening the victim with a 10-300 Gbps DDoS attack the next day unless the victim paid a ransom of 1 Bitcoin (~$615) to a certain address. cybercriminals also stated that they would charge in multiples (20 Bitcoins), once they commence the DDoS attacks and if the victim wants to get it stopped thereafter.

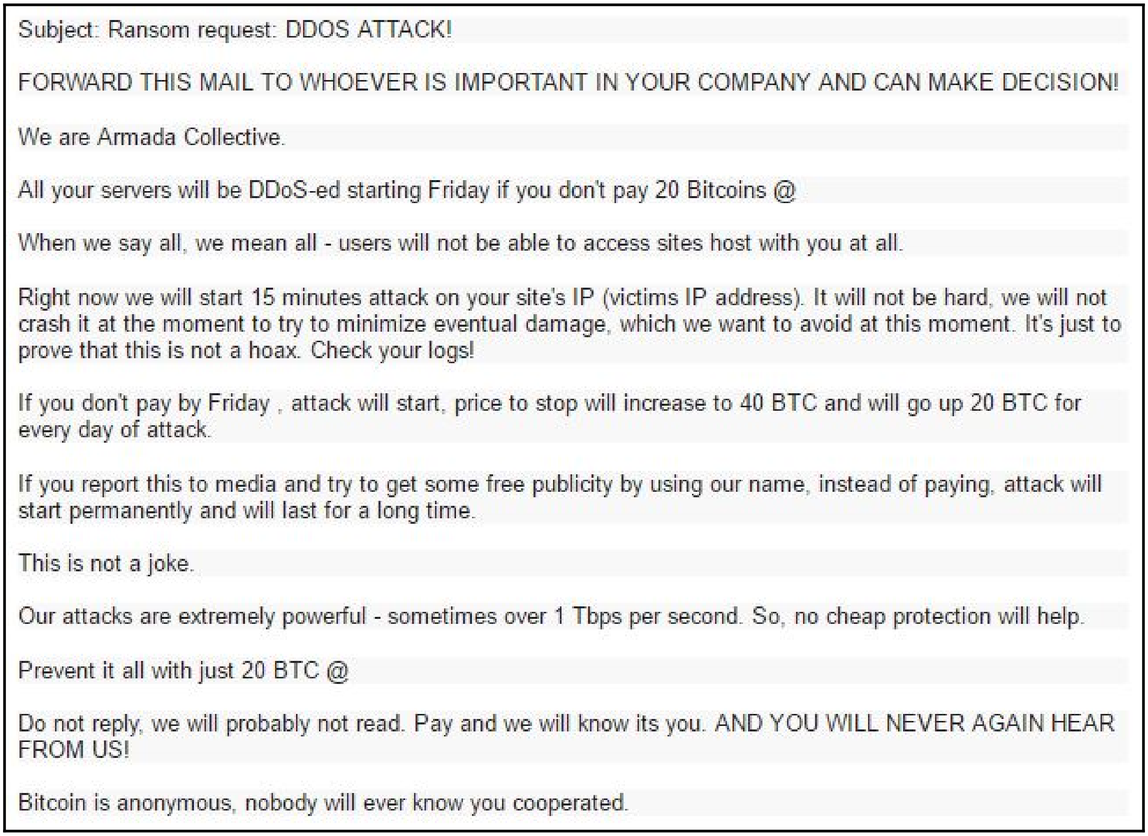


We are a HACKER TEAM - Armada Collective

1 - We have checked your information security systems, setup is poor; the systems are very vulnerable and obsolete.
2 - We'll begin attack on Tuesday 06-09-2016 8:00 p.m.!!!!!
3 - We'll execute some targeted attacks and check your DDoS servers by the 10-300 Gbps attack power
4 - We'll run a security breach test of your servers through the determined vulnerability, and we'll gain the access to your databases.
5 - All the computers on your network will be attacked for Cerber - Crypto-Ransomware
6 - You can stop the attack beginning, if payment 1 bitcoin to bitcoin ADDRESS:
1Pnv9xaEdBFGXzhX6EDo2XAgrDxxdg25WU
7 - If you do not pay before the attack 1 bitcoin, the price will increase to 20 bitcoins
8 - You have time to decide! Transfer 1 bitcoin to ADDRESS: 1Pnv9xaEdBFGXzhX6EDo2XAgrDxxdg25WU
Bitcoins e-money https://en.wikipedia.org/wiki/Bitcoin
Bitcoins are very easy to use.
Instruction:
1.You have to make personal bitcoin wallet. It is very easy. You can download and install bitcoin wallet to your PC.
There are lots of reliable wallets, such as: https://multibit.org/ https://xapo.com/
But there are much easier options as well. You can make bitcoin wallet online,
for example blockchain.info or coinbase.com and many others.
You may also transfer money directly from exchanger or bitcoin ATM to the decryption address provided to you.
2. You can top up the credit on your bitcoin wallet in most convenient way:
- To buy bitcoins in the nearest bitcoin ATM; refer to the address on a website: coinatmradar.com/countries/
- by means of credit card or different payment systems such as PayPal, Skrill, Neteller and others or by cash,
for example:
https://localbitcoins.com/buy_bitcoins
https://exchange.monetago.com
https://hitbtc.com/exchange
How to make bitcoin wallet with Google for the additional information

Extortion e-mail received by one of the victims

These kinds of extortion attempts became quite common last year when a group of cybercriminals using the DD4BC name started employing them. Europol had also arrested the DD4BC group members last year, but other such impersonators appeared, Armada Collective being one of them.



Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @

When we say all, we mean all - users will not be able to access sites host with you at all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by Friday , attack will start, price to stop will increase to 40 BTC and will go up 20 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 20 BTC @

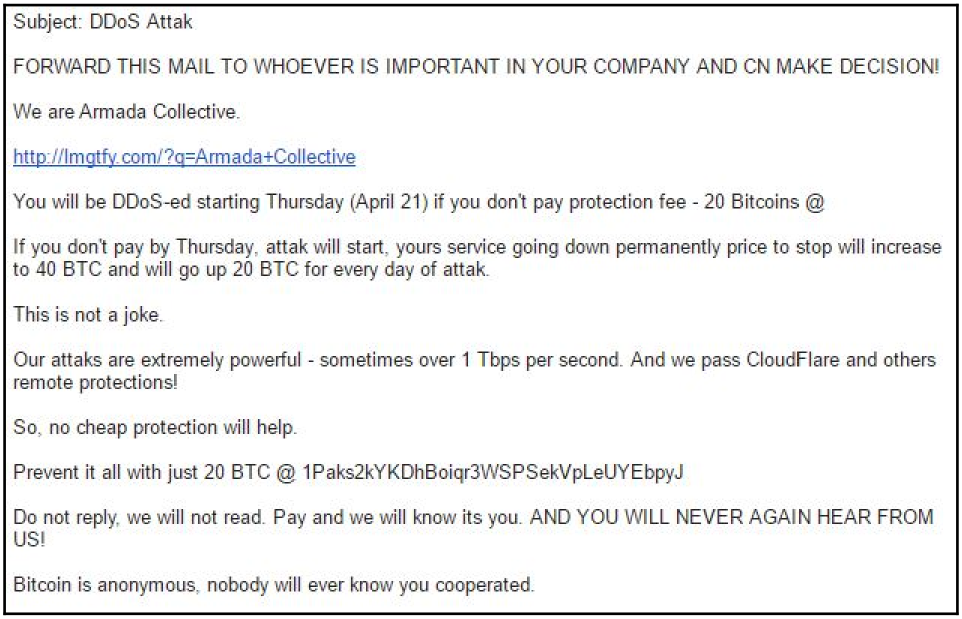
Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

One of the other legitimate e-mails from Armada Collective

One of the most famous legit attacks of the group was against ProtonMail where they forced the e-mail provider to pay approximately $6000 to stop a massive DDoS attack. ProtonMail initially ignored their e-mail in the beginning and an attack was launched the same night that took the service offline for 15 minutes. Another attack occurred the next day wherein the service provider took appropriate steps to mitigate it. At that point in time, the attacks went up in full force in both sophistication and bandwidth reaching over 100 Gbps targeting more of the ISP provider's upstream infrastructure attacking targeted weak spots in its network. After 90 minutes of downtime for the entire ISP, ProtonMail finally gave in and decided to pay the ransom to Armada Collective.

After the ProtonMail event, extortion attempts from the group came down until the winter of 2016 wherein multiple companies started reporting similar DD4BC extortion attempts.



Subject: DDoS Attak

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CN MAKE DECISION!

We are Armada Collective.

http://lmgtfy.com/?q=Armada+Collective

You will be DDoS-ed starting Thursday (April 21) if you don't pay protection fee - 20 Bitcoins @

If you don't pay by Thursday, attak will start, yours service going down permanently price to stop will increase to 40 BTC and will go up 20 BTC for every day of attak.

This is not a joke.

Our attaks are extremely powerful - sometimes over 1 Tbps per second. And we pass CloudFlare and others remote protections!

So, no cheap protection will help.

Prevent it all with just 20 BTC @ 1Paks2kYKDhBoiqr3WSPSekVpLeUYEbpyJ

Do not reply, we will not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

Fake e-mails from Armada Collection

Security evangelists weren't able to pin any of the other attempts on the real Armada Collective group, but their extortion numbers grew exponentially and in full swing targeted any website owner, not just large enterprises that could afford the ransom.

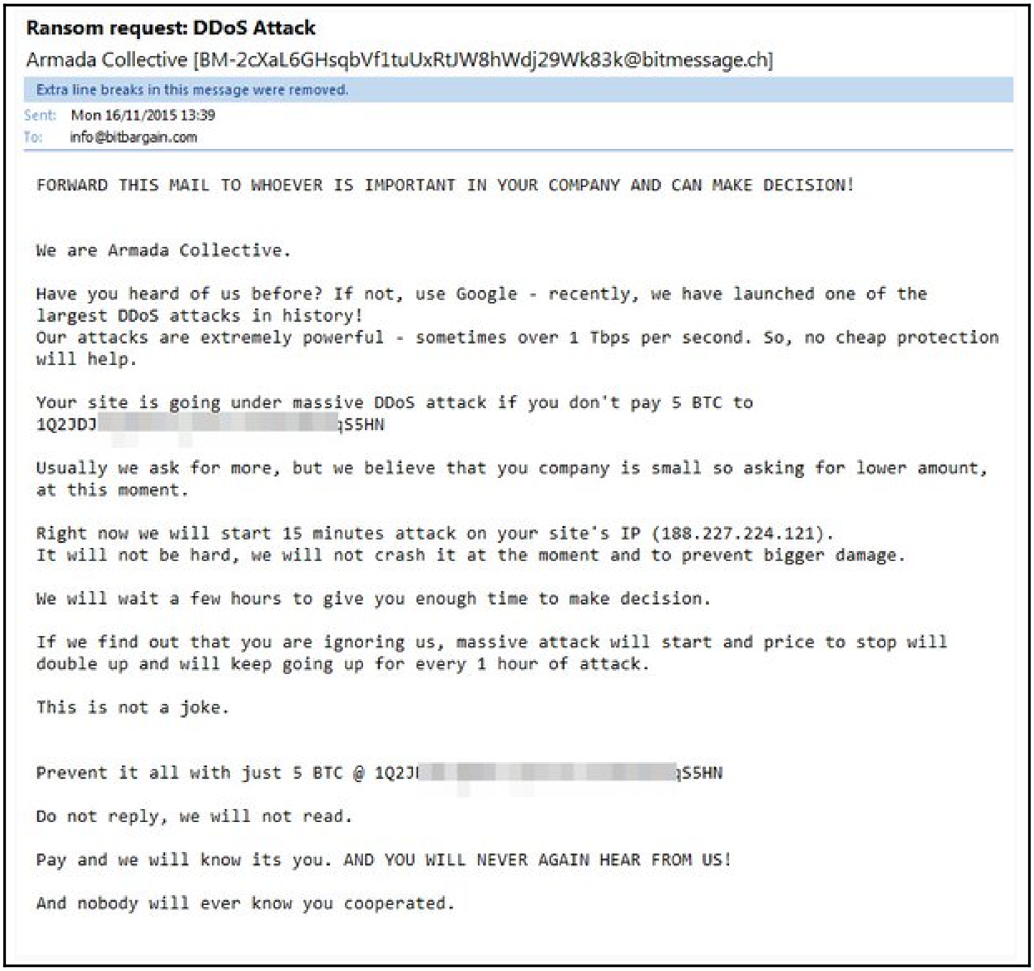
CloudFlare reported that a group of cybercriminals, using a definite list of Bitcoin addresses in its e-mails, was only threatening to launch DDoS attacks on websites in the name of Armada Collective, but they never came through. Soon after the initial incident, multiple e-mails in the form of Armada Collective ransom e-mails were targeted towards small businesses in Switzerland.

At a point in time, it was clear that one couldn't distinguish the real Armada Collective ransom e-mails from the impersonators, which spawned enormously following the successful ProtonMail attack.

Consequently, multiple cybercriminal groups now duplicate this modus operandi and spread similar ransom extortions while the major groups continue to launch their threats and attacks.

To date, this group is known to have targeted Australian organizations, Japanese, Swiss, and Thai financial institutions including providers such as ProtonMail, Hushmail, Runbox, and so on.

The most recent ransom e-mail that Delport received also illustrates that these cybercriminals behind the attacks are incorporating new elements in their tactics. The e-mail mentions that the infrastructure will be hit by Cerber ransomware, which is interesting due to the current hype surrounding ransomware infections across the world.



Ransom request: DDoS Attack
Armada Collective [BM-2cXaL6GHsqbVf1tuUxRtJW8hWdj29Wk83k@bitmessage.ch]

Extra line breaks in this message were removed.

Sent: Mon 16/11/2015 13:39
To: info@bitbargain.com

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

Have you heard of us before? If not, use Google - recently, we have launched one of the largest DDoS attacks in history!
Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Your site is going under massive DDoS attack if you don't pay 5 BTC to
1Q2JDJ[redacted]S5HN

Usually we ask for more, but we believe that you company is small so asking for lower amount, at this moment.

Right now we will start 15 minutes attack on your site's IP (188.227.224.121).
It will not be hard, we will not crash it at the moment and to prevent bigger damage.

We will wait a few hours to give you enough time to make decision.

If we find out that you are ignoring us, massive attack will start and price to stop will double up and will keep going up for every 1 hour of attack.

This is not a joke.

Prevent it all with just 5 BTC @ 1Q2J[redacted]S5HN

Do not reply, we will not read.

Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

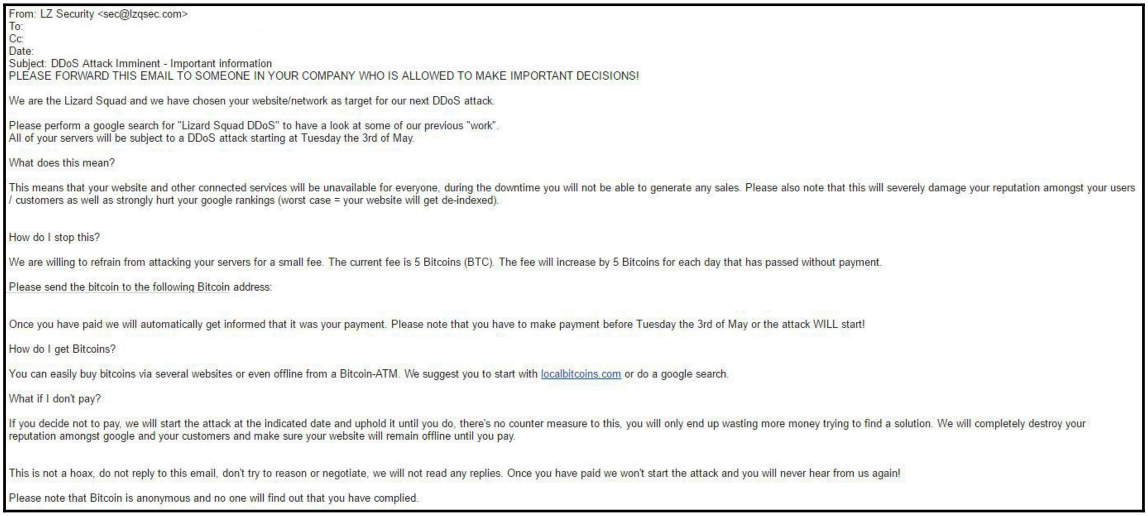
And nobody will ever know you cooperated.

Extortion e-mail from Armada Collective to UK Bitcoin exchange firm BitBargain

Lizard Squad

Lizard Squad is another cybercriminal group known for their claims of DDoS attacks primarily against the gaming industry. Lizard Squad rose to fame in 2014 when the loosely organized group launched enormous denial of service attacks on the Sony PlayStation network and Microsoft Xbox online gaming services on Christmas day.

Their services were taken offline completely for more than 158 million subscribers. Members of the cybercriminal group also responded to media requests on why the group had attacked the network by stating "because we can". Even though Microsoft had restored their Xbox live services shortly after the initial attack, Sony took more than two days to restore its PlayStation Network.



From: LZ Security <sec@lzqsec.com>
To:
Cc:
Date:
Subject: DDoS Attack Imminent - Important information
PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Lizard Squad and we have chosen your website/network as target for our next DDoS attack.

Please perform a google search for "Lizard Squad DDoS" to have a look at some of our previous "work".
All of your servers will be subject to a DDoS attack starting at Tuesday the 3rd of May.

What does this mean?

This means that your website and other connected services will be unavailable for everyone, during the downtime you will not be able to generate any sales. Please also note that this will severely damage your reputation amongst your users / customers as well as strongly hurt your google rankings (worst case = your website will get de-indexed).

How do I stop this?

We are willing to refrain from attacking your servers for a small fee. The current fee is 5 Bitcoins (BTC). The fee will increase by 5 Bitcoins for each day that has passed without payment.

Please send the bitcoin to the following Bitcoin address:

Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment before Tuesday the 3rd of May or the attack WILL start!

How do I get Bitcoins?

You can easily buy bitcoins via several websites or even offline from a Bitcoin-ATM. We suggest you to start with localbitcoins.com or do a google search.

What if I don't pay?

If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution. We will completely destroy your reputation amongst google and your customers and make sure your website will remain offline until you pay.

This is not a hoax, do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again!

Please note that Bitcoin is anonymous and no one will find out that you have complied.

Fake ransom threat by Lizard Squad

More recently similar e-mails like that of Armada Collective group have been seen claiming to be from the hacker group Lizard Squad. As per CloudFlare, it is assessed that these are the same actors posing as different DDoS groups since the 'fake' Armada Collective group was widely reported, and therefore this could have impacted the group's ability to extort organizations. Now they appear to be using another criminal group's name in order to once again appear credible.

The e-mails have absolutely similar modus operandi to the previous ransom e-mails. The Lizard Squad group threatens with DDoS attacks unless an extortion amount is paid to the Bitcoin address before a deadline. Each of the e-mails posted to victims by this cybercriminal group is exactly identical including a Bitcoin address that has been reused in all of them. Reusing the Bitcoin address signifies that this group of cybercriminals has no way to identify which company would have paid their ransom. If the group is legitimate, one would expect to see a unique Bitcoin address for each individual target company.

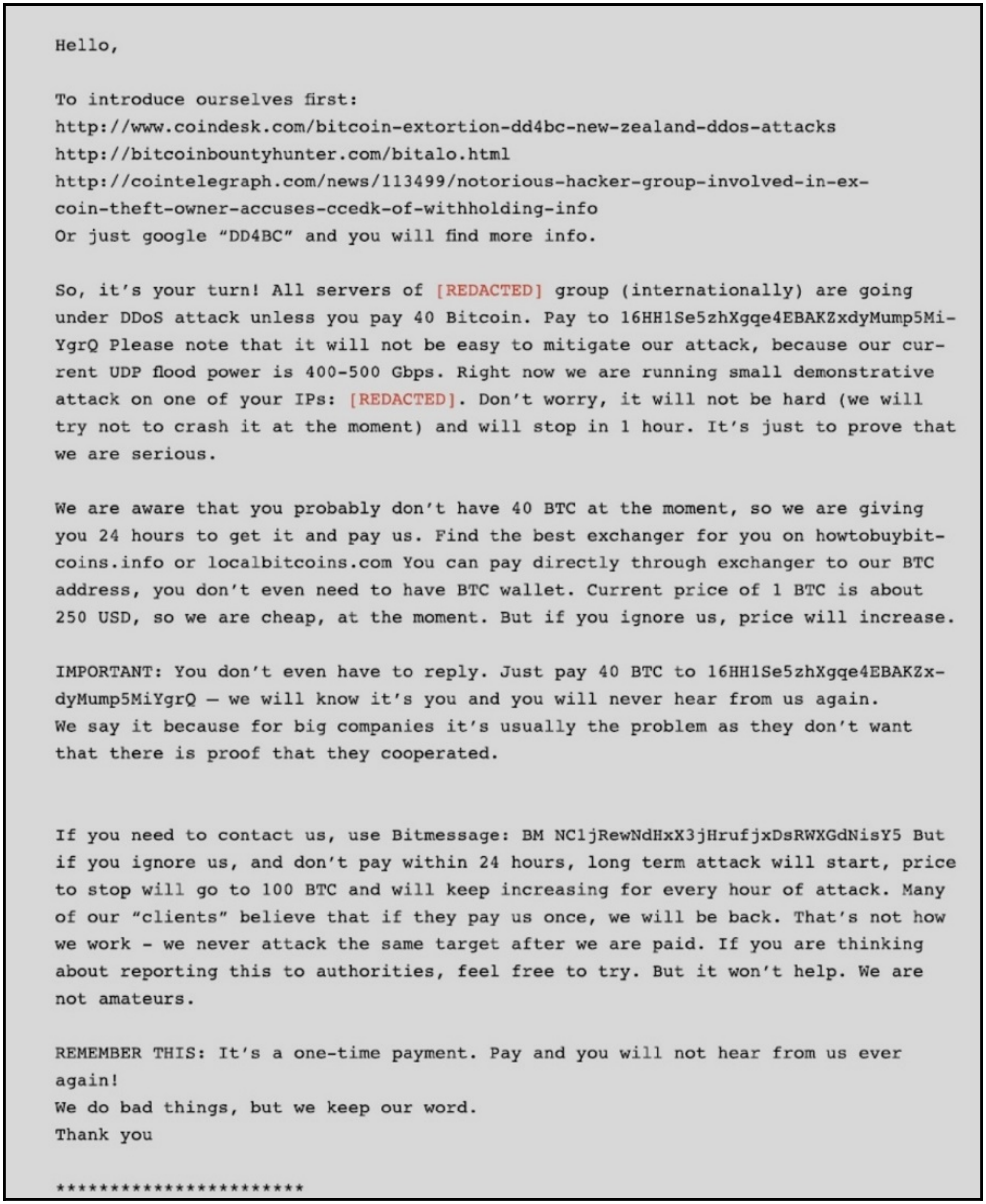
DD4BC

DDoS for Bitcoin (**DD4BC**) is another cybercriminal group that has been progressively more quite active and increasing the frequency if its DDoS extortion attempts. DD4BC initially focused on gaming and payment processing industries. Progressively they targeted multiple industries including financial institutions (banks, trading platforms, insurance, and so on) across multiple countries including US, Asia, Europe, Australia, and New Zealand.

The DD4BC extortion life cycle includes:

1. Initializing a test DDoS attack that used to range from a few minutes to a few hours to prove the competency of the group.
2. Asking ransoms via Bitcoin suggesting that they are assisting the victim by making them aware of the DDoS vulnerability.

3. More powerful attack campaigns asking for higher ransoms emphasizing DD4BC's view of "pay up now or pay more later".



Hello,

To introduce ourselves first:
http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks
http://bitcoinbountyhunter.com/bitalo.html
http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-ex-coin-theft-owner-accuses-ccedk-of-withholding-info
Or just google "DD4BC" and you will find more info.

So, it's your turn! All servers of [REDACTED] group (internationally) are going under DDoS attack unless you pay 40 Bitcoin. Pay to 16HH1Se5zhXgqe4EBAKZxdyMump5MiYgrQ Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps. Right now we are running small demonstrative attack on one of your IPs: [REDACTED]. Don't worry, it will not be hard (we will try not to crash it at the moment) and will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 40 BTC at the moment, so we are giving you 24 hours to get it and pay us. Find the best exchanger for you on howtobuybitcoins.info or localbitcoins.com You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet. Current price of 1 BTC is about 250 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don't even have to reply. Just pay 40 BTC to 16HH1Se5zhXgqe4EBAKZxdyMump5MiYgrQ – we will know it's you and you will never hear from us again.
We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated.

If you need to contact us, use Bitmessage: BM NC1jRewNdHxX3jHrufjxDsRWXGdNisY5 But if you ignore us, and don't pay within 24 hours, long term attack will start, price to stop will go to 100 BTC and will keep increasing for every hour of attack. Many of our "clients" believe that if they pay us once, we will be back. That's not how we work - we never attack the same target after we are paid. If you are thinking about reporting this to authorities, feel free to try. But it won't help. We are not amateurs.

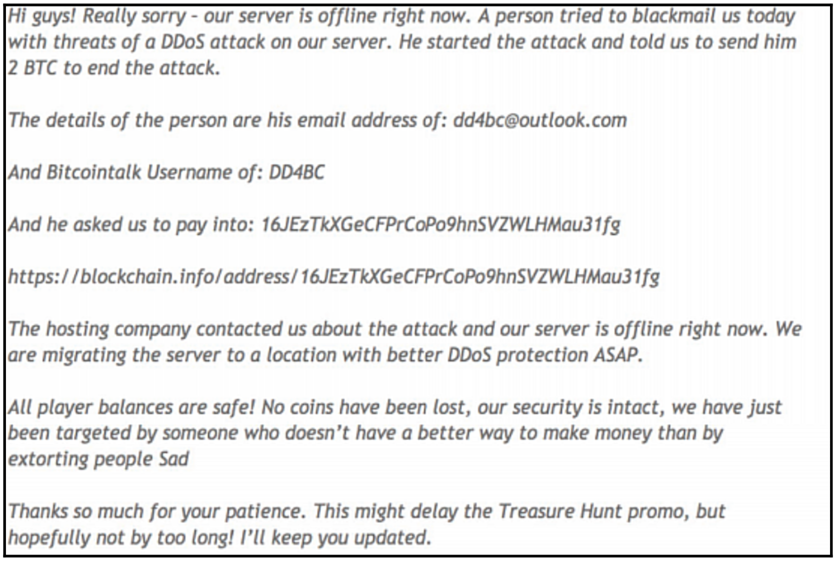
REMEMBER THIS: It's a one-time payment. Pay and you will not hear from us ever again!
We do bad things, but we keep our word.
Thank you

****

A sample e-mail sent by DD4BC

A recent study by one of the DDoS protection vendors established that most of the actual attacks have been UDP Amplification attacks - taking advantage of UDP protocols. As we discussed earlier, UDP flooding via botnet is a much flexible and easier form of attack that merely blocks the whole network by means of pushing unwanted UDP traffic. Such attack vectors are technically one of the easiest and most impactful ones - made easier with the help of rentable botnets and publicly available scripts.

As per the observed statistics for DD4BC, preliminary warning attacks generally range from 10 - 15 Gbps, which goes to as high as 40 - 60 Gbps if the victim refuses to pay the extortion demands. Although DD4BC has consistently advertised across extortion e-mails 400 - 500 Gbps of DDoS capacity, but they have never used it.



Hi guys! Really sorry - our server is offline right now. A person tried to blackmail us today with threats of a DDoS attack on our server. He started the attack and told us to send him 2 BTC to end the attack.

The details of the person are his email address of: dd4bc@outlook.com

And Bitcointalk Username of: DD4BC

And he asked us to pay into: 16JEzTkXGeCFPrCoPo9hnSVZWLHMau31fg

https://blockchain.info/address/16JEzTkXGeCFPrCoPo9hnSVZWLHMau31fg

The hosting company contacted us about the attack and our server is offline right now. We are migrating the server to a location with better DDoS protection ASAP.

All player balances are safe! No coins have been lost, our security is intact, we have just been targeted by someone who doesn't have a better way to make money than by extorting people Sad

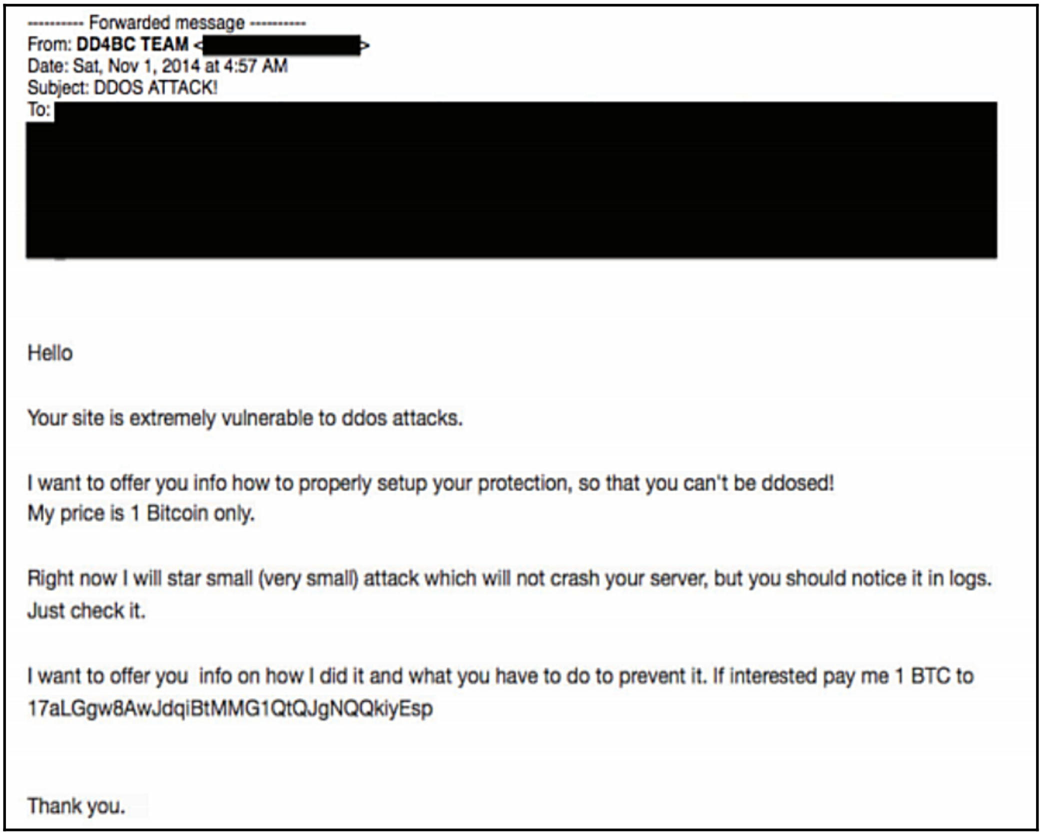
Thanks so much for your patience. This might delay the Treasure Hunt promo, but hopefully not by too long! I'll keep you updated.

A DD4BC victim posts information about the attack and ransom demand

The cybercriminals behind DD4BC have carried out more than 150 attacks out of which more than 50% of them have been directed towards financial service companies. This is fundamentally due to the *per minute impact* of service downtime in this associated industry (BFSI), then other businesses operating in healthcare, tourism, and so on.

Most of the DD4BC attacks observed have been SSDP and NTP reflection or amplification attacks, certain Layer 7 attacks have also been observed. In a limited number of cases, if the informed ransom was not paid and the test attack was mitigated by the victim, DD4BC started campaigns looking for Layer 7 attack techniques.

In some of the associated campaigns, DD4BC informed victims about the DDoS vulnerability existing in their environment and offered DDoS protection plans in exchange for Bitcoin payments.



---------- Forwarded message ----------
From: **DD4BC TEAM** <[redacted]>
Date: Sat, Nov 1, 2014 at 4:57 AM
Subject: DDOS ATTACK!
To: [redacted]

Hello

Your site is extremely vulnerable to ddos attacks.

I want to offer you info how to properly setup your protection, so that you can't be ddosed!
My price is 1 Bitcoin only.

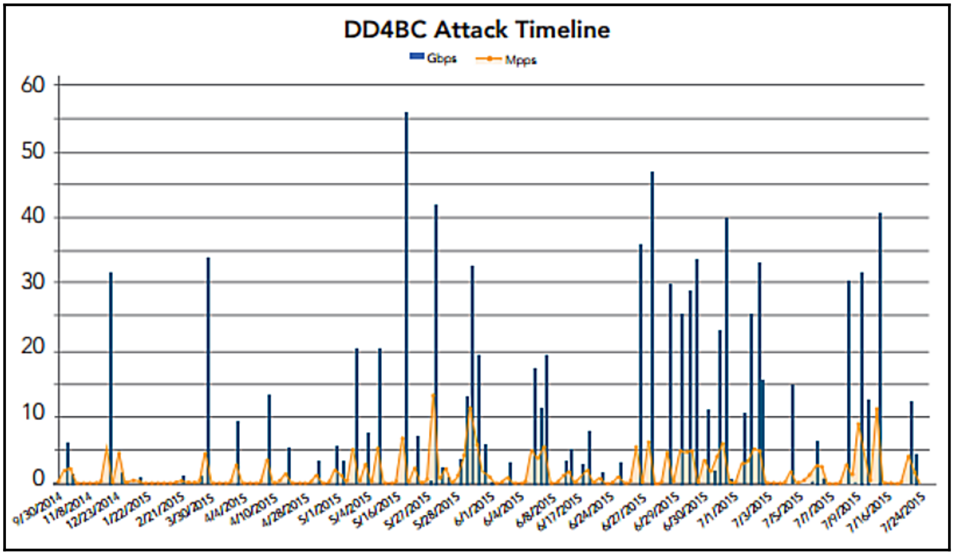
Right now I will star small (very small) attack which will not crash your server, but you should notice it in logs.
Just check it.

I want to offer you info on how I did it and what you have to do to prevent it. If interested pay me 1 BTC to
17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp

Thank you.

E-mail from DD4BC offering protection in exchange for one Bitcoin

The following timeline from `https://www.akamai.com` shows the attack bandwidth and **million packets per second** (**Mpps**) measurements for Akamai mitigated DD4BC attack campaigns from September 2014 - July 2015. The timeline graph also includes the attack dates that are related to DD4BC.



Attack timeline of bandwidth and packets per second for DD4BC events

Imposters

Some of the other imposters involved in the DDoS extortion campaigns were:

- Kadyrovtsy
- RedDoor
- ezBTC

Kadyrovtsy

Under the alias **Kadyrovtsy**, cybercriminals had started a new campaign blackmailing banks and online marketing agencies demanding a ransom of 15 Bitcoins (around £5,500, as of June 2016). The businesses generally have around four to five days to comply. As per the e-mails provided by the group, they have Bitcoin addresses uniquely linked to the victim.

As per **Link11 Security Operation Center** (**LSOC**), contrary to the behavior of most DDoS impersonators, Kadyrovtsy does not just stick to sending out extortion e-mails. These cybercriminals back the seriousness of their demands with warning attacks between 50 and 90 Gbps, which is quite enormous in nature. These demonstration attacks last up to an hour and for unprotected targets, this results in service downtime.

Kadyrovtsy mostly relies on ICMP floods and DNS reflection techniques. These DDoS extorters had been majorly operating in Europe since the end of April 2016. As per the report by Link11, their name resembles the paramilitary units that have fought under the pro-Russian Chechen President Akhmad Kadyrow.

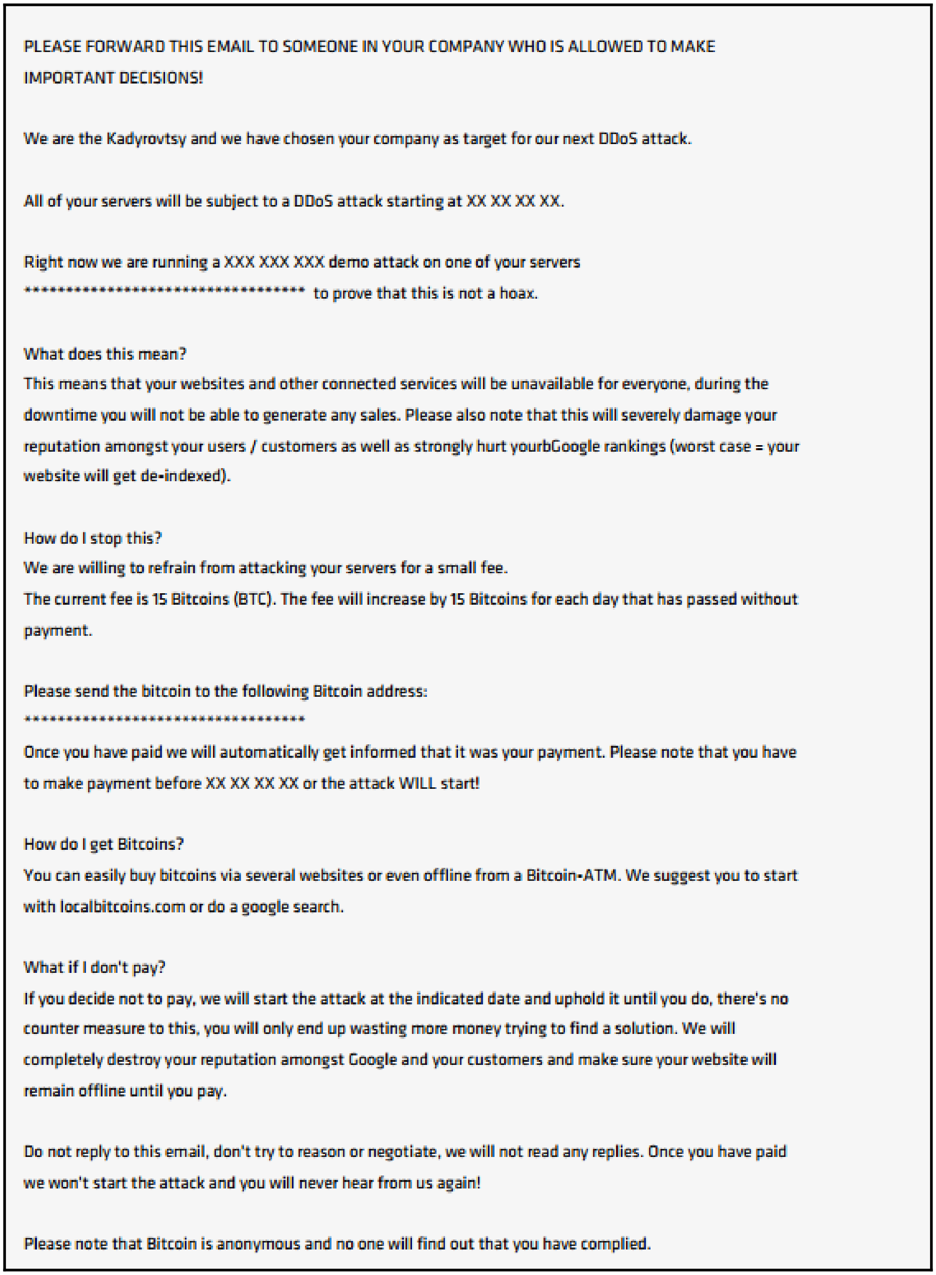
These cyber offenders have even started to expand their operations to most of the European countries since the end of April. As per BSI, the groups have already commenced blackmailing businesses across the US too.

Key extortion attempts include:

- **April 22nd 2016:** Kadyrovtsy stressed British financial businesses with a 90 Gbps volume attack. CERT UK had circulated a warning in their weekly updates about the cybercriminals.
- **May 7th / 8th 2016:** Kadyrovtsy commenced an extortion wave against the largest banks in Poland. The Pekao Bank was one of the victims. As per the reports the warning attacks had peak bandwidths between 10 and 50 Gbps.
- **May 19th 2016:** The group targeted a Dutch payment service provider who received an extortion e-mail and suffered a warning attack potentially bringing down their service.
- **Since May 26th 2016:** Since the end of May, Kadyrovtsy has been targeting businesses in Germany and as per their modus operandi backing their demands with high-volume DDoS attacks.

The LSOC observed and identified that the group had changed in their approach since the arrival of the group. The key elements that had changed with time include:

- Changes in e-mail address - even though the group is changing their e-mail addresses, they all are registered with the e-mail provider `sigiant.org` (which is well known to be used by cybercriminals). This also clarifies that the group has multiple members in their team.
- Variation in ransom - Each extortion e-mail is customized as per the country wherein the ransom amount is flip-flopped between 15 and 20 Bitcoins.
- Time to pay - The victims earlier had around four to five days to comply with the e-mail by the group. Now this timeframe has reduced to only 24 hours. If it is not paid within 24 hours the cybercriminals will initiate the attack.
- Language - With time the extortion e-mails have changed in expressions. Earlier, the e-mails were known to be quite blunt and written in terrible English. In the current ransom demands the wording, grammar, and spelling are a lot better.



PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Kadyrovtsy and we have chosen your company as target for our next DDoS attack.

All of your servers will be subject to a DDoS attack starting at XX XX XX XX.

Right now we are running a XXX XXX XXX demo attack on one of your servers
*********************************** to prove that this is not a hoax.

What does this mean?
This means that your websites and other connected services will be unavailable for everyone, during the downtime you will not be able to generate any sales. Please also note that this will severely damage your reputation amongst your users / customers as well as strongly hurt yourbGoogle rankings (worst case = your website will get de-indexed).

How do I stop this?
We are willing to refrain from attacking your servers for a small fee.
The current fee is 15 Bitcoins (BTC). The fee will increase by 15 Bitcoins for each day that has passed without payment.

Please send the bitcoin to the following Bitcoin address:
****
Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment before XX XX XX XX or the attack WILL start!

How do I get Bitcoins?
You can easily buy bitcoins via several websites or even offline from a Bitcoin-ATM. We suggest you to start with localbitcoins.com or do a google search.

What if I don't pay?
If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution. We will completely destroy your reputation amongst Google and your customers and make sure your website will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again!

Please note that Bitcoin is anonymous and no one will find out that you have complied.

One of the extortion e-mails from Kadyrovtsy

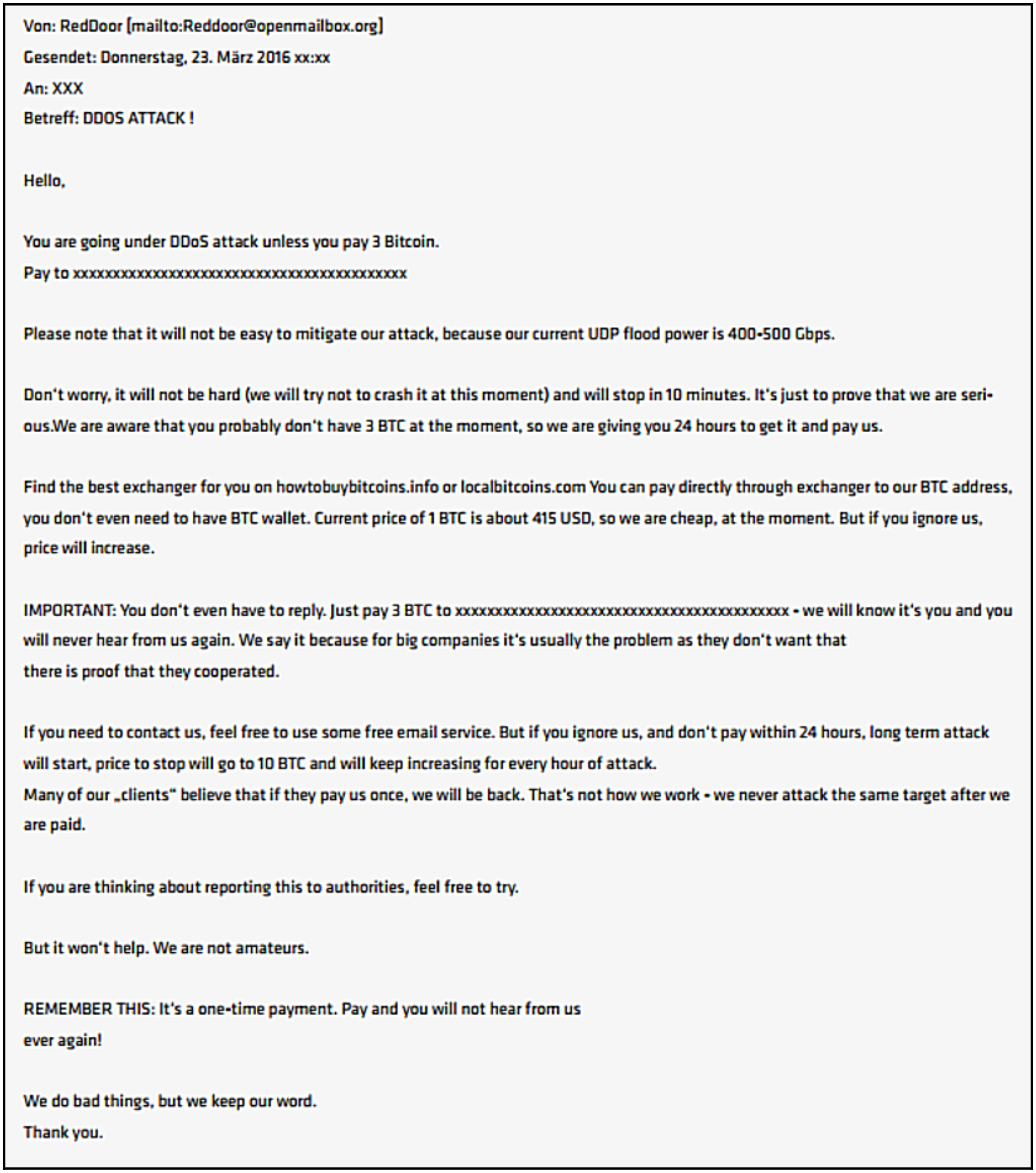
RedDoor

RedDoor is another cybercriminal group known for their extortion e-mails threatening with DDoS attacks primarily against the e-commerce industry. A new wave of DDoS extortions from this group was identified by Link11 Security Operation Center wherein they had over served the group threatening online vendors in Germany. Ever since March 23rd the LSOC is cooperating with affected e-commerce providers and the authorities to support the investigations.

This group with the alias "RedDoor" demand a ransom of three Bitcoins across all the victims they target. This group is operating with the same modus operandi of other DDoS extortionists. The cybercriminals in their DDoS extortion campaign send out e-mails using an anonymous e-mail service in which they demand the ransom. The targeted victims are provided to wire the payment onto an individual Bitcoin account within 24 hours.

RedDoor threatens with large volume DDoS attacks in case the victims decide not to comply with the e-mail. The extorters threaten to use UDP floods with a potential bandwidth of 400 to 500 Gbps. In addition, they inform the victim that the ransom would jump up to 10 Bitcoins and will rise by the hour once the attack is initialized.

The extortion e-mails are quite similar to those of DD4BC, but the style of operations resembles the work of Armada Collection. Due to such characteristics, it can be assumed that the group is an impersonator of these extortion groups. With the current focus primarily towards German e-commerce businesses, it is expected that these extortions will spread out to other industries as well.



Von: RedDoor [mailto:Reddoor@openmailbox.org]
Gesendet: Donnerstag, 23. März 2016 xx:xx
An: XXX
Betreff: DDOS ATTACK !

Hello,

You are going under DDoS attack unless you pay 3 Bitcoin.
Pay to xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps.

Don't worry, it will not be hard (we will try not to crash it at this moment) and will stop in 10 minutes. It's just to prove that we are serious.We are aware that you probably don't have 3 BTC at the moment, so we are giving you 24 hours to get it and pay us.

Find the best exchanger for you on howtobuybitcoins.info or localbitcoins.com You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet. Current price of 1 BTC is about 415 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don't even have to reply. Just pay 3 BTC to xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx - we will know it's you and you will never hear from us again. We say it because for big companies it's usually the problem as they don't want that
there is proof that they cooperated.

If you need to contact us, feel free to use some free email service. But if you ignore us, and don't pay within 24 hours, long term attack will start, price to stop will go to 10 BTC and will keep increasing for every hour of attack.
Many of our „clients“ believe that if they pay us once, we will be back. That's not how we work - we never attack the same target after we are paid.

If you are thinking about reporting this to authorities, feel free to try.

But it won't help. We are not amateurs.

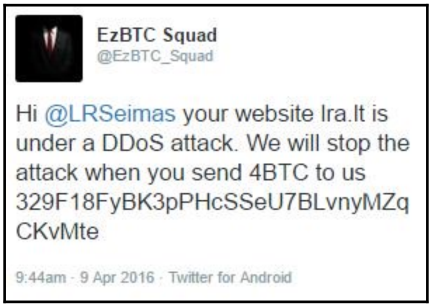
REMEMBER THIS: It's a one-time payment. Pay and you will not hear from us
ever again!

We do bad things, but we keep our word.
Thank you.

Original RedDoor extortion e-mail

ezBTC Squad

This is one of the new cybercriminal groups known for their extortion attempts threatening for DDoS attacks primarily against anyone across platforms. Recently the group ezBTC Squad attempted to run a ransom campaign using a Twitter account to deliver their ransom note. The second screenshot shows an example wherein an online crowdfunding charity portal was being targeted by a ransom campaign from the same group.

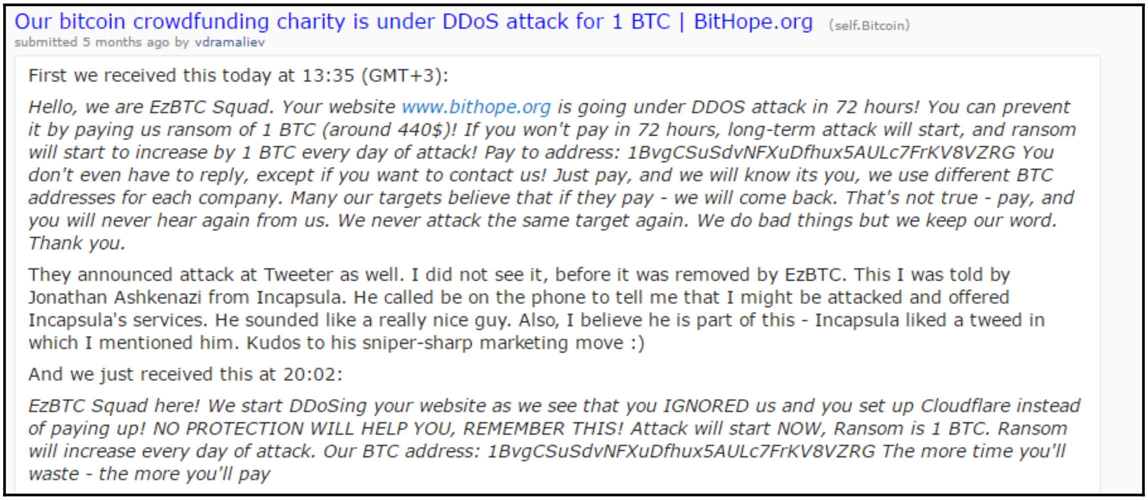


EzBTC Squad
@EzBTC_Squad

Hi @LRSeimas your website lra.lt is under a DDoS attack. We will stop the attack when you send 4BTC to us 329F18FyBK3pPHcSSeU7BLvnyMZqCKvMte

9:44am · 9 Apr 2016 · Twitter for Android

Ransom campaign using a Twitter account



Our bitcoin crowdfunding charity is under DDoS attack for 1 BTC | BitHope.org (self.Bitcoin)
submitted 5 months ago by vdramaliev

First we received this today at 13:35 (GMT+3):

Hello, we are EzBTC Squad. Your website www.bithope.org is going under DDOS attack in 72 hours! You can prevent it by paying us ransom of 1 BTC (around 440$)! If you won't pay in 72 hours, long-term attack will start, and ransom will start to increase by 1 BTC every day of attack! Pay to address: 1BvgCSuSdvNFXuDfhux5AULc7FrKV8VZRG You don't even have to reply, except if you want to contact us! Just pay, and we will know its you, we use different BTC addresses for each company. Many our targets believe that if they pay - we will come back. That's not true - pay, and you will never hear again from us. We never attack the same target again. We do bad things but we keep our word. Thank you.

They announced attack at Tweeter as well. I did not see it, before it was removed by EzBTC. This I was told by Jonathan Ashkenazi from Incapsula. He called be on the phone to tell me that I might be attacked and offered Incapsula's services. He sounded like a really nice guy. Also, I believe he is part of this - Incapsula liked a tweed in which I mentioned him. Kudos to his sniper-sharp marketing move :)

And we just received this at 20:02:

EzBTC Squad here! We start DDoSing your website as we see that you IGNORED us and you set up Cloudflare instead of paying up! NO PROTECTION WILL HELP YOU, REMEMBER THIS! Attack will start NOW, Ransom is 1 BTC. Ransom will increase every day of attack. Our BTC address: 1BvgCSuSdvNFXuDfhux5AULc7FrKV8VZRG The more time you'll waste - the more you'll pay

Online crowdfunding charity targeted by ezBTC

Defense techniques

Regardless of the types, categories, and sophistication of DDoS attacks, general protection techniques fall short, in general, ensuring mitigation and ensuring business continuity. The most well-known DDoS protection mechanisms such as blackholing and router filtering are usually not optimized and planned to mitigate complex attack patterns that are seen today.

Perimeter security devices such as NGFW and IPS/IDS even though they offer attack detection capabilities, they do not mitigate complete DDoS protection against all attack vectors. These perimeter devices do provide fundamental defense techniques such as flood protection and resource protection through a rate limiting across multiple layers that detects and prevents sessions exhaustion attacks, and so on, but they are not designed to mitigate comprehensive DDoS attack vectors across Layer 3, Layer 4, and Layer 7.

DDoS mitigation remains one of the complex areas that requires correlation across multiple factors including deep packet inspection, pattern classifying clustering techniques, and critical assets that need to be protected along with its relevant threshold. DDoS mitigation these days requires not only a novel approach that detects transforming new DDoS attack vectors, but also mitigates the effects of the attack to make sure that services run during the phase of an attack.

The most optimal protection strategy is to have a defense in depth layered protection approach that would allow filtering at various levels, corresponding to different types of attack vectors. To withstand a DDoS attack the essential constituent is to recognize the type of attack being launched and the purpose of the cybercriminal. With an adequate DDoS protection strategy, DDoS solution is able to:

- Have reliable and cost-efficient scalability
- Mitigate the attacks in real time than only detecting it
- Identify anomalies and illegitimate traffic from the good traffic, not only to just detect the attack patterns as defined in the signatures
- Include a secure architecture to deploy upstream to guard all points of vulnerability

A DDoS protection plan built on the preceding approach should deliver the following protection attributes:

- Enable immediate response on DDoS attacks across all the layers (Layer 3, Layer 4, and Layer 7) through integrated detection and blocking mechanisms
- Provides enhanced verification capabilities than what is currently provided by existing security solutions (signature based)

- Should focus on classifying the attacks based on behavior analysis so to recognize traffic with malicious intent
- Mechanisms to handle high volumetric attacks and potential to block spoofed packets against valid business transactions
- Provision of enabling on demand positioning of DDoS solution (as per the business decision)
- The solution with intelligent processes having the capacity to cleanse malicious traffic ensuring maximum reliability

According to *Bhattacharyya, Dhruba,* and *Jugal Kalita. "DDoS Prevention", DDoS Attacks, 2016*, an effective traceback mechanism should have the following properties:

- The involvement of ISPs should be low
- It should not incur any additional memory cost in routers or switches
- The false positive rate of detection should be low
- The deployment of the traceback system should not be a challenge
- It should be able to identify the original source of attack with the help of a single packet

Tools to protect against DDoS attacks

Different companies in the market offer services to defend against DDoS attacks. Some of them approach the DDoS mitigation by setting up appliances in the client's infrastructure while others use capabilities within ISP providers and other channel traffic through dedication traffic scrubbing or cleaning centers. Nevertheless, all the previous approaches follow the same principle, that is, filtering out the malicious traffic created by cybercriminals.

Some of the implementation approaches also need to be considered, as a few of them provide DDoS protection services that are always on and some of them enable it on demand. For considering potential DDoS defenses, the **time to live** (**TTL**) on the enterprises DNS is also very important. If the company has a long TTL value on their DNS, they will not be able to switch DNS records rapidly to a new secure location in the case of an attack. It is an important factor to be considered while preparing for the DDoS defenses.

The least effective method from an overall DDoS mitigation perspective is the approach wherein traffic filtering equipment is installed on the client side.

One of the things to notice is that there is no silver bullet for protection against DDoS attacks. While choosing a vendor for DDoS solutions there are multiple parameters that should be reviewed, which includes but is not restricted to - scalability of the solution, economically viable for an organization, dependency on existing services within the environment, manual efforts for solution servicing, coverage against attacks Layer 3, 4, and 7, provisioning clean traffic, protection against encrypted and non-HTTP based traffic, use cases that would be covered as per the industry, and so on.

The following are the top DDoS protection solutions providing defense across all the layers:

- **Imperva Incapsula** - It is a cloud-based service that protects web portals, applications, infrastructure, and data from DDoS attacks including performance improvements via **Content Delivery Network** (**CDN**). Their solution suite consists of **Web Application Firewall** (**WAF**), a CDN, DDoS mitigation, and load balancers. It has data centers globally and has scrubbing centers more than any other DDoS protection providers. It also offers a comprehensive protection against DDoS with multiple service models including always on and on demand DDoS protection.
- **Akamai** - Akamai Technologies is known for having one of the largest CDNs operating globally. They provide cloud-based services for web optimization and media delivery and security solutions. Akamai (Prolexic) is one of the most well-known DDoS protection service providers having multiple service models for all sizes of business.
- **Arbor Networks** - They are the security division of Netscout providing cloud and on premise DDoS protection suite of services across all industries. Large service providers majorly opt for their solution and DDoS protection services (across Layer 3, Layer 4, and Layer 7) that work on the basis of signaling. Their service models include on demand traffic scrubbing services along with 24/7 DDoS protection support.
- **Cloudflare** - Cloudflare is a cloud-based easily deployable solution. Of late, the solution is very aggressive in the market and has a lot of potential. It is an easily deployable solution focused only on protection against HTTP and HTTPS-based traffic, that is, it can prevent Layer 3, Layer 4, and Layer 7 attacks for web traffic only. The solution doesn't have full coverage against the infrastructure and non HTTP based DDoS Threats (across Layer 3, 4).

- **F5 Networks** - F5 Networks Silverline provides multiple DDoS protection service offerings on premise, in the cloud, and even hybrid solutions. Silverline provides protection against volumetric and application level attacks across Layer 3, Layer 4, and Layer 7.

On-site mitigation techniques are the most important factors to assist a DDoS protection in combination with other solutions discussed previously. This includes a large variety of potential capabilities built within the organization in terms of security design and architecture, harmonization of security tools, and homogeneous configurations across security devices. The main idea being that the organization is ready across all layers and has a security equation practice in nature.

Mitigation techniques

Based upon the characteristics of the DDoS attack there are multiple techniques available for organizations of all sizes, besides specific DDoS protection tools. Based on the type of DDoS attacks, the following section will describe precise mitigation techniques.

For bandwidth exhaustion attacks

- **Scalability:** The enterprise architecture should focus on a scalable infrastructure and should have appropriate use cases defined to provision required bandwidth to the target business services while potential DDoS triggers are identified, checked, and mitigated in the case of an actual attack. This strategy has two positives - first it decreases the risk of service failure and secondly it gives additional time for DDoS mitigation to come into play.

- **Black hole routing**: With DDoS detection techniques, once an attack is identified the malicious traffic can be directed to be dropped and discarded. It is beneficial when the DDoS participants are small.

- **Distributed hosting**: Distributing business services is crucial for any organization since it provides a comfort that even during the phase of an attack the critical services would be up and running from multiple locations. On the other hand, it is relatively difficult for cybercriminals to target all the business services distributed across various locations simultaneously.

For resource exhaustion

- **Patch Management**: It is vital that all accessible services within any systems are patched and updated with the latest vendor software's. All the systems should be hardened and configured with only necessary services required or approved by the business, that is, all the unnecessary services should be disabled or removed.

- **Rate and Connection limiting**: Rate limiting should be applied to inbound traffic and such configurations can be configured on perimeter security devices such as **Firewalls / Next Generation Firewalls** (**NGFW**), Intrusion Detection, and Prevention systems.

- **Connection aging**: Perimeter nodes should be configured to close idle connections. This would preserve the connection table against consuming resources unnecessarily and would lead to making resources available for new connections.

- **Load balancing**: Load balancing segregates the traffic across distributed environments and supports business service to strive even in the phase of an attack.

For application-based attacks

- **Application security controls**: A combination of software development security controls can help mitigate vulnerabilities that could further cause DDoS attack campaigns:
- **Secure application development**: Secure Software Development Life cycle prevents developers from releasing vulnerable software that could be exploited by cybercriminals. Periodic vulnerability and penetration testing exercises should be conducted to identify gaps across applications and services exposed to the Internet.
    - Custom use cases should be enabled for identifying the breach of security events. Based on the thresholds identified for an application, alerts should be configured and excessive requests should be handled.
    - The inclusion of CAPTCHA's for business approved events within the portal can help slow down application attacks.
    - Logging and monitoring security events for unique business logics as per the service offering could prevent multiple attacks.

- **Traffic Filtering**: Perimeter security devices such as IDS/IPS/WAF are useful to prevent malicious traffic from propagating. These technologies could also help in multiple areas such as filtering unwanted attack traffic and reducing inbound requests to the application (as per the architecture).

Leading practices for enterprises

- **Be prepared** - All enterprises should have an incident response plan in which DDoS attack scenarios should be included as per the threat landscape of the organization. As per the plan mitigation strategies should be defined and DDoS protection across all the layers should be evaluated.
- **Design for failure** - Design your network and application architecture with scalability and flexibility. It should be designed for failure. it should be ready to withstand any types of attacks and minimize business impact. Bottlenecks within the environment should be identified and compensating controls should exist across the network.
- **Security monitoring** - Continuous monitoring of the network should be in place and abnormal network patterns should be investigated. Netflow analysis can be a good way to detect attacks.
- **Traffic filtering** - Perimeter devices and services such as firewalls, IPS, and blackhole routing can drop some of the unwanted traffic. For protection against Layer 7 application-based attacks WAF can be a good line of defense. It can be customized as per the application behavior for best results. Unnecessary ports and unused services should be disabled.
- **Server configuration** - Regular patch management and hardening of the devices should be conducted. Especially critical servers exposed should be hardened and configured securely as per the leading practices and guidelines.
- **Not being at the mercy of Content Delivery Network (CDN) provider** - CDN providers are usually not designed to protect assets from DDoS attacks. cybercriminals can easily bypass the caching provided by the CDNs and can directly send requests to the backend servers. To avoid such cases, it is recommended to partner with the DDoS protection service furthermore to the onsite mitigation technique.

Future trends

According to *Bhattacharyya, Dhruba,* and *Jugal Kalita. "DDoS, Machine Learning, Measures", DDoS Attacks, 2016*, a major reason for networks or organizations frequently coming under DDoS attacks is due to the easy availability of a large number of attack tools in the public domain that can easily be set up and used to launch attacks. Unwanted traffic is sent to the victim from a number of bots or compromised computers on the Internet. The evolution of DDoS threats from basic Layer 3/4 protocol based attacks to sophisticated Layer 7 attacks is as devastating as ever. Attackers are also improving their skills to launch attacks at different scales and levels to keep themselves always one step ahead to evade detection mechanisms in parallel with the continuous efforts made by defenders.

These days, we have already seen the intensity of DDoS attacks generating a volume of more than 400 Gbps. The attacks are getting flexible and are easy to launch without ample knowledge of the attacks or vulnerabilities. Multi stage attacks are also getting mainstream wherein multiple attacks combine with sophisticated Layer 7 attack vectors targeting to take services down. Even if the duration of the attack is in minutes, it is potentially enough to cause much damage to the organization and its services.

With new evolutions, such as Internet of Everything or IoT, DDoS attacks are expected to transform using the capabilities of devices and sensors that are connected to the Internet. Already malware such as LuaBot has been executed in wild targeting Linux platforms transcending multiple attack vectors. We will see more of such cases and our protection techniques evolving with time.

The key motivating factor for conducting such attacks is the desire to gain profit through extortion, which we will see transcending in 2017. Most of the industries who will be targeted for DDoS attacks and extortions will be those who are driving towards getting their business digital or who heavily rely on online presence. These primarily include, online retails, healthcare, **Banking, Financial services and Insurance** (**BFSI**), and media.

DDoS protection techniques will remain to transform as per the growing threat landscape by plugging in advanced machine learning mechanisms to identify and mitigate the attacks. With such DDoS protection tools at our disposal, the overall DDoS protection frameworks and strategies will be more efficient and effective.

Thus enterprises that are continuing to rely on existing protection solutions - or worse, no solution at all - should reassess their position in light of these pervasive threats.

Summary

In this chapter, we provided an extensive insight towards DDoS extortion and its types followed by detailed discussions on current trends in DDoS attack types, detection, prevention, mitigation, and tolerance.

In the next chapter, we will focus on data breaches and data theft extortions especially business e-mail scams, which account to cyber intrusion methods to conduct unauthorized transfers of funds involving multiple nations.

3
Avoiding Data Theft Extortion

In this chapter, we will have a look at data theft, which are attacks where attackers take sensitive data as hostage and extort the users and the corporation. The sensitive data can also include hijacked accounts that are held ransom. We will also learn about a third variant of Business E-mail Compromise (BEC), which is a sophisticated e-mail scam that targets businesses working with foreign partners that regularly perform wire transfer payments. In the strictest sense BEC is not digital extortion as most of the extraction in BEC is money, but there are cases where the executives' data was held as ransom.

This is a mid-level topic, but practical examples will make it easy to understand.

Specifically, we will cover the following topics in this chapter:

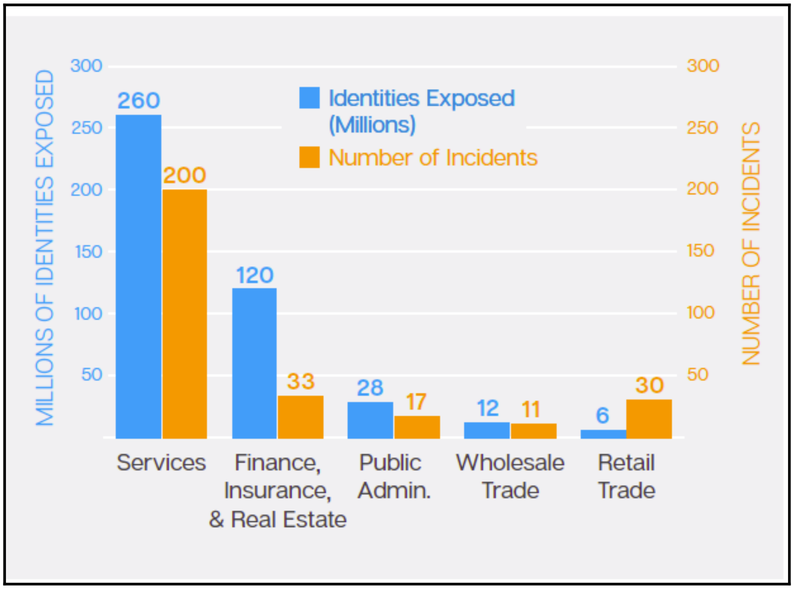
- Data theft
- Account theft
- How to defend against account theft extortion
- Business E-mail Compromise (BEC)
- How do BEC schemes work
- How to defend against BEC

Data theft

News and reports of data breaches and data theft extortions affecting financial institutions, governments, retailers, universities, hospitals, and other entities dominate the bulletins with increasing frequency. This is simply the tip of the iceberg, with the vast majority of incidents remaining unreported and undisclosed. To better understand these breaches, it is significant to have an understanding of the term "Data breach". International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27040 defines a data breach as:

> *"Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed."*

Data theft extortion is another type of cyber extortion wherein a cyber criminal steals or claims to have stolen sensitive data from an organization and then demands a ransom for its safe return.



High level sectors breached by number of identities exposed and incidents as per trend micro analysis

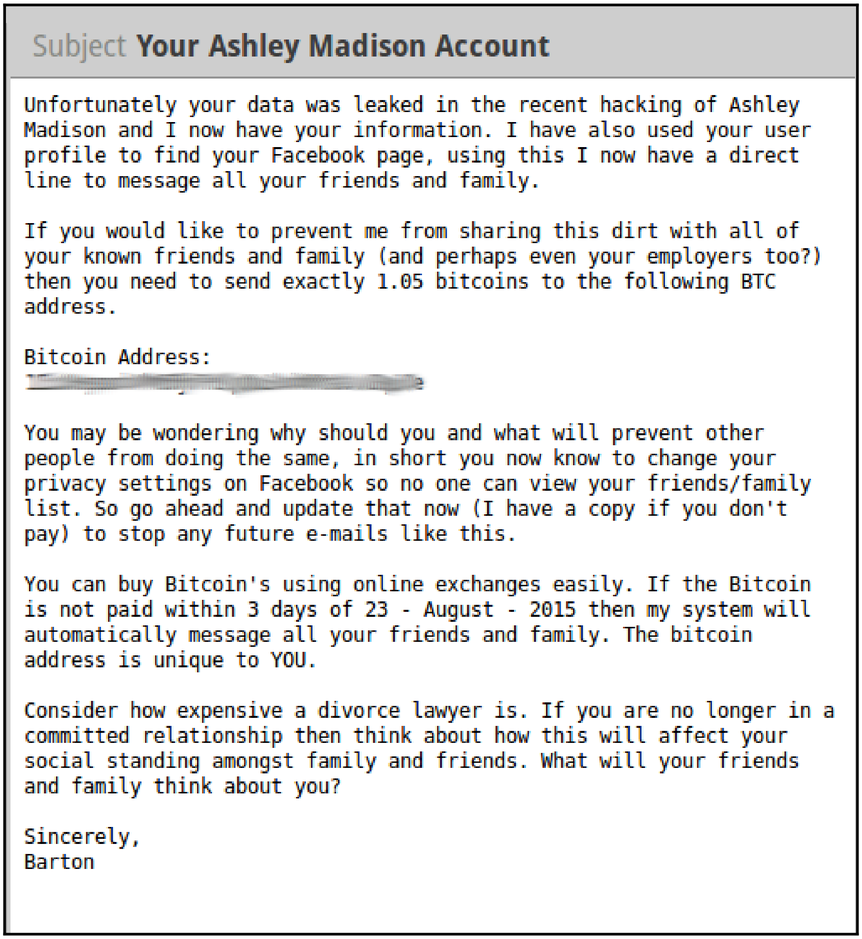
A wide range of confidential and sensitive data is compromised and extorted across all industries from businesses, both big and small, as well as individuals. These data types include Personally identifiable information (PII), financial, health, education, payment card data, log-in credentials, intellectual property, and others. In the news bulletin, data breaches are more or less always attributed to hacking or malware attacks. While these do play a big role, they do not account for all incidents.

Perpetrators and cyber criminals who compromise the confidential and sensitive data refer to a diverse group, which includes insiders, individual criminals, as well as organized and state-sponsored groups. Stolen data is frequently used to commit crimes such as financial fraud, theft, revenge, identity and intellectual property, blackmail, espionage, and extortion.

Data breaches and extortions have turned out to be a part of the daily news. Several prominent data breach incidents have been publicly disclosed and extorted. They did attract a lot of media attention and prompted individuals and organizations of all sizes to ask, "How secure is our data?" The key incidents that recently made headlines include:

- Hacktivist group, Anonymous, hacked into US Census Bureau computers and leaked employee data.
- Hacking team-the creators of surveillance software-was hacked and 400+GB worth of data was leaked.
- 21.5 million Americans had their social security numbers and other sensitive data stolen in the "second" breach of the OPM's background check database.
- Hackers stole detailed information on 104,000 taxpayers from the Internal Revenue Service (IRS) website by exploiting an online tool.
- Hackers broke into the massive University of California, Los Angeles (UCLA) hospital network to access computers that stored the sensitive records of 4.5 million people.

- Ashley Madison-an online dating service that exclusively caters to extramarital affairs-was hacked, resulting in the theft of 37 million site members' records. The hack was also used for extortion.



Subject **Your Ashley Madison Account**

Unfortunately your data was leaked in the recent hacking of Ashley Madison and I now have your information. I have also used your user profile to find your Facebook page, using this I now have a direct line to message all your friends and family.

If you would like to prevent me from sharing this dirt with all of your known friends and family (and perhaps even your employers too?) then you need to send exactly 1.05 bitcoins to the following BTC address.

Bitcoin Address:
[redacted]

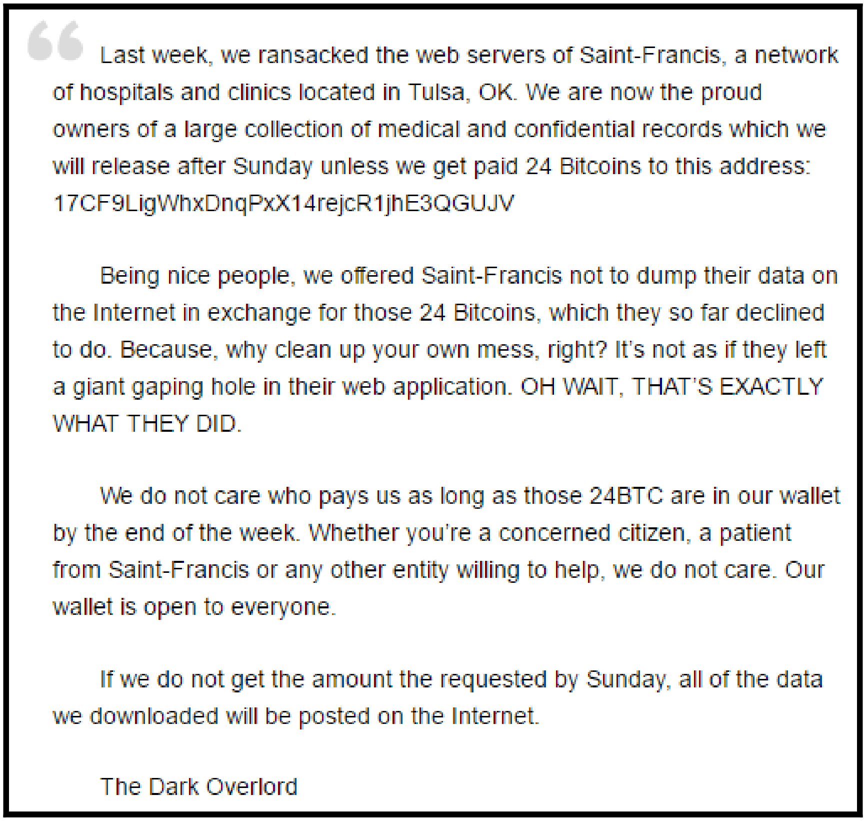
You may be wondering why should you and what will prevent other people from doing the same, in short you now know to change your privacy settings on Facebook so no one can view your friends/family list. So go ahead and update that now (I have a copy if you don't pay) to stop any future e-mails like this.

You can buy Bitcoin's using online exchanges easily. If the Bitcoin is not paid within 3 days of 23 - August - 2015 then my system will automatically message all your friends and family. The bitcoin address is unique to YOU.

Consider how expensive a divorce lawyer is. If you are no longer in a committed relationship then think about how this will affect your social standing amongst family and friends. What will your friends and family think about you?

Sincerely,
Barton

- Walmart Canada, CVS, Costco, and Sam's Club's online photo service sites were compromised via a third-party vendor.



Last week, we ransacked the web servers of Saint-Francis, a network of hospitals and clinics located in Tulsa, OK. We are now the proud owners of a large collection of medical and confidential records which we will release after Sunday unless we get paid 24 Bitcoins to this address: 17CF9LigWhxDnqPxX14rejcR1jhE3QGUJV

Being nice people, we offered Saint-Francis not to dump their data on the Internet in exchange for those 24 Bitcoins, which they so far declined to do. Because, why clean up your own mess, right? It's not as if they left a giant gaping hole in their web application. OH WAIT, THAT'S EXACTLY WHAT THEY DID.

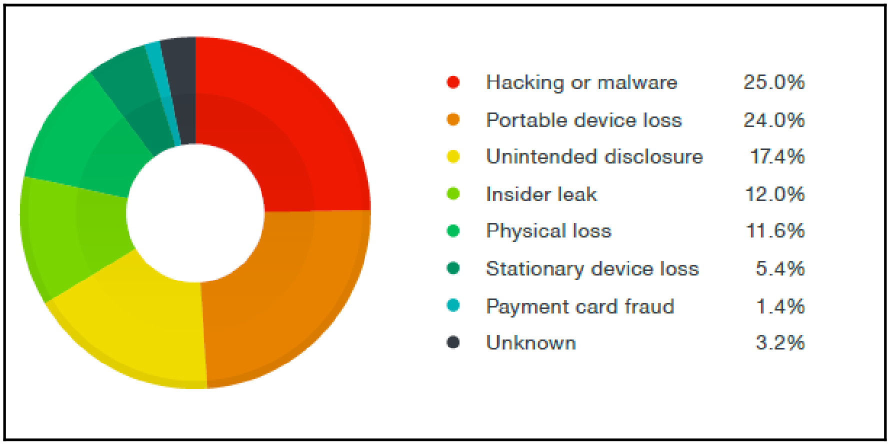
We do not care who pays us as long as those 24BTC are in our wallet by the end of the week. Whether you're a concerned citizen, a patient from Saint-Francis or any other entity willing to help, we do not care. Our wallet is open to everyone.

If we do not get the amount the requested by Sunday, all of the data we downloaded will be posted on the Internet.

The Dark Overlord

"TheDarkOverlord" group posted several stolen healthcare databases for sale when their extortion attempt was not entertained.

The number of data breach disclosures extortions also connecting big retailers is increasing, which can only signify that small and medium businesses or organizations are also being persistently targeted even if they are not making headlines. Nonetheless, the damage done to everyday individuals, irrespective of whether their sensitive data was stolen from a large corporation or a small corner store, is still the same - they face serious risks of identity, financial, and other types of fraud. The biggest denominator of having data extortion is having a data breach.



Breach method observed across industries as per Trend Micro analysis

Even though data breaches are more or less always attributed to hacking or malware attacks, there are also other methods that need to be emphasized on. While certainly, these attacks do play a big role, they only account for a quarter of all of the reported incidents. Other commonly observed breaches means include:

- Insider leak: Wherein a trusted individual or person of authority with appropriate privileges steals data
- Payment card fraud: Payment card data that is stolen using physical skimming devices
- Loss or theft: Physical theft of portable drives, laptops, office computers, files, and other physical properties that contain confidential and sensitive information
- Unintended disclosure: Methods wherein through mistakes or negligence, sensitive data is exposed
- Unknown: For a certain small number of cases, the actual breach method is unknown or undisclosed

In reality, any business or organization that processes and/or stores confidential and sensitive data are a potential breach target. As long as the confidential and sensitive data can be monetized through fraud and other crimes, data breaches are going to happen and with increasing frequency in the future. From a business or an organization's point of view, data breaches are unavoidable and unpredictable. No defense is impregnable against determined adversaries. Having an effective alert, containment, and mitigation processes are critical.

Mobile computing platforms such as phones, tablets, wearables, and other devices as well as the apps that run on them are fast becoming primary computing platforms worldwide. App development is constantly being made simpler. Buying, selling, and marketing apps have been made easier through established online marketplaces. Apps support revenue models that are profitable for developers. The entire ecosystem has been designed to remove market entry barriers and encourage the development of new and innovative apps. All these contribute to the explosion of apps catering to every activity imaginable. Everyday users aren't aware that sensitive data is collected, processed, stored, and transmitted through apps and not necessarily in a secure manner. In the next couple of years, apps and mobile computing devices are bound to become major data breach targets.

It is crucial to build public awareness of the risks and repercussions of sensitive data getting compromised. Heightened awareness will lead to increased caution and the pressure will mount on governments and businesses or organizations to come up with effective and permanent solutions.

Because the data breaches have become a daily affair, individuals may have also become desensitized to having their personal, financial, health, education, and other data compromised and sold in criminal marketplaces. This desensitization could be the product of several factors:

- There is an overload of day-to-day news articles on data breaches
- Stolen personal and sensitive data are not as tangible as, for example, a stolen mobile phone
- The immoral and high consequences of having personal and sensitive data stolen are not instantly felt
- There is a lack of understanding of the repercussions of personal and organization sensitive data theft

News bulletins are quick to report on data breaches, but they rarely follow up on what happened to the stolen data. Tracing the movement of stolen data can be difficult since:

- The data may surface after weeks or months or not at all in Deep Web marketplaces.

- When the corresponding data is traded, it's not openly advertised as belonging to a particular breach, business, or organization. This helps criminals avoid drawing unwanted attention and scrutiny.
- Breach victims won't release information and facts that would make the stolen data easy to identify.
- Millions of records are available 24*7 for purchase in Deep Web market places and stolen data may be hiding in plain sight.
- Access to the stolen data usually requires purchasing it and that is expensive and a potential criminal offense.

The enterprise view

Data breaches are in general complex events. Any business or organization that processes and/or stores confidential and sensitive data is a potential breach target. As per the global analysis by Trend Micro, even if enterprises have an incident response plan to tackle data breaches, figuring out the extent of damage done and handling the response can still be a challenging task. After a breach is identified or discovered, the primary questions that typically need to be answered include:

- What data or records were stolen?
- How long has the breach been going on?
- How did the attacker's bypass defenses?
- How deep did the attackers penetrate the network?

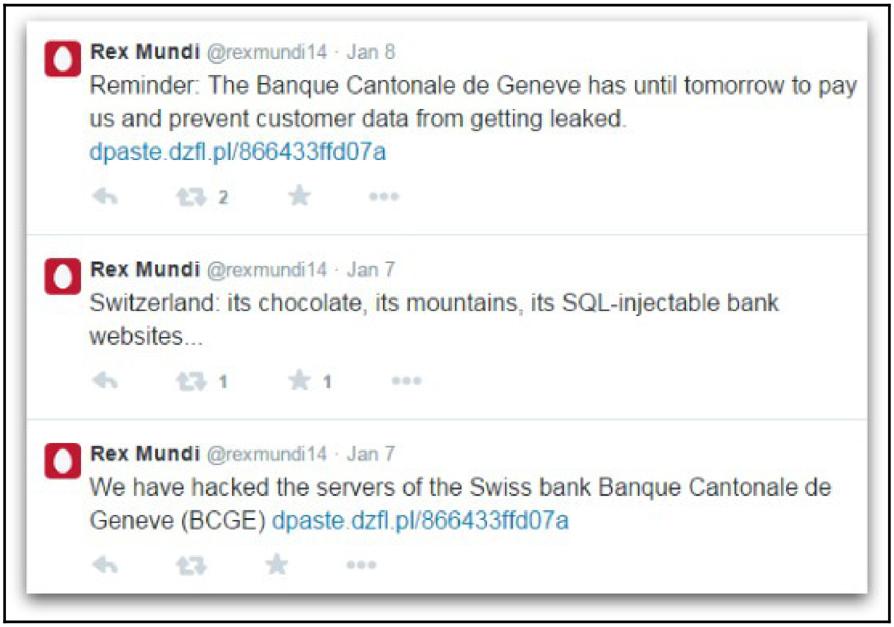
These are certainly difficult questions to answer. Incidents need to be quickly measured and evaluated as time is critical when combating active breaches.

It is near impossible to predict if, why, when, where, and how an organization will be targeted or get breached. Breach approaches and the data targeted vary widely across industries and even businesses or organizations within the same industry. Data breaches are typically planned and calculated well out, though accidental data breaches also occur. Some data breaches are discovered within a matter of hours or days, while others take months or years to get exposed. In a majority of the data breach incidents, the stolen personal and organization sensitive data is used for criminal purposes, while in a few cases, the breaches were unintentional.

Whether it is an insider attack, or criminal fraud focused on websites and point-of-sale (POS) devices, data breaches continues, costing victims more than ever. The number of mega breaches climbed to the highest level since 2013. Even though the number of breaches where the full extent of a breach was not revealed, increased; fewer companies declined to publish the numbers, unless required to do so by law.

Extortion e-mail schemes tied to data theft

As per the reports from the Internet Crime Complaint Center (IC3) they continue to receive reports from the targeted people who have acknowledged receiving extortion attempts through e-mail. The recipients have largely told that their personal information, such as their name, address, phone number, credit card details, and other crucial personal details, will be released in the wild if a ransom is not paid. The recipient is generally instructed to pay in Bitcoin, which is a virtual currency that provides a high degree of anonymity to the transactions. The recipients are usually given a crisp deadline.



Rex Mundi @rexmundi14 · Jan 8
Reminder: The Banque Cantonale de Geneve has until tomorrow to pay us and prevent customer data from getting leaked. dpaste.dzfl.pl/866433ffd07a

2

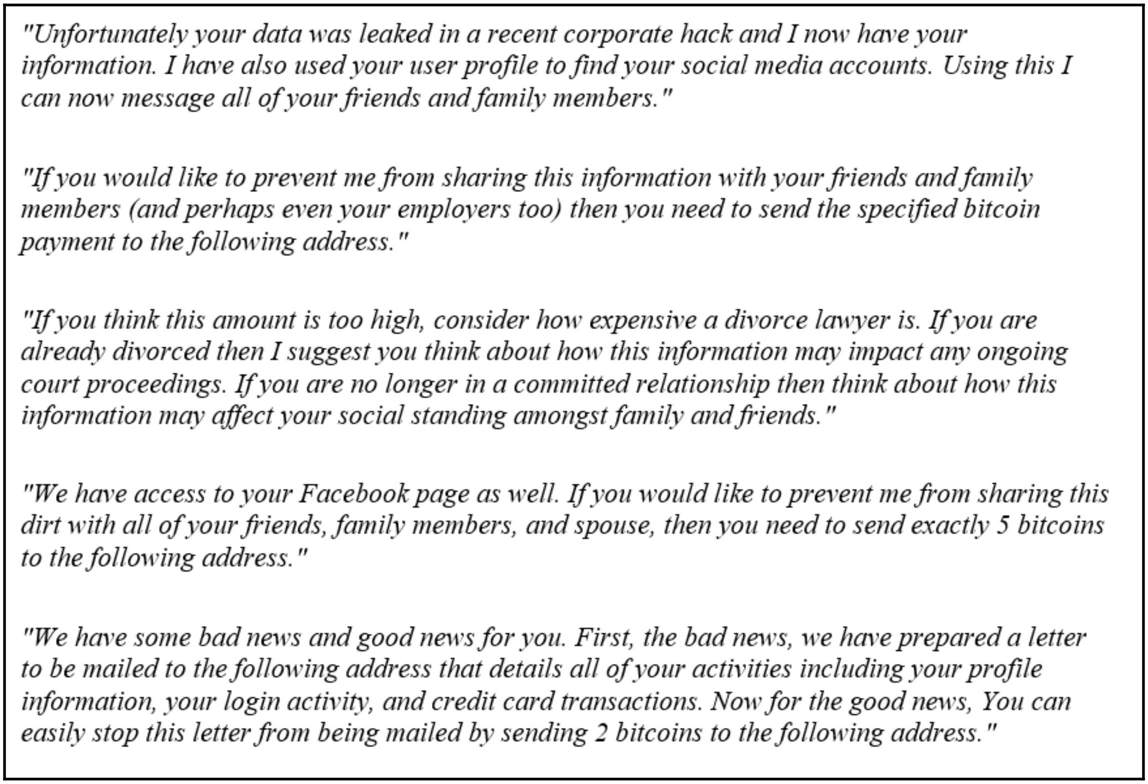
Rex Mundi @rexmundi14 · Jan 7
Switzerland: its chocolate, its mountains, its SQL-injectable bank websites...

1 1

Rex Mundi @rexmundi14 · Jan 7
We have hacked the servers of the Swiss bank Banque Cantonale de Geneve (BCGE) dpaste.dzfl.pl/866433ffd07a

Sample extortion message targeting a Swiss bank

The ransom sum varies from 2 to 5 Bitcoins or approximately US $729 to $3647.



"Unfortunately your data was leaked in a recent corporate hack and I now have your information. I have also used your user profile to find your social media accounts. Using this I can now message all of your friends and family members."

"If you would like to prevent me from sharing this information with your friends and family members (and perhaps even your employers too) then you need to send the specified bitcoin payment to the following address."

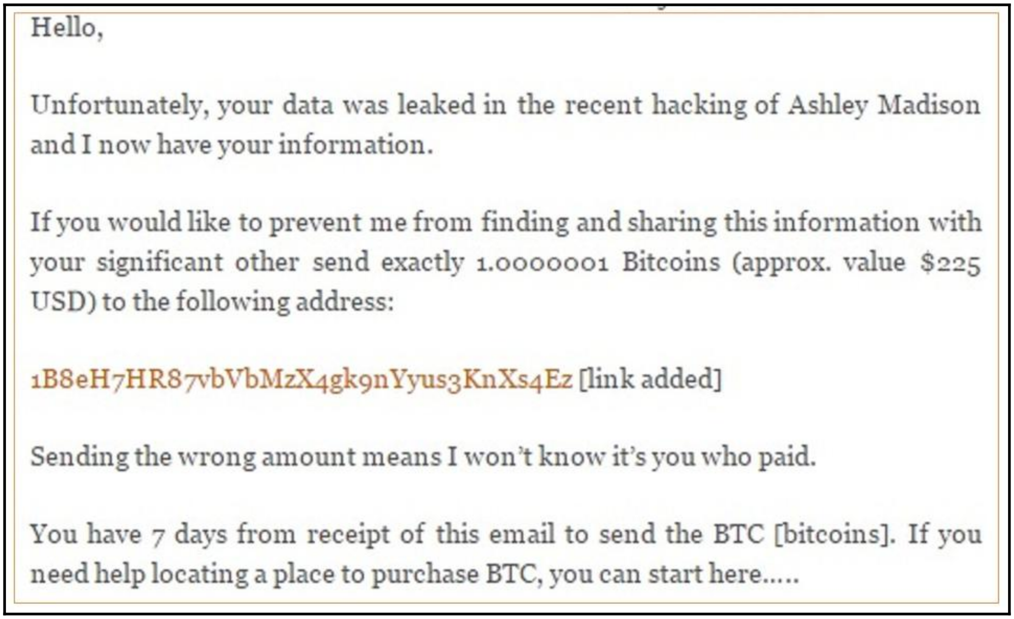
"If you think this amount is too high, consider how expensive a divorce lawyer is. If you are already divorced then I suggest you think about how this information may impact any ongoing court proceedings. If you are no longer in a committed relationship then think about how this information may affect your social standing amongst family and friends."

"We have access to your Facebook page as well. If you would like to prevent me from sharing this dirt with all of your friends, family members, and spouse, then you need to send exactly 5 bitcoins to the following address."

"We have some bad news and good news for you. First, the bad news, we have prepared a letter to be mailed to the following address that details all of your activities including your profile information, your login activity, and credit card transactions. Now for the good news, You can easily stop this letter from being mailed by sending 2 bitcoins to the following address."

Samples of extortion e-mails

Fraudsters and cyber criminals also quickly use the news release of a high profile data breach to initiate an extortion campaign. The federal agencies do believe multiple individuals are involved in these extortion campaigns based on variations in the extortion e-mails globally.



Hello,

Unfortunately, your data was leaked in the recent hacking of Ashley Madison and I now have your information.

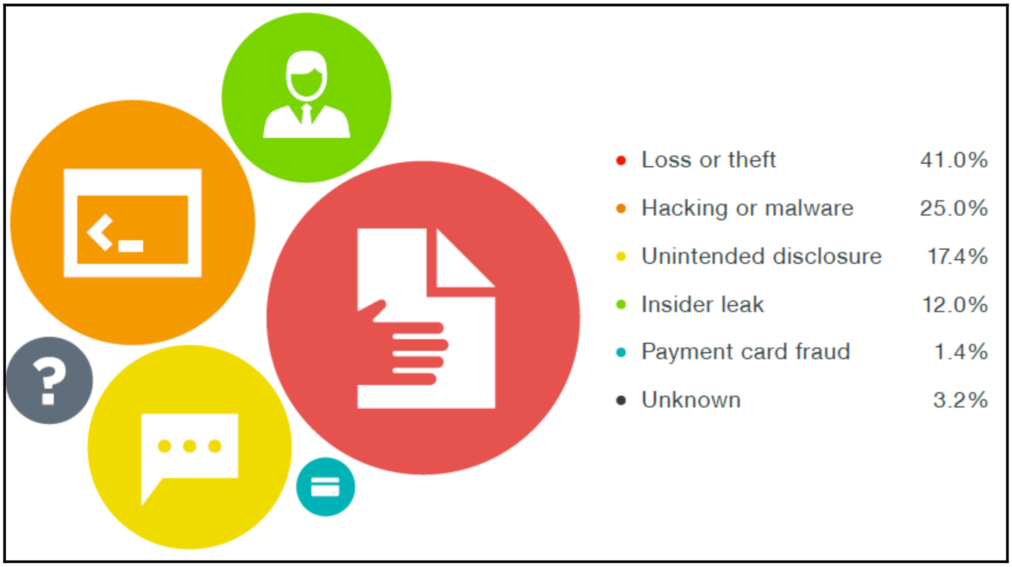
If you would like to prevent me from finding and sharing this information with your significant other send exactly 1.0000001 Bitcoins (approx. value $225 USD) to the following address:

1B8eH7HR87vbVbMzX4gk9nYyus3KnXs4Ez [link added]

Sending the wrong amount means I won't know it's you who paid.

You have 7 days from receipt of this email to send the BTC [bitcoins]. If you need help locating a place to purchase BTC, you can start here.....

Cyber criminals harvesting on the data leaked in the Ashley Madison case



Probability of using different breach methods

Method of breach

Device loss or theft is the likeliest breach method. As per the research and analysis from Trend Micro, the possibility of different data breach methods being used (note that breach methods are mutually exclusive). The top way to which sensitive data was compromised was through loss or theft. This included the loss or theft of portable devices (USB keys, backup drives, laptops, and so on), physical records (files, receipts, bills, and so on), and stationary devices (office computers, specialized equipment, and so on).

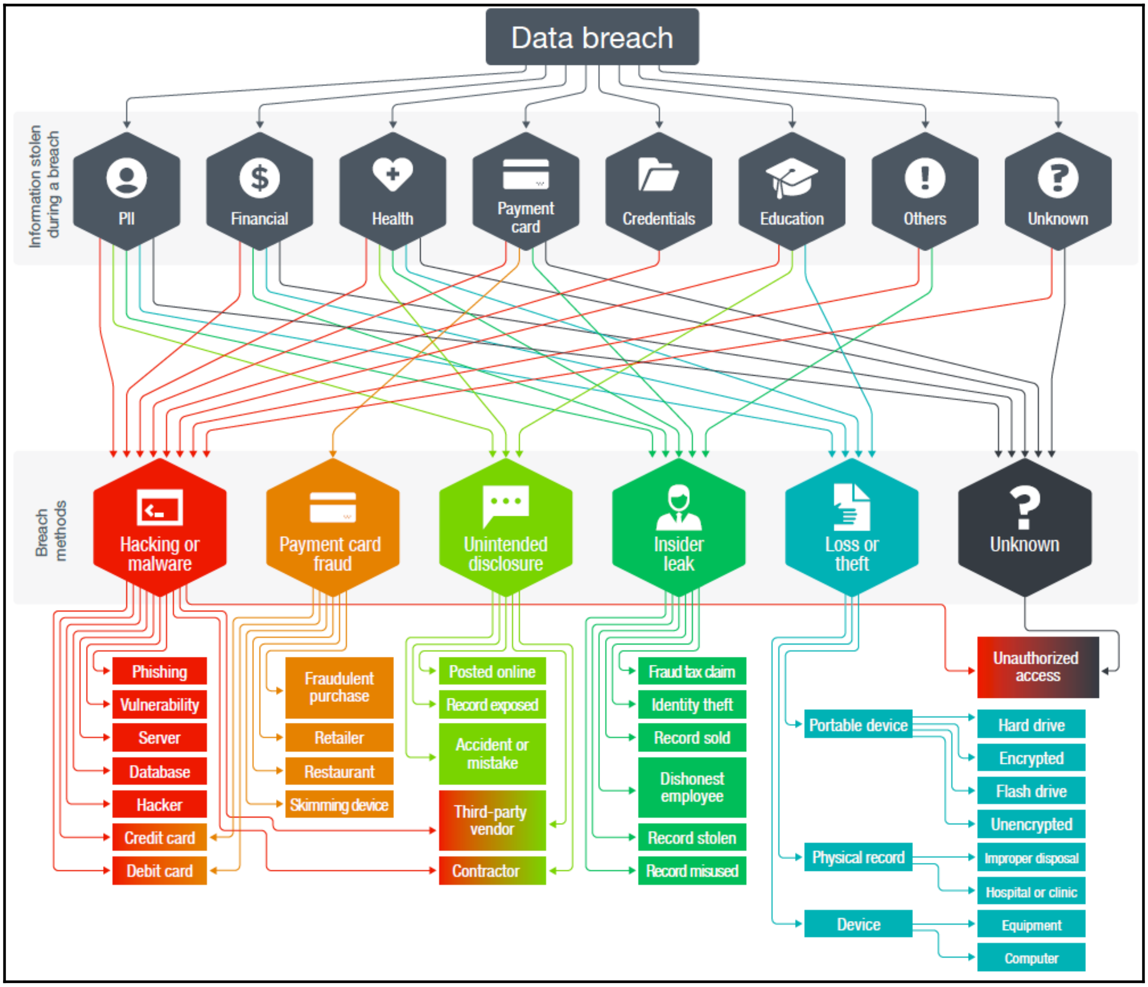
Hacking or malware attacks comprised the next major threat, followed by unintended disclosure and insider threats. Payment card data compromised via skimming, keylogging, or similar methods posed less than a 2% risk. In slightly more than 3% of the cases, the actual breach method remained unknown.

Hacking or malware are the prime go-to breach methods

Data breaches are multifaceted events with numerous probable scenarios. Based on the Trend Micro analysis, they created a Bayesian network to model commonly observed data breach scenarios:

- As per the model, hacking or malware was used to compromise all record types. Hacking and malware attacks usually include phishing, exploiting vulnerabilities, gaining unauthorized access, and compromising systems, servers, and databases. Credit and debit card data was also compromised via hacking or malware attacks.
- In incidents where the breach method is unknown, PII and financial, payment card, and/or health data were most likely compromised.
- Retailers and restaurants were frequent victims of payment card fraud. Skimming devices are used, but PoS RAM scrapers are by far the most popular tools for collecting payment card data. Stolen payment card data is often used to make fraudulent purchases.
- Unintended disclosures exposed PII and health and education data. Unintended disclosures happen when data is accidentally posted online, leaked through negligence, or exposed because of mistakes or negligence on the part of third-party vendors and contractors who handle information.
- Insiders targeted PII and financial, payment card, health, and other data. Selling data to outside parties is the common crime committed by insiders.

- PII and financial, health, and education data were frequently compromised through loss or theft. This includes the loss or theft of portable devices (USB keys, backup drives, laptops, and so on), physical records (files, receipts, bills, and so on), and stationary devices (office computers, specialized equipment, and so on).



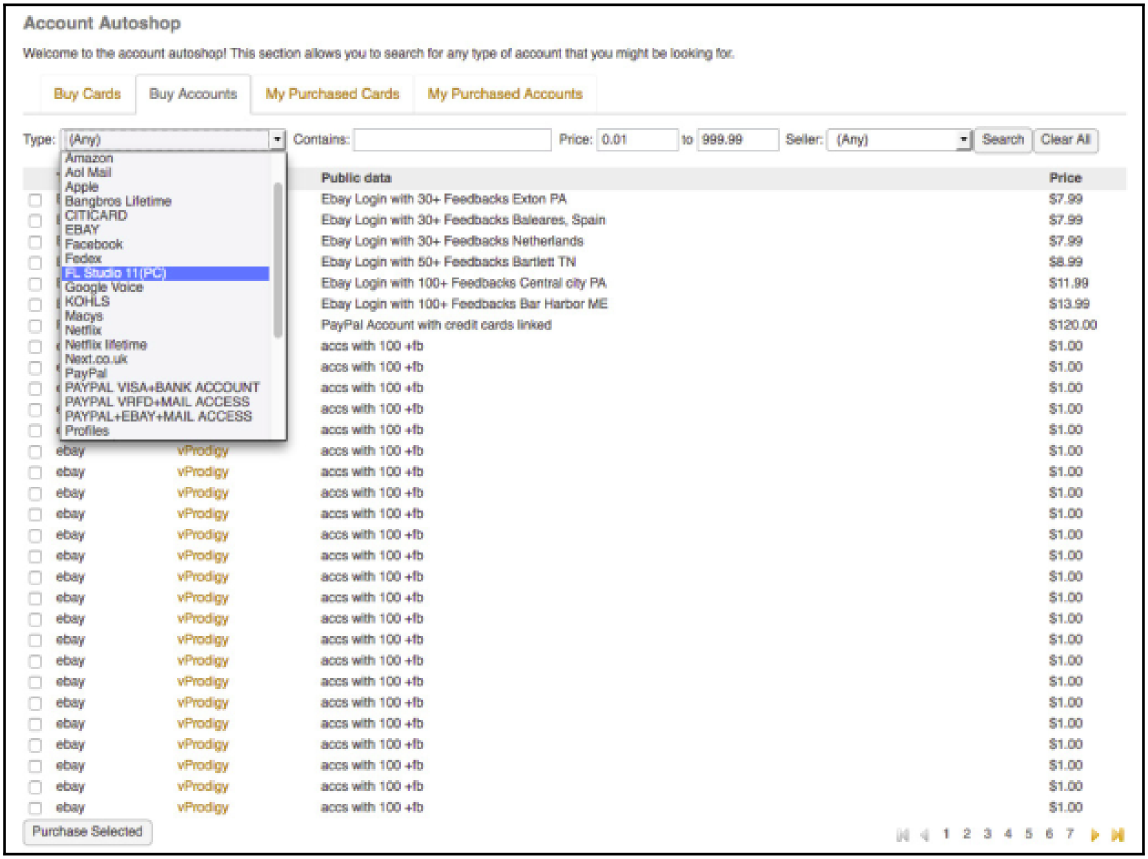
Bayesian network showing commonly observed data breach scenarios

Account thefts - accounts for sale

Different types of accounts are available for sale in Deep Web marketplaces. Some of them are as follows:

Mobile phone, eBay, Uber, and PayPal accounts for sale

- Accounts for various mobile phone operators in the US are available for up to US$14 per account.
- Compromised PayPal and eBay accounts are commonly available for purchase. Facebook, FedEx, Google Voice, Netflix, Amazon, Uber, and other accounts are also sold.
- Compromised Uber accounts have also recently become very popular in Deep Web marketplaces, as these can be fraudulently charged with phantom rides.
- Stolen accounts from victims in Canada, Australia, the United Kingdom (UK), and other European countries are readily available for purchase. Criminals probably prefer to distribute their fraud operations worldwide in order to improve the probability of success and reduce operational risks.
- There are no price differences between verified and unverified PayPal accounts. The available balance on each account is listed to help potential buyers make informed purchases. The seller can sell the same compromised account to multiple parties. The buyer accepts the risk that the accounts could have been flagged and locked.
- PayPal and eBay accounts, which are mature (has months or years of transaction history), are sold for up to US$300 each. Mature accounts are less likely to be flagged for suspicious transactions.



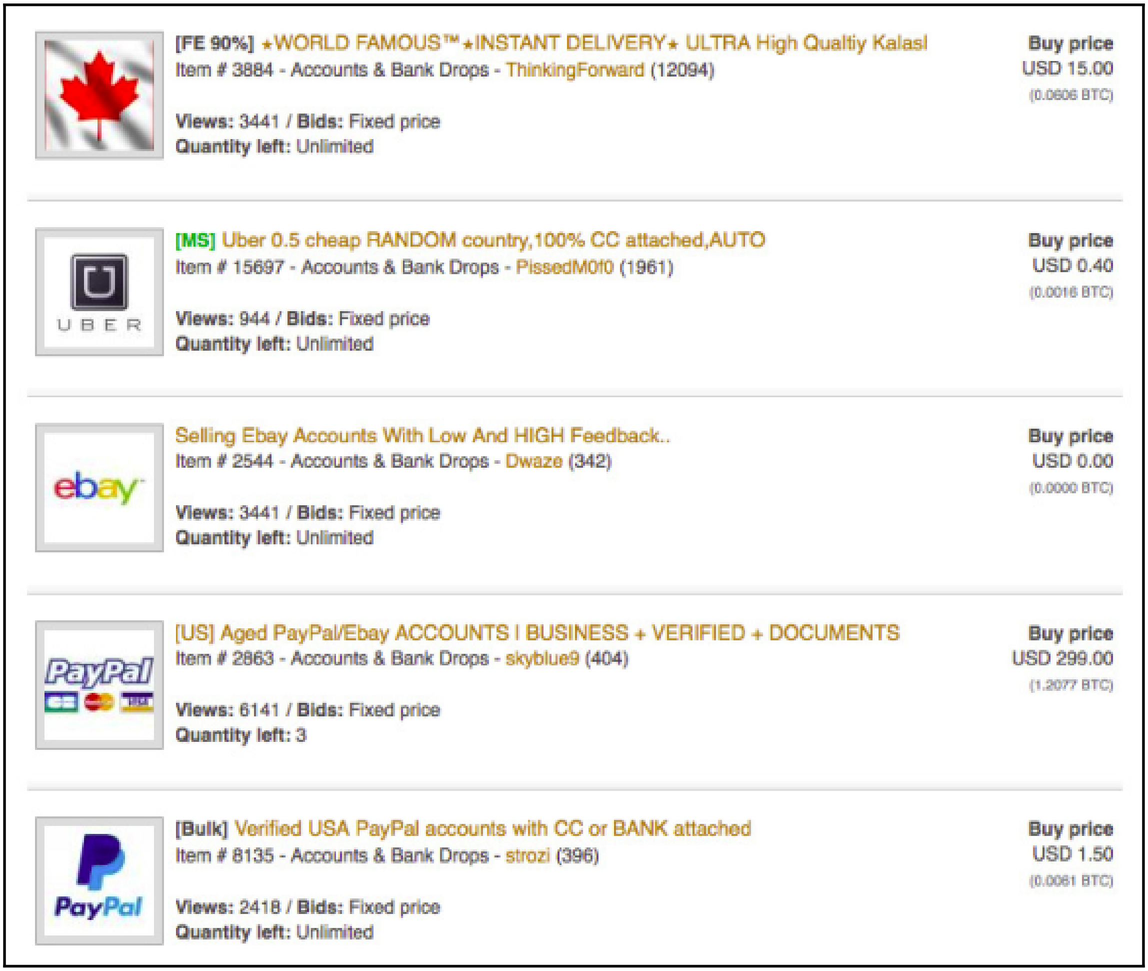
Account Autoshop

Welcome to the account autoshop! This section allows you to search for any type of account that you might be looking for.

Type: (Any) Contains: Price: 0.01 to 999.99 Seller: (Any)

			Public data	Price
□			Ebay Login with 30+ Feedbacks Exton PA	$7.99
□			Ebay Login with 30+ Feedbacks Baleares, Spain	$7.99
□			Ebay Login with 30+ Feedbacks Netherlands	$7.99
□			Ebay Login with 50+ Feedbacks Bartlett TN	$8.99
□			Ebay Login with 100+ Feedbacks Central city PA	$11.99
□			Ebay Login with 100+ Feedbacks Bar Harbor ME	$13.99
□			PayPal Account with credit cards linked	$120.00
□			accs with 100 +fb	$1.00
□			accs with 100 +fb	$1.00
□			accs with 100 +fb	$1.00
□			accs with 100 +fb	$1.00
□			accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00
□	ebay	vProdigy	accs with 100 +fb	$1.00

Miscellaneous accounts for sale



[FE 90%] ⋆WORLD FAMOUS™⋆INSTANT DELIVERY⋆ ULTRA High Qualtiy Kalasl
Item # 3884 - Accounts & Bank Drops - ThinkingForward (12094)

Views: 3441 / **Bids:** Fixed price
Quantity left: Unlimited

Buy price
USD 15.00
(0.0606 BTC)

[MS] Uber 0.5 cheap RANDOM country,100% CC attached,AUTO
Item # 15697 - Accounts & Bank Drops - PissedM0f0 (1961)

Views: 944 / **Bids:** Fixed price
Quantity left: Unlimited

Buy price
USD 0.40
(0.0016 BTC)

Selling Ebay Accounts With Low And HIGH Feedback..
Item # 2544 - Accounts & Bank Drops - Dwaze (342)

Views: 3441 / **Bids:** Fixed price
Quantity left: Unlimited

Buy price
USD 0.00
(0.0000 BTC)

[US] Aged PayPal/Ebay ACCOUNTS I BUSINESS + VERIFIED + DOCUMENTS
Item # 2863 - Accounts & Bank Drops - skyblue9 (404)

Views: 6141 / **Bids:** Fixed price
Quantity left: 3

Buy price
USD 299.00
(1.2077 BTC)

[Bulk] Verified USA PayPal accounts with CC or BANK attached
Item # 8135 - Accounts & Bank Drops - strozi (396)

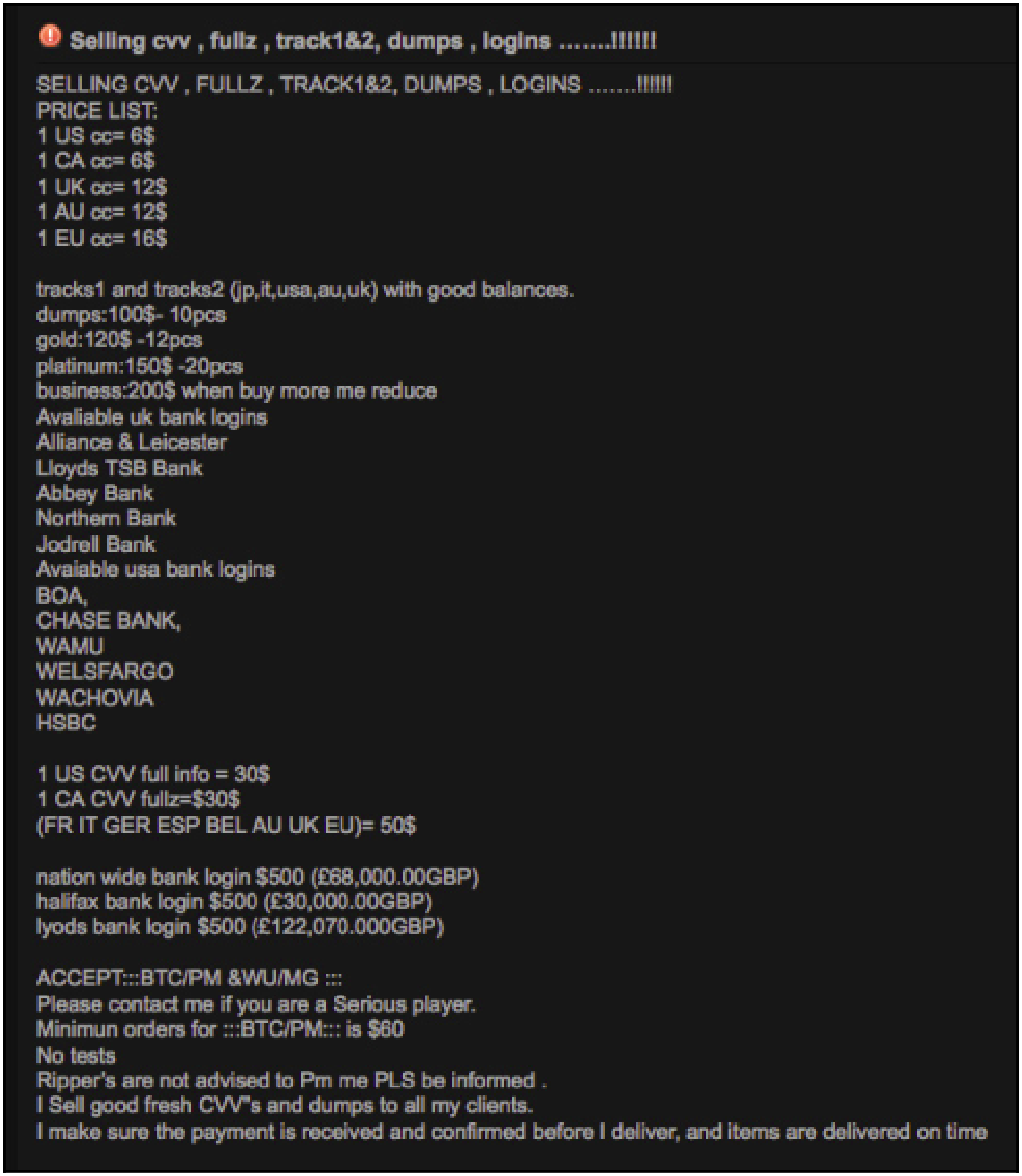
Views: 2418 / **Bids:** Fixed price
Quantity left: Unlimited

Buy price
USD 1.50
(0.0061 BTC)

Credentials for sale

Bank login credentials for sale

Log-in identifications and credentials for banks around the world are sold at steep prices of between US$200 and US$500 per account in Deep Web marketplaces. The larger the available balance of an account, the higher its selling price. Banking malware has been and continues to be a massive problem in Brazil. As such, it is not surprising to find so many compromised Brazilian bank log-in credentials available for purchase.



Selling cvv , fullz , track1&2, dumps , logins ....!!!!!!

SELLING CVV , FULLZ , TRACK1&2, DUMPS , LOGINS ....!!!!!
PRICE LIST:
1 US cc= 6$
1 CA cc= 6$
1 UK cc= 12$
1 AU cc= 12$
1 EU cc= 16$

tracks1 and tracks2 (jp,it,usa,au,uk) with good balances.
dumps:100$- 10pcs
gold:120$ -12pcs
platinum:150$ -20pcs
business:200$ when buy more me reduce
Avaliable uk bank logins
Alliance & Leicester
Lloyds TSB Bank
Abbey Bank
Northern Bank
Jodrell Bank
Avaiable usa bank logins
BOA,
CHASE BANK,
WAMU
WELSFARGO
WACHOVIA
HSBC

1 US CVV full info = 30$
1 CA CVV fullz=30
(FR IT GER ESP BEL AU UK EU)= 50$

nation wide bank login $500 (£68,000.00GBP)
halifax bank login $500 (£30,000.00GBP)
lyods bank login $500 (£122,070.000GBP)

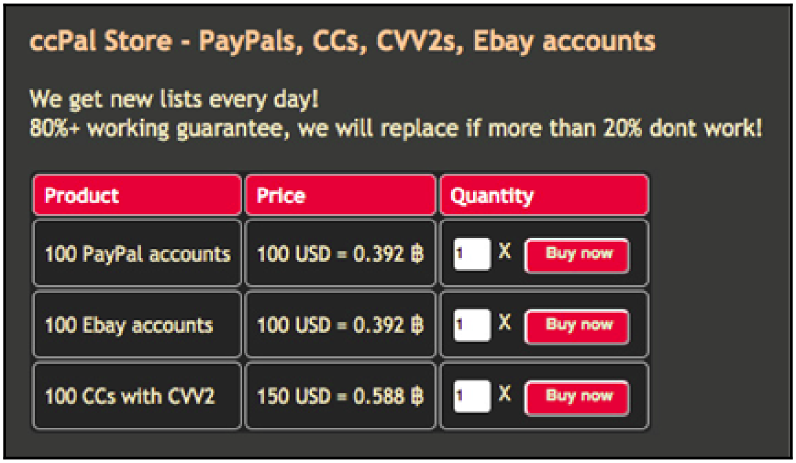
ACCEPT:::BTC/PM &WU/MG :::
Please contact me if you are a Serious player.
Minimun orders for :::BTC/PM::: is $60
No tests
Ripper's are not advised to Pm me PLS be informed .
I Sell good fresh CVV"s and dumps to all my clients.
I make sure the payment is received and confirmed before I deliver, and items are delivered on time

US and UK bank credentials for sale

Credit card sales are brand agnostic

Credit card sale forums and Deep Web marketplaces sell payment card data to any person who is willing to pay. Card data sells for different prices in various forums. The prices depend on supply and demand, whether cards are validated or not, and how much money the criminals can potentially steal from them before they are deactivated.

- Buying credit card data in bulk reduces unit prices. In some cases, sellers only sell card data in bulk, which could indicate that they have been freshly acquired.
- Unlike earlier, there no longer appears to be differences in prices with regard to card brand. This is probably because of an oversupply of credit cards from numerous data breaches.
- Credit cards from every continent - Europe, Asia, Africa, North and South America, and Australia are available in carding forums.



ccPal Store - PayPals, CCs, CVV2s, Ebay accounts

We get new lists every day!
80%+ working guarantee, we will replace if more than 20% dont work!

Product	Price	Quantity
100 PayPal accounts	100 USD = 0.392 ฿	1 X Buy now
100 Ebay accounts	100 USD = 0.392 ฿	1 X Buy now
100 CCs with CVV2	150 USD = 0.588 ฿	1 X Buy now

Credit cards for sale

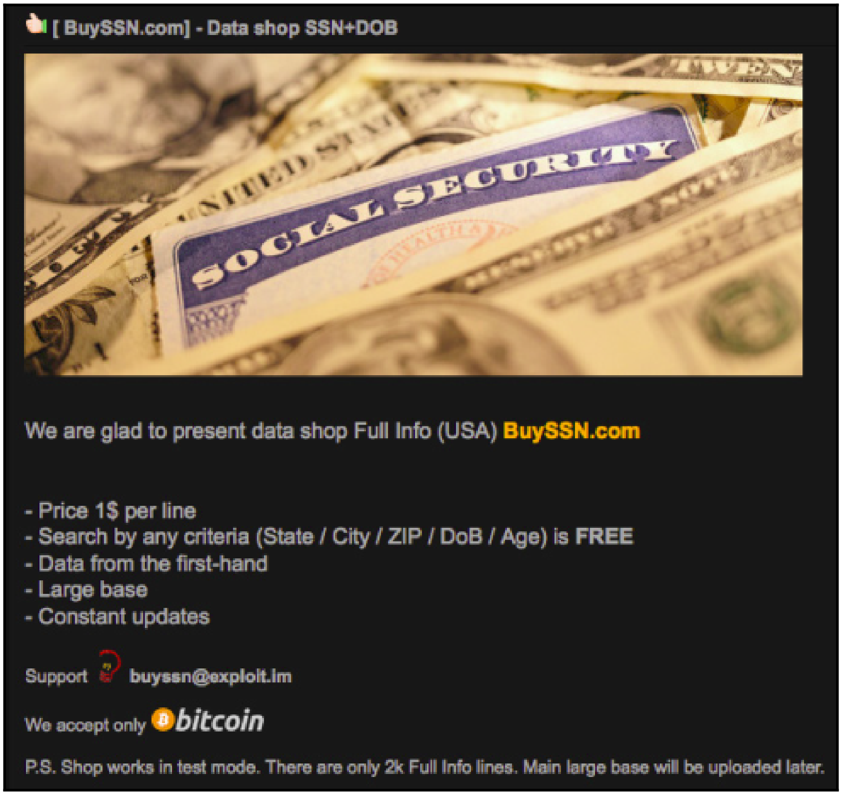
- Non-US credit cards fetch higher per-unit prices compared with US ones.

Carding forums have search functions that allow buyers to select credit cards from different states and/or issuing banks. Using stolen cards to make purchases near the geographical locations where they were stolen is less likely to be flagged as "suspicious".

PII prices fall due to oversupply

Personally identifiable information (PII) is another hot product available for purchase in Deep Web marketplaces at comparatively reasonable prices:

- PII is normally sold on a per-line basis at US$1 per line. Each line contains a name, a full address, a date of birth, a Social Security number, and other information. Cyber criminals need to purchase only a few lines to commit identity fraud.
- The average price of PII has fallen from around US$4 in 2014 to US$1 this year. This is probably due to an oversupply of PII from numerous data breaches.



[BuySSN.com] - Data shop SSN+DOB

We are glad to present data shop Full Info (USA) BuySSN.com

- Price 1$ per line
- Search by any criteria (State / City / ZIP / DoB / Age) is FREE
- Data from the first-hand
- Large base
- Constant updates

Support buyssn@exploit.im

We accept only bitcoin

P.S. Shop works in test mode. There are only 2k Full Info lines. Main large base will be uploaded later.

Selling Personal Identifiable Information (PII)

The perceived and actual monetary values

At this point in time wherein the lack of privacy and security are considered major issues, the value of the data is becoming more and more relevant. As per Trend Micro's survey and analysis from thousand customers across US, Europe, and Japan they found that:

- The most valued personal data type comprises passwords at US$75.80.
- Health information and medical records came second, valued at an average of US$59.80. US respondents put the highest value on their health records at US$82.90 while European consumers considered theirs to be worth US$35.
- Social security numbers came in third at US$55.70.
- Payment details ranked fourth at US$36.60. US citizens priced this information at US$45.10 while the Japanese valued it at US$42.20. Europeans priced it at US$20.70.
- Purchase history ranked fifth, valued at US$20.60. US respondents again valued it most compared with the Japanese and Europeans.
- Physical location information ranked sixth, valued at US$16.10. US citizens priced it at US$38.40 while those from Japan and Europe priced it a paltry US$4.80 and US$5.10, respectively.
- Home address ranked seventh, valued at US$12.90. US consumers once more priced it at US$17.90. Japanese respondents pegged this information at US16.30 while those from Europe priced it at US$5.00.
- Personal photos and videos ranked eighth, valued at US$12.20. US respondents priced them at US$26.20 while those from Japan and Europe only priced them at US$4.70.
- Marital status information was pegged at an average of US$8.30. Japanese consumers priced it at US$12.70 while those from the US and Europe pegged this information at US$6.10 and US$6.00, respectively.
- Name and gender information were least valued at US$2.90.

One conclusion that could be drawn from the survey was that the US respondents valued nearly all their personal information more than their counterparts from other countries. Besides cultural differences, this could also be due to how much US consumers value their privacy and how their day-to-day lives revolve around their own personal information amid the social media boom.

Another thing that stood out was how everyone considers passwords their most valuable information. This is a strong indicator of how connected people have become in the age of the Internet.

While the perceived value of stolen data differs from its actual selling price, the final dollar value of loss lay on to a business by the cyber criminal is considerably complex and higher than both the perceived value and selling price.

Defending against data and account theft extortion

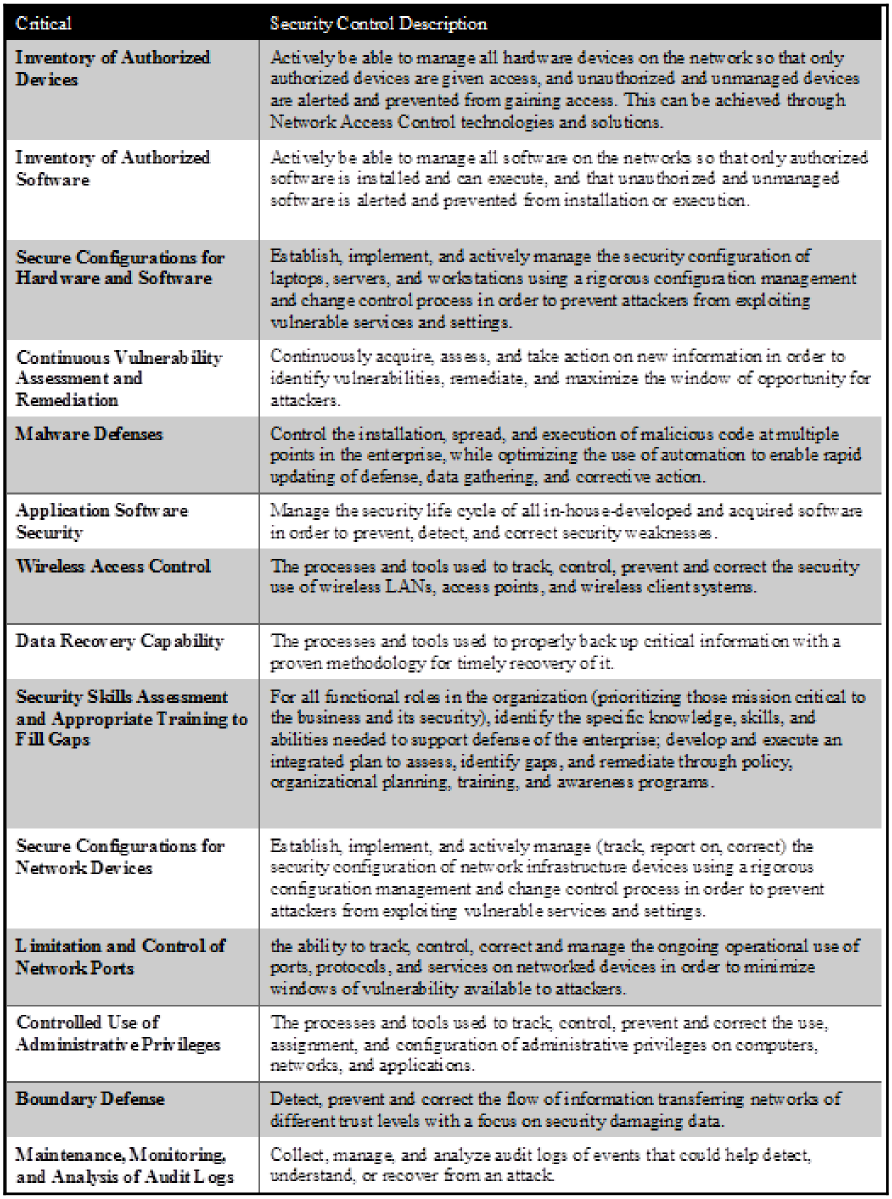
Here are some key tips to protect you from personal data theft:

- Do not open e-mails or attachments from unknown entities and individuals.
- Monitor bank account statements regularly and credit reports at least once a year for any fraudulent activity.
- Do not communicate with the subject by any chance.
- Do not store sensitive or embarrassing photos of yourself online, on a public domain, or on your mobile devices with applications having privilege to access to your gallery.
- Use strong alpha numeric passwords and do not use the same password for multiple websites and applications.
- Never provide sensitive personal information of any sort via e-mail to any third party or individuals not known to you. Be aware, many e-mails requesting your personal information give the impression to be legitimate.
- Ensure security settings for social media accounts are turned on and set at the highest level of protection.
- When providing PII, credit card information, or other sensitive information to a website, ensure the traffic transmission is secure by verifying the URL prefix includes https, the status bar displaying a "lock" icon, and so on.

Enterprise security measures

Data breaches are unavoidable and thus having proactive and effective alerting, containment, and mitigation processes is critical.

Center for Internet Security (CIS), have laid out the following critical cyber security controls for effective cyber defense that address new risks posed by an evolving threat landscape:



Critical	Security Control Description
Inventory of Authorized Devices	Actively be able to manage all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are alerted and prevented from gaining access. This can be achieved through Network Access Control technologies and solutions.
Inventory of Authorized Software	Actively be able to manage all software on the networks so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is alerted and prevented from installation or execution.
Secure Configurations for Hardware and Software	Establish, implement, and actively manage the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
Continuous Vulnerability Assessment and Remediation	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and maximize the window of opportunity for attackers.
Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
Application Software Security	Manage the security life cycle of all in-house-developed and acquired software in order to prevent, detect, and correct security weaknesses.
Wireless Access Control	The processes and tools used to track, control, prevent and correct the security use of wireless LANs, access points, and wireless client systems.
Data Recovery Capability	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
Security Skills Assessment and Appropriate Training to Fill Gaps	For all functional roles in the organization (prioritizing those mission critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.
Secure Configurations for Network Devices	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
Limitation and Control of Network Ports	the ability to track, control, correct and manage the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.
Controlled Use of Administrative Privileges	The processes and tools used to track, control, prevent and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
Boundary Defense	Detect, prevent and correct the flow of information transferring networks of different trust levels with a focus on security damaging data.
Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Key Cyber Security Controls

Implementing all the preceding security controls can be very costly, time consuming, and would require dedicated teams for proactive daily operations, monitoring, response, and maintenance. A large business or organization generally ought to have the resources to implement all of them, but most small businesses can only meet the expense to implement a subset of the controls critical to their businesses. These critical security controls provide a comprehensive set of strategies and executing even a subset of them will go a long way in preventing data breaches.

While the following are important steps, a large number of data breaches for an enterprise could also have been prevented following some fundamental enterprise security measures, including, but not restricted to:

- Patching vulnerabilities
- Deploying effective e-mail filters
- Using intrusion prevention and detection software
- Restricting third-party access to company data
- Maintaining good software hygiene
- Employing encryption where appropriate to secure confidential data
- Implementing **data loss prevention (DLP)** technologies across data at rest, data in transit, and data in use

Evidently, most of these relate to preventing external assaults. When it comes to mitigating the possibility of malicious or accidental insider threats, enterprises need to focus on employee education and data loss prevention.

Fundamental security hygiene should be drilled into employees the same way the public community are told to cover their mouths when they cough or sanitize their hands in hospitals. Enterprises have to also be making use of data loss prevention technologies to locate, monitor, and protect their data, wherever it is within the organization, so there is comprehensive monitoring and clarity on who is doing what, with what data, in real time. DLP can alert and block certain types of data from leaving an enterprise perimeter, such as credit card numbers, sensitive information, and other confidential documentation.

Security has to be a crucial part of operations and employee behavior, instead of an add-on or something to pacify auditors and compliance requirements. Data breaches are not likely to stop any time soon, but the scale and impact of them could undoubtedly be reduced if organizations of all sizes recognize that security goes well beyond the bounds of the CIO or the IT manager. Security is in every single employee's hands.

Have measures to detect insider attacks, much like external attacks. Insiders are usually the trusted individuals or persons of authority with corresponding privileges who steal data. They can be encouraged by money, ideologies, coercion, and their egos. More than one of these reasons are frequently put into play. Dealing with insider threats is considered a very difficult task. Broadly speaking, prevention and mitigation techniques can be grouped into two categories - technical and non technical:

- Technical steps to stop insider attacks use security best practices as we discussed earlier in the critical security controls. Predominantly insider attacks should be accorded with the same level of prioritization as external attacks. Like external attacks, insider attacks can't be prevented and so they need to be detected as quickly as possible. Monitoring and logging events such as what data is moving within a network can be used to detect potentially suspicious behavior. Data leakage prevention can play a major role to identify internal attacks. The key principle of defense is to assume compromise. This also includes identifying compromised insiders. Proper access controls and segregation of duties should be put in place to ensure that employees can't access information that they do not need for their day-to-day functions. The credentials of employees who leave organizations should be immediately disabled to prevent security leaks.
- Non-technical means of security are equally effective in preventing insider threats. Employee discontent increases the risks that insider attacks pose. Good management practices in handling delicate situations, recognizing and rewarding employees, and looking after employee well-being all help diffuse potential insider threats. In a nutshell, happy employees are less likely to turn against their employers.

Security software firms offer bundled packages to small businesses that include anti-malware, anti phishing, and web filtering solutions. These are easy to set up, require minimal administration, and provide excellent security out of the box. Some security technology firms also include network access control, device control, DLP, patch management, and application control solutions in their small-business bundles. Windows come with a built-in easy to configure software firewall. Most wireless routers come with built-in hardware firewalls.

All of these technologies collaborate to protect a business from data breaches. One of the major key technologies that all businesses or organizations should consider deploying is disk and device encryption. Since, as we discussed previously, the loss or theft of portable devices (USB keys, backup drives, laptops, and so on) poses a major data compromise risk to the organization of all sizes. Disk and device encryption will make the data on the stolen devices unusable and inoperable to all but the most resourceful criminals.

In short, any business or organization that processes and stores sensitive or confidential data are a potential breach target. In today's unified and interconnected world, data breach prevention policies and plans should be considered an integral part of business operations. Eventually, no defense is impregnable against determined adversaries.

The key belief of defense is to assume compromise and take countermeasures to:

- Quickly identify and respond to ongoing security breaches
- Contain the breach and halt the loss of sensitive data
- Proactively prevent breaches by securing all exploitable avenues across enterprises
- Apply lessons learned to further investigate, strengthen defenses, and prevent repeat incidents

Business E-mail Compromise (BEC)

Business E-mail Compromise (BEC) which sometimes is also called Business Email Scam is defined as a sophisticated and highly impactful scam, targeting organizations and businesses working with foreign suppliers and/or businesses that often perform wire transfer payments. The scam is generally carried out by compromising legitimate business e-mail accounts through techniques such as social engineering or cyber intrusion methods to conduct unauthorized transfers of funds. BEC scams are thus a type of payment fraud that utilizes spoofed accounts to send wire transfer instructions. These are mostly global scams with subjects and victims across multiple countries.

Most victims report using wire transfers as a most common method of transferring funds for business purposes; though, some victims report using checks as a common method of payment. The fraudsters and cyber criminals use the method most commonly associated with their victim's common business practices.

In addition there have been cases potentially identified wherein the data is held hostage by the cyber criminals and extortion attempts have been made to executives of small and medium organizations. Even though this aspect will be covered in detail while we discuss Ransomware extortions, BEC's are eventually a sub product of the overall equation. We have also provided insights from the deep web, wherein we have illustrated what kind of stolen personal information is readily available for cyber criminals to transcend the BEC approach.

As per the latest figures from the FBI, over the past years (particularly in the last two years), Business E-mail Compromise (BEC) schemes have caused at least $3.1 billion in total losses to roughly 22,000 organizations around the world. Ever since January 2015, there has been a 1,300% surge in recognized exposed losses, amounting to an average loss of $140,000 per scam. The impending damage and effectiveness of these BEC campaigns enforced the FBI to issue a public service statement describing how such scams operate and how much loss it can cause to targeted organizations regardless of the organization size.

Advanced threats are ever changing and with this shift towards schemes such as BEC, it is more likely that any enterprise across the globe may likely become the target. Business E-mail Compromise is becoming mainstream and has a wide impact across regions and enterprises. Prudently planned and researched, these scams target specific roles (and thus the associated employee) in an enterprise. Either the associated employee becomes the target of this attack or becomes the unaware victim.

Generally these schemes and associated e-mails do not generally use malware or URLs that are usually found in typical credential phishing schemes. Labeled "business e-mail compromise" by the FBI, these are also recognized as CEO fraud, whaling attacks, man-in-the-e-mail, and other unsavory titles. The majority of these scam e-mails are purpose made to imitate C level executives and trick unwary employees across crucial roles in an organization.

According to the Internet Crime Center (IC3), such attacks increased by more than 270% in 2015 alone. Victim companies come from approximately 80 countries, resulting in more than $2 billion in losses since late 2013.

With such scams impeding the momentum of business services, one may not even realize or know that they are a victim of a fraud right away. The business and corresponding systems continue to run usual and everything seems like business as normal. Security tool alarms do not go off and there is no ransom note. That is the point. Such scams global in scope, have grown to target companies both large and small in every part of the world. As of New Zealand to Belgium, organizations from every industry have suffered tremendous losses.

A few of the recent scams from Proofpoint include:

- One of the East Asian subsidiaries at Ubiquiti Networks, Inc. revealed that it had given more than $45 million in payments over an extended period to cyber criminals who were using impostor e-mails to pose as an existing supplier to the organization.
- Crelan, a Belgian bank in recent times lost more than $70 million due to impersonator e-mails, realizing the fraud only after the company conducted an internal audit.
- In New Zealand, a higher education provider, TWoA, lost more than $100,000 when their CFO fell victim to an impersonator e-mail, believing the payment request came from the organization's president.
- Luminant Corp., an electric utility company in Dallas, Texas sent a little over $98,000 in reply to an e-mail request that they believed was coming from a company executive. Later it was learned that attackers sent an impersonator e-mail from a domain name with just two letters transposed.
- Ubiquiti Networks - the finance department was targeted by a fraudulent request from an outside entity that resulted in $46.7 million being transferred to an overseas account held by external third parties after an employee was impersonated.
- Mattel - a finance executive wired more than $3 million to the Bank of Wenzhou after the "new CEO" requested a vendor payment. According to reports, Mattel quickly realized that it had been a victim of a fraudulent request and worked with Chinese authorities to get the money back.
- FACC - the Austrian aircraft parts maker, whose customers included Airbus, Boeing, and Rolls-Royce, stated that they had fired their chief executive after cyber criminals stole Euros 50 million ($55.7 million) in an e-mail scam.

With these scams and potential dangerous schemes, cyber criminals are taking the time to gather personal information and absorb the processes within a company. As soon as they are armed with this material, they target judiciously a selection of employees with a spear phishing e-mail intended to get access to confidential business data or transfer money into an unknown account.

The victims of the BEC scam range from small businesses to large corporations. The victims continue to deal with a wide variety of goods and services, indicating that a specific sector does not seem to be targeted.

It is largely unidentified how victims are carefully chosen; however, the perpetrators monitor and study their selected victims using social engineering practices prior to initiating the BEC scam. The perpetrators are able to accurately identify the individuals and protocols necessary to carry out wire transfers within a specific business environment. Victims may also first receive "phishing" e-mails asking for additional details about the business or individual being targeted (name, travel dates, and so on).

Some people conveyed being a victim of numerous Scareware or Ransomware cyber intrusions immediately preceding a BEC occurrence. These intrusions can primarily be enabled through a phishing scam wherein a victim obtains an e-mail from an apparently legitimate source that comprises a malicious link. The victim clicks on the link, and it downloads malware, allowing the actor(s) independent access to the victim's data, including passwords or financial account information.

The BEC scam is related to other methods of fraud, including but not limited to romance, employment, lottery, and rental scams. The victims of these scams are typically U.S. based and may be enlisted as unaware money mules. The mules collect the fraudulent funds in their personal accounts and are then directed by the perpetrator to quickly hand over the funds to another bank account, usually outside the U.S. Upon direction, mules may open bank accounts and/or shell corporations to further the fraud scheme.

Thus the potential targets and methods can be narrowed down to:

- Businesses and personnel using open source e-mail
- Individuals responsible for handling wire transfers within a specific business
- Spoof e-mails that very closely impersonate a legitimate e-mail request (for example, "Code to admin expenses" or "Urgent wire transfer")
- Fraudulent e-mail requests for a wire transfer are well-worded, specific to the business being victimized

The fraudsters at your gates

Successful masquerader e-mails result from using a variety of research tactics against a company. Activities may comprise scouring social media portals and news bulletins to delving into company trash to learn more about executives, company business, and their direct reports if any. One may get skillfully masked phone calls on a variety of subjects directed at learning more about the clients, personnel, and suppliers. Understanding the organization process and knowing business partners is one of the most crucial factors to a successful attack.

Cyber attackers with a severe reconnaissance strategy capitalize money and time in intelligence gathering. The initial step is qualifying a worthy target. If a business has several supply partners and executives who frequently travel abroad, this business is one of the ideal targets for the spam. Taking benefit of the time difference and the countless hours a business executive spends in transit and unreachable is key to a successful attack.

There are generally two major angles involved with targeting business executives. In the case of the constantly traveling business executive, this is the individual who intruders and perpetrators study and seek to impersonate. They use all the resources available to understand the targets agenda, peers, and direct reports. It is likely that the organization will have phone calls to gather additional information to learn more about the suppliers and customers. As an example, having information on a company's travel agency can be considered as valuable information to an attacker.

An organization's CEO is generally an always traveling executive and the typical target in such scams, hence the term CEO fraud. Thus on the receiving end, another executive with financial authority may perhaps be the one that receives the last minute "before I board the plane request" from the CEO (impersonated by an attacker). The instructions may contain wire transferring a payment to a supplier who is usually located in the same area that the CEO is visiting.

This type of scenario can simply victimize any executive's direct subordinates and associates who routinely process payments. Another plan includes understanding an organization's dealers, how they generally invoice, and by means of their language, financial practices, forms, and procedures to, for example, modify bank account data for a forthcoming payment. If the impersonators are successful, one may have been making settlements and payments to them for months without ever knowing about it.

How impersonators fake you out

Primarily LinkedIn and other social media portals are the "go to" resource for profiling targets and the intended victims. Attackers profile senior management and C-level executives by examining and investigating content within social media portals, company PR releases, and any news articles about the business. From there, social snooping efforts uncovers the direct reports.

Fresh employees in accounting and finance places are extremely sought after by cyber criminals and attackers that use impostor e-mails. They make the seamless victim for an impostor attack. Being new to an organization, the new employees may not have the essential sense that something may be off with a payment request. They certainly don't know or have enough knowledge about the business suppliers, dealers, or are in a rush to make a decent impression and not know when to slow down and inquiry a transaction.

Once investigation on the organization and its senior employees and executives is complete, attackers now have a complete profile of the business. Also, there is a high probability that a decent part of the business relationships would be known and perhaps aware of a couple of special company projects or code names.

They have files and reports on most senior level or C-level executives, particularly those in financial positions; they will also know who their direct reports are and what their corresponding function is. In the next stage, these cyber criminals' emphasize on impersonating the organization's regular suppliers or partners that work with the company.

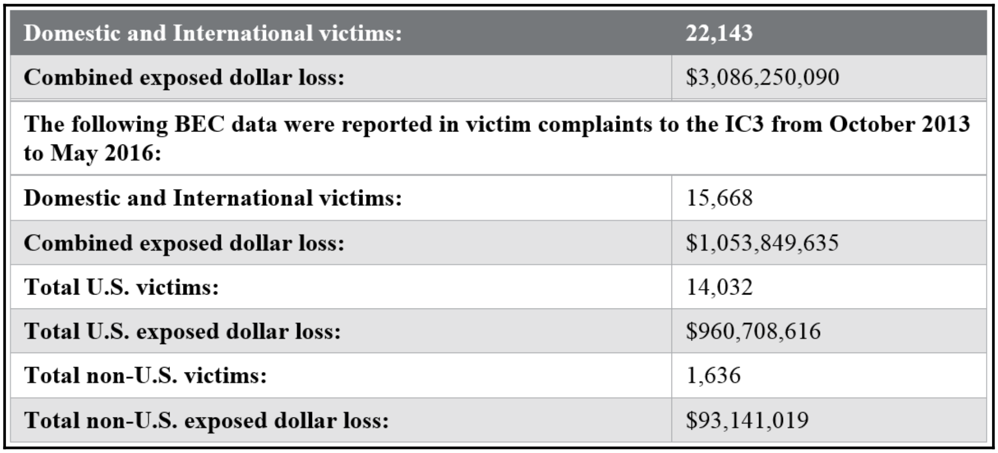
If attackers aim to impersonate someone inside the company, they may also register a domain name that is one or two letters off from yours. This makes a look-alike domain for use in the fraud e-mail along with spoofed e-mail addresses of senior employees and executives previously profiled. Frequently, attackers also create domain and e-mail addresses a short while before sending the fraud e-mail. In other cases, they may do the same thing, but impersonate a supplier or another business such as an accounting or law firm that usually requests payment from the company.

The statistics behind Business E-mail Compromise (BEC)

The BEC scam endures growing, change, and target businesses of all dimensions.

As per IC3, since January 2015, there has been more than a 1,300% increase in identified exposed losses. This scam has been stated by victims in all 50 states and in 100 countries. Intelligence also shows that fraudulent transfers have been sent to approximately 79 countries with the majority going to Asian banks located within China and Hong Kong.

The following BEC figures were reported to the Internet Crime Complaint Center (IC3) and are derived from multiple victim complaints filed with international law enforcement agencies and financial institutions:



Domestic and International victims:	**22,143**
Combined exposed dollar loss:	$3,086,250,090
The following BEC data were reported in victim complaints to the IC3 from October 2013 to May 2016:	
Domestic and International victims:	15,668
Combined exposed dollar loss:	$1,053,849,635
Total U.S. victims:	14,032
Total U.S. exposed dollar loss:	$960,708,616
Total non-U.S. victims:	1,636
Total non-U.S. exposed dollar loss:	$93,141,019

Statistics behind BEC

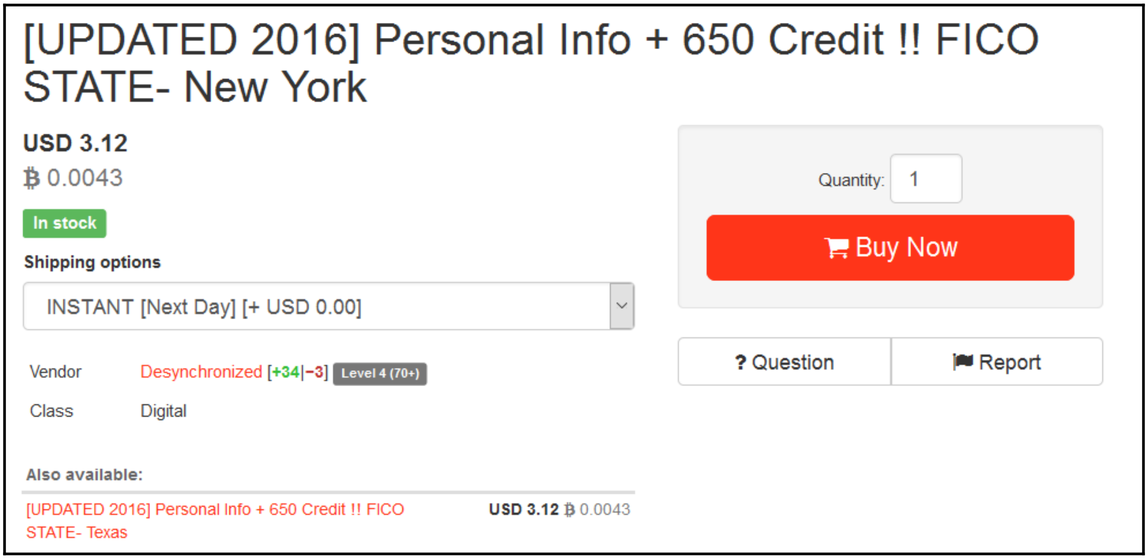
How do BEC schemes work?

Previously also known as the Man-in-the-E-mail scam, a BEC scam typically starts when senior employees of a business including leading business executives' electronic mail accounts are compromised and spoofed, with the impostor sending e-mails to an unknowing employee instructing them to wire large sums of money to foreign accounts.

While approximately less number of cases involve the use of malware, BEC schemes are usually recognized for relying purely on social engineering techniques, making them even difficult to detect. Recent incidents presented how employees were tricked by e-mails masquerading as legitimate e-mails coming from business executives requesting for information.

Multiple versions of BEC scams have been illustrated here:

- Version 1: The Bogus Invoice Scheme - This is the one most common type of scheme targeting general users wherein a cybercriminal contacts a customer via phone or e-mail asking to modify or change the payment location of the invoice or funds to be wired for invoice payment to an alternate, fraudulent account.
- Version 2: CEO Fraud - This is the most common scam targeting organizations of all sizes. In this version, the cybercriminal spoofs an e-mail account of senior management and requests (on behalf of the executive) to another employee requesting a wire transfer to an account that the criminal controls.
- Version 3: Account Compromise - In multiple cases an employee or a person's e-mail gets hacked and requests for payments are sent from the corresponding employees e-mail to multiple business partners/vendors available on the employee's contact list. This typically involves payment requests directing to fraudster controlled accounts. The following screenshot illustrates the personal information being sold in the deep web containing all the details:



[UPDATED 2016] Personal Info + 650 Credit !! FICO STATE- New York

USD 3.12
฿ 0.0043

In stock

Shipping options

INSTANT [Next Day] [+ USD 0.00]

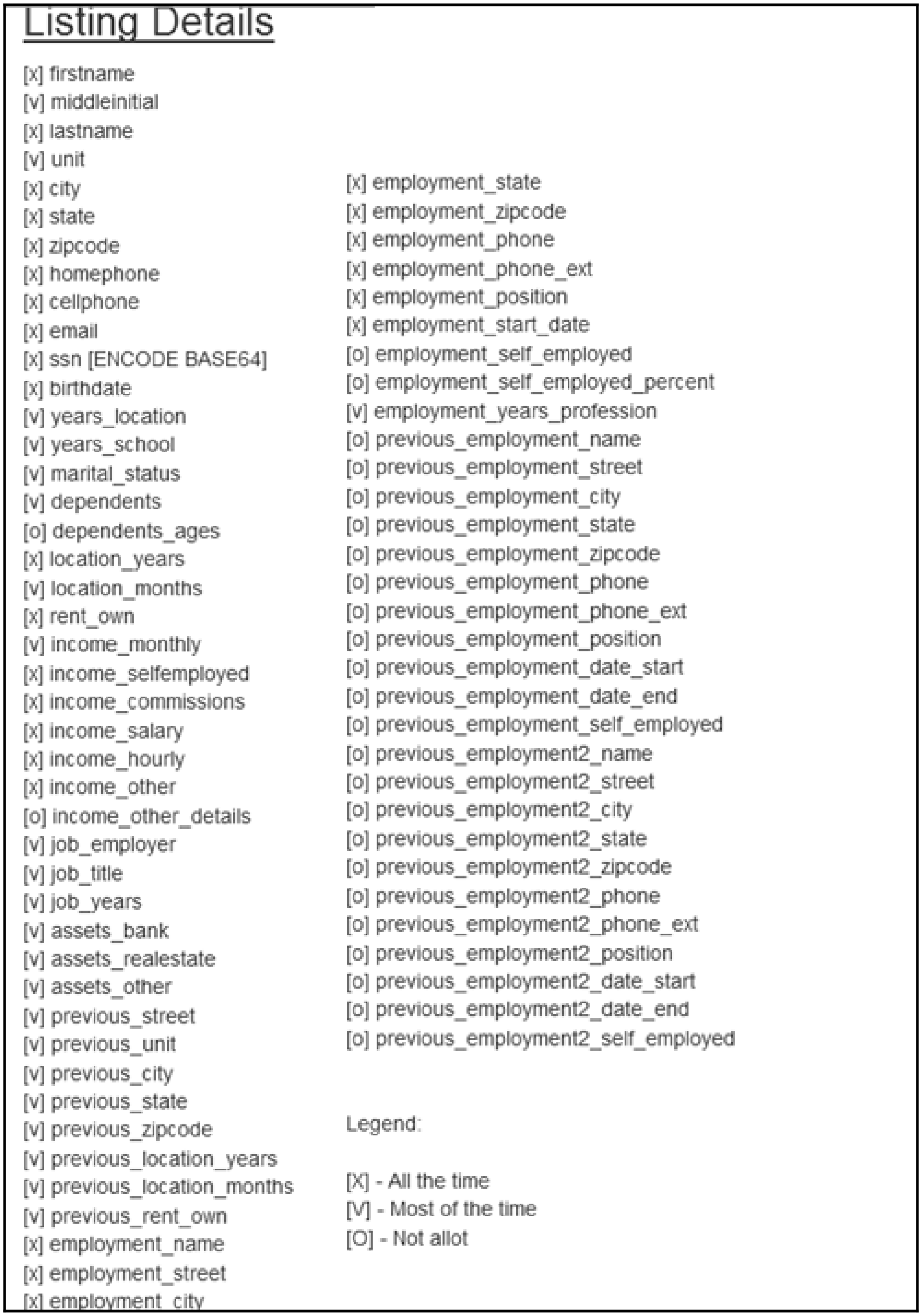
Vendor	Desynchronized [+34|−3] Level 4 (70+)
Class	Digital

Also available:

[UPDATED 2016] Personal Info + 650 Credit !! FICO STATE- Texas	**USD 3.12** ฿ 0.0043

Quantity: 1

Stolen personal information being sold in the Deep Web



Listing Details

[x] firstname
[v] middleinitial
[x] lastname
[v] unit
[x] city
[x] state
[x] zipcode
[x] homephone
[x] cellphone
[x] email
[x] ssn [ENCODE BASE64]
[x] birthdate
[v] years_location
[v] years_school
[v] marital_status
[v] dependents
[o] dependents_ages
[x] location_years
[v] location_months
[x] rent_own
[v] income_monthly
[x] income_selfemployed
[x] income_commissions
[x] income_salary
[x] income_hourly
[x] income_other
[o] income_other_details
[v] job_employer
[v] job_title
[v] job_years
[v] assets_bank
[v] assets_realestate
[v] assets_other
[v] previous_street
[v] previous_unit
[v] previous_city
[v] previous_state
[v] previous_zipcode
[v] previous_location_years
[v] previous_location_months
[v] previous_rent_own
[x] employment_name
[x] employment_street
[x] employment_city

[x] employment_state
[x] employment_zipcode
[x] employment_phone
[x] employment_phone_ext
[x] employment_position
[x] employment_start_date
[o] employment_self_employed
[o] employment_self_employed_percent
[v] employment_years_profession
[o] previous_employment_name
[o] previous_employment_street
[o] previous_employment_city
[o] previous_employment_state
[o] previous_employment_zipcode
[o] previous_employment_phone
[o] previous_employment_phone_ext
[o] previous_employment_position
[o] previous_employment_date_start
[o] previous_employment_date_end
[o] previous_employment_self_employed
[o] previous_employment2_name
[o] previous_employment2_street
[o] previous_employment2_city
[o] previous_employment2_state
[o] previous_employment2_zipcode
[o] previous_employment2_phone
[o] previous_employment2_phone_ext
[o] previous_employment2_position
[o] previous_employment2_date_start
[o] previous_employment2_date_end
[o] previous_employment2_self_employed

Legend:

[X] - All the time
[V] - Most of the time
[O] - Not allot

Details of information available that is hacked

- Version 4: Data Theft - This scheme involves the e-mail of role-specific employees in the company being compromised and then used to send requests not for fund transfers, but also for personally identifiable information (PII) of other organization employees and executives. This can, therefore, serve as a jump-off point for more damaging BEC attacks against the company itself.

Some of the incidents and scenarios are isolated and some occur prior to a fraudulent wire transfer request. Victims generally report they have fallen for these BEC scenarios, even if they were able to successfully identify and avoid the traditional BEC incidents.

All these schemes are considered very simple and generally, play out as follows:

1. The business e-mail account of a senior management employee at a business is compromised. This is achieved through malware or social engineering.
2. The scammer's research about the employees, look for travel schedules, and read other business e-mails through the compromised executive account.
3. An employee at the compromised company receives an e-mail request to transfer funds, seemingly from upper management at their company.
4. The employee, believing the e-mail to be legitimate, transfers the funds to the criminals.
5. Businesses and personnel using open source e-mail are mostly targeted by business e-mail compromise scams. In numerous cases, the attacker's spoof e-mails of people within enterprises who are authorized to submit payment requests and then send them to individuals with the authorization to process them. Employees who handle wire transfers are over and over again targeted.

Fraudsters approach to e-mail

Attackers may initiate communication with your company in a variety of ways. Nonetheless, it typically boils down to an apt one shot e-mail or a more conversational approach involving quite a few e-mails and phone calls.

The apt one shot e-mail

The one-shot fraud e-mail depends on sending the e-mail at the perfect time. Preferably, attackers time the transfer of a fraud e-mail to coincide with their target's travel schedule. The attackers may by this time have access to one or more employees' inboxes in order to pull this off. Cyber criminals lie in wait to take benefit of the most opportune time to approach the victim with a fraud e-mail. The message may come across as urgent, "I need the wire-transfer to be completed before I reach Beijing." On the other hand, it could also be more casual "I am just about to board the plane and I almost forgot we need to wire a payment to..."

In many such cases, fraudulent e-mails go undetected. After all, since the e-mails don't include malware, URLs, or malicious attachments there's no "signature" to raise an alert. It is just a simple text message from a domain with no reputation score. Occasionally messages may even include, "Sent from my iPad" or somewhat similar in the signature line to help mask poor grammar typically found in fraudulent e-mails coming from another country.

Wealth management and investment firms are also targeted with this tactic of one-shot fraudulent e-mails. In such cases, it includes aiming high net worth investors. Attackers focusing on wealthy investors, in the similar way they target senior management and C-level executives. The profiling on investors and learning about their connections primarily assists them to make a forged wire transfer request appear legitimate.

Another example of such a tactic does not necessarily ask for a wire transfer, but may ask for sensitive information in quick one-liner e-mails. For example, a fraudulent e-mail asking employee W2s under the guise of a "wage review". This type of e-mail may also target senior management executives from the Human Resources department for example, by sending a fraudulent e-mail requesting the W2s to one or more of their associates.

The conversationalist

Sometimes these scam e-mails unfold over an extended period. Through this tactic, the target could be a senior executive involved with M&A activity, new products, or even strategic partnerships. In this case, attackers create a fraudulent e-mail as the way to inform the victim about an upcoming acquisition or partnership, calling for an upcoming wire transfer. These scam e-mails generally ask for secrecy and discretion in performing the wire transfer as they show it as a top-secret business activity. Fraudulent e-mails appear credible, often citing closely held project details or company code names. In this case, the impersonator traps the victim into doing their bidding under a veil of secrecy.

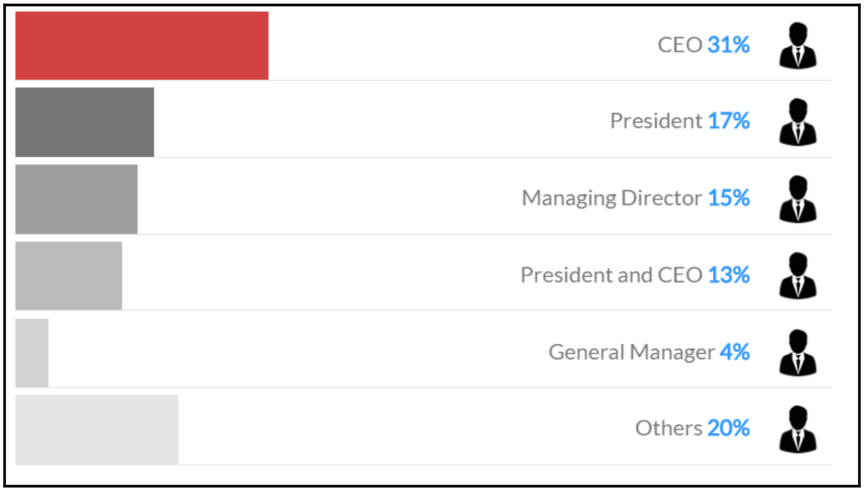
The conversationalist may possibly also imitate a supplier or dealer and start out an innocent appearing conversation about the newest invoice status. If responded, the conversation can quickly grow into changing bank account information. Every now and then, these scam e-mails contain fabricated e-mail dialogues between key executives to back-up their need for a wire transfer. If the victim doesn't catch on to the trick and the spoofed e-mail addresses and requests look legitimate enough, these fraudulent e-mails can silently draw off funds from the company over an extended period of time.

What makes the conversationalist threat bold and practical is that it often comprises a phone call to get past policies requiring verbal confirmation of payment requests. In some cases, the fraudulent e-mail may consist of contact information for a third party, for example, a person that supposedly works at the company's accounting or law firm to contact for further instructions. Contact phone numbers are then set up looking forward to a follow-up call. Attackers may preemptively call ahead of time to let the victim know the request is coming. This commonly takes place during non-work hours when an attacker may know that the target executive is abroad, in transit, or otherwise not reachable.

Which company positions are most targeted in BEC schemes

As per the analysis from leading vendors http://www.trendmicro.com, employees from businesses' finance departments are found to be the most targeted by BEC schemes. The CFO, or the chief finance officer, was found to be the most targeted as per their study. This makes complete sense, in view of the fact that these employees are most likely the ones in charge of tasks such as transferring funds to other parties.

The following figure shows the high level analysis:



Most targeted company positions by fraudsters

How to defend against BEC?

There are a number of methods to protect organizations and businesses against BEC scams and fraudulent e-mails. Businesses with an increased awareness and understanding of such scams tend to make out when they have been targeted by BEC cyber criminals, and are thus more unlikely to fall victim.

Organizations that position vigorous internal prevention techniques across all levels (especially targeting front line employees who may be the recipients of initial phishing attempts), have also been proven to be highly successful in recognizing and deflecting BEC attempts. The leading practices shared in this section are primarily based on the FBI alerts and guidelines by financial institutions who have successfully detected this scam.

This is one of the most comprehensive lists, and most organizations across industries cannot practically implement all of these suggestions, but it is recommend to implement the controls which are practical for your specific operations to decrease the risk of being victimized by this scam. At the same time while these measures are helpful, they are not a cure-all defense against the determined impersonator:

- Strengthen Internal Processes - To counter the scams and threats of this nature, organizations must bring together policies that ensure that no one person or single e-mail can authorize transactions. Instead, there needs to be a mixture of communication channels verifying any request for confidential or financial information. Consider additional IT and financial security procedures, including the implementation of multiple factors for the verification process. The internal processes and verification procedures may include the following:
- Forward e-mails and include the correct e-mail address (e-mail chain) to ensure the intended recipient receives the e-mail.
- Remain vigilant of sudden changes in business practices.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Out of Band Communication: Establishing more than one communication channel to verify important transactions. Establish other communication channels, such as telephone calls, to verify significant transactions.
- Digital Signatures: Use digital signatures on both sides of transactions.
- Delete Spam: DO NOT click on spam links or open any attachments in the spam. Spam may potentially have malware attached to an e-mail attachment that might have a large impact to the organization.
- Multi-factor authentication could be considered for corporate e-mail accounts. It mitigates the threat of a subject gaining access to an employee's e-mail account.
- One of the practices followed by some financial institutions customer requests can be put on hold for international wire transfers for an additional period of time, to verify the legitimacy of the request.

Fighting against these type of scams

- **Security awareness and training**: Training tops the list of strategies to combat against these types of scams. This can range from a friendly e-mail reminder to look twice at any payment request, to online classes designed to help employees spot a fraudulent e-mail. Typically, training includes how to examine e-mail addresses for authenticity and being aware of e-mails calling for secrecy or acting quickly.

While training should always be an integral part of a security program, adding another facet to an already long list of things that employees need to pay attention to is not very impactful. Especially, when considering these fraudulent e-mails are highly targeted to take advantage of executive travel schedules and specific knowledge about the company and personnel.

- **Authentication Standards Domain-based Message Authentication, Reporting & Conformance (DMARC), and DomainKeys Identified Mail (DKIM)**: DKIM filters out some impersonator e-mails, but not all. DMARC is a comparatively new standard and many regional ISPs are still in the planning stages of implementation, so usage is inconsistent across geographies. It also cannot protect against fraudsters using display name spoofing, similar sounding domains, or DNS servers publishing phony routing information.

  Sender Policy Framework (SPF) will cut down on some variants of e-mail spoofing, but it cannot detect impostor e-mails that come from an intentionally misspelled domain.

- **Improve Payment Verification Procedures:** Establishing mature and improved policies around payments is another way companies seek to protect themselves from fraudulent e-mails. The FBI suggests implementing a two-step verification process that includes checks via phone calls. Using encrypted e-mail with digital signatures can also help ensure employees are communicating with intended parties.

  Fraudulent e-mail requests for a wire transfer are well-worded, specific to the business being victimized, and do not raise suspicions to the legitimacy of the request. The phrases "code to admin expenses" or "urgent wire transfer" have been reported by victims of BEC scams and they should be alerted.

  Improving payment policies can definitely help, but it may not guard against the determined fraudster who sets up dedicated phone numbers for verification or reaches out to employees with authentic sounding follow-up calls. It also may fail when dealing with employees who are new, in a hurry, or have a situation that does not conform to policy guidelines. For such cases, self-assessment is to be trained to employees.

- **Multi-Layered Approach:** There is not a single solution available that can solve the breadth of the fraudulent e-mail security problem. What's needed is multiple controls - a blend of complementary solutions that provide a multi-layered approach to cyber security where prevention, early detection, attack containment, and recovery measures are considered collectively.
- Avoid unrestricted / free / potential no-pay web-based corporate e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- Be vigilant of what is posted to social media and corporate portals, especially description of jobs, organizational structure, and out of office details.
- Significant Changes: Be cautious of sudden changes in business practices. For instance, if an existing business contact unexpectedly asks to be contacted via their personal e-mail address when generally the communications are via business e-mail, the request could be fraudulent. At all times confirm via other channels that you are still connected with your legitimate business partner:
- From a security tools perspective, create an intrusion detection system (IPS) rule that flags e-mails with extensions similar to company e-mail

- Scrutinize all the requests for transfers of funds and reconfirm via previously known numbers, not the numbers that are usually provided in the e-mail request

- Through analytics and other measures, know the behavior and conducts of your customers, including the details of, reasons behind, and the amount of payments

What to do when hit by the BEC scam

The moment an organization realizes that they have been a victim of such a scam it is encouraged to communicate this to the organization's financial institution (ideally within 24-48 hours) and corresponding law enforcement. If informed instantly, financial institutions and law enforcement have potentially some time to recover the stolen funds, even if the funds were sent internationally.

Based on the preceding controls and parameters, a self-assessment questionnaire should be created and examined across business units categorizing the employee roles into Check, Confirm, and Coach. This would also assist organizations with an internal review to determine how the attack could potentially occur and if changes are needed to the processes and technologies.

Summary

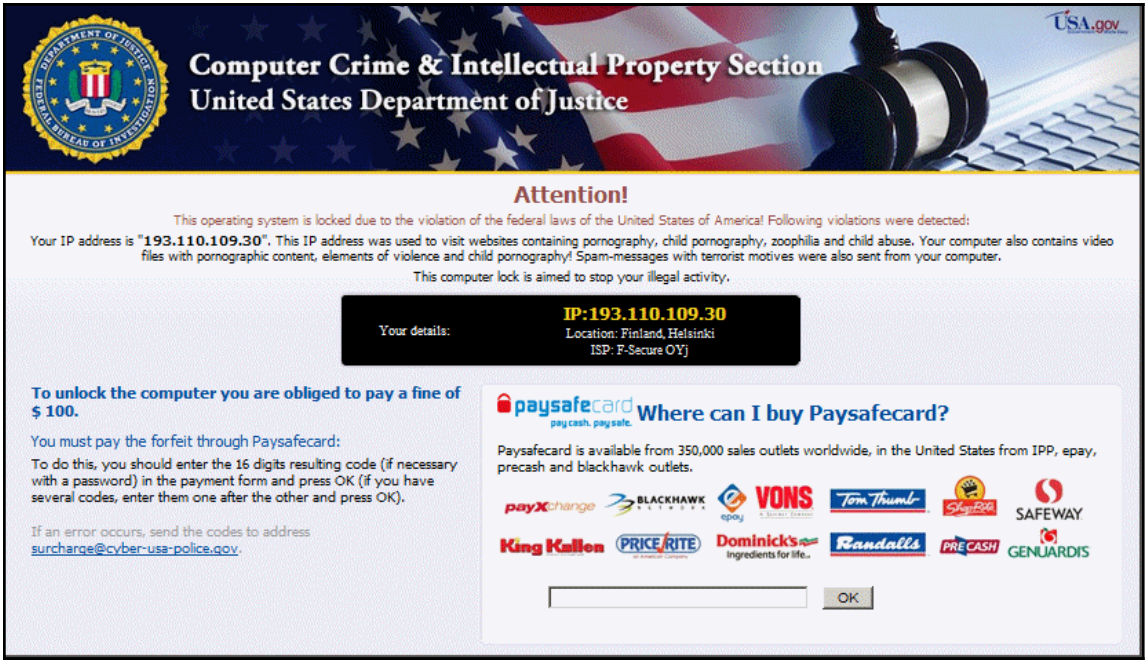
The theft of data from a user or an enterprise is serious business and can affect one in a lot of ways, from personal losses to losses of business secrets. Account theft is similarly problematic. In this chapter, we looked at ways of identifying and mitigating these attacks and looked at Business E-mail compromise, another scam that aims at stealing money from unsuspecting or confused victims.

In the next chapter, we will learn in detail about locker ransomware and how it plays on human emotions to extract money from victims.

4
Mitigating Locker Ransomware

Most of us are used to comfortably sitting in front of our computers, regardless of whether we are working or doing something in our free time. The communication process with machines has become unavoidable, automatic, almost like second nature. We like the control we have over computers, the privacy they provide, and the utmost helpfulness that we get from them in our daily lives. The relation has become so simplified, that, unless we get a new software or a new machine that we need to get used to, the process gets semi-conscious, and we get practically numb.

Imagine then the scenario, when sitting cozily in the safe haven of a computer desk, a warning sign carrying the FBI logo suddenly flashes on the screen, accompanied by a warning message with sex crime incrimination. The user is shocked to see that they are being prosecuted by the FBI, that the computer has been locked, and that the access can only be gained back in case a certain amount of money is paid to the attacker for exchange of retrieved computer access.



Computer Crime & Intellectual Property Section
United States Department of Justice

Attention!

This operating system is locked due to the violation of the federal laws of the United States of America! Following violations were detected:

Your IP address is "**193.110.109.30**". This IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

Your details: **IP:193.110.109.30**
Location: Finland, Helsinki
ISP: F-Secure OYj

To unlock the computer you are obliged to pay a fine of $ 100.

You must pay the forfeit through Paysafecard:

To do this, you should enter the 16 digits resulting code (if necessary with a password) in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address surcharge@cyber-usa-police.gov.

Where can I buy Paysafecard?

Paysafecard is available from 350,000 sales outlets worldwide, in the United States from IPP, epay, precash and blackhawk outlets.

Image: Police Reveton (Image credit: *Go Remove Malware*)

Screenplay-worthy as it may seem, this is a real-life scenario. The event is only a snip of numerous stories used by cybercriminals when they invade people's sense of privacy and strong feelings of fear, shame, and guilt to extort money by preventing computer access using lockerware.

Human conscience is the same across the planet. All ransomware is based on creating some horror or anxiety in the victim's life and locker ransomware is no different. Hackers know this fact. They just use varied means to exploit the same vulnerability in unique manners. The locker ransomware story that emerged in Russia in 2009 used pornographic images that condemned the victims by playing with their sense of shame and fear. Condemning someone with pornography is one of the easiest guilt-tripping methods - it works equally well when the victim is totally innocent of unlawful behavior. Almost anyone would rather pay several dozen dollars than face reporting the crime to the police, especially when all that is necessary is calling or sending an SMS to a premium phone number.

Shame is not the only key value that makes people susceptible to extortion. Any data kept on a computer can be held hostage and abused to force the victims into ransom payment. Nonetheless, its functionality is similar across the board.

Locker ransomware prevents computer or mobile device access by locking the manual input devices. The blockage is simple, yet functional - it is like cutting an electrical cord. When electricity has nothing to run through, the end devices cannot be used unless the cord is repaired. In a similar way, no command can be communicated or executed through the keyboard or the mouse when they are brought down to limited functionality. The victim can use the numerical keys only to type the ransom amount when, at the same time, critical computer files are held hostage as inaccessible. When the payment process is completed, the access to the data is restored.

Having in mind that lockerware is nowadays considered a less evolved ransomware variant, victims can feel relieved that, at least, the files have not been encrypted with advanced level cryptography. In general, unlike the instances of attacks by crypto ransomware, files on a computer under an attack of lock screen ransomware are not touched and are left as they are.

The technical aspects of locker ransomware may not be progressive, but the practical application turned out to be profitable. This is a crucial fact that shows why, for a prevalent number of years in the last decade, crypto ransomware was forgotten in favor of locker ransomware, which managed to overtake the initial rise of encryption methods.

In this chapter, we will investigate:

- Different stages of a lockerware attack
- Notable field cases
- Locker ransomware mitigating strategies
- Practical steps for businesses under attack

Why is lockerware a major field player?

In their paper *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks* the authors *Kharraz, Robertson, Balzarotti, Bilge,* and *Kirda* display the results obtained from an analysis of 1,359 ransomware samples of 15 different families gathered in a long-term ransomware study for the period between 2006 and 2014. To meet the representative data criteria, authors collected malware samples including lockerware, from several sources. More than a half of the data (48.38%) was collected from public malware repositories, 37.9% was collected from Anubis Networks, and the remaining 13.8 percent was retrieved by browsing through online security forums. The paper offers a comprehensive presentation of ransomware evolution for the critical eight years.

While it is essential to recognize the paramount contribution of the paper, readers must keep in mind the warning that comes from the authors when they talk about the primary use of the paper. Scientific prediction is the main tool of the purpose of research. When data collection and analysis has serious statistical limitations, it is critical to approach the end results with caution and to read them in view of the methods used. In this respect, the authors emphasize the importance of generating mitigation techniques, but also alert to the key difference between reports produced by security professionals and scientific studies. Most security reports produced by private companies are based on ad hoc scenarios and provide little, if any detailed information about defense methods.

This is a limitation that this paper tries to address by offering effective ransomware mitigation techniques.

We are particularly interested in the findings and the solutions proposed for locker ransomware families, explicitly in light of the sample size included in the total number of analyzed cases in the paper, which goes over 94 percent. Although the authors draw a conclusion that malware is in the greater part failing than it is effective, it is vital to gauge the light-headed interpretation considering the preceding limitations.

Even when the malware lacked technical attributes necessary to perform a successful attack and remained instead on the level of superficial threats that failed to keep data hostage, the failure only served as an additional motivation for cybercriminals to generate new improved versions of ransomware. There was a segment in the pool of cases that caused severe damage to victims. Having in mind the try-and-test approach used by offenders, once an effective malware sample is discovered, it can become a hot and profitable black market commodity.

The 1,359 sample sizes were distributed among 15 ransomware families with 99 variants. From the 15 families, 22.66% were **WinLock** samples, 17.95% were **Reveton** samples, and 38.48% were **Urausy** samples. WinLock and Reveton, especially Reveton, notably caused the greatest amount of damage in lockerware history by spreading worldwide and in several languages. Researchers did not fail to point out that these three locker malware families used polymorphic attacking techniques. Police ransomware is still the most treacherous lockerware, constantly adopting new infection methods.

Aside from the chief lock screen families mentioned previously, the sample included smaller lockerware groups, such as **Tobfy**, **Loktrom**, **Calelk**, **Krotten**, **BlueScreen**, **Kovter,** and **Weelsof** which showed up to be less effective. While analyzing attack types, the authors distributed the ransomware samples in four groups. Many variants used combined methods from the set of five that the researchers singled out: file encryption, file deletion, screen locking, data stealing, and MBR changes.

Although the samples were assigned to several classes, the way in which attacks were executed from a file perspective was similar across the sample. Each malicious process worked alike the next one by requesting access to similar filesystems. File deletion was immanent to the popular Reveton and WinLock, although they also undeniably locked the screen and, in the case of Reveton, stole information.

The paper provides abundant value in reference to exploring locking procedures. Regardless of the type, all ransomware samples must lock the screen and establish a persistent desktop, Although the technique is different for different variants.

Screen locking command process

A large number of the samples investigated by *Kharraz, Robertson, Balzarotti, Bilge, and Kirda* (61.22%) applied the following screen locking procedure:

1. Use the `CreateDesktop` command to generate a new desktop environment.
2. Cut off additional processes.
3. Enable the `SwitchDesktop` function to activate the created desktop and receive victim input.
4. Assign the desktop to a thread by the `SetThreadDesktop` command.

However, notable lockerware families such as **Urausy**, **Reveton**, and **Winlock** used a different screen locking method:

1. Download the lock screen as a HTML page.
2. Display the image in full screen mode in Internet Explorer with hidden controls.
3. Disable keyboard toggle shortcuts (for example, Windows key + Tab).
4. Disable special keys by installing hook procedures for monitoring keyboard input events.

In the case of Reveton, the Windows keys were disabled in order to block the victims from accessing the **Start** menu. Over 70 specific variants in the 15 examined families were aiming at disabling the Esc key to prevent the victims from accessing the Windows Task Manager.

The convenience of payment vouchers

The study analyzed the ways by which users were instructed to pay the ransom money. 88.22% of the total users were forced to purchase untraceable payment cards such as **Moneypak**, **Paysafecard**, and **Ukash**.

Anonymous payment vouchers are later sold underground through forums and instant messenger systems. As they are capped as black money, the attackers must exchange them for lower value than the actual nominal value placed on them. Few variants from the **Kevtor** family ransomware on the other hand demanded a purchase of a specific computer-unlocking software. The average cost for the victims in the sample was set between 150$ and 250$. Regardless of the way the money was extorted, lockerware was extremely practical, as demonstrated both by the study and by abundant emergences across the globe.

Reveton - when the police locks your screen

The fact that it is classified as less evolved by cybersecurity professionals does not make lockerware any less dangerous in terms of reach and financial benefit for criminals. In the *Police Ransomware - Threat Assessment* public document from 2014 **Europol** reports of significant ransomware profits concerning **Reveton**, the ultra-lucrative advanced-level locker variant that had been persecuted and handled by join action of European law enforcement agents.

On several occasions in this book we have emphasized that it is difficult to evaluate and draw conclusions from ransomware statistics due to the fact that the cybercrime area is distinguished by underreporting. Still, certain prognosis can be made. Overall collected numbers pertaining to Reveton go up to a global profit of *one* million euros per year. In the Threat Assessment paper, Europol affirms that around three percent of the targeted victims have actually paid the ransom.

An operation led by Europol that tackled a complex cybercrime network over the last couple of years gave an idea of the powerful success behind Reveton. In a series of organized incidents, tens of thousands of computers were reached on a global level, collecting over million euros each year. On a different occasion, cybercriminals attacked over 25,000 computers in eleven European countries and accumulated over 70,000 euros from 800 people who decided to pay the ransom. The actual 70,000 euros got laundered on the black market for an exchange value of 40,000 euros.

From delivery to execution

Ransomware works in complex ways. The affected devices, the encryption technologies, the payment methods, and the scare tactics are mixed in various ways so that no single ransomware type incorporates the same attributes in the same way. Cybercriminals are ever-creative and relentlessly search for new vulnerabilities that can bring the greatest profit with as little risk as possible.

Although there are minor peculiarities to how lockerware emerged and evolved in varied historic scenarios, several general characteristics promote it and keep it tight into a special ransomware family. The scare tactics employed by lockerware work with screen locking, while the payment method is usually an SMS or a call to a premium rate phone number. Additional means of payment are the hardly traceable payment vouchers issued in specific countries, such as MoneyPak, Paysafe, or Ukash. Known targeted devices include Windows and Android software, whereas the encryption technique is simple and is executed by a 660-bit and 1024-bit algorithm.

The main target of lockerware variants like Reveton were workstations of individual end users. Businesses were excluded, assumedly because of the nature of the cybercrime that works best when an individual faces shame, fear, and guilt alone or because of the stronger defensive approaches undertaken by businesses and organizations in general. Nevertheless, lockerware needs to pass the conventional malware cycle stages to reach its targets - delivery, payload, infection, and execution.

In previous chapters, we have demonstrated versions ways by which ransomware can target users. The means are diverse, but they always accrue intertwined actions in the delivery-payload-infection system and they regularly include the fear component. Malicious websites, payloads by other malware carriers, spam e-mails, malvertisements, or vulnerability exploits compose just a fragment of the actions by which lockerware, once executed, locks the computer screen, blocks file access, and presents a flashing screen message demanding ransom payment and presenting instructions on how to actually complete the transaction. Unlike previous classic malware variants, which worked undercover stealing information, locker and crypto-ransomware are quite blunt directly informing the user of the infection. **Lockerware** is an open attack, which cannot be more open: it comes right in the front of the screen demanding immediate attention.

Lockerware delivery

To spread, ransomware must have an initial point of attack through external channels. Delivery encompasses clickbaiting or seemingly legitimate browsing actions. Lockerware is usually downloaded by accident, when users have no idea that they are downloading wrongful material until the malware starts creating problems. User behavior that can invite and trigger harmful attacks includes:

- Visiting compromised or malicious websites
- Opening an e-mail attachment
- Clicking a phishing link
- Downloading a payload carrier from another software
- Opening a malicious ad

A few of the delivery channels, such as malvertising, are very difficult to prevent. Other variants work very hard by exploring and exploiting host vulnerabilities until they discover a weak spot that is later used to take over authority and infect the host.

Payload carriers

Payloads are the concrete carriers of the malicious code. Another name by which they are known is droppers. Carriers or droppers are small files that, downloaded without giving a hint that they are corrupted, instigate the infection by simultaneously downloading the executable ransomware and holding data hostage. The files involved in a payload carrier can be as common as an infected Microsoft Word document or a corrupted e-mail attachment.

Infection spreading

There is no pause between the payload and the infection stages. When the carrier has been loaded on the user system it either instantly spreads the infection or gets activated by building a communication channel to the "command and control" server, which is used to establish contact with the victim and notify ransom payment instructions. Due to its anonymity and the possibility to hide computer locations by hoodwinking IP addresses, the prevalent communication option for cybercriminals is the **Tor** (**The onion router**) network.

Lockerware execution

Locker ransomware starts executing by searching for previously assigned extensions. While certain lockerware instances have specifics regarding execution, most types of malware usually search all system drives and attached removable-storage media. However, while the crypto ransomware will search and encrypt system files, locker ransomware targets only the input interface devices and keeps user system files safe and sound. In this case, restoring system files to the original condition does not require a lot of effort. Once the ransom is paid, the user gets normal access to the keyboard and the mouse. However, there are combined instances of lockerware that apply simple encryption and delete certain types of files.

Desktop locking techniques

It does not come as a surprise that locker ransomware has used inventive attacking strategies and managed to find new ways to propagate, encrypt files, exfiltrate end user information externally, and avoid being detected. Infection, propagation, and scaring techniques have not come short. Locker ransomware is famous for using a persistent desktop message that is displayed on the victim's screen right after infection.

The message screen contains the ransom notice generally constituted of two parts, one of which is the actual extortion note, and another which provides payment instructions. The locker ransomware message can be created by using various methods. A common way is through dedicated API functions. By using API functions a new desktop is created which becomes the default configuration and locks out the victim out of the compromised system. An often applied lockerware alterative is using HTML or additional techniques that generate persistent windows to display the ransom note.

In the end, unless lockerware brings back the money invested in the longer run, it may be interesting short-term, but financially infeasible for cybercriminals who want to make profits on long-term basis. This is why ransomware is continually updated to precede anti-malware software and adjusted to fit the needs of different end users by using customization completed in underground forums.

Stages of lockerware development in action

The simple, Although scary ransom message takes a lot of preparation, planning, execution, and protection work, which needs to be completed before the attacks get initiated. Cybercriminal groups use contacts with the black market to purchase and set up the necessary elements for launching the attacks. A very insightful observation of the works of lockerware was conducted by the team of **Europol** security specialists who worked along several national law enforcement agencies to tackle the aforementioned advanced Reveton emergence from 2012. Offenders not only take care to prepare, but also must foresee the future by thinking of ways to cover traces of payment transactions and develop money laundering schemes.

Infrastructure preparation

Before the ransomware attacks take place attackers must establish an infrastructure. Establishing an infrastructure consists of a series of actions that depend on the type of executed malware, but it normally includes five steps:

- Generating hosting servers for the malware and exploit kits, as well as images for the locker screen
- Creating scripts to define the victim's country of origin and drop zones for the voucher codes
- Setting up several additional C&C servers and spare server paths as redirects
- Renting and registering a batch of replaceable hosting domains with similar names to host the malware and the compromised websites that communicate the malware
- Upgrading the hosting to an invulnerable level through proxies, globally distributed servers, double VPN, fast flux, or instant messaging

Exploit kits

To deliver the attacks, perpetrators must use exploits, usually as **exploit kits**. Usually hosts to malware and exploit kits are compromised computers that are arranged to act as drop zones for balancing accounts or for cashing out the voucher codes.

Traffic redirection

When the infrastructure is set the offenders lure the victims into clicking compromised websites through **traffic redirection**. It is not at all simple to hack a regular functional website. Outdated software doubles-up the vulnerability risk. When Java, Flash, or Adobe Reader plugins are not regularly updated they serve as a lockerware invitation. Europol reports of prominent online shops or news websites that are being used for traffic redirection to malicious sites hosting ransomware. A usual way to find extortion victims is by using malvertisements as a proxy and by buying redirects from "traffickers" who sell the redirects by piece.

Spreading the infection

Victim's systems can be infected in several ways. Regardless of the actual way it is distributed, the infection normally starts quietly, without the victim's knowledge. Only later, when the attack is launched, the victim wakes up to the reality of the situation. The infections can be delivered through:

- Drive-by downloads coming out of malicious websites or advertisements, often those hosting pornographic material
- Spam e-mails with compromised attachments or website links
- Pirated content, such as music, movies, and software downloaded file sharing websites
- Corrupted files from social networking websites, instant messaging apps, and video sharing websites

In the Reveton story, users who fell victim to the attack and decided to pay the ransom money to get back the access to the computer and the data paid an amount between 50 EUR and 150 EUR or the actual national currency equivalent value. In many cases the payment did not guarantee normal computer access for the victims. Computer screens still remained locked and the victims had to ask for professional assistance to remove the lockerware.

How to cash out - money laundering techniques

When the screen is locked, it is impossible to transfer money through online payments using the same computer. Therefore, extortionists have thought of an alternative way to monetize the crime by using prepaid online payment solutions that cover the money trail and cannot be traced back to the criminals. The flashy locked screen always contains payment instructions advising the victims to purchase a voucher. The voucher card contains a multi-digit code that can be inserted in the pop-up window on the screen. Solutions like payment vouchers are not only convenient for offenders, but are also user-friendly, as they are available for victims in a specific national variant at nearly every corner. European-located variants include **Ukash** and **Paysafecard**. The screen payment instructions usually include locations of retailers, ATMs, kiosks, and petrol stations in the victim's country of origin.

As expected for situations in which the profit comes from illegal sources, it is impossible to cash in large or even smaller amounts of unlawfully collected money without becoming suspicious. When the ransom money gets laundered through specialized laundering services, it usually decreases in value down to 50 percent of the nominal value of the payment vouchers. The laundering agents use varied inventive techniques to cash out the money and pay the profits to the extortionists:

- Loading the funds from the vouchers on compromised credit and debit cards, using money mules to withdraw the cash from ATMs, and wiring back the cash minus the commission to the offenders
- Selling the vouchers at 50% discounted rates for electronic money through illegal exchange websites
- Cashing out the payment voucher codes through online gambling platforms, betting, and casino websites

Details from one specific operation conducted by Europol disclosed that by using several different money laundering schemes, an amount of 10,000 EUR per day was laundered just from one organized group that dealt with police ransomware. The money laundering groups employ money mules distributed across locations around the world. The money mules use a number of accounts and fake IDs to launder the money. Fake accounts are executed through digital currency wallets, gambling platforms, money exchangers, and electronic money mediators.

The advancement of locker ransomware - Winlock

When ransomware started to rise in 2005, it initially used encryption techniques. We have already mentioned the **GPCoder** and the **Trojan.RANSOM,** which used simple encryption. However, by 2010, several instances of malware based on locked screens bolstered lockerware to the prime position. It all started in Russia, where a dozen of members of an organized cybercriminal group worked in unison to attack thousands of computers in Russian and other Slavic language-speaking countries by using pornographic images scareware tactics. The malware was named **WinLock** and the lucrative business model ended when the Russian authorities closed the extortion operation by arresting a group of ten cybercriminals.

> The members of the organized gang that were arrested in August 2010 used WinLock to lock a victim's screen with a ransomware message containing pornographic images and demanding users to send a premium-cost SMS in amount between 300 and 1,000 rubles in order to unlock the computer screen and gain control over the computer. The minimal cost in the range at the time equaled to $9.72 and it allegedly earned the cybercrime gang an amount as high as 16 million USD. The scam was perpetrated in Russia, Ukraine, Moldova, and Belarus. It became very popular in the period until the gang members got arrested and charged, and the computer equipment got seized.

WinLock namely spread through malicious news sites, made certain elements of the Windows operating system dysfunctional, and then displayed the ransomware message. Although it was financially very lucrative for its creators who thrived on the ignorance and lack of experience of naïve users, it was considered a less advanced malware by security experts.

Basically, the user screen gets locked with an unknown password when the Trojan starts the infection sets on auto-run through registry keys. The lockerware then disables the task manager and blocks specific tools from normal functioning. Users are interrupted from doing any regular work and the annoying ransomware pop-up window gets continually reproduced while the message with the pornographic images flashes on the uppermost window.

In 2011, the basic Trojan variant from 2010 was upgraded to emulate the highly criticized Windows Product Application. Through the fake reactivation kit, the ransomware informed users that they need to reactivate the installation due to previous fraudulent installation. The new online activation actually demanded from the victims to call an international number from a list of six options and enter a six-digit code. The fake re-installation package claimed that the calls are free, but that was never the case. Instead, the calls were rerouted to a premium-rate international number, which increased the charges by putting the users on hold.

By 2013, police ransomware has already evolved in multiple lockerware variants, whereas recent emerging cases include complex encryption techniques. Along with Reveton, offenders worked on a new Trojan-based spam campaign that used malware allegedly hosted on the open-software platforms **SourceForge** and **GitHub**. The malware was based on the **Stamp.EK** exploit kit and was spread through projects hosted on the sites claiming to provide fake celebrity nude pictures and YouTube videos.

The malware detected as **Trojan:Win32/Reveton** stands out for its specific infection techniques spread through obscene images taken from a pornography site, as well as fake air rifle stores and Windows for Dummies sites. Even Twitter pages were included among the droppers. The SourceForge and GitHub ransomware variants involved not one, but several sub-variants that either locked the screen or additionally encrypted files demanding ransom payment through coded vouchers. One example locked the computer desktop with a black screen stating that it originates from the US Department of Justice that has assumedly blocked the computer use due to the user being engaged in federal law violations, specifically child pornography, illicit software use, and copyright infringement. The blocking screen also included a notification that a video recording is on.

Although it is inconceivable how anyone would think that the law enforcement could use these tactics to implement legal measures, the malware seemed to work. It scared the victims into payment of $300 through the MoneyPak vouchers. As usual, the ransomware gave detailed instructions about locations for purchasing the vouchers including Walmart, Kmart, and Rite Aid. Additionally, a timer was ticking out raising the pressure by announcing immediate initiation of a criminal procedure unless the ransom money is paid before the 48-hour deadline expires.

The attacks launched through SourceForge and GitHub have a lot in common with the noteworthy advocate of locker ransomware Reveton, although the differences in execution.

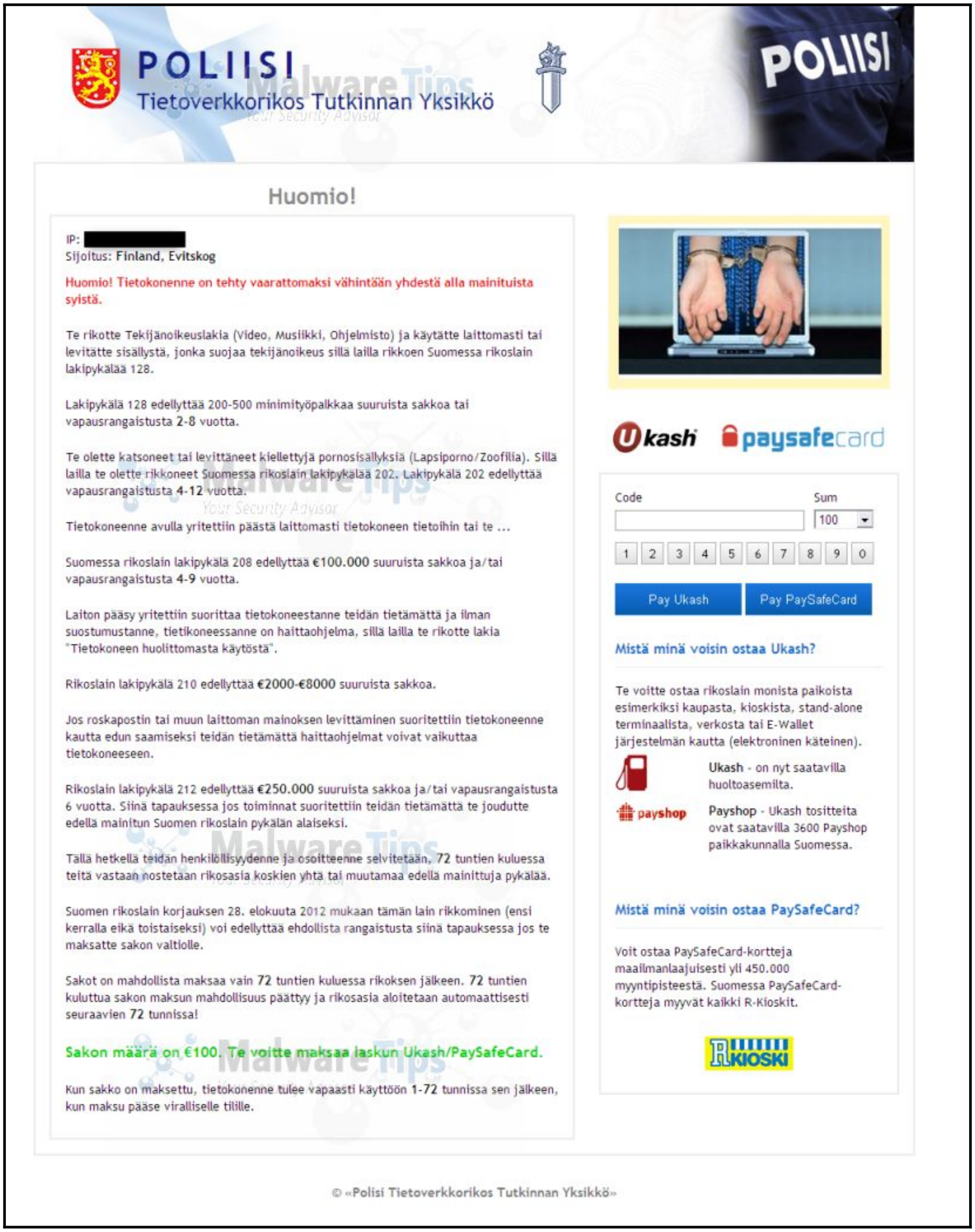
The latest known emergence of the police ransomware was shaped in 2014 and has already spread way further than the country or origin - Russia, targeting victims in Northern and Western Europe, not leaving US citizens out. In the beginning, Reveton's object of desire were Windows end users, but recent instances include OS and Android users.

Reveton takes over the world

The spread of Reveton from 2012 onward was momentous. Its "policing" methods not only took over countries in Europe, but had compelling success in the US and Canada, too. The ransomware attacked using the same intimidation tactics such as unlicensed software, child pornography, and the user IP address being displayed on the locked screen, while applying original methods in specific situations. To localize the attacks, hackers adjusted the lock screen templates with logos from the national law enforcement agency of the country in question. A French macarons confectionery `Laduree`, whose website was attacked with a variant of the police ransomware claiming to execute an action by the *Gendarmerie nationale,* the French police force. On the other hand, the UK scenarios included logos from the Metropolitan Police Service, or in a sophisticated and precise version, a logo from the Police National E-Crime Unit. In another UK scenario, victims were scared with copyright infringement notification that comprised of a logo from the leading UK royalty collection society *PRS for Music Limited* and an accusation of illegal music download.

The ransomware was customized to the US by placing the FBI logo on the display screen and by asking for a $200 ransom payment completed through theMoneyPak prepaid voucher card. Although the police incessantly worked and several arrests were made worldwide, the black Reveton market was active and by 2014 came out with a payload method which, in addition to the lock screen method, contained complex attacking techniques such as password stealing malware.

The Reveton ransomware story did not circumvent the Finnish either. As usual, it was claiming to come from the Finnish police and it was translated into Finnish language. The screen notice included the text "*Tietoverkkorikosten tutkinnan yksikkö*", which in Finnish means *Information Networks Crime Unit*. This particular police ransomware worked by expanding the Internet Explorer browser to full screen and presenting a message from the national police of Finland with allegations of the user visiting illegal websites or sending illegal spam messages. The charges referred to sites containing animal and child abuse or to e-mails on the subject of terrorism. The story worked despite the shaky fact that the Finnish police does not have the aforementioned department at all. Additionally, the language quality was barely acceptable and the contact address was registered to *cyber-metropolitan-police.co.uk* and the domain was registered in Poland to a person with a false identity called Mr. "be happy". There were many wavering facts, yet victims fell prey.



POLIISI
Tietoverkkorikos Tutkinnan Yksikkö

Huomio!

IP: [redacted]
Sijoitus: **Finland, Evitskog**

Huomio! Tietokonenne on tehty vaarattomaksi vähintään yhdestä alla mainituista syistä.

Te rikotte Tekijänoikeuslakia (Video, Musiikki, Ohjelmisto) ja käytätte laittomasti tai levitätte sisällystä, jonka suojaa tekijänoikeus sillä lailla rikkoen Suomessa rikoslain lakipykälää 128.

Lakipykälä 128 edellyttää 200-500 minimityöpalkkaa suuruista sakkoa tai vapausrangaistusta **2-8** vuotta.

Te olette katsoneet tai levittäneet kiellettyjä pornosisällyksiä (Lapsiporno/Zoofilia). Sillä lailla te olette rikkoneet Suomessa rikoslain lakipykälää 202. Lakipykälä 202 edellyttää vapausrangaistusta **4-12** vuotta.

Tietokoneenne avulla yritettiin päästä laittomasti tietokoneen tietoihin tai te ...

Suomessa rikoslain lakipykälä 208 edellyttää **€100.000** suuruista sakkoa ja/tai vapausrangaistusta **4-9** vuotta.

Laiton pääsy yritettiin suorittaa tietokoneestanne teidän tietämättä ja ilman suostumustanne, tietikoneessanne on haittaohjelma, sillä lailla te rikotte lakia "Tietokoneen huolittomasta käytöstä".

Rikoslain lakipykälä 210 edellyttää **€2000-€8000** suuruista sakkoa.

Jos roskapostin tai muun laittoman mainoksen levittäminen suoritettiin tietokoneenne kautta edun saamiseksi teidän tietämättä haittaohjelmat voivat vaikuttaa tietokoneeseen.

Rikoslain lakipykälä 212 edellyttää **€250.000** suuruista sakkoa ja/tai vapausrangaistusta 6 vuotta. Siinä tapauksessa jos toiminnat suoritettiin teidän tietämättä te joudutte edellä mainitun Suomen rikoslain pykälän alaiseksi.

Tällä hetkellä teidän henkilöllisyydenne ja osoitteenne selvitetään, **72** tuntien kuluessa teitä vastaan nostetaan rikosasia koskien yhtä tai muutamaa edellä mainittuja pykälää.

Suomen rikoslain korjauksen 28. elokuuta 2012 mukaan tämän lain rikkominen (ensi kerralla eikä toistaiseksi) voi edellyttää ehdollista rangaistusta siinä tapauksessa jos te maksatte sakon valtiolle.

Sakot on mahdollista maksaa vain **72** tuntien kuluessa rikoksen jälkeen. **72** tuntien kuluttua sakon maksun mahdollisuus päättyy ja rikosasia aloitetaan automaattisesti seuraavien **72** tunnissa!

Sakon määrä on €100. Te voitte maksaa laskun Ukash/PaySafeCard.

Kun sakko on maksettu, tietokonenne tulee vapaasti käyttöön **1-72** tunnissa sen jälkeen, kun maksu pääse viralliselle tilille.

Code
Sum
100

1 2 3 4 5 6 7 8 9 0

Pay Ukash | Pay PaySafeCard

Mistä minä voisin ostaa Ukash?

Te voitte ostaa rikoslain monista paikoista esimerkiksi kaupasta, kioskista, stand-alone terminaalista, verkosta tai E-Wallet järjestelmän kautta (elektroninen käteinen).

Ukash - on nyt saatavilla huoltoasemilta.

Payshop - Ukash tositteita ovat saatavilla 3600 Payshop paikkakunnalla Suomessa.

Mistä minä voisin ostaa PaySafeCard?

Voit ostaa PaySafeCard-kortteja maailmanlaajuisesti yli 450.000 myyntipisteestä. Suomessa PaySafeCard-kortteja myyvät kaikki R-Kioskit.

© «Polisi Tietoverkkorikos Tutkinnan Yksikkö»

Image: Police ransomware in Finland (Image credit: `Malware Tips`)

The Finnish malware was **W32/Ransom family Trojan** variant spread by a Java runtime exploit or by Adobe Acrobat PDF reader exploit. The cybercriminals demanded the ransom to be paid by **Paysafecard**, a payment voucher sold at Finnish kiosks and applicable online for safe and untraceable payment transactions.

Modern variants of police ransomware

Some of the most common variants of police ransomware include:

- Trojan: W32/Reveton
- TROJ_REVETON.SM4
- TROJ_REVETON.SM6

The US variant proposed a new infection method. Instead of arriving as an `.exe` file, it comes in as a `.dll` file. Once this Reveton variant installs, it works by creating files on the user operational system. The created files are different for different Windows versions:

- For Windows XP the command is the following:

```
%USERPROFILE%\Start Menu\Programs\Startup\[reveton_filename].dll.lnk
```

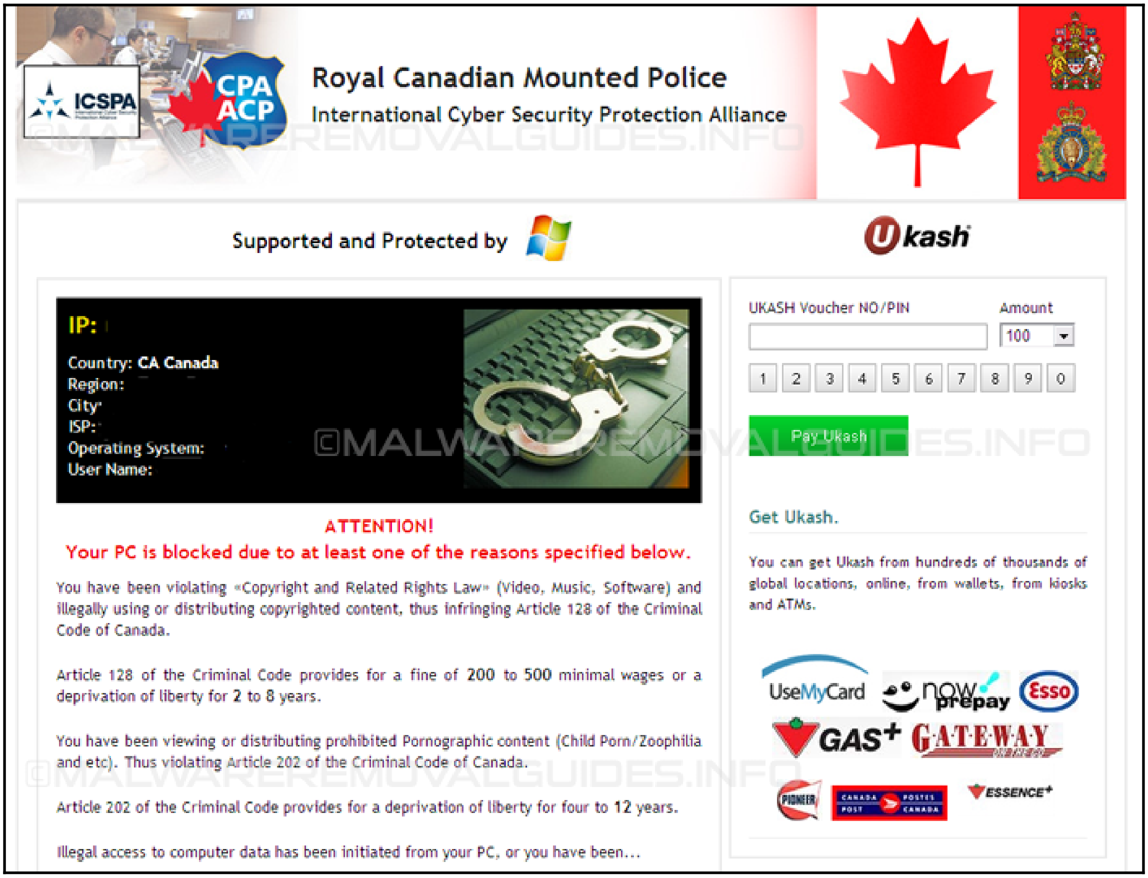
- For Windows 7 the command is the following:

```
%USERPROFILE%\AppData\Roaming\Microsoft\Windows
\StartMenu\Programs\Startup\[reveton_filename]dll.lnk
```

Recent Reveton malware variants are well-covered in the Windows Task Manager since the file extensions are not visible in their real form. They can be seen as `regsvr32` or `rundll32`, *a common way of running* `.dll` files as program files.

`TROJ_REVETON.SM4` and `TROJ_REVETON.SM6` were by far the most successful in the US, additionally reaching several European countries and even going as far as New Zealand and Australia.

In the *Smart Protection Network datasheet,* Trend Micro reports that 62 percent of the attacked users were from the United States. The second place was taken by Australia with 13 percent. Germany and Canada followed by 7 and 6 percent respectively, while Italy and New Zealand had a fair share of 2 percent each in the total numbers. The United Kingdom, Belgium, the Netherlands, and Switzerland are worth mentioning, each of the countries holding one percent of the whole.



Royal Canadian Mounted Police

International Cyber Security Protection Alliance

Supported and Protected by

IP:

Country: CA Canada
Region:
City:
ISP:
Operating System:
User Name:

ATTENTION!

Your PC is blocked due to at least one of the reasons specified below.

You have been violating «Copyright and Related Rights Law» (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 128 of the Criminal Code of Canada.

Article 128 of the Criminal Code provides for a fine of 200 to 500 minimal wages or a deprivation of liberty for 2 to 8 years.

You have been viewing or distributing prohibited Pornographic content (Child Porn/Zoophilia and etc). Thus violating Article 202 of the Criminal Code of Canada.

Article 202 of the Criminal Code provides for a deprivation of liberty for four to 12 years.

Illegal access to computer data has been initiated from your PC, or you have been...

Get Ukash.

You can get Ukash from hundreds of thousands of global locations, online, from wallets, from kiosks and ATMs.

Reveton variant related to the Royal Canadian Police (Image credit: `Malware Removal Guides`)

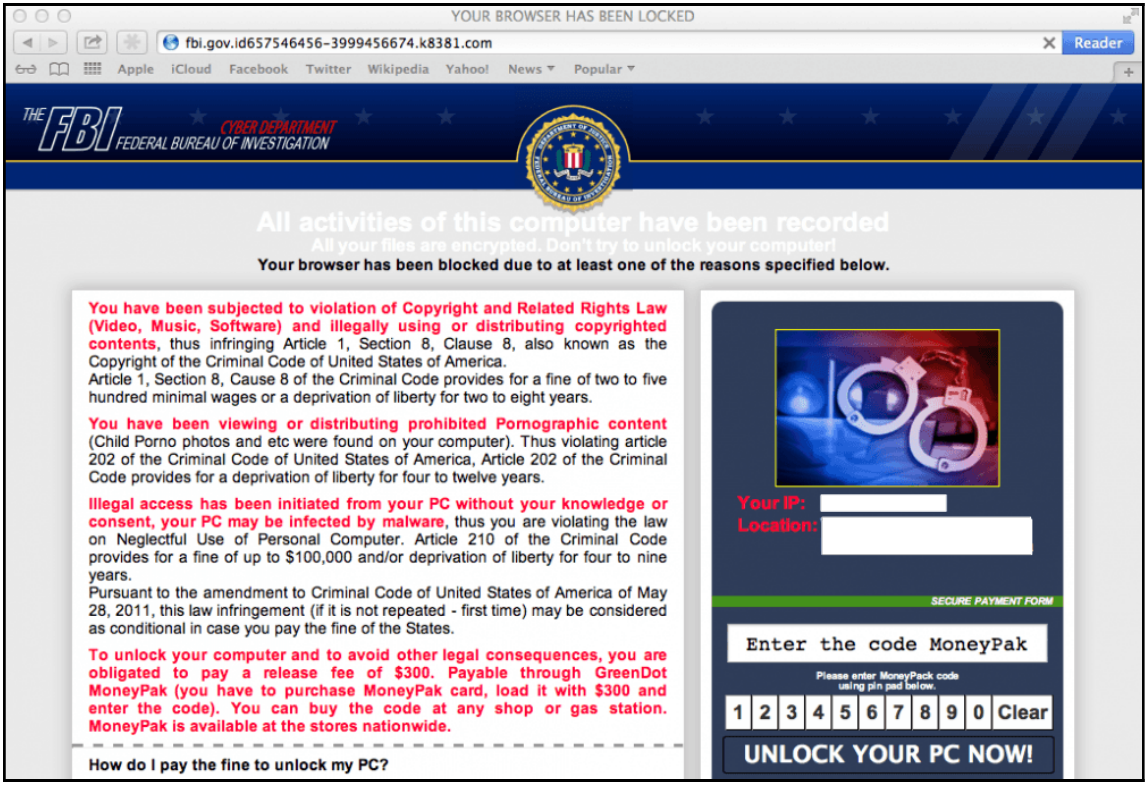
Although the actions undertaken by the malware are akin to the previous variants, the one that targeted current users displayed a warning message from the Homeland Security National Cyber Security Division and from the ICE Cyber Crime Center. In the usual manner, the text of the message stated that the computer had been locked due to the user being engaged in illegal cyberactivity, and must therefore pay a MoneyPak card ransom of the amount of $300 USD within 48 hours.

Reveton was getting reshaped and transformed in parallel with the evolution of ransomware in general. It started infecting mobile devices, the remaining operating systems, and got strengthened by advanced encryption. At a later stage, the more complex malware applied the screen-locking technique, such as the one seen in the Backdoor MBR wiper ransomware that attacked several South Korean banking institutions through the "fake website" browser technique and causing significant damage to the system by wiping out certain files in the Master Boot Record.

Reveton strikes against OS X

The threat that surfaced against OS X software in 2013 had the similar blueprint as the Trojan Reveton that scared victims with accusations of pornography. However, this concrete ransomware did not perform the usual lock screen attack, but actually loaded onto the web browsers and blocked normal page closure.

The attacks were executed exploring a feature in the Safari browser, in situations where the users searched for popular keywords or visited high-traffic websites. The fake URL that was trying to lure users into the ransom trap was `fbi.gov.id657546456-3999456674.k8381.com`. Obviously, hackers have not grown tired of abusing the FBI name, which strikes a frightening chord in most users, especially when accompanied with the typical shaming message about child pornography. The release ransom amount for the OS X malware was set at $300.



All activities of this computer have been recorded

All your files are encrypted. Don't try to unlock your computer!

Your browser has been blocked due to at least one of the reasons specified below.

You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.
Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or deprivation of liberty for four to nine years.
Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.

How do I pay the fine to unlock my PC?

Your IP:

Location:

Enter the code MoneyPak

Please enter MoneyPack code using pin pad below.

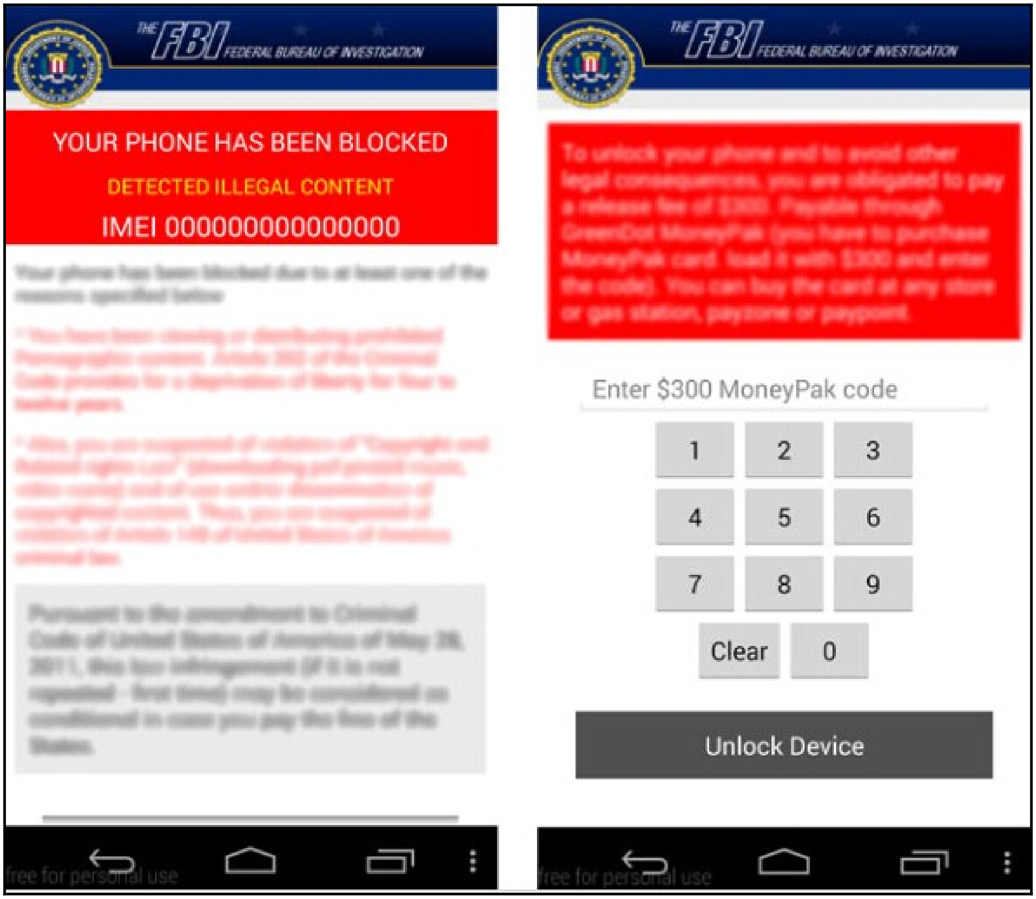
Classic FBI Reveton attacks the Safari browser (Image credit: `Digital Trends`)

The "restore from crash" features incorporated in the Safari browser are actually all throughout the works of the ransomware. When Safari is restarted from a malware attack, it goes back to the last visited page following the command in the "restore from crash feature". The user is left powerless, unable to initiate the "leave page" or the "force quit" commands to close the page. Ignoring the message does not do any good and so the vicious ransomware cycle perpetuates unceasingly.

Android.Lockscreen

A key notion that each Android user needs to contemplate before getting a new application from Google Play concerns the permissions that a specific software requires to install itself. In the thrill of the new app, users rarely investigate the needed permissions thoroughly and just go for the **Install** button recklessly, leaving an open door for malicious attacks.

Although locker ransomware falls second place when compared to cryptoware on Windows systems, it holds the gold medal for mobile devices. Most people are almost lost without their smartphone as the device holds important contacts and files needed daily. Due to its size and convenience, having it locked by an annoying lock screen malware is worrisome and frustrating. Cybercriminals understand that a ransom can be paid fast when communication becomes necessity. Thus, the emergence of **Android.Lockscreen** ransomware that targets mobile users should have been almost expected, if not predicted, and constantly fought against with software updates and bonus defense measures.



YOUR PHONE HAS BEEN BLOCKED

DETECTED ILLEGAL CONTENT

IMEI 000000000000000

Your phone has been blocked due to at least one of the reasons specified below

* You have been viewing or distributing prohibited Pornographic content. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

* Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, etc) and of use and/or dissemination of copyrighted content. Thus, you are suspected of violation of Article 148 of United States of America criminal law.

Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

To unlock your phone and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the card at any store or gas station, payzone or paypoint.

Enter $300 MoneyPak code

Image: Android Lockscreen (Image credit: `Yoocare blog`)

It all started very simply. The device got infected through compromised links and third-party applications, whereas the malware generated a new random PIN code to lock the user out of the device, present a screen message with the instructions to call technical support, and pay the ransom through the delivered service. The simple ransomware scenario made the resolution as easy as the infection, as the new custom PIN was already included in the source code of the launched malware. When cybercriminals got their lesson and learned from their mistakes, a new improved version came to light. The newest Android.Lockscreen included a feature for generating a limitless number of pseudorandom PIN codes.

This was the point when the lock screen ransomware for Android turned finally infeasible and started to create real problems for Android users. In addition to the pseudorandom numbers creation, the new malware overtook the device admin privileges. The first step of the infection was executed through the `Math.Random()` function. In this way, attackers adopted 6 to 8-digit numbers to replace the regular codes. As each phone generates a new code series, the codes become almost unbreakable once the malware hits. The second step abuses the phone administrator role to update the current PIN and presents a system error on the screen urging the victim to get in touch with the hackers and ask for a new code. Victims were unable to use the phone and were left only with two possible alternatives - waiting for repair and paying the ransom money.

ANDROIDOS_LOCKER.A - a new name with the same tactics

The ANDROIDOS_LOCKER.A is a ransomware variant that was downloaded through a specific URL hosted in two separate IP addresses in the U.S. and in the Netherlands. Normally, users got hooked up by the URL name that includes the word "porn". This malware activates once the device is in use unlocked. It tries to install its own user interface as the first screen that the user sees, thus preventing the user from uninstalling the malware UI since that is the only UI that they have access to. The antivirus feature is also hidden by the malicious interface. The ransomware performs code analysis of the attacked device and tries to connect to a number of URLs running pornographic content, which work as its C&C servers.

The best way to guard against Android malware is prevention. As mobile devices are highly personable, the user has major personal responsibility in adhering to some of the caution tips and rules that save a lot of trouble down the road. This critical process must always include regular software updates. Outdated software is one of the barest vulnerabilities that makes a device appealing to attackers. This is where they strike first. The second best tool for a safe device, aside from keeping up with the updating prompts, is avoiding untrustworthy application stores and dubious links. A provider reputation can be evaluated by the type of permissions requested when a new installation needs to be completed. As in the case with the ANDROIDOS_LOCKER.A ransomware, malicious applications require screen-locking permissions, as well as a permission to change device settings or overlay messages. Asking for that type of control over the device command is a surefire sign that something weird is happening and that the installation should be avoided.

Best practices for mitigating Lockerware

Coming up with solutions to defenses from malware has been on the forefront of the minds of security specialists. As ransomware develops, so do mitigation tactics. Many of the defense mechanisms come under the common ransomware mitigation umbrella. Having in mind that different families perform attacks in similar ways, this is not unusual.

Nothing can act as effectively against malware infections as raising user awareness and providing adequate education. In the end, it is the end users who stand in the first line of attack and are the key players that can undertake protection measures by practicing healthy online regimen to avoid attacks. The danger here has an emotional background and comes from the numbness that takes over once a user sits in front of the computer we mentioned at the beginning of this chapter. It is not that the dangers are unknown. It is more a question of acting upon emotional impulses when clicking links or opening e-mails with enticing content.

Another risky behavior that needs to be brought to light is negligence, or, more precisely, inertia. It can be summarized with a metaphor from the popular US television show "Last Week Tonight". In a notorious episode the host John Oliver discusses computer password security with his guest Edward Snowden. Upon presenting several unsafe password versions, Oliver finally comes up with a version that Snowden supports. A good password, as Snowden says, is a personalized phrase that cannot be easily randomized by a computer. However, it is the final sentence by Oliver that explains why people fall victims to cybercrime. He says that, although he now knows all password safety aspects, he is still not going to actually change the password once he opens up his computer. He is just not going to do it, he confirms. People just do not do that because of forgetfulness and sometimes, because of pure downright laziness.

Science verdict - three advanced malware mitigation strategies

While *Kharraz et al.* conducted the long-term study (*UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware*) from 2015, they did it with the idea of discovering and analyzing the technical facets of malware mitigation strategies by observing the behavior of known ransomware families. The purpose was not only to describe how attacks were executed, but to do it exactly with the idea of fighting against the menace.

Here, we abstract and discuss three advanced strategies referring yet not limited to detecting locker ransomware, delivered as a result of the longitudinal study for the period from 2006 to 2014.

API call monitoring

This strategy comes as a natural outcome of the attacker's preferred tactics to use Windows API functions in a large proportion of lock screen samples. The primary purpose of these tactics is to lock the attacked user's desktop. Although it is not a new approach, API call monitoring can help tackle ransomware attacks with little technical investment. When applying the strategy, the `GetThreadDesktop`, `CreateDesktop` and `SwitchDesktop` command series can be translated into a series of API calls and allethroughte malware detection. Offenders can evidently acquire an advanced approach by using native APIs for direct system locking. The effort in this type of locks is however cumbersome as the native APIs require specific documentation and thus limit the scope of the screen locking attack. Each new native API could change in different versions.

Monitoring filesystem activity

File encryption or file deletion as part of the lockerware attack can be completed through the **Master File Table** (**MFT**) when it is monitored for malicious activity. A ransomware attack always creates some key status changes in the MFT within very short periods. This reflects in entries of the deleted files executed in the Master File Table. Alternatively, MFT entry files with encrypted content do not possess the same system path such as the files within the directory. The difference is in the file `$DATA` attribute.

In this way, malicious MFT entries, regardless of whether they are producing deletion or encryption can be classified as separate from benevolent MFT entries by delivering appropriate training to the classifiers who can isolate the differences between the "good" and the "bad" MFT entries.

An additional method to separate benevolent and malevolent system activity involves monitoring all the filesystem requests created by user-mode processes. When the user system is designed in such a way that it incorporates adequate system protection, all corrupted requests can be eliminated before they get to the driver.

The bonus benefit of this mitigation method is the recovery of deleted files. The approach is somewhat different for resident and non-resident `$DATA` attributes in the MFT entry. When the `$DATA` attribute is resident, the file content is recovered by having it copied to another location. Otherwise, the `RunList` function in the MFT entry needs to be disintegrated from the MFT entry and the raw data needs to be moved to another location. Only then can the file recovery can be completed. This needs to be a timely executed operation since certain file clusters can be moved to another location during the process while the content gets overwritten.

Installing decoy resources

The use of decoy files for detection of attacks, regardless of whether they come from the outside or from the inside is not a novelty approach. Decoy services have been traditionally applied in hashed passwords security and to detect data gained from hosting services in illegal ways. Their role is to increase the likelihood of detecting malicious processes in the early stages for new, as well as for traditional malware.

We stated on a couple occasions before that malware works in the similar aggressive fashion across various ransomware families. To delete the files in a very short time, the malicious process adopts a comprehensive approach, aiming at all files in different paths and with different extensions. Thus, it becomes possible to define a filesystem activity which reflects normal interaction. Attackers can still avoid detection by generating attacks that mimic regular user behavior. This is where decoy or deceptive files are brought into play.

One effective mitigation technique pertains to installation of decoy files in multiple disk locations and their constant monitoring. While they are in use, it is important that the decoy files are indexed at multiple places and generated in a way that makes it complicated for offenders to identify them.

Mitigating lockerware - a comprehensive action review

Even if your organization takes the necessary time and effort to prevent ransomware attacks and applies advanced protective measures, there is no guarantee that every unit in a large computer network is safe. Lockerware is fairly personalized and prevention is founded on prevention and awareness. Delivering the ransom money is also no guarantee that the malware will be cleaned or that the user and the organization are safe from future attacks. It is critical to react immediately or at least within two weeks since the incident. However, action needs and can be undertaken before, during, and after the incident and Chief Information Officers should adopt a comprehensive approach.

Response plan development

Prompt action is almost impossible if actors are unprepared. At a moment of crisis, decision-making can be weak and if the organization does not have an incident response plan at hand, the consequences of the infection can exacerbate. Developing a solid plan for fighting malware infections is the first mitigation task that should be completed by the responsible business leaders in the organization.

A well-developed plan will prevent the company falling victim to payment at the moment of panic happening in the coal-and-ice a few hours after the attack.

Several behaviors are key-avoiding payment and rather immediately referring to the incident plan, disconnecting infected units from the network, employing company digital security teams in line with the incident plan, keeping records of the information, and notifying law enforcement authorities.

Security awareness and education

We have underlined the essential role of awareness in malware mitigation. As usual, it is not sufficient to provide an ad hoc security training. When a threat needs to be identified, only constant refreshers will do the job. Social engineering is the prevalent way of spreading malware. Security education will not only assist risk avoidance, but will also reduce the damage and prevent severe further impact. End users should be educated about how to act in front of their personal computers. A purposeful security education would produce a change in malware perception and culture and evade off-the-cuff behavior. In the end, this always comes down to bypassing suspicious links or malicious e-mails.

Patching

The US Computer Emergency Readiness Team from the Department of Homeland Security estimates that over 85% of attacks can be prevented by security patching. **Patching** should be applied and regularly maintained on the operating system and on the additional software and anti-malware solutions installed on a computer.

The security patch is a remedial change performed on a computer asset to improve and ward off the weakness of a vulnerability. By using the cyclical process of identifying and mitigating existing threats, it removes the current exploitation and also mitigates future exploration of the vulnerabilities.

Robust monitoring

Situations in which the lockerware has used the command and control servers or when malware spreads from one to another host can be prevented by robust monitoring. The process is executed by applying host and network monitoring methods and by using effective security information and an event management malware detection plan.

Restrictions to unnecessary services

Restricting software installation surpasses personal responsibility and is a method that can be executed on the organizational level. Not every user station needs to have full functionality. Certain restrictions to the tools and applications necessary to perform the work on a station will prevent infections and can be applied to services, software, IP addresses, and unused devices.

Disabling services

The decision about which services should be restricted comes down to the business in question and there is no one-size-fits-all approach. Obviously the lead IT engineers or the IT department in an organization should decide about the enabling and the disabling of specific services. Certain debatable or risky services can be used subject to additional approvals or permissions for a limited time or scope of operation.

Restricting software

A number of ransomware variants, especially those that apply a level of encryption can make changes to critical files. Although lockerware is not primarily aimed at file encryption there are advanced malware type for which software restriction is an appropriate anti-threat measure.

Blocking IP addresses

A superb way of mitigating lockerware is blocking the ToR network. Most ransomware attacks use ToR gateways to communicate with the command and control centers. Once the ToR is blocked, offenders' communication path is broken off and they have to think of finding alternative ways of delivering the infection. Newest infection techniques not only apply communication through ToR, but also website traffic redirection. The innovation does not hypothesize that IT departments should now altogether abolish IP address blocking, but that they should include it in the mitigation strategy as a measure of historically proven worth.

Removing unused devices

This action prevents possible further infection spreading and it should be applied to varied physical devices such as mapped drives, USB storage devices or memory sticks, smartphones, and cameras. All writeable devices should be removed from a station when not in use.

File exchange management

Businesses are based on sharing and it is impossible to do a job unless certain files are shared and worked on collaboratively. Once the process of file sharing becomes a routine, security gets on wobbly feet. To keep the filesystem safe, organizations should establish best practices for sharing data and files in a safe and secure manner. An effective way to minimize risks is application of digital signatures.

Discerning effects of e-mail security

With due regard to personal beliefs, we must not leave out the key fact that e-mail security considerations are the religion of evading malware. If there was ever a malware mitigation commandment it should be the "Do not open a suspicious e-mail" statement. Risky files belong to the family of executable files. Users should particularly avoid e-mails containing attachments with phishing-prone extensions, such as `.exe`, `.js`, `.vbs`, and `.ps` files or document files that can support macros, such as `.doc`, `.xls`, or `.xlm`.

However, the first component of e-mail security is technical control on company level. Efficient e-mail security methods include anti-spam and phishing prevention filters, blocking e-mails that contain hyperlinks, and quarantining images and attachments. To avoid spreading the infection, macros option can also be disabled in office applications.

Software updates

Mitigating malware by software updates includes not only regular operating system updates, but also additional software installations and anti-malware tools. The actual components always depend on the operating system in use and should involve the web-browsing tools and the e-mail client.

While certain software includes malware applications by default, such as the Windows Defender in Windows 10, many will need special anti-malware measures. Mobile devices, for example, require specific protection and regular software updates are critical. Prompts for Android updates are a regular part of Google's annual security reports. Latest browsers include in-built tools that prevent clicking on malicious links and compromised websites. For example, Smart Screen is a tool in Microsoft browsers that discovers potentially suspicious pages. It checks visited sites against a set of dynamic criteria and asks for permission for further browsing and feedback reporting. In case of malicious links, the tool will block the page and advise on caution. The tool also employs a record of whitelisted and blacklisted applications, and examines downloads against a list of incorporated and user-reported unsafe files. Each suspicious link is accompanied with a warning advice.

Data backup

Even if the files are not encrypted, many lock screen malware variants perform file deletion in the execution process. In case of lockerware, the smart defense tactics encompasses keeping the files on an external, non-mapped drive or device. In case the physical separation method is impossible, regular system restore or manual sync methods can be enabled as secondary mitigation tactics.

Data backup is vital. If it were not for the possibility to restore files from backups, full data recovery after a ransomware attack would have been impossible without paying the ransom. No backup means that the ransomware had its work done. Offenders often fail to go for the fair play option by unlocking the screen. In such situations recovery from backups is the only solution. Even when ransomware has certain backup files infected, there are steps that CIOs can undertake to minimize the malware impact:

- Regularly conduct and maintain backups
- Write-protect and store backups offline and offsite
- Use versioning to ensure reputable media are available for use for a certain period of time before the infection
- Test backups to affirm reliability and data restoration capacity
- Check backups for risks by applying anti-virus scans

Cloud storage and security solutions

The advantages of cloud storage are undeniable. However, advanced sharing and external storage is an additional security risk. In this respect, the cloud space cannot only serve as storage for files, but also as a location for implementing advanced security solutions. For example, the Microsoft OneDrive cloud feature employs a protection mechanism against ransomware. When in use, the OneDrive feature provides extra space in the cloud for storing, sharing, and syncing files. Additionally, it serves for work on shared documents or feature updates from multiple remote locations.

While the risk certainly grows exponentially, modern cloud storage solutions provide improved malware protection through concrete cloud-based ransomware prevention methods that adopt modern ecosystem-wide detection techniques. It is crucial to remember that cloud security can be tailored to suit the needs of the particular enterprise and that costs and time can be saved, while simultaneously providing increased safety. This is called the "elastic" approach to security and it can be successfully deployed to cloud solutions with shared responsibility and dynamic workflow.

File history or system protection recovery

Specific operating systems have applied software tools that enable file restoring. The File Restore and the System Protection features on Windows 10 and 8.1 or Windows 7 respectively need to be enabled for certain files restoring. While the feature is useful and practical, it must be remembered that it is not omnipotent and will not work in situations when backup files are deleted or possibly encrypted.

Mitigation by deception technology

Kharraz and his research partners accentuated the use of decoy resources to effectively fight malware attacks. The use of decoy resources is called **deception technology**. It is a specialized advanced method for prompt detection and analysis of infections applying automated precise techniques that can work almost in real time. Deception tools are proactive and divert attacks by applying deceiving measures that defend against threats by preventing encryption. The decoy resources build a layer of protection and are usually generated from licensed operating system software or imitations of such software.

Quick five-step guide for businesses under attack

With so many applicable defense techniques, it can be challenging to decide on the first critical decisions and steps to take when an attack takes place. Therefore, it is practical to have a short reference document that serves as a reminder that there is always something that you can do, even when you have not prepared thoroughly in advance.

We have summarized the critical steps that can be undertaken when a ransomware attack has taken place for users of recent versions of the Windows operating system. Some of the actions will work in any situation, regardless of the system in use.

While reading it as a basic guide, it is worth remembering that no amount of first-aid recovery will surpass the effects of an extensive anti-malware preparedness plan conducted by professionals. Moreover, specific devices and operating systems require a tailor-made approach that may not be effective in specific circumstances. The wise decision overall is to get professional help:

- **Disabling sync features:** Enabled syncing features makes it easier for offenders to instigate attacks that will overwrite files, especially when they use crypto ransomware. By disabling sync features you can prevent targeting data in the cloud.

- **Removing malware from the affected devices:** Running a full scan is vital to remove the malware from the infected devices, including synced or mapped drives. Many operating systems come with a built-in basic anti-malware tool, which is not 100% effective. An advanced anti-malware software tool is the ultimate protective solution.

- **File recovery:** File recovery depends on the system version in use. For example, Windows users can recover files through the File Restore or System Protection functions.

- **Blocking the payment transaction:** Under certain circumstances, the payment transaction can be blocked, even if you have already started the payment process. This is throughble when the files have been successfully recovered without using the help provided by the attackers.

- **Contacting law enforcement and reporting the crime:** Getting in touch with the relevant cybercrime authority in the country is important not only for taking action in the concrete case, but also for predicting future criminal behavior and for undertaking protective measures to prevent similar attacks to other victims. Sending a report to the relevant software authorities is also recommended. By clicking the **Send Report** button you protect yourself and your organization, show solidarity, and contribute to a great business practice in building effective advanced anti-threat solutions.

Summary

While introducing evolution of ransomware in Chapter 1, Introduction to Cyber Extortion, we noted that over the last few years we have seen a re-emergence of crypto ranomsware, which is getting popular, advanced, and dangerous. When there is a new pioneering method, it is easy to forget about the harm done by the predecessors.

We dedicated this chapter to explain the widespread presence and the malevolent strategies of lockerware, even in the last couple of years, when a new player has taken over. We explored a large ransomware study that draws a conclusion that various lockerware variants were included in 94 percent of the examined cases, thus confirming the practicality and the profitability of this extortion method. To understand the malware process, we presented the techniques used in notable filed cases and the various scenarios of the ransomware families used on a global level.

Further on in the chapter, we demonstrated specific actions in the lockerware process, providing details about the stages of delivery, payload, infection, and execution. We emphasized the importance of awareness and the key role of end users in the mitigation. To conclude the chapter, we specified applicable mitigation strategies and gave instructions about long-term security planning and about immediate actions that can save the day when you are under attack.

In the next chapter, we will focus on crypto ransomware and intent to give the reader some detailed knowledge on stages of this ransomware. For every stage of the attack, different public high-profile ransomware cases will also be explored.

5
Crypto Ransomware Prevention Techniques

This is a deep dive into crypto ransomware with the intent to give the reader detailed knowledge on stages of this ransomware. For every stage of the attack, different public high profile ransomware cases will be explored. Although there are only four stages, they will be in-depth exploring various ways that the initial infection occurs, comparing encryption techniques and speed at which data is locked, how data is held hostage, as well as how the ransomware propagates to other devices or servers on the network. The chapter will end with information, which helps one identify which ransomware hit them.

The defense will be discussed in depth and perhaps this will be the most interesting topic for most readers.

In this chapter, we will cover the following topics:

- Crypto ransomware
- Ransomware's target
- Stages of ransomware
- Defense in depth

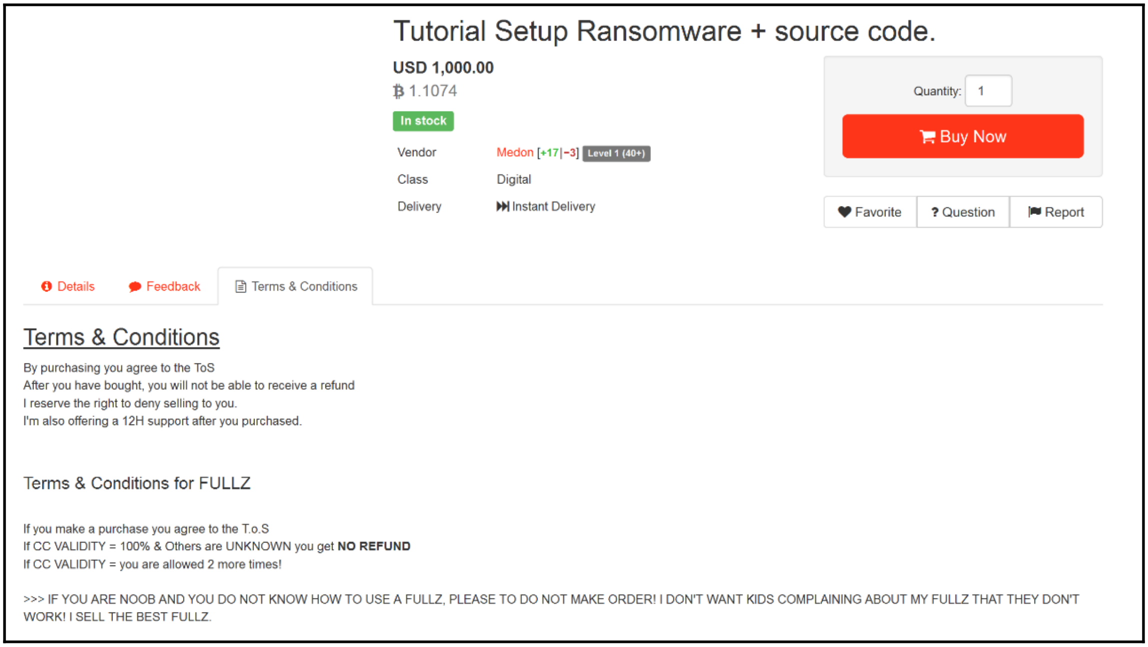
Crypto ransomware

Unlike other variants of ransomware, crypto ransomware targets the system storage and the data - encrypting entire data that is stored on the computer. Once encrypted the data is rendered useless unless the user obtains the decryption key. These days, everyone is going digital and storing their sensitive data on their computers and mobile devices. Most of them do not create periodic backups of their data or are not aware of the need to have backups as a safeguard against potential data or computer theft or ransomware attacks. Such fundamental weaknesses are exploited by crypto ransomware to exploit victims with sophisticated ransomware campaigns, extortion, and so on.

Once the users are trapped with crypto ransomware, it indexes the files available on the system and encrypts all the files and formats. Until all the files are encrypted by the ransomware, the ransomware persists and executes under the radar. Once the ransomware message is presented to a victim, by this time the damage is already done to the victim's data. In most scenarios, once the victim is infected, the ransomware doesn't affect the critical system files or functionalities and does not deny access to the system. Thus, this enables victims to do multiple activities apart from accessing the data that is encrypted.

One of the key aspects of the ransomware is that each infection has a time limit after which the decryption key may not work or the contents may get permanently deleted in case the ransom is not paid by the victim. Victims generally don't think rationally especially under time limits and thus in most cases they tend to pay the ransom.

In 2016, approximately 64% of ransomware was detected as crypto ransomware by leading security vendors from the total number of samples analyzed by a leading security vendor. In contrast to locker ransomware, crypto ransomware is more sophisticated and provides access to the Internet so victims can purchase crypto currencies to pay the ransom. Some sophisticated ransomware that is derived from crypto ransomware also provides victims with a portal to buy crypto currencies with adequate "How To's" and detailed information on payments.



Tutorial Setup Ransomware + source code.

USD 1,000.00

฿ 1.1074

In stock

Vendor	Medon [+17|-3] Level 1 (40+)
Class	Digital
Delivery	⏭ Instant Delivery

Terms & Conditions

By purchasing you agree to the ToS
After you have bought, you will not be able to receive a refund
I reserve the right to deny selling to you.
I'm also offering a 12H support after you purchased.

Terms & Conditions for FULLZ

If you make a purchase you agree to the T.o.S
If CC VALIDITY = 100% & Others are UNKNOWN you get **NO REFUND**
If CC VALIDITY = you are allowed 2 more times!

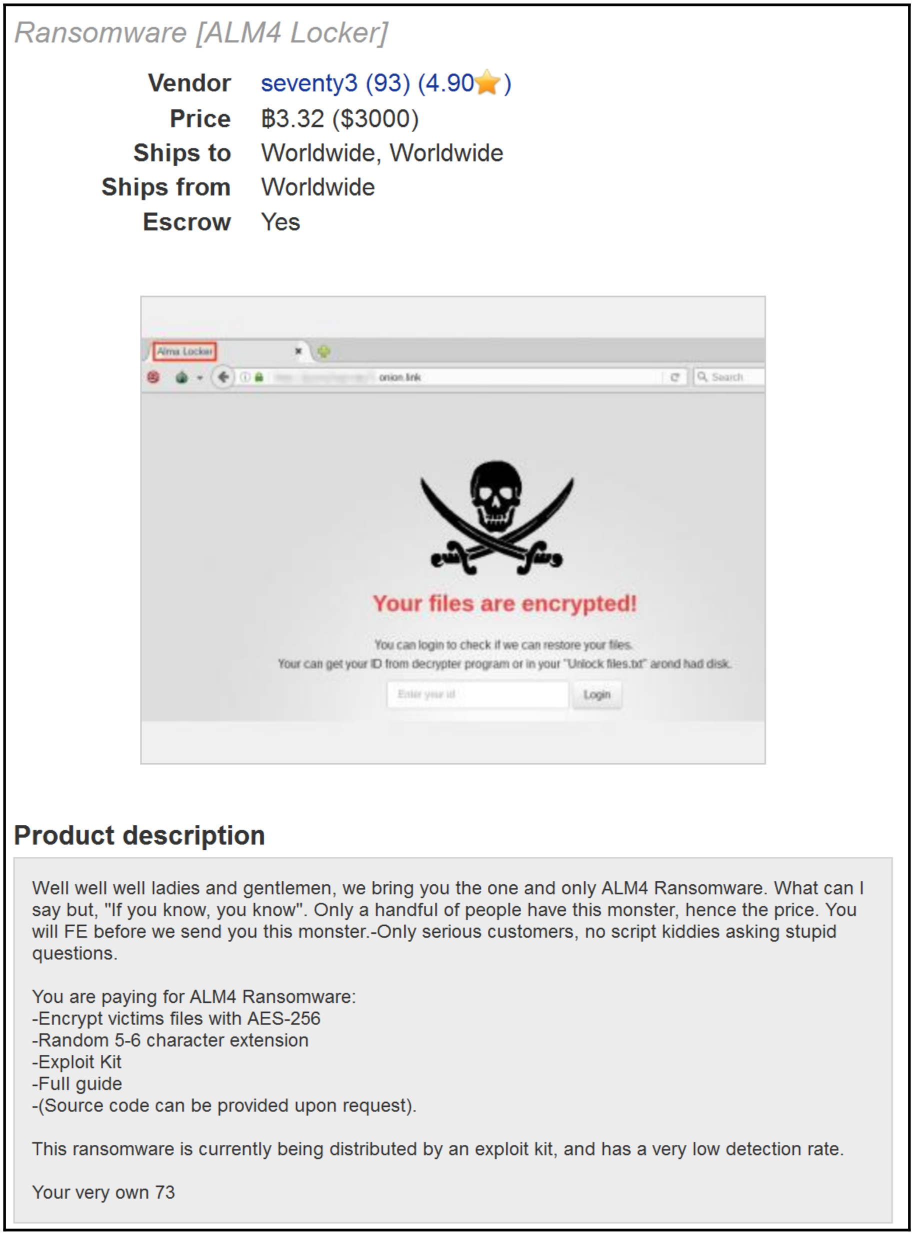
>>> IF YOU ARE NOOB AND YOU DO NOT KNOW HOW TO USE A FULLZ, PLEASE TO DO NOT MAKE ORDER! I DON'T WANT KIDS COMPLAINING ABOUT MY FULLZ THAT THEY DON'T WORK! I SELL THE BEST FULLZ.

Ransomware tutorial and setup available in Darknet

Earlier, crypto ransomware versions were not as effective and sophisticated as today's variants. Ransomware authors at that point in time didn't rely on strong algorithms and key management - such as the keys were stored within the system itself or within the malicious file (ransomware). In certain cases, it was also identified that the key used to be similar across multiple samples, which signifies that if a key has been used to unlock one of the ransomware infected machines, it could further be used for other systems infected by the ransomware.

The authors of the ransomware employ strong encryption algorithms, for instance, RSA, AES, and 3 DES with an oversized key in the ransomware. In multiple variations of the ransomware developed by novice cybercriminals, they store keys within the ransomware itself. As they are against this practice, experienced ransomware authors tend to produce exclusive asymmetric keys for the respective infected node. The association of public/private encryption with robust policies within the ransomware limits the victim's response to:

- Payment of ransom
- Losing their data



Ransomware [ALM4 Locker]

Vendor	seventy3 (93) (4.90⭐)
Price	฿3.32 ($3000)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	Yes

Your files are encrypted!

You can login to check if we can restore your files.
Your can get your ID from decrypter program or in your "Unlock files.txt" arond had disk.

Product description

Well well well ladies and gentlemen, we bring you the one and only ALM4 Ransomware. What can I say but, "If you know, you know". Only a handful of people have this monster, hence the price. You will FE before we send you this monster.-Only serious customers, no script kiddies asking stupid questions.

You are paying for ALM4 Ransomware:
-Encrypt victims files with AES-256
-Random 5-6 character extension
-Exploit Kit
-Full guide
-(Source code can be provided upon request).

This ransomware is currently being distributed by an exploit kit, and has a very low detection rate.

Your very own 73

Another variant of ransomware available in Darknet

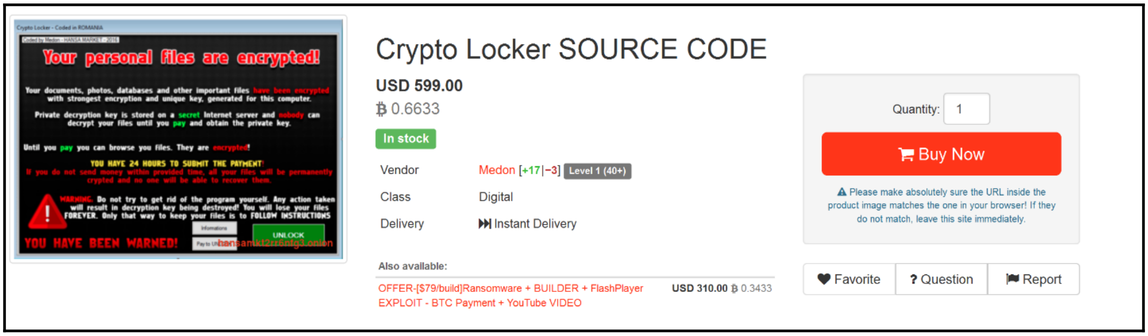
The effectiveness of the ransomware is directly proportional to the cyber criminal's expectation, that is, novice authors tend to focus only on the associated profit from immature victims, on the other hand, experienced malware authors tend to target campaigns to hold hostage the sensitive data across systems of large businesses and organizations - evading law enforcements. Primarily due to the fact that multiple users tend to have concerns about different aspects of data - for instance, documents, videos, photos, applications, and so on. A number of ransomware variants are available and they are spreading comprehensively targeting the attack surface.

Crypto ransomware - scenarios and variants

This section emphasizes on interesting crypto ransomware variants transcending across the globe.

CryptoLocker

This ransomware has been all over the place at a point in time, in some form or the other. The actual CryptoLocker botnet was closed in the second quarter of 2014, but by then cybercriminals had already extorted nearly US $3 million from targeted victims. Since then, the name and approach have been widely used and imitated, although all the operations these days are not directly associated with the actual one.


Crypto Locker - Coded in ROMANIA

Coded by Medon - HANSA MARKET - 2016

Your personal files are encrypted!

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

Until you pay you can browse you files. They are encrypted!

YOU HAVE 24 HOURS TO SUBMIT THE PAYMENT!

If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

WARNING. Do not try to get rid of the program yourself. Any action taken will result in decryption key being destroyed! You will lose your files FOREVER. Only that way to keep your files is to FOLLOW INSTRUCTIONS

YOU HAVE BEEN WARNED!

hansamkt2rr6nfg3.onion

Crypto Locker SOURCE CODE

USD 599.00

฿ 0.6633

In stock

Vendor	Medon [+17|−3] Level 1 (40+)
Class	Digital
Delivery	⏭ Instant Delivery

Quantity: 1

Please make absolutely sure the URL inside the product image matches the one in your browser! If they do not match, leave this site immediately.

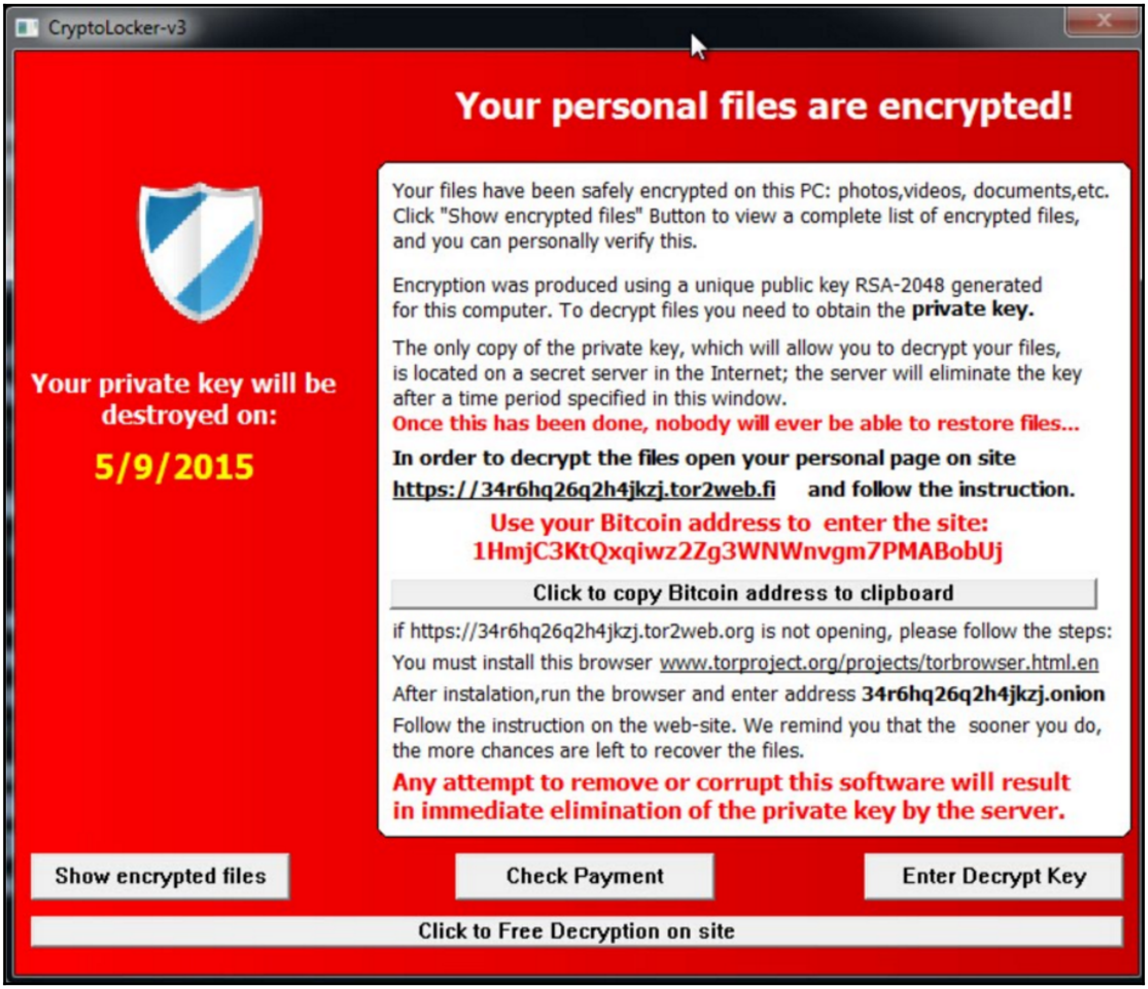
Also available:

OFFER-[$79/build]Ransomware + BUILDER + FlashPlayer EXPLOIT - BTC Payment + YouTube VIDEO **USD 310.00** ฿ 0.3433

CryptoLocker in Darknet

To date, it continues aggressively with several variants having been discovered. It is primarily distributed via exploit kits and spam. It primarily targets users within corporate environments, and executes on common versions of Windows including Windows XP, Windows Vista, Windows 7, 8, and 10.

The ransomware encrypts files with specific file extensions using an RSA 2048 bit key and AES-256. When it finishes encrypting the targeted files, a screen prompts the user to send a ransom of two Bitcoins within a 96-hour period in order to receive a decryption key. If funds are not received, the decryption key is destroyed, rendering the user's files inaccessible. The ransom can also be paid via MoneyPak (USA), CashU, Ukash, or Bitcoin, which is used in the majority of cases. Once paid, a decryption key is sent to the infected system; the ransomware usually initiates decryption of the targeted files, though there have been some instances reported in which decryption does not occur.



Your personal files are encrypted!

Your private key will be destroyed on:

5/9/2015

Your files have been safely encrypted on this PC: photos,videos, documents,etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...

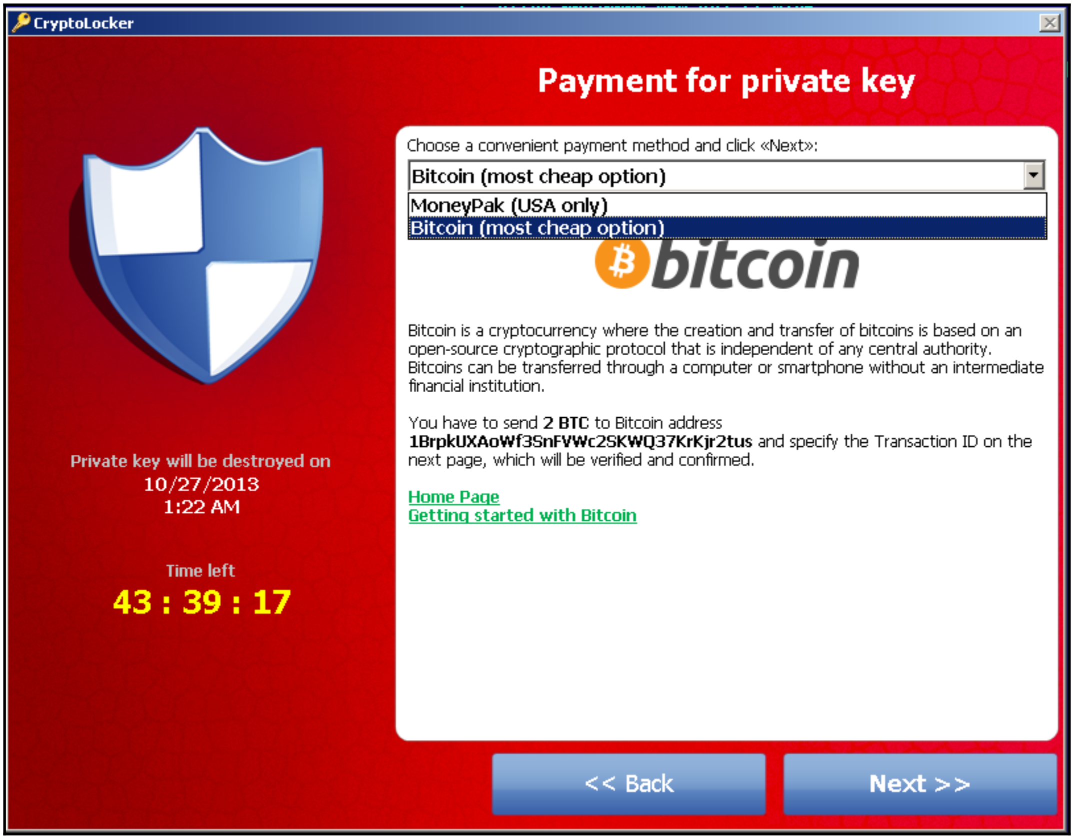
In order to decrypt the files open your personal page on site
https://34r6hq26q2h4jkzj.tor2web.fi and follow the instruction.

Use your Bitcoin address to enter the site:
1HmjC3KtQxqiwz2Zg3WNWnvgm7PMABobUj

if https://34r6hq26q2h4jkzj.tor2web.org is not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**
Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

CryptoLocker version 3 ransom message



Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

MoneyPak (USA only)
Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address **1BrpkUXAoWf3SnFVWc2SKWQ37KrKjr2tus** and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Private key will be destroyed on
10/27/2013
1:22 AM

Time left
43 : 39 : 17

CryptoLocker ransomware ransom

Unfortunately, CryptoLocker is effective. It is significantly more advanced than previous ransomware programs in three respects:

- The methods used for encrypting files
- The covert and effective nature of its delivery mechanism
- The architecture of the Command and Control decryption server

CryptoLocker programmers have implemented both asymmetric and symmetric encryption using the native CryptoAPI found in the Windows Operating System. Each victim machine is assigned a 2048-bit RSA public/private key pair by the Command and Control servers. The Command and Control server then sends only the public key down to CryptoLocker malware on the victim host.

The malware then encrypts each file with a uniquely generated 256-bit AES (Cipher-block chaining mode) key, which is encrypted with the RSA public key and stored at the beginning of the file. Since the AES key is discarded after the file is encrypted, it is now only decipherable by the holder of the victim's RSA private key, which is only stored on the Command and Control server.

When CryptoLocker executes on the victim's host, it makes multiple requests to a list of more than 1000 domains (see the sample in the following table) that have been generated randomly based on the current date using an algorithm. Within that daily-generated domain list, a few will resolve and connect to the Command and Control server. It was observed that many of the domains are acting as pass-through proxies for the actual Command and Control server that is hidden elsewhere to prevent the takedown.

Table 1 - Example of Domains
`ctotujnmdjphxdu.org`
`dclffueprfhkgf.biz`
`hwuiingqeuubi.org`
`jmrfxxpcmspvi.org`
`kqnvwyqyqqmkab.biz`
`lhkbianumwfs.biz`
`nqktirfigqfyow.org`
`qficuwythvxmc.biz`
`yuwspfhfnjmkxts.biz`

CryptoLocker is disseminated through spam e-mails sent to corporate e-mail addresses. Phishing e-mails may mimic communications from shipping companies indicating expected delivery dates/times, and they contain an attachment. The executable has a PDF icon and takes advantage of the hidden extensions that are set by default by the Windows OS.

An analysis of the kill-chain reveals that the Cutwail botnet is being used to disseminate the spam. The attachment is an executable that is a dropper known as Upatre. It connects to a site (via secure channel Secure Sockets Layer or "SSL") to grab a copy of the Gameover Zeus Trojan. The Zeus Trojan then connects to another site and grabs a copy of CryptoLocker. This method suggests that the threat architects appear to have hired a distribution service that uses Cutwail/Upatre/Zeus to disseminate the phishing e-mails and CryptoLocker. By tunneling via malware that's already known to be effective, CryptoLocker maintains a low profile, decreasing the likelihood that it will be detected prior to successful attack execution.

Locky

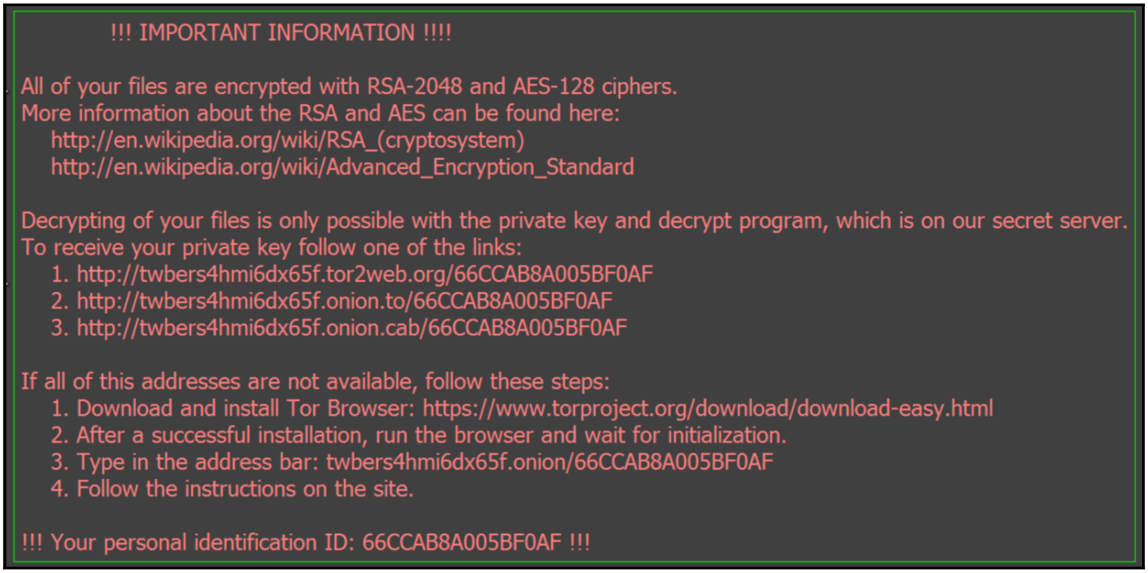
Locky is comparatively a new kind of ransomware with a similar approach as earlier ones. This ransomware is spread widely via spam usually in the form of an e-mail presenting as an invoice. With a classical message instructing users to enable macros to read the document, this ransomware is as destructive as previous ones, the minute it is scrambled upon. As soon as the macros get enabled, this malware initiates encrypting files across the system with AES encryption scheme. Once the encryption is complete, it demands the ransom in Bitcoins.

All the campaigns that are involved in propagating Locky ransomware work on a massive scale. One of the widely known instances of Locky remains when one organization reported blocking approximately 5 million e-mails connected with this malware, over the course of two days.

In the first quarter of 2016, multiple institutions within the healthcare sector were targeted and infected with Locky ransomware - one of the most known cases being the assault on Hollywood Presbyterian Medical Center. Fortunately, the healthcare data was unaffected, but other systems essential for routine operations such as CT scans, emergency room systems, and normal operations were affected. Eventually, the medical center had to pay a ransom of 40 Bitcoins to unlock their computing instances even after getting wide support from law enforcement agencies. In further analysis, it was identified that the attack was a consequence of a random malicious e-mail.

If we relatively compare the sophistication and techniques among other ransomware variants, Locky can be called reasonably less complex, but it is propagating rapidly. RSA 2048 and AES 128 ciphers are used by Locky to encrypt files. Locky also sets a wallpaper to show the victims what to do next. Using links, victims are usually presented with instructions so they can directly understand how and where to proceed for more information.

Multiple security vendors stated that this malware was developed by Dridex - which is a criminal organization known for operating banking malware. This malware is majorly distributed with Microsoft Word attachments and all the files once encrypted are renamed with the `.locky` extension. Signature-based detection generally doesn't work with Locky due to the fact that each binary of Locky is uniquely hashed and after infection, it deletes backup shadow copies of the OS.



```
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
   http://en.wikipedia.org/wiki/RSA_(cryptosystem)
   http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
   1. http://twbers4hmi6dx65f.tor2web.org/66CCAB8A005BF0AF
   2. http://twbers4hmi6dx65f.onion.to/66CCAB8A005BF0AF
   3. http://twbers4hmi6dx65f.onion.cab/66CCAB8A005BF0AF

If all of this addresses are not available, follow these steps:
   1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
   2. After a successful installation, run the browser and wait for initialization.
   3. Type in the address bar: twbers4hmi6dx65f.onion/66CCAB8A005BF0AF
   4. Follow the instructions on the site.

!!! Your personal identification ID: 66CCAB8A005BF0AF !!!
```

Locky instructions

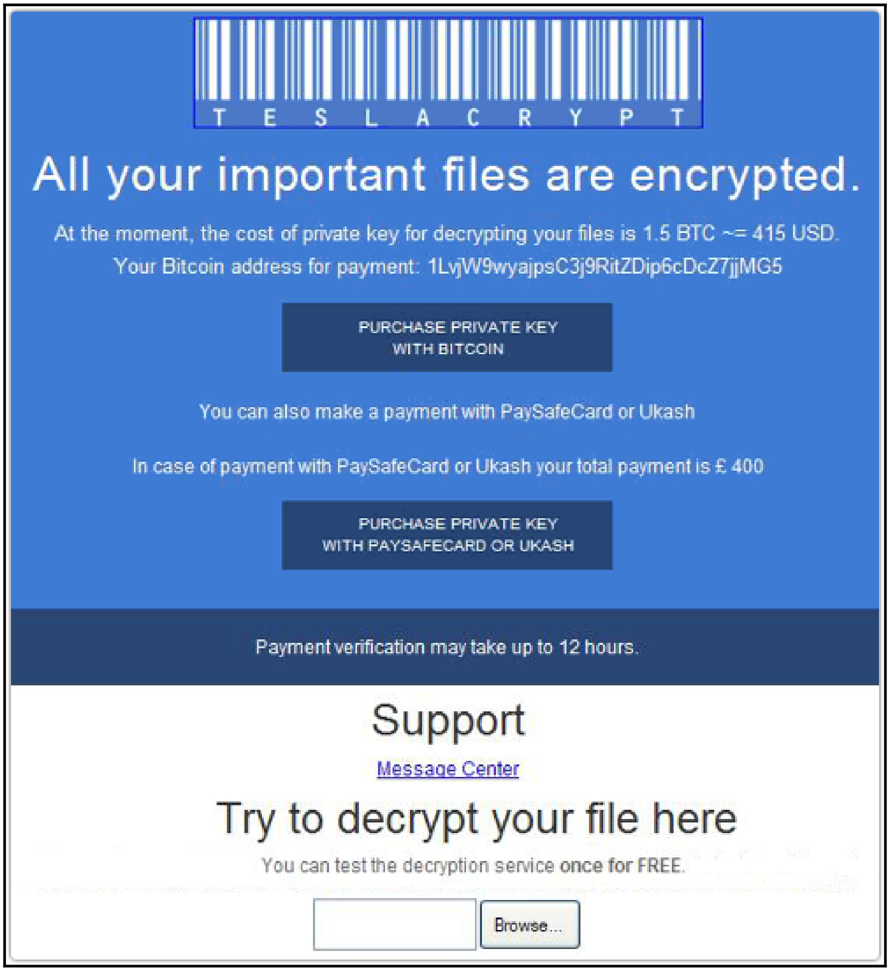
TeslaCrypt

TeslaCrypt is another form of ransomware that has gone mainstream and as most of the earlier variants; it uses an AES algorithm scheme for encrypting files. One of the interesting aspects of this malware is that it solely targets Adobe vulnerabilities and propagates via Angler exploit kits, which exploits Adobe Flash vulnerabilities. In the absence of Adobe it exploits Silverlight and Internet Explorer.

This ransomware dissects itself in the Microsoft `temp` folder and also provides multiple payment options including Ukash, PaySafeCard, and Ukash. Fundamentally it works through a compromised web portal wherein Angler is embedded within an iframe. Once the victim is rerouted to a landing page, it performs certain checks (where it checks for anti-viruses, conducts host analysis, and so on) and then if it succeeds, Flash is exploited and then used to downstream the payload in the Microsoft `temp` folder. This malware, as the majority of other variants, copies itself to `%appdata%` wherein it stores the key and list of indexed files. Once the files are encrypted it uses the `.exx`, `.ecc`, `.mp3`, and `.ezz` extensions. Although it bears a resemblance to CryptoLocker in the way it's designed, they do not share the common source code.

TeslaCrypt has evolved multiple times with the following changes:

- From symmetric encryption it was configured to asymmetric AES encryption. This revision occurred when Cisco researchers had released the Talos TeslaCrypt decryption tool.
- It was revised again when Kaspersky labs released the decryptor tool for TeslaCrypt. The malware authors then again remediated the flaw and released another version that also appended the `.mp3` extension once the files were encrypted.



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~= 415 USD.
Your Bitcoin address for payment: 1LvjW9wyajpsC3j9RitZDip6cDcZ7jjMG5

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is £ 400

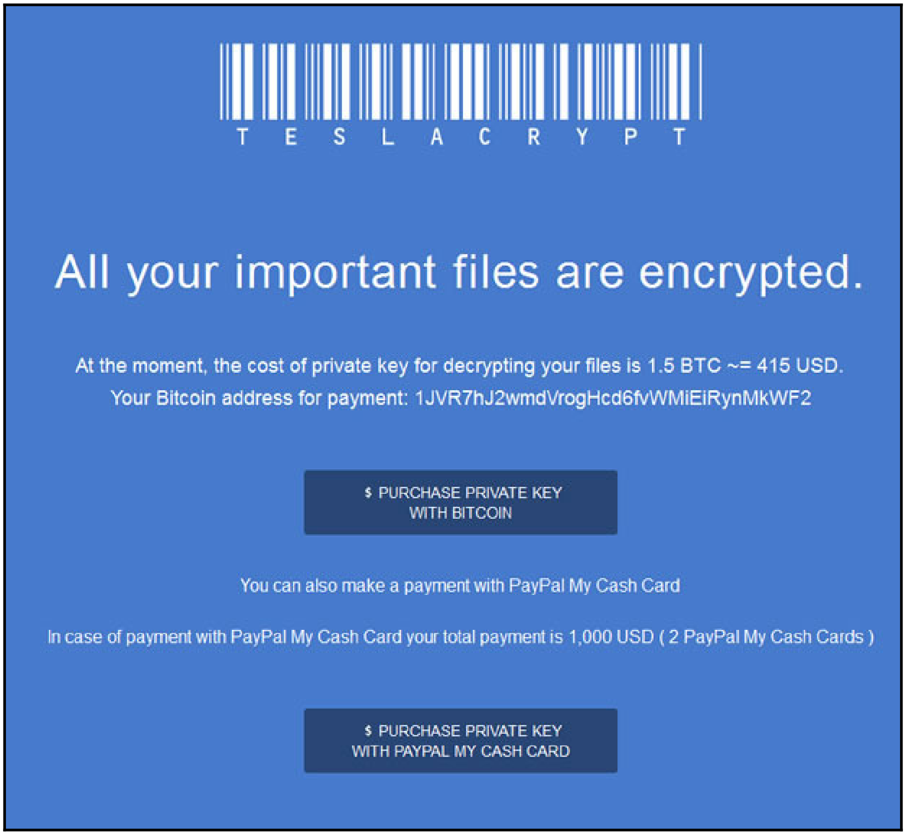
Payment verification may take up to 12 hours.

Support

Try to decrypt your file here

You can test the decryption service once for FREE.

TeslaCrypt ransom message



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~= 415 USD.
Your Bitcoin address for payment: 1JVR7hJ2wmdVrogHcd6fvWMiEiRynMkWF2

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1,000 USD (2 PayPal My Cash Cards)

Another example of a TeslaCrypt message

TeslaCrypt was known earlier for having targeting limited file types related to Windows platform-based games, which further got evolved with encrypting PDF, Word, and image formats such as JPEG. Another interesting aspect was that it also allowed the victims to decrypt only one file for free showing good faith.

CryptoWall

With the fall of CryptoLocker rose another ransomware called CryptoWall. There have been multiple variants including Cryptobit, CryptoWall (2, 3), CryptoDefense, and so on, which followed the same distribution channels as CryptoWall, that is, via spam and exploit kits. Another common method was malvertising on the Zedo ad network. Thus, numerous websites unconsciously distributed the ads, which even they didn't realize were bad.

The early form of the ransomware used the RSA public encryption key, which in its later version used a private AES key, which was further masked using a public AES key. It has changed multiple times and it is even used for setting up malware to steal Bitcoin wallets. It encrypts a diverse set of file types than that of CryptoLocker.

The malware binary too replicates itself to the Windows `temp` folder (`%temp%`) and launches a new event of the `explorer.exe` process and executes the Cryptowall binary along with it. It then connects to Invisible Internet Project (*I2P*) proxies, which then further connects to a Command and Control (CandC) server using a unique hash value generated for that instance. Ones the server is connected, the CandC server updates the system with a public key (which is unique to the system) and delivers instructions for ransom in the language based on the location of the machine (via geolocation).

Variants of this malware still use I2P proxies to interconnect with CandC servers and use Tor for collecting ransom payments from targeted victims. Unlike its predecessor Cryptolocker, the Cryptowall ransomware targets the Windows OS globally.

CTBLocker

This malware is majorly a ransomware as a service, wherein cybercriminals spread the malware globally via multiple affiliates (including novices, botnet managers, and so on), which it recruits for a share of the ransom (which would be paid by potential victims). This business model (of affiliation) was made popular by fake anti-viruses, phishing, and click fraud schemes. This strategy did work for this ransomware wherein it achieved a large volume of malware infected at a much more rapid rate.

The malware distribution channel and associated business model are quite interesting if we put it in perspective. For this ransomware, the majority of the model's affiliates tend to pay the ransomware operators (members who spread the ransomware to a wide audience) a fee (or a small fraction for each ransom) to use the malware. As a result of the affiliate business model, the ransomware uses potentially all the infection vectors available. In common cases, cybercriminals depend on various exploit kits and malicious e-mail campaigns. Due to the business model and potential target of this ransomware, it is available in multiple languages including Dutch, German, Italian, Spanish, French, English, Latvian, and so on. It especially propagates to American and European countries.

It also uses a blend of symmetric and asymmetric encryption to limit victims from having the right to access their files. It uses **Advanced Encryption Standard** (**AES**) and **Elliptic Curve Cryptography** (**ECC**) to encrypt files. The applied principle for CTB-Locker is that the AES encryption scheme is used to encrypt all the files and the mean of decryption is encrypted by means of an ECC public key. As a result, cybercriminals who retain the ECC private key can only decrypt the encrypted files.

One of the unique aspects of this malware is that it doesn't require access to the Internet or any interaction with its Command and Control servers to activate encrypting files in the system. The connection to the Internet is not required up until the victim's efforts to decrypt their encrypted files. As other malware, all the communication corresponding to ransom payment is over Tor and proxies that relay Tor traffic.

> Recently multiple variants of CTBLocker were seen encrypting web portals that were hosted by WordPress. The ransomware was referred to as Critroni - wherein the intruder penetrated websites and swapped its `index.php` / `index.html` file with different files that were used to encrypt the website data with the AES 256 encryption scheme. In this case, the ransom messages were displayed on the homepage of the website. This variant targeted websites that relied on outdated versions of WordPress or vulnerable plugins.

Ransomware's targets

As per the mindset of cyber criminal groups, any computing resource is a potential target due to the profitability of multiple attack vectors, which can be derived as per the weakness existing in the victims systems. As society is becoming more dependent on technology and associated constant access to data within these technologies, the threat landscape of such malware intensifies. As per leading security vendors, the most frequent targets of ransomware have been personal systems, organization servers/databases, and mobile devices.

As per the recent ransomware trends, targeted campaigns are rising across the globe. Earlier, ransomware authors didn't consider who their victims were, provided that the ransoms were paid. With that viewpoint, ransomware propagated across regions with multiple types of users used to hit millions of users and even if a fraction of those victims paid the ransom - the campaign was considered successful.

The following sections list the key targets of ransomware.

Businesses of all sizes

Overall, organizations of all sizes across industries are targeted rigorously these days. Associated systems of businesses are more likely to hold sensitive data and documents that are critical for its services - for instance, business reports, client's data, a database of information, IPs, financial documents, and so on. Disrupting services for any organization or losing critical information holds a huge impact across its service lines.

For example, if POS devices across a retail shop become unavailable due to a ransomware hit, the sales would be affected and the business would halt imposing huge losses every minute. New sophisticated ransomware variants can enumerate multiple systems associated by an infected system including file share servers, and so on, signifying that with one system getting infected, the potential of other systems to get infected also increases.

Even though most large organizations have scheduled periodic backups and may have adequate disaster recovery plans, most small and medium businesses lack that kind of discipline. For large enterprises usually, it's been observed that individual end users may not be considered in scope for disaster recovery - primarily focusing only on the other key services. Due to such elements, organizations across all sizes become a viable target for cybercriminals and ransomware.

Ransomware has not excluded any particular industry, but the following industries have been identified to be specifically targeted.

The healthcare sector

Traditionally, this sector was not a target for ransomware attacks. Of late the healthcare sector is being targeted predominantly with multi-level campaigns of malware variants. One of the most attention grabbing successful ransomware scenarios observed was with Hollywood Presbyterian Hospital Medical Center, which was infected with Locky ransomware. The hospital administration had to pay the ransom to get the systems released.

Soon after this, multiple systems that were accountable by Los Angeles Country health department got infected. Interestingly, in this case, the health department restored its operations from the backup and didn't pay any ransom. In the same way, multiple hospitals in Germany were infected with a ransomware variant and didn't pay any ransom to the ransomware campaigners and further got it restored from their backups.

Public agencies - educational institutions and law enforcement agencies

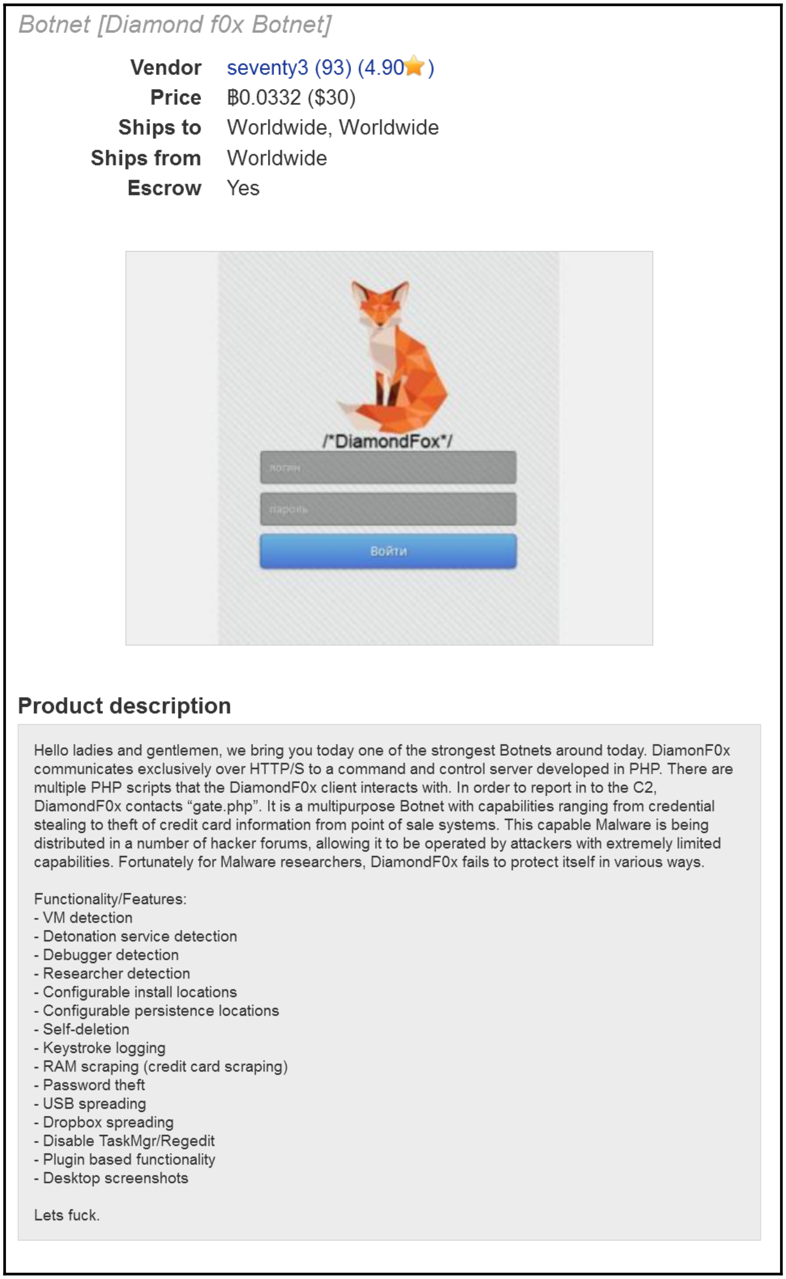
Multiple cases of ransomware have been observed recently across public agencies such as universities and law enforcement agencies. cybercriminals assume public agencies are more likely to have sufficient funds to pay the considerable ransom. There have been various reports of education institutions and law enforcement agencies being hit by crypto ransomware.

Horry County school district in South Carolina paid approximately $8500 as a ransom, when the FBI investigation produced no other alternatives. In another similar case, multiple elementary schools run by New Jersey school were hit by ransomware wherein they demanded a ransom of 500 Bitcoins (approximately US$ 416,995). This incident was considered to be one of the most disrupting cases since the cybercriminals compromised systems and files used by students.

Financial institutions

Ransomware is often spread via established botnets spreading phishing campaigns, spam e-mails, and malicious links. Financial institutions have been a frequent target of large botnets schemes, for example, Ramnit and Dyre botnets. A lot of traction has been seen by cybercriminals towards putting efforts against infecting systems across institutions in the finance sector.

As per the comprehensive analysis conducted by leading security vendors - the most targeted countries for this sector with approximately 40% is the United Kingdom and Unites States with approximately 36%.



Botnet [Diamond f0x Botnet]

Vendor	seventy3 (93) (4.90★)
Price	฿0.0332 ($30)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	Yes

Product description

Hello ladies and gentlemen, we bring you today one of the strongest Botnets around today. DiamonF0x communicates exclusively over HTTP/S to a command and control server developed in PHP. There are multiple PHP scripts that the DiamondF0x client interacts with. In order to report in to the C2, DiamondF0x contacts “gate.php”. It is a multipurpose Botnet with capabilities ranging from credential stealing to theft of credit card information from point of sale systems. This capable Malware is being distributed in a number of hacker forums, allowing it to be operated by attackers with extremely limited capabilities. Fortunately for Malware researchers, DiamondF0x fails to protect itself in various ways.

Functionality/Features:
- VM detection
- Detonation service detection
- Debugger detection
- Researcher detection
- Configurable install locations
- Configurable persistence locations
- Self-deletion
- Keystroke logging
- RAM scraping (credit card scraping)
- Password theft
- USB spreading
- Dropbox spreading
- Disable TaskMgr/Regedit
- Plugin based functionality
- Desktop screenshots

Lets fuck.

Home users

In the niche of cyber security, people are thought of as one of the weakest links. They are considered one of the most vulnerable targets. Ransomware is one of the best effective malware against personal computing users who are considerably not fluent with systems or ransomware and how specifically it works and impacts their computing environment. The home user is the most affected group wherein in the majority of cases users don't even have the bare minimum access to technical assistance. In many cases, it has been identified that due to lack of support, the user feels secluded/helpless, which further increases the pressure to pay the ransom demanded. In addition, there have been cases in which users were aware of the freely available solution, but due to limited knowledge or technical capabilities were not in a position to employ the solution.

All the information and data (documents, photos, videos, games, and so on) stored by an average user is personally valuable to users and despite this most users will not have an effective standby plan to successfully recover from malware and crypto ransomware assault.

As per surveys conducted by Symantec, it was identified that approximately 25% of average users do not have any backup at all, while 55% of users backed up files. Out of this 55% only 25% of users used to backup files only once a week while the rest of the users backed up once a month or less frequently than that. This signifies that the majority of users are exposed when it comes to crypto ransomware assaults.

As we have seen previously, most ransomware even encrypts and deletes the shared backup drives connected with the system (which acts as the local backup) - it is crucial for home users to define a strategy to reduce the impact of an attack, if it succeeds in the first place.

Stages of ransomware

The following are the diverse stages of a ransomware assault irrespective of whether it is a targeted attack or a mass distribution attack:

1. Initial infection
2. Encryption/locking
3. Holding hostage
4. Propagation

Having considerable knowledge on each stage of the attack and having insight on **indicators of compromise** (**IOC**) to identify the ransomware sufficiently assists in defending against such assaults or at the very least reduce the impact of attacks.

In the following section, we will emphasize on dissecting all the phases of a ransomware and will brief on where the activities of a malware differ as per the type of attack. For example, one of the major differences among targeted attacks and a mass distribution attack is the time taken to execute all the phases of the ransomware. The overall time of getting a mass distribution attack executed is often approximately 15 minutes (from initial infection, encryption, and holding hostage to the victim receiving the ransom), which is very low relatively.

This is due to the fact that these attacks would not look forward to exploit systems beyond the current system. On the other hand, targeted attacks tend to look at a much wider set of systems to have a much greater footprint. cybercriminals look forward to affecting the complete business than individual systems due to the impact and profitability possibilities. Targeted attacks are more difficult to attack since it is generally operations by a focused group than automated systems spreading and executing mass distribution ransomware.

Initial infection and exploitation

The initial phase of ransomware is to infect an end user system by any possible means. cybercriminals use numerous methods to spread ransomware out of which the primary ones include:

- E-mail attachments comprising of malicious documents and malware
- Advertising - through various legitimate and illegitimate channels
- Drive by downloads - which exploits vulnerabilities

As all of us understand, for a malware assault to be successful the ransomware needs to be executed on a host. The way ransomware authors approach potential targets is through spam/phishing e-mails or an exploit kit that exploits vulnerabilities across multiple applications and platforms. These exploit kits work well with environments that are running misconfigured/outdated software applications on their systems.

Numerous cybercriminals use such forms of exploit kits packaged with malware, which they stealthily place on authentic websites or bogus web portals that resemble a reliable brand or website. When a legitimate user visits such forged portals that host such types of kits, it automatically scans the system of the potential user and checks for the OS version, browsers, framework, and applications running at the browser/OS level and if they are vulnerable it exploits and follows the next steps for the ransomware.

War driving

War driving is a general term that is used when random attacks are launched on an enormous scale. Classical examples include:

- Phishing e-mails sent to a mailing or distribution list generally having more than thousands of e-mail addresses
- Websites wherein exploit kits have been embedded that further compromise a potential user's system when they visit such malicious websites

In the majority of cases, organizations that don't follow mature security practices are the ones who are the prime victims of such attacks.

E-mail attachments

In many cases, malware does land up in systems through e-mail attachments. The e-mail resembles to be coming from a known entity such as a financial institution, healthcare provider, or employer and do consist of a message that the user could relate to for instance - monthly statement, payroll information, and so on.

In such cases, within each e-mail the attachments are carefully selected to mask their actual intention. In general, the files that are attached do have a `.exe`, `.doc` / `.docx` or `.xls` extension, which the system would identify as an executable or Microsoft Word or Excel files:

- Sometimes if the system settings are set to disable the display of extensions, even though the name of the file is `BobPayroll2016.doc.exe` the target user will see only `BobPayroll2016.doc` and may assume the file to be a normal harmless document.
- In other cases, documents with the `.doc` / `.docs` / `.xls` extension would have malicious macros embedded - wherein if a user executes the document and enables the macros, malware automatically gets executed. In Microsoft installations, macros are by default enabled.

At all times ransomware is carried onto computing devices via multiple stages of downloaders - particularly to avoid detection from anti-malware solutions. Authors of such malware also extend the profitability by introducing an affiliate model - wherein they pay a fraction of the ransom to potential actors who infect multiple targets using any of their techniques, for instance via botnets spreading widespread phishing campaigns, and so on. Such threat actors that assist ransomware and malware authors to distribute sophisticated ransomware are majorly botnet operators who see this as an easy and quick revenue stream to earn from their existing services.

Drive-by downloads

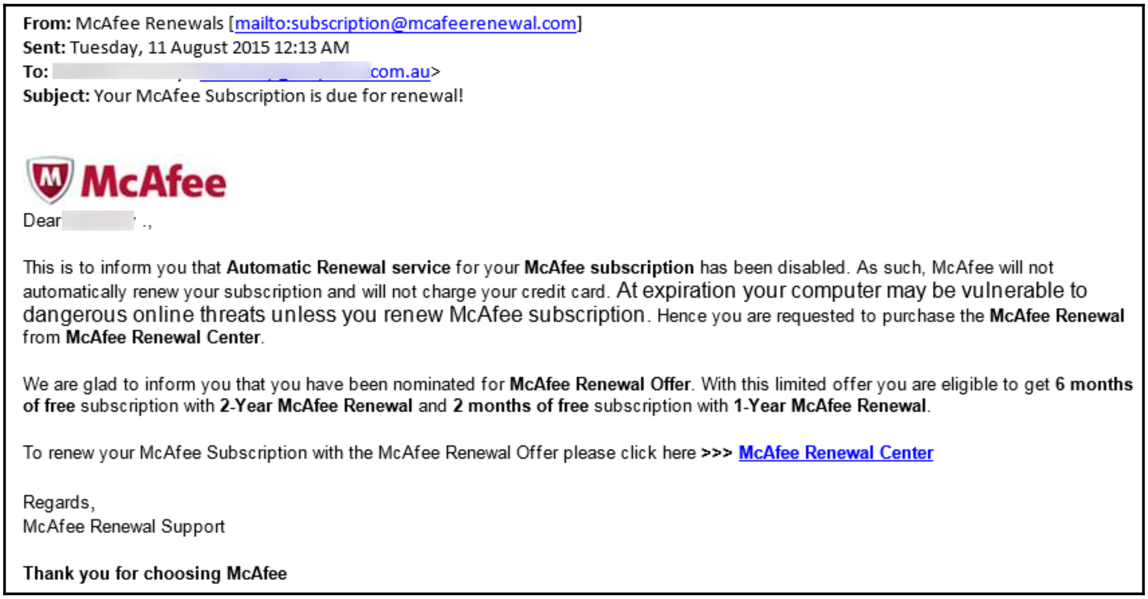
Many times general users accidently become victims by merely visiting compromised websites. Multiple instances have been seen wherein malicious code gets downloaded just by scrolling over banner ads. These are drive-by downloads that fundamentally tend to exploit browser, application, and operating system vulnerabilities. For instance, as we discussed earlier the exploit kits used by CryptoWall to load - Angler, Nuclear, and so on, exploit the vulnerabilities in Java, Flash, and other platforms.

Phishing campaigns

Phishing and spam e-mails are the most commonly used delivery methods for spreading malicious content to a wide network of users. Most organizations even after conducting multiple awareness programs across all employees, most businesses find their employees still getting trapped with such campaigns where they click on attachment and links. If we see holistically, just one click of an employee is enough to infect the entire organization's network and compromise its systems. As we saw previously, large botnet operators are used to send massive spam and customized e-mails to an organization. Botnet services are relatively cheaper and thus novice cybercriminals who tend to earn quick money can purchase ransomware from ransomware authors and massive botnets from botnet operators and run phishing campaigns masquerading multiple businesses that would attract potential targets to click on those e-mails.

Targeted attacks

In the case of targeted attacks, the cybercriminals identify a target or multiple targets and on a case by case basis, try to figure out as much information as possible. For instance, in one of the recent cases cybercriminals gathered information about a company through one of the job description posted by them. They understood that within the targeted firm, McAfee products have been extensively used. Thus, they ran a phishing campaign and sent multiple phishing e-mails to the firm's employees, with a message to have a chat with the support team. Once the victim initiates a chat session with the cybercriminals the intruder installs the malware on the system thus neutralizing the critical defenses. Once this is done the ransomware encrypts every available resource in the environment.



From: McAfee Renewals [mailto:subscription@mcafeerenewal.com]
Sent: Tuesday, 11 August 2015 12:13 AM
To: [redacted]com.au>
Subject: Your McAfee Subscription is due for renewal!

Dear [redacted] .,

This is to inform you that **Automatic Renewal service** for your **McAfee subscription** has been disabled. As such, McAfee will not automatically renew your subscription and will not charge your credit card. At expiration your computer may be vulnerable to dangerous online threats unless you renew McAfee subscription. Hence you are requested to purchase the **McAfee Renewal** from **McAfee Renewal Center**.

We are glad to inform you that you have been nominated for **McAfee Renewal Offer**. With this limited offer you are eligible to get **6 months of free** subscription with **2-Year McAfee Renewal** and **2 months of free** subscription with **1-Year McAfee Renewal**.

To renew your McAfee Subscription with the McAfee Renewal Offer please click here **>>>** McAfee Renewal Center

Regards,
McAfee Renewal Support

Thank you for choosing McAfee

This way, during the infection stage, these steps are used to get the payload to the end user system. This payload could potentially be the actual ransomware or a malicious application that would create a backdoor in the system through which multiple variants of malware can be pulled to the system to execute multiple attacks.

Command and Control (C2)

Once the ransomware is executed and installs itself to the target system it makes contact with the Command and Control server. The Command and control server in most cases provides further instructions to the end node. Most of the prevailing anti-virus and anti-malware solutions block the malware if it has a known signature to the corresponding malware. Endpoint security software's and perimeter security devices (such as Firewalls, IPS, and so on) retain a list of proxies and commands and control servers that are related to malwares and thus detect their presence when the infected system attempts to communicate to malwares. Certainly this is not one of the effective measures, primarily due to the fact that it is complex to build an all-inclusive list of Command and Control servers. In addition, Command and Control servers can be procreated and sealed within no time.

cybercriminals have thus transformed their approaches to use a dynamic domain algorithm that would generate a list of domains (in thousands), and tries to establish a connection with each of them. Defending the anonymized Command and Control servers remains the primary objective of the cybercriminals as it is essential to the survival of a botnet. In an interesting case, a security vendor exposed a Russian Cyber Criminal group so-called APT29 - where the communication protocol they were using was Twitter feeds. They had also utilized steganography techniques to embed commands within images.

Like in most of the cases earlier, the ransomware used to replicate itself in multiple locations within the system, such as:

- `<%startup%>`
- `<%appdata%>`
- `<%rootdrive%>/random_folder/`
- `<%WINDOWS%>`
- `<%TEMP%>`

Once the malware is executed, it from time to time checks the system to identify the backup files and folders so to encrypt them first or delete it so to prevent the restoration of services through them. Essentially such actions are implemented to eliminate any means available to the targeted system for recovering from the attack without paying the ransom impairing the campaign.

Multiple ransomwares including Locker and cryptolocker tend to execute commands to get rid of all the volume shadow copies from the infected instance. Modern malware has a tendency of killing the processes (of operating systems as well as third parties) associated with backups and then encrypting the backup files or potentially deleting them to provide no opportunity of backup to the user.

Such instances and awareness of malware behavior could potentially help security administrators to enable comprehensive security logging and create use cases or security scenarios in the SIEM - Security Incident and Event Management solutions so to alert them when such actions take place.

Encryption/locking - delivery and execution

Once a system is infected with ransomware, as preferred by the ransomware owner - this becomes the launching pad for propagating the infection all over the organization's network. Once all the systems that are footprinted by the ransomware get infected, the public keys are delivered to all the bots.

Once the initial process of exploitation is over, the real payload gets delivered in the system. The payload is mostly delivered by means of an encrypted channel, which in most cases is a custom encryption layer (as a replacement for SSL) over and above a typical HTTP connection. It's quite difficult to identify the malicious content over the wire due to the malware using strong encryption. It's thus a good idea to frequently scan a few crucial locations with the operating system for objects possessing malicious behavior. It sets up a good line of defense.

File encryption

Once the ransomware is replicated across all the systems targeted by the malware, it will perform a key exchange in a secure manner with the Command and Control server and establish encryption keys that would be used on the corresponding infected systems. Ransomware generally tags each system with a unique identifier, which also gets presented to the victim during the stage when instructions are shared. This is also the same medium through which the Command and Control segregates the encryption keys used for corresponding infected systems.

As soon as the malware is deployed in a system, it executes and initiates the steps as per its design - which in a majority of cases is to disable the corresponding system's services or index the files available in the system to select the critical file for encryption. Alongside, by means of victim's prevailing access rights, the malware also scans all available physical and cloud-based drives to identify prospective data that can be encrypted.

At this point in time, the victim would not sense any effect of the malware. Strong encryption modes are also used by modern crypto ransomware - for instance, RSA 2048, which even eliminates the option of the user to determine the key used for decrypting the files.

Intentionally, most encryption schemes used today include strong encryption, for instance AES 256 - which victim's cannot decipher by their own. In addition, new categories of ransomware do not need to even contact a Command and Control server for exchanging keys. SamSam for instance is a malware wherein the malicious software in itself does all the encryption locally without having any outbound connect to the Internet. This is crucial for security administrators to understand that if they haven't identified any outbound connection from their internal network showing symptoms of communication with a Command and Control server, it doesn't signify that ransomware may not be present.

During encryption, the file naming convention is handled differently by different ransomware. For example, CryptoWall v3 does not encrypt the filenames, while v4 randomizes the extension and filename. In another instance, Locky adds a Locky extension at the end and such conventions are useful for an organization to fingerprint the variant based on such characteristics. Based on multiple aspects such as the bandwidth quality, malicious application behavior, and number of devices affected - the encryption process timeline varies from a few minutes to days. A distributed network may take days to completely encrypt all the nodes, whereas an independent node would get encrypted in minutes.

Former versions of ransomware such as cyrptolocker are used to encrypt local system files primarily before expanding out to attached services and network devices. The new variants have transformed their approach with encrypting the backup first -that is, they scan for file shares discovering files that include the file or folder name with a date such as `sql20161209.bak`. Once these files and folders are encrypted they target other file types. It is thus useful for security practitioners to be aware of such techniques and evolution of ransomware across each stage. This would assist them to have an adequate incident response plan. Cyber attackers target to encrypt the crucial files of an organization first (which also includes the files and folders with recent dates) and may follow multiple approaches including the ones shared previously. In addition, due to the persistence mechanism contained within potential crypto malware, if any system gets disrupted for instance with a reboot, the modern ransomware processes pick up from where it was left off encrypting the system until it is completed.

At this stage, there are a few crucial things that we should realize, that is, all ransomware principally intends to extort money from victims, but operationally and technically they can be completely different. Even though in earlier sections we have defined how different various types and variants of ransomware are, we will delve a bit more to further see how they work on an operational and technical level.

Ransomware encrypting files

Crypto ransomware characteristically has been seen using both types of encryption techniques - symmetric and asymmetric techniques. In Symmetric encryption as everyone is aware of, using a single key encryption and decryption takes place. In this case, ransomware generally requests the ransomware author for the encryption key to encrypt the system or generates a key within the infected system and shares it with the cyber criminal. Once the files are encrypted the malware make sure that the key is not available in the system or is obfuscated so that the victim is not able to identify it and able to decrypt encrypted files without paying the ransom.

One of the key advantages of using this encryption scheme is that symmetric algorithms performance wise it is much faster and uses small keys than asymmetric encryption mechanisms. The performance of the malware is a critical parameter since cybercriminals look forward to encrypting as soon as possible before its behavior is identified and alerted.

The other encryption scheme used more frequently nowadays is the asymmetric encryption. In this scheme there is a public and private key involved wherein the public key is the key used for encrypting and the private key is used for decrypting the data that is encrypted. Ransomware once downloaded and executed, tends to download the public key too in many cases and keeps the private key with the ransomware owner itself. Even if the victim has access to the public key, it is of no use for them since they would require a private key for decrypting the files.

The major drawback of using the public key is that encrypting files and folders would be relatively much slower than symmetric key encryption. In the case of ransomware, taking more time to perform actions signifies a massive risk from a cyber criminal's perspective - the risk of security solutions identifying the pattern of operation or malicious behavior of services, running in the background and may alert the system administrator. Sophisticated ransomware tends to use a blend of symmetric and asymmetric encryption algorithms. In many scenarios where crypto ransomware uses asymmetric encryption unique public private keys are also generated for infected systems. The scenarios can get more complicated and difficult for security solutions to trace the pattern

In general, the location of the keys for encryption and decryption does have a vital impact on the overall effectiveness of the scheme. The subsequent sections will elaborate a few malware families detailing how the approaches differ at this stage.

Public key download

A variant of CryptoWall, Cryptodefense utilizes both symmetric and asymmetric encryption mechanism. It uses the AES algorithm to encrypt the files on the infected system. In the infected system itself, a 256 bit AES key is generated and once the files are encrypted the same key is encrypted with an RSA asymmetric public key (which the system received after interaction with the Command and Control server). The resultant encrypted AES key is then stored in the system's infected files. Even though the AES key is available in each encrypted file, the victim cannot use it since the RSA private key is owned by the ransomware owner (which is required to decrypt the encrypted AES key).

cybercriminals use such an approach and generally have a unique RSA asymmetric key pair for each infection. This provides them an assurance that one private key would not decrypt all the encrypted files. One of the ways this malware can be stopped is if the communication to Command and Control a server is identified and disrupted, then the encryption procedure cannot be successful.

Embedded public key

One of the ransomwares that postulates another approach operationally is CTBLocker. This ransomware uses both the encryption schemes too, with a difference that it embeds the public key for RSA asymmetric encryption with the initial download of the payload itself.

The ransomware author holds the private key. The rest of the procedures are quite similar as earlier - malware generates an AES symmetric key for the encryption process, which is encrypted with an RSA public key. The encrypted key is added with the encrypted data and the victim cannot restore the environment in any attempt to recover the AES key, due to the RSA private key being held with the ransomware author.

The only advantage of using such a method is that the ransomware can commence the process of file encryption without communicating to any Command and Control server. cybercriminals make sure that for each infection there is some level of customization and there is a different public key available. Otherwise, if a victim receives a private key - an attempt to decrypt other infected systems using the same key can be made, vandalizing the scheme.

Embedded keys

Malware targeting mobile operating systems, for instance, Android malware (Simplocker) uses the AES symmetric encryption algorithms to encrypt files on the end user devices. The AES key is contained within the malware and thus the malware is not required to communicate to Command and Control servers for any additional files. In this case, the malware authors can invoke the malware by providing instructions and commands via SMS messages - for instance to encrypt or decrypt the files contained within the user device. Since the key is available within the malware package, if identified it can be used to decrypt the encrypted files within the device.

Such kind of malware design is not a technique that is used widely in case of crypto ransomware. These methods are typically only seen in malware that has been created by novice cybercriminals.

Ransomware locking screens

This category of malware blocks the infected victims from accessing their computing devices operating system and corresponding services. In these scenarios, a ransom message is displayed to the victim in a continuous loop giving the impression that the message is continuously displayed. Such malware mostly uses the features and relative APIs provisioned by the core operating system and services.

Windows and mobile locker ransomware

Mostly all the malware threats infecting operating systems to lock down users employ approaches that are similar in nature. The malware displays the message in full screen mode of the operating system - either using a browser window or creating a window using the operating system APIs. The window presenting the message to the user usually tends to be the only window that the malware creates.

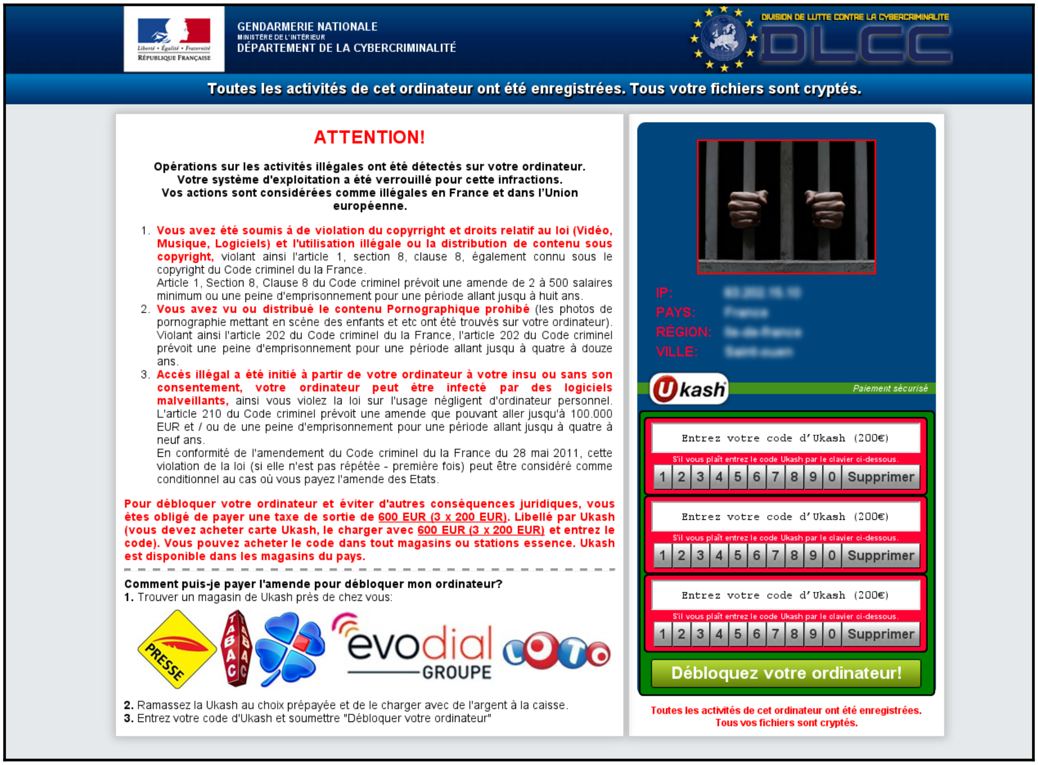
In mobile platforms such as Android, the ransomware usually creates an activity window for displaying the ransom message. It also checks periodically whether the message window is presented to the user by using techniques such as ExecutorService objects provisioned via Android.

In multiple cases it has been observed that the malware has a service running in the background to make certain that their window is active and overriding all the other services. The service also monitors the other applications and services that the victim may invoke to kill the ransomware processes. In case some services exist to end the malicious processes, the malware service that monitors those ends such services and processes.

Certain forms of malware utilize the shutdown messages and processes to signal to other services that the operating system is shutting down. This lets the malware close other processes that may obstruct activities of the malware.

The message content presented to the user via a window is generally contained within the malware itself, but there have been scenarios wherein customized messages have been downstreamed from the Command and Control server. Customizing the message is common across cybercriminals for switching the language to serve the message in the local language where the infection happened, using geo location.

Locking browsers is a different category wherein binary executables are not used and neither access to underlying operating systems is locked. Through advertising and other mechanisms, targeted users are redirected to a web portal hosted on a server wherein malicious browser-based ransomware such as Browlock is hosted. Such malware is deployed completely using client side technology and primarily contains JavaScript code with HTML to present the ransom message to the user.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
DIVISION DE LUTTE CONTRE LA CYBERCRIMINALITE
DLCC

GENDARMERIE NATIONALE
MINISTÈRE DE L'INTÉRIEUR
DÉPARTEMENT DE LA CYBERCRIMINALITÉ

Toutes les activités de cet ordinateur ont été enregistrées. Tous votre fichiers sont cryptés.

ATTENTION!

Opérations sur les activités illégales ont été détectés sur votre ordinateur.
Votre système d'exploitation a été verrouillé pour cette infractions.
Vos actions sont considérées comme illégales en France et dans l'Union européenne.

1. **Vous avez été soumis á de violation du copyrright et droits relatif au loi (Vidéo, Musique, Logiciels) et l'utilisation illégale ou la distribution de contenu sous copyright,** violant ainsi l'article 1, section 8, clause 8, également connu sous le copyright du Code criminel du la France.
   Article 1, Section 8, Clause 8 du Code criminel prévoit une amende de 2 à 500 salaires minimum ou une peine d'emprisonnement pour une période allant jusqu à huit ans.
2. **Vous avez vu ou distribué le contenu Pornographique prohibé** (les photos de pornographie mettant en scène des enfants et etc ont été trouvés sur votre ordinateur). Violant ainsi l'article 202 du Code criminel du la France, l'article 202 du Code criminel prévoit une peine d'emprisonnement pour une période allant jusqu à quatre à douze ans.
3. **Accès illégal a été initié à partir de votre ordinateur à votre insu ou sans son consentement, votre ordinateur peut être infecté par des logiciels malveillants,** ainsi vous violez la loi sur l'usage négligent d'ordinateur personnel. L'article 210 du Code criminel prévoit une amende que pouvant aller jusqu'à 100.000 EUR et / ou de une peine d'emprisonnement pour une période allant jusqu à quatre à neuf ans.
   En conformité de l'amendement du Code criminel du la France du 28 mai 2011, cette violation de la loi (si elle n'est pas répétée - première fois) peut être considéré comme conditionnel au cas où vous payez l'amende des Etats.

Pour débloquer votre ordinateur et éviter d'autres conséquences juridiques, vous êtes obligé de payer une taxe de sortie de 600 EUR (3 x 200 EUR). Libellé par Ukash (vous devez acheter carte Ukash, le charger avec 600 EUR (3 x 200 EUR) et entrez le code). Vous pouvez acheter le code dans tout magasins ou stations essence. Ukash est disponible dans les magasins du pays.

Comment puis-je payer l'amende pour débloquer mon ordinateur?
1. Trouver un magasin de Ukash près de chez vous:

2. Ramassez la Ukash au choix prépayée et de le charger avec de l'argent à la caisse.
3. Entrez votre code d'Ukash et soumettre "Débloquer votre ordinateur"

IP: [redacted]
PAYS: [redacted]
RÉGION: [redacted]
VILLE: [redacted]

Entrez votre code d'Ukash (200€)
S'il vous plaît entrez le code Ukash par le clavier ci-dessous.

Entrez votre code d'Ukash (200€)
S'il vous plaît entrez le code Ukash par le clavier ci-dessous.

Entrez votre code d'Ukash (200€)
S'il vous plaît entrez le code Ukash par le clavier ci-dessous.

Toutes les activités de cet ordinateur ont été enregistrées.
Tous vos fichiers sont cryptés.

Browlock sample

Holding hostage

When all the indexed files and folders within the infected system are encrypted, the malware presents a message to the user with information about the malware, the damage done to the corresponding system and infrastructure, instruction on what to expect next, where to send the ransom, along with the payment options and other details for the victim to unlock the system.

With the demand instructions, victims are provided with a few days to pay the extortion ransom after which the ransom would increase or data would get compromised or deleted. In many systems, the way the extortion instructions are described can help trace the ransomware that has potentially infected the system. In most cases as per my analysis, the instructions are protected and saved on the hard disk of the infected system itself along with the encrypted files.

In other occurrences, specific placeholders and locations are used to save the message. Locky for instance takes an exclusive approach wherein it not only pushes files on the victim's instance, but also alters the victim's operating system wallpaper with instructions on how to pay the ransom and decrypt the files. CyrptoWall v3 uses the `HELP_DECRYPT` file to store the instructions and v4 uses the `HELP-YOUR-FILES` file. There are variances across malware categories, but such insight is useful to identify the exact variant and create a proactive approach to defense.

Of late, there has been an interesting behavior of malware where the messages self-destruct themselves, that is, the ransomware cleans itself from the victimized computing device to avoid leaving any traces that would assist security professionals and vendors to proactively identify the ransomware. This aids the malware operator's campaign by presenting no symptoms of any malware to the security solutions deployed within the system and network infrastructure.

As soon as the ransom amount is paid and verified by the ransomware authors, the private key is delivered from the corresponding Command and Control server and decryption commences automatically. The verification from malware authors can take from 2 hours to 72 hours. In rare cases, decryption also fails on some files, but in such cases no support from malware authors/operators is available.

Propagation

Once the malware is executed, the propagation takes place via multiple avenues as we discussed previously - for instance through the infected system propagation takes place via the contact list available within the system, cloud drives, network storage, and other connected devices. As we have discussed earlier, the propagation is major via spear phishing e-mails with attachments that are malicious in nature. These attachments are majorly Microsoft Office or Adobe PDF objects with malicious code/ransomware contained within them.

The other way was advertising where web portals hosted malicious ads and unintentionally users are redirected towards the malicious websites and are victimized via drive by downloads where the ransomware deploys itself in their respective devices. Often times, malware from legitimate sources have been identified infecting general user's worldwide - for example, from leading financial institutions, media agencies, and so on.

Defense in depth

Ransomware assaults against organizations of all sizes are transcending day by day. In the first quarter of 2016 multiple attacks were targeted towards the healthcare sector. Since these attacks and campaigns are profitable for cybercriminals with all the organizations and individuals being vulnerable, it's a profitable business that is becoming mainstream. The consequences of such malware campaigns are far broader than just the cost of the ransom. From the productivity loss in business, to unavailability of services to business customers, the impact is enormous.

Thus, the success of an organization in defending against such malware attacks is mainly dependent upon the understanding of one's environment, what the critical assets that could be targeted are, and what is the current level of preparedness to mitigate and contain such attacks.

It is also considered wiser to discuss one's organization's preparedness with other organizations so a pool of knowledge related to processes and tools to defend against such types of ransomware and cyber security risks increases the preparedness of the organization.

There are multiple strategies that can be defined and practiced to protect from sophisticated ransomware campaigns. These strategies assist in providing defense against potential malware getting in the environment or succeeding in the first place. Out of the following strategies, some of them might include facets that are already considered for your environment that could be narrowed down further for comprehensive protection.

Protection against ransomware can be segregated into the following categories:

- Defining a security architecture
- Perimeter defense controls:
    - IPS
    - Firewalls
- Vulnerability assessment
- Patch management
- Specific measures

Defining a security architecture

An essential and often missing element in an information security program to protect against malware is a well-defined and complete information security architecture that reflects the business decisions and the information security policy decisions of the organization. In many cases, the security architecture is described as a network topology that also reflects information security technology. An effective information security architecture is one that reflects business decisions, is understandable by a wide audience, and is defined using different levels of elaboration that provides detailed guidance for the various parts of the organization.

The purpose of an **enterprise information security architecture** (**EISA**) is to address the organization's need for a holistic approach to IT security to provide enterprise-wide guidance to ensure that information security is approached in a consistent manner and with a consistent level of risk. The architecture is intended to provide guidance for the organization as a whole. The value of the architecture will be in its applicability to the organization's business and its usability by a wide audience for protecting against sophisticated malware.

Need for a security architecture

The basis of security architecture is to implement the security building blocks in such a way to provide the appropriate levels of protection to the business information and processes of an organization.

An information security architecture is designed to be strategic and in layers to protect from sophisticated threats such as malware - it is meant to have a longer life than a blueprint, design requirement, or a topological chart or configuration. If it is too specific, it becomes constrained by current circumstances. If it is too comprehensive or general, it cannot deliver direction and guidance. It is meant to assist in making choices associated with the identification, acquisition, design, application, implementation, deployment, and operation of elements in the organization's technical environment.

The information security architecture should support many communities, departments, and lines of business, and represent the long-term view of technical direction. Information Security Architectures agree for multiple implementations based on the realities of the moment and caution should be exercised to prevent the information security architecture from becoming a blueprint for a specific implementation. The information security architecture provides the overall guidance for managing IT risk across the organization.

The purpose of an Enterprise information security architecture should be to address the organization's need for a holistic approach to information security to provide enterprise-wide guidance to ensure that information security is approached in a consistent manner and with a consistent level of risk. The architecture is intended to provide guidance for the organization as a whole. The value of the architecture will be in its applicability to the organization's business and its usability by a wide audience.

The result, then, should be an architecture that supports:

- Crucial data placements across the key enterprise services for reducing the impact of any malware
- Defines the key security control in terms of technology adoption and processes to reduce the risk identified for the business

Following the principle of least privilege

The principle of least privilege is one of the factors why most ransomware is successful, this is due to the fact that even if users are not required to have admin privilege provided to them, they often have an account with higher privileged role. If a user is not expected to perform certain actions, then the roles assigned to the user should be restricted to perform those actions. If admin rights are not required by the users it should not be provided. This way, even malware would not be able to impact the files and services due to such access restrictions. Another approach can be to provide read only access to users especially for the network shares (where the user is not expected to make changes). This would restrict ransomware to encrypt those files. Shared which are open to all or which allow anonymous access should be reviewed and eradicated. This declines the scope of ransomware.

Perimeter defense controls

As we have seen, threat sources are adaptive in nature. An effective ransomware defense program should move away from a stagnant security paradigm to an adaptive security framework. That is, the solution and measures across perimeter should include the ability to deal with change and threats that change on almost a daily basis at the first level. To do so and be effective, businesses need to reconsider their method towards security and create a comprehensive and holistic security strategy built on business-aligned risk management to achieve resilience against modern cyber threats.

The perimeter is now dynamic in nature:

- Businesses need drive corporations today to connect their enterprise to the Internet and third parties, thereby increasing risk
- With the advent of the extended enterprise, the concept of the perimeter is changing
- When unauthorized access can be obtained remotely, private information about employees, customers, business partners, patients, passengers, and so on can be stolen or abused

Beyond perimeter defense and monitoring, cyber threat monitoring approaches should also incorporate a layered approach that considers attack scenarios where perimeter controls in a combination of security analytics would detect and mitigate the potential threat vectors across organizations. In addition to this, leveraging technologies with perimeter countermeasures can attribute and identify suspicious or "utlier" activity that may be malicious in nature to specific users.

The overwhelming majority of corporate enterprises employ a perimeter security model, which is hard exterior, soft interior. This is where modern malware gets an opportunity to exploit. Typical perimeter defenses include technologies such as firewalls/next generation firewalls, proxies, and intrusion detection/prevention systems (IDS), which if configured well against the identified threats and security use cases, should be in a position to halt the malware infection.

Proxy design and implementation is difficult in nature (primarily due to fine tuning of policies as per the organization needs) and it frequently depends on maintaining the security as per the organizational focus areas, which may be limiting users to restricted business portals during business hours or restricting users to access to a portal which they shouldn't have access to. Even with perfect IDS, firewalls, and proxies, there is always some application data or micro applications that may need to be detected using customized application signatures infused to the security solutions.

From a perimeter context and particularly for protection against malware, the key considerations should be taken for the following crucial areas:

- Network Device Configuration primarily focuses on:
    - Firewalls
    - Routers
    - Content Filters
    - LAN Switches
    - Network Intrusion Detection or Intrusion Prevention Systems
    - Antivirus
    - Wireless Access Points
    - VPN Devices
    - Web Proxy Servers
- Internal Network Architecture considerations primarily focus on:
    - Internal LAN requirements
    - Network Services and their corresponding security
    - Network Connection/Access Control
    - Documentation of network configuration and architecture
    - Guest access
    - Access to internal applications/segregation of zones

- External Connection considerations primarily focuses on:
    - Third Party access to internal networks
    - User Authentication for external connections
    - Segregation of internet connections
    - Wireless Connections

Endpoint protection

It should be determined if enterprise commercial products can aid in improving security at the endpoints of a network. Consider the following items:

- Anti-malware - Anti-malware generally detects harmful items within the system, prevents modification by users, scans the system frequently, auto-protects the system by running scans automatically upon performing a function, as well as provides protection from attacks
- Firewalls/Host-based Intrusion Detection Prevention - End point security tools that provide stringent controls over the system ports and services include Host based Intrusion Detection System (IDS) or Intrusion Prevention System (IPS), which identifies any form of anomalies across the environment by continuously monitoring the behavior of the targeted system

Firewalls

A **firewall** in its simplest form is a boundary guard between two networks, usually an internal private network and the Internet. The main purpose of a firewall is to guard a trusted network against mistrusted parties on the outside that could access or tamper with internal information and resources. Firewalls can be implemented as either hardware and software, or a combination of both. Firewalls are not just filters, but also gateways and chokepoints.

A firewall should provide the following key features and characteristics:

- **Monitor all incoming and outgoing traffic:** All traffic from inside the network to the outside, and vice versa, should pass through the firewall. This can be achieved by logically blocking all access to the local network except via the firewall.

- **Source or destination based blocking:** Blocking unwanted incoming traffic from a specific source or to a specific destination is provided by a firewall. An example would be the blocking of all incoming port `80` requests to all servers except the web server.
- **Outgoing network traffic blocking:** A firewall should provide mechanisms for the system administrator to block all outgoing requests to websites that are considered harmful based on the company's security policy. A firewall can contain the risk of phishing through network traffic blocking.
- **Content filtering:** Network traffic content analysis can help scan for virus signatures and other common threats.
- **Support for Virtual Private Network (VPN) connections:** VPNs allow secure connections from the Internet to a corporate network. Firewalls can be used to establish a site to site and remote access VPNs to securely connect the various sites and users to the organization.
- **Immunity to penetration:** The firewall itself is impervious and stable. This implies the use of a trusted and secure operating system.

Firewall classification

Firewalls can be broadly classified into different types based on factors such as:

- The type of protection offered:
    - Host-based firewalls (personal firewalls)
    - Network-based firewalls (enterprise firewalls)
- Implementation:
    - Hardware firewalls
    - Software firewalls
- Protection methodology:
    - Packet filter
    - Stateful packet inspection
    - Connection filter
    - Application proxy filter

Classification based on the type of protection offered

The kind of firewall installed for a large organization is different than one installed on a user's desktop, but it is one of the security solutions that can identify potentially malicious traffic across the environment:

- **Host-based firewall:** A personal firewall is most often a software application installed on a single host and it protects just that computer. However, host-based firewalls can also be implemented as separate hardware components, or they are built into other network devices. A host-based firewall does not provide extensive reporting and management features.
- **Network firewall:** Network firewalls have the capacity to screen network traffic for a number of computers. They provide extensive reporting and management features and even allow the configuration of multiple firewalls in a single step.

Classification based on implementation

- **Hardware firewalls**: An integrated appliance that has firewall software preinstalled on a device with its own operating system is called a hardware firewall.

  Hardware firewalls can be implemented as dedicated personal computers with hard disks or as solid state application-specific integrated circuit (ASIC) devices. ASIC firewalls are generally faster performers. Hard disks, on the other hand, can be a potential single point of failure.

- **Software firewalls**: Firewall applications that can be installed on the user's operating system are called software firewalls. Software firewalls can be implemented either as a packet filter or a process filter. Process filters can be easily tricked into allowing malicious code to access the network.

Classification based on technical methodology

- **Static packet filter:** The static packet filter checks the source and destination IP addresses in the network header and the source and destination port numbers in the transport header in addition to determining the protocol of the data packet. This information is used by the static packet filter to determine whether to permit the corresponding data packet, or to discard it at the point of entry as per the firewall's rules into the network.

The filtering unit denies all packets that are explicitly denied by the set of rules, allows all packets that are explicitly allowed by the set of rules and drops all other unknown packets. Traditionally, static packet filters are stateless - they do not keep track of connection sessions. This implies that networks protected are still susceptible to ping floods and **Denial of Service** (**DoS**) attacks.

- **Stateful packet inspection:** The packet filter examines the network and transport headers for similar information as the static packet filter. In addition, it provides state awareness by maintaining a table of connection streams. This table is called the "Connection Bypass table".

  All data packets, which have the same monitored network and transport headers, form a unique connection stream. Each packet that arrives is associated with a connection stream. If the data packet is associated with a connection stream already in the table, it is allowed without any further verification. However, if the packet arrives on an unknown connection stream, it is first verified as per the firewall rules and permitted only after it passes the inspection. This means that the packet filter is aware of the difference between a new and an established connection.

- **Connection filter:** The connection filter maintains a Connection Verification table that maintains the TCP flag sequences. The connection filter verifies that the TCP handshaking process is valid by examining the state of the flags.
- **Application proxy filter:** The application proxy examines the network header for the source and destination IP address, the transport header for the source, the destination port numbers, and the header of an application protocol such as HTTP, Telnet, and so on. This type of firewall actually reconstructs the packet inside the host, thereby protecting it from covert attacks. But such reconstruction at the application layer has a performance penalty and it increases the latency of the application.

Key requirements

Now let us look at the key requirements from a ransomware perspective, which includes the following:

Operation requirements

- Blocks unwanted incoming/outgoing traffic between selected end points (for instance common Command and Control servers)
- Enables scanning for virus/malware signatures and other common threats
- Provides granular policy definitions to develop specific security policies by user, group, content, or bandwidth
- Supports seamless and agentless integration with the approved standard directory services
- Supports the common routing protocols : BGP, OSPF, EIGRP, and IGRP
- Provides an intuitive working user interface to ensure that staff can be trained in operating the system
- Supports application level backups using the vendor provided tools that can be scheduled on a regular basis

Performance and capacity requirements

- Supports the peak traffic/number of simultaneous connections/connection rate that is expected
- Supports any load from the variously defined user communities
- Supports communications from multiple time zones
- Synchronizes with the approved trusted time source

Availability requirements

- Provides 99.999% availability
- Utilizes local and global replication features to support performance, failover, and high availability

Reliability requirements

- Meets any applicable service continuity requirements
- Detects and notifies when event data is corrupted
- Fails elegantly without taking any other infrastructure component or node down with it
- Provides disaster recovery and failover options

Monitoring and notification requirements

- Can be monitored using the approved system management capability
- Aligns with the security and network management program

Intrusion Prevention System (IPS)

IPS is one of the most valuable security systems that provides protection across all the layers with an attempt to identify and block/trigger alerts as per the actions defined as per the threat use cases.

Key requirements

The key requirements from a ransomware perspective include:

Operation requirements

- Supports processes and features for labeling custom checks, attack vectors, or other controlled events (for example, through a vulnerability description language)
- Provides the capability of declining updates (or rolling the system back to its previous state)
- Supports false negative notification (for example, notifying the IDS operator to the fact that the system cannot handle an intense workload and is starting to miss events)
- Processes fragmented packets
- Supports additional customization of each signature according to specific user requirements (for example, to reduce false positives)
- Notifies personnel when the IDS detects an attack, misuse, or another anomaly including sending a notification to the central console of the system, registering events in the event database, Syslog server, and so on
- Logs the type of event, date and time of detection, the sensor that detected that specific event, the source and destination addresses related to the event registered, and detailed content of all data fields related to the event
- Provides an event tracing mechanism that allows you to record all events in exactly the identical sequence and at precisely the same speed at which the hacker or intruder was operating
- Supports remote management of an unlimited number of sensors
- Supports a hierarchical management, allowing the system to switch between two consoles automatically, without user intervention
- Supports group operations (for example, updating the attack signature database, applying templates, and starting and stopping groups of sensors)
- Provides the ability to specify priorities for detected attacks and vulnerabilities both statically and dynamically

- Provides a comprehensive report generating mechanism (for example, reports at various levels of detail, information on the identified attack along with the operating systems and applications vulnerable to it, cases of false positives, methods of elimination, and so on)
- Supports prevention mechanisms including closing the network connection to the attacking host, blocking the intruder's user account, reconfiguring network equipment and security tools, automatic elimination of the vulnerability, and so on
- Protects against rogue access points
- Provides an intuitive working user interface to ensure that staff can be trained in operating the system
- Supports application level backups using the vendor provided tools that can be scheduled on a regular basis

Performance and capacity requirements

- Supports the peak number of simultaneous connections/traffic volume/connection rate that is expected.
- Note the number of packets that this node needs to handle should be computed at the protocol level and not at the business function or user activity level
- Supports any load from the variously defined user communities
- Supports communications from multiple time zones
- Synchronizes with the approved trusted time source

Availability requirements

- Provides 99.999% availability
- Utilizes local and global replication features to support performance, failover, and high availability

Reliability requirements

- Meets any applicable service continuity requirements
- Detects and notifies when event data is corrupted
- Fails elegantly without taking any other infrastructure component or node down with it

Maintainability requirements

- Provides updates to the signature database

- Uses industry standard repositories to store output data that supports local and geographic failover

Monitoring and notification requirements

- Can be monitored using the approved system management capability
- Aligns with the security and network management program

Key network security controls

The following are the key network security controls that should be focused upon across all size of businesses to protect against malware of all sizes:

Key Perimeter Categories	Sub Categories	Perimeter Controls
Network security	Network Security	Computer networks should be segregated from external networks and all connections to external networks including the Internet, outsourced vendors, and business partners should be authorized and provided in a secure manner.
Network security	Network Security	All remote access to the organization's network must be authenticated and provided based on business requirements.
Network security	Network Management Responsibility	Any changes on an organization's network, introduction of new networks, connection to external networks, and so on, should be done after consultation and approval from a corresponding IT security department.
Network security	Internet Access for organizations	The Internet access should be provided from a central location. All branches, administrative offices, and corporate center departments that are connected to the organization's backbone should access the Internet only through the organization's central gateway. Users located in remote offices should not be allowed to access the Internet through this gateway.

Key Perimeter Categories	**Sub Categories**	**Perimeter Controls**
Network security	Internet Access for organizations	Central Internet gateway should be set up and managed. All users should be authenticated before being allowed access. Users having Internet access privileges should have a unique user ID and password defined on the Internet gateway server. The user ID should be mapped to a specific IP address, which will reduce the chance of unauthorized access due to sharing of user ID.
Network security	Restricted URL/Internet Access for organizations	Internet URLs and portals that are restricted as per the organization's policy should have an exception provided only to the users with a business need. The user should send the request for Internet access, after approval from the IT-Networking Dept / Corporate Center.
a) Need for access		
b) Website(s) URL, if any specific requirement		
Network Security	Internet Access Limitation	Full Internet access should not be provided. There should be restriction on Internet access based on working time and day and download/upload limits should be defined for normal users.
Network Security	Internet Access Limitation	Internet connection should not be provided on desktops having privileged access to critical applications/databases, such as a desktop with administrator access to core business applications or databases.
Network Security	Security at Internet Gateway	Internet gateway should be secured through a Firewall, which should prevent any inbound access to the Internet Proxy.

Key Perimeter Categories	**Sub Categories**	**Perimeter Controls**
Network Security	Security at Internet Gateway	All normal or encrypted traffic through Internet gateway should be scanned for viruses and contents. Anti-virus software should be installed on the Internet gateway server and configured properly.
a) Whenever a user downloads/uploads a file, it should be scanned for viruses.		
b) If a virus is found, then the download/upload should terminate and the user informed on the status.		
c) Usage of the Internet should be consistent with the normal business requirements.		
Network Security	Security at Internet Gateway	Internet access should be controlled to ensure that only business related sites are accessible. URL filtering software should be used to automate the task of filtering essential websites. The IT networking department is responsible for implementing the access policy on the URL filter in consultation with security.
Network Security	Security at Internet Gateway	Monitoring should be performed at Internet Gateway level including Top Users, Most visited URL, and Policy Violation. Real-time live reports should be generated to assess the performance and volume of traffic being utilized.

Key Perimeter Categories	**Sub Categories**	**Perimeter Controls**
Network Security	Security at Internet Gateway	In the case of any major outbreak/security incident having a business wide impact, it should be ensured that impact is minimized by various means (policies on perimeter systems), which may include blocking of Internet access for the users.
Network Security	Segregating Server and User Segments	Critical application servers should be protected by Firewalls. These servers should be accessible only from their respective user segments. The Firewall should restrict user access to essential ports on the respective servers.
Network Security	Segregating Server and User Segments	For critical locations, network segmentation for different user groups should be implemented at network level.
Network Security	Segregating Server and User Segments	There exists restrictions on connection time for high-risk applications, which are considered sensitive. This can be achieved through manual policies on the enforcement points (firewalls, web application firewalls/proxies, and so on).
Network Security	External Networks	External networks should be separated from the organization's network through access control devices/network access control.
a) Depending on the type of access and criticality of application, the access control should be implemented either as access control lists on routers or through dedicated firewalls.		

Key Perimeter Categories	**Sub Categories**	**Perimeter Controls**
b) Access control devices should restrict access to essential IP addresses and ports. Wherever feasible, the resources that are required to communicate or accessed by the external network should be segregated on a separate segment of the firewall.		
c) Any access to such resources from the external network should be secured by user ID/password over an encrypted channel.		
d) An automatic session time-out should be set for remote-access technologies after a specific period of inactivity.		
e) IDS should be installed to monitor the traffic from external networks.		
f) All such access should be removed or disabled as soon as the requirement is over.		
Network Security	Network Management	Physical and logical ports and services, which are not specifically required for business functionality, should be protected by disabling/blocking.

Key Perimeter Categories	**Sub Categories**	**Perimeter Controls**
Network Security	Network Management	Equipment identification should be enabled on network devices based on the sensitivity of applications and data communication.
Network Security	Network Management	Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
Network Security	Network Management	Networks should be configured securely to not disclose any internal IP addresses and routing information to unauthorized users. Mechanisms including Network Address Translation (NAT), Port Address Translation (PAT), Filtering of route advertisements, and so on, should be implemented.
Network Security	Network Management	All default or vendor-supplied authentication credentials should be changed before deployment or use of Network/Security devices for the bank.
Network Security	Network Management	All remote access on network/security devices should be protected using cryptographic techniques such as SSH, VPN, and SSL for web-based management.
Network Security	Network Management	All network and security devices should be updated by respective application owners with latest upgrades and security patches regularly on release.

Key Perimeter Categories	Sub Categories	Perimeter Controls
Network Security	Network Management	All the network and security devices should be in time synchronization with a standard time device/server. This standard time device/server should be in sync with time values from industry accepted standards such as Internet/GPS. This time data should be protected from any unauthorized modifications.
Network Security	Access Controls on Network and Security Devices	Access to network devices should be controlled by access control lists.
Network Security	Access Controls on Network and Security Devices	Access to network/security devices should be provided on a need to have basis. Physical and logical access for diagnostic and configuration ports should be controlled.

Vulnerability assessments

Vulnerability assessments are point-in-time exercises intended to identify and analyze vulnerabilities associated with technology assets. This aids the organization to identify security loopholes that could be exploited by known malware variants. Vulnerability assessments focus on current operations including process, procedure, and state of technology assets.

Organizations must establish a formal program with defined roles and responsibilities for managing vulnerability scans and assessments, including:

- Development and management of vulnerability assessments processes and procedures.
- Architecture reviews.
- Security controls, limitations, network connections, and restrictions must be tested to assure conformance with applicable standards.
- Internal and external vulnerability scans must be run at least quarterly:
    - Internal scans must also be conducted after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

    - A vendor certified by the payment card industry must perform quarterly external vulnerability scans. Scans conducted after network changes may be performed by the company's internal staff.
- Penetration testing must be conducted at least once a year and after any significant infrastructure or application upgrade or modification (for example, major release, widespread upgrade of major router IOS version, change of border firewall vendor, and so on). Penetration testing must include:
    - Network-layer penetration tests
    - Application-layer penetration tests

These processes and procedures must include follow-up actions leveraging the IT Asset Management data (for example, configuration information, OS versions, and patch levels) to validate and track findings in order to determine appropriate remediation efforts

Vulnerabilities identified must be resolved according to the remediation management process.

Configuration management

Configuration management is the practice of standardizing the configuration of similar technology assets based on documented configurations developed by subject matter experts in accordance with applicable policies and approved by functional leadership.

Organizations must document baseline configurations for all technology assets. These standards must:

- Be designed in compliance with applicable security requirements
- Be kept up to date by the functional areas responsible for the technology asset
- Be integrated as part of the system build process and consistently enforced across all functional areas
- All technology assets must be configured consistently with the applicable baseline configuration

Patch management

The purpose of patch management is to identify controls and processes that will provide appropriate protection against threats that could adversely affect the security of the information system or data entrusted on the information system. Effective implementation of these controls will create a consistently configured environment that is secure against known vulnerabilities in operating system and application software.

It helps reduce vulnerabilities through the following phases:

- Performing security impact analysis of patches
- Testing and approving patches as part of any changes to system configuration
- Updates the existing or initial configurations to include the implemented patch
- Assessing patches to ensure they were implemented properly
- Monitoring systems/components for current patch status

Using leading industry standards such as NIST SP 800-40 helps establish a comprehensive patch management process.

Patch management also includes 'virtual patching', which uses Deep Packet Inspection and shields vulnerabilities in critical systems until an actual patch is available and deployed.

Vulnerability remediation management

Vulnerability remediation management is the practice of evaluating identified vulnerabilities, assigning risk based on likelihood and impact, planning an appropriate response, tracking the response through completion, and periodically verifying completion. Examples of processes that provide inputs to the vulnerability remediation management process include t*echnology risk assessments*, t*hreat monitoring*, and v*ulnerability Assessments*.

Organizations must evaluate the relevance of reported vulnerabilities and identify the associated risk to an organization's technology assets. The determination of risk must take into account:

- Hardware details, software versions, and the configuration of an organization's information systems as recorded in the asset inventory.
- The likelihood of occurrence.
- The impact of an occurrence.
- Any applicable compensating controls.

- Respective stakeholders from an organization must be notified immediately when there is a reason to believe there has been, or imminently will be, impact to the confidentiality, integrity, and/or availability of production system.
- All system components and software must have the latest vendor-supplied security patches installed within one month of approval by change management.
- The organization must identify an appropriate response to each technical vulnerability based on risk and the alternatives available. The response must consider the root cause(s) of the vulnerability. The technical vulnerability resolution may, among other things, include:
    - **Software Release**. If a software release is available to fix the vulnerability it should be tested and deployed following proper change management processes. Depending on the urgency of the deployment the change request may be submitted as an emergency change request.
    - **Compensating Control**. If no software release is available to address the vulnerability, or if the deployment of the software release is determined to create an unacceptable risk, alternative controls may be deployed to prevent the exploitation of the vulnerability. As in the case of the software release approach, an emergency change request may be appropriate. Examples of compensating controls include changes to technical configuration and standards and changes to processes.

Assessing ports, services, and protocols

It is crucial to determine which ports, services, and protocols are unnecessary by assessing which ones are the least used and do not support a functional use. Systems should be configured so that only the necessary ports, protocols, and services are integrated into support of the organization's functional needs and level of risk tolerance.

Any unnecessary open ports and available protocols and services provide entry points for attackers attempting to attack a system. These risks are increased if there are known vulnerabilities associated with a given port, protocol, or service.

In addition, the remote connections should be provided for system users with a defined functional requirement. If remote connections are approved for use by the organization, use the security requirement guidelines to identify the security configurations for remote access.

Secure software installation

It should be determined how the installation of software should be managed. The simplest approach is establishing controls on computers that prevent any self-installations by users and require software installation to be done at the organizational level. However, this option may not be practical for a few organizations. Other methods for controlling the installation of software that may be considered include:

- **Whitelisting**: All software is checked against a list approved by the organization
- **Checksums**: All software is checked to make sure the code has not changed
- **Certificate**: Only software with signed certificates from a trusted vendor is used
- **Path or domain**: Only software within a directory or domain can be installed
- **File extension**: Software with certain file extensions such as `.bat` cannot be installed

Specific measures

The following are the more narrowed down security measures that should be focused upon based on the type of ransomware to be protected against:

- There have been multiple instances wherein security vendors have emulated the domain generation algorithm and can disseminate this to organizations so they can block the domains that particular ransomware is likely to be using in the future. Blocking these domains in advance will improve the likelihood of preventing the key from being sent to the victim, and hence obstruct malware's ability to encrypt users' files.
- If a malware does infect systems in your organization and successfully encrypts files, it is advised to disconnect infected hosts from the network and shut down the computers promptly (hard shut down). It may be possible to forensically restore some files that are on the disk that may not have been overwritten.

Instances of infected systems can also be reported to the FBI at `https://www.ic3.gov`.

- Performing regular image backups at the local level and data backups at the enterprise level is essential to recover from an attack. It is recommended that system restore is enabled on hosts. It is also advised to keep a recent backup offsite. Besides enabling the recovery of backed up files, a system restore will help ensure that the host is cleaned of primary and secondary malware.
- Network detection and **domain name system** (**DNS**) monitoring are advised. Our research observed the following network and DNS indicators:
    - Modern malware frequently generates new domains on a daily basis.
    - It scans domains for successful resolution.
    - Malicious domains show as new in DNS cache.
    - NXD - the majority of these domains will not resolve and multiple NXD responses will be observed from one asset in less than a minute.
    - Domains are pseudo-randomly generated and contain higher entropy than typical domains. These domains are measured at 3.7 bits/bytes and above.
- Restrict all the employee's permissions to "read" until otherwise other methods are required as per the business.
- Review and audit accesses periodically to shared folders.
- Configure organization security policies to restrict macros (by default), restrict execution of `.exe` files until approved (or create a whitelist), and restrict auto play from devices and services when connected to the host.
- Educate and provide to employees periodically.
- The following are two samples of detection logic specifically for Cryptolocker, which may enable detection based on these observables:
    - `If asset > 10 DNS_NXD_RESPONSE < 30s then Alert andand Quarantine(Asset)`
    - `If DNS_Request == NON_Cached || NXD andand Entropy(Domain) > 3.70 then Alert andand Quarantine(Asset)`

Summary

Today, these advanced malwares primarily target files that are handled by end users either for professional or personal usage. Active directories, exchanges, cloud applications, and so on, have not been targeted precisely until now by such ransomware, but this is one of those sides that can change in the future - principally due to the importance and value of such elements towards an organization. It is highly recommended to define a comprehensive security architecture and practice security controls as per the organization's threat landscape since, even when the malware transforms and revolutionizes our base practices will be in a position to provide a strong defense at all sophisticated ransomware.

In the next chapter, we will emphasize on mobile ransomware and will look at how extortion is reaching the masses via mobile devices.

6
Exploring Mobile Extortions

The number of users getting infected with mobile ransomware is incrementing day by day and of late it was identified that this trend has almost increased by four times over the last year. This chapter emphasizes on mobile ransomwares and details how via mobile devices extortion is reaching common people.

The topics covered in this chapter are as follows:

- Mobile malware - an increasing security risk
- Mobile ransomware
- Ransomware timeline
- Protecting your mobile phone
- Future predictions

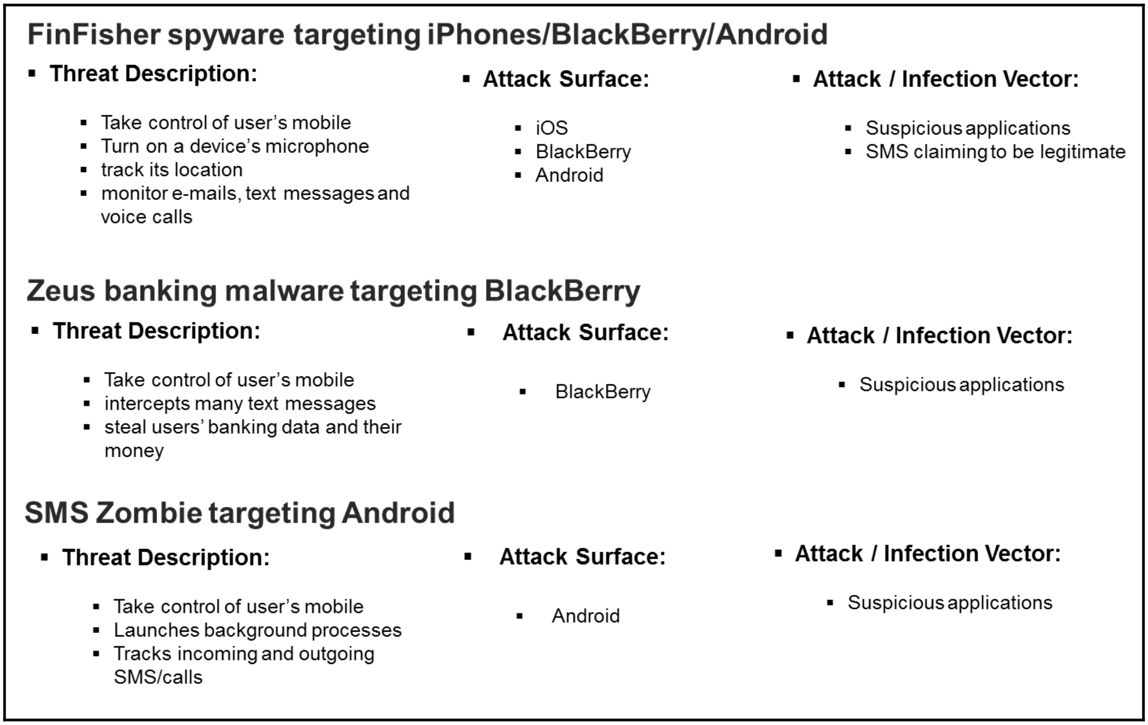
Mobile malware - an increasing security risk

Extortion and ransomware is an ever growing challenge for the users of mobile devices. As we had discussed earlier, locking and file encrypting variants of malware have been triggering multiple infections transcending financial and data losses across industries. Such lock screen and crypto ransomware have made their way to multiple mobile platforms.

Similar to malware on computing devices, malware threats are evolving in recent times adding sophisticated techniques. Malware authors/operators are implementing and embracing similar techniques that have proven to be effective against desktop computing environments in addition to traditional types of mobile malware, for instance - SMS Trojans.

As during early times with Windows operating system, mobile platforms too now face the lock screens with police ransomware type of scareware that tricks the victims deceptively accusing of accessing illegal content via their devices. In addition, Cryptolocker ransomware has revolutionized the malware trend with significant extortion campaigns - it also expands itself to mobile platforms having an enormous impact to the mobile users having practically no way to reclaim the files.

Mobile devices these days contain everyday data used by organizations and individuals, that is, average individuals prefer to keep data on smartphones for easy and quick access than PCs, which gives an opportunity to malware authors to utilize and exploit this chance, increasing the risk of losing data. If we notice the trend, the malware authors have already started targeting users across European and American markets. Multiple variants of Simplocker and Lockerpin was observed infecting victims primarily in the USA.



FinFisher spyware targeting iPhones/BlackBerry/Android

- **Threat Description:**
  - Take control of user's mobile
  - Turn on a device's microphone
  - track its location
  - monitor e-mails, text messages and voice calls
- **Attack Surface:**
  - iOS
  - BlackBerry
  - Android
- **Attack / Infection Vector:**
  - Suspicious applications
  - SMS claiming to be legitimate

Zeus banking malware targeting BlackBerry

- **Threat Description:**
  - Take control of user's mobile
  - intercepts many text messages
  - steal users' banking data and their money
- **Attack Surface:**
  - BlackBerry
- **Attack / Infection Vector:**
  - Suspicious applications

SMS Zombie targeting Android

- **Threat Description:**
  - Take control of user's mobile
  - Launches background processes
  - Tracks incoming and outgoing SMS/calls
- **Attack Surface:**
  - Android
- **Attack / Infection Vector:**
  - Suspicious applications

Early mobile malware samples

Mobile ransomware

We have already discussed ransomware in the earlier chapters and extortion across multiple streams - that is, malware that infects a user's system or computing resources and then demands a ransom from the users to release those hijacked resources. The major categories for mobile ransomware and extortion include the same - lock screen and crypto ransomware.

In the former form of malware, cybercriminals would target the resources, in turn restricting access to the device, whereas the later form of malware emphasizes on controlling the files residing on mobile devices. Both types of malware have been predominantly active in the operating system space since 2013, even though they have existed for years. Mobile ransomware authors have been targeting individuals as well as businesses.

As with the trends observed with malware in the operating system for end user computing devices, ransomware authors have commenced creating targeted malware for mobile devices with similar techniques and sophistication seen on Windows and other OS malware. It would be logical to assume that such trends would be seen also with evolving technology ecosystem such as IoT.

Data stored on mobile devices is valuable, comprehensive, and is used extensively than what individuals used to store and work with PCs. Thus, malware authors find it extremely worthwhile to invest their time in customizing most sophisticated malware for mobile devices across multiple platforms.

Common infection vectors

Malware targeting PC's that are primarily used for extortion classically fulfill the definition even for mobile devices - that is, infecting and spreading across devices, masquerading as a legitimate application. In most cases widely held applications from gaming, general utility, and pornography-related industries are chosen to increase the probability of a user to view and download the application (which is essentially a malware). In multiple scenarios, the **apk's** (**application packages**) only resemble the mobile icon and name of the actual application, although in other scenarios malware authors in addition to the original function of the application extend the code that is malicious in nature. In multiple cases, this increases the odds of malicious behavior going undetected.

Certainly, once a malware author redefines the code, it breaks the digital signature of the application package. Thus, the author now has to resign the application and submit it with a different developer account. In more than 95% of cases, ransomware may not be found on the official application stores, but the ways in which a general user is tricked to download the application is transcending with time. There have been instances wherein multiple security vendors have reported multiple samples of malware such as AV scareware, phishing spyware, and ads redirecting to malicious application to companies such as Google and Apple.

Malware authors are customizing and varying the techniques for infecting users since sophisticated exploit driven techniques do not work very well on mobile platforms. For instance, prior to the actual payload being tossed, at an intermediate stage a dropper application is used.

Malware Command and Control communication

As with the majority of malware used for extortion, once successfully deployed most of the malware reports back to a **Command and Control** (**C2**) server. For mobile devices, in most of the circumstances it is reported to C2 for tracking, sending device information, for example - the model of the device, IMEI number, the language of the device, the location of the device, and so on. On the other hand, if a stable consistent channel is established between the device and C2 then the possibility is high of the malware listening and executing commands provided by the ransomware operators via C2. This also further goes beyond to create a network of infected mobile devices to have the malware operator control over the botnet created by such malware.

A few of the following functions and commands have been dissected by ransomware targeting mobile platforms in addition to its primary function of locking the device or displaying the ransom instructions to the user:

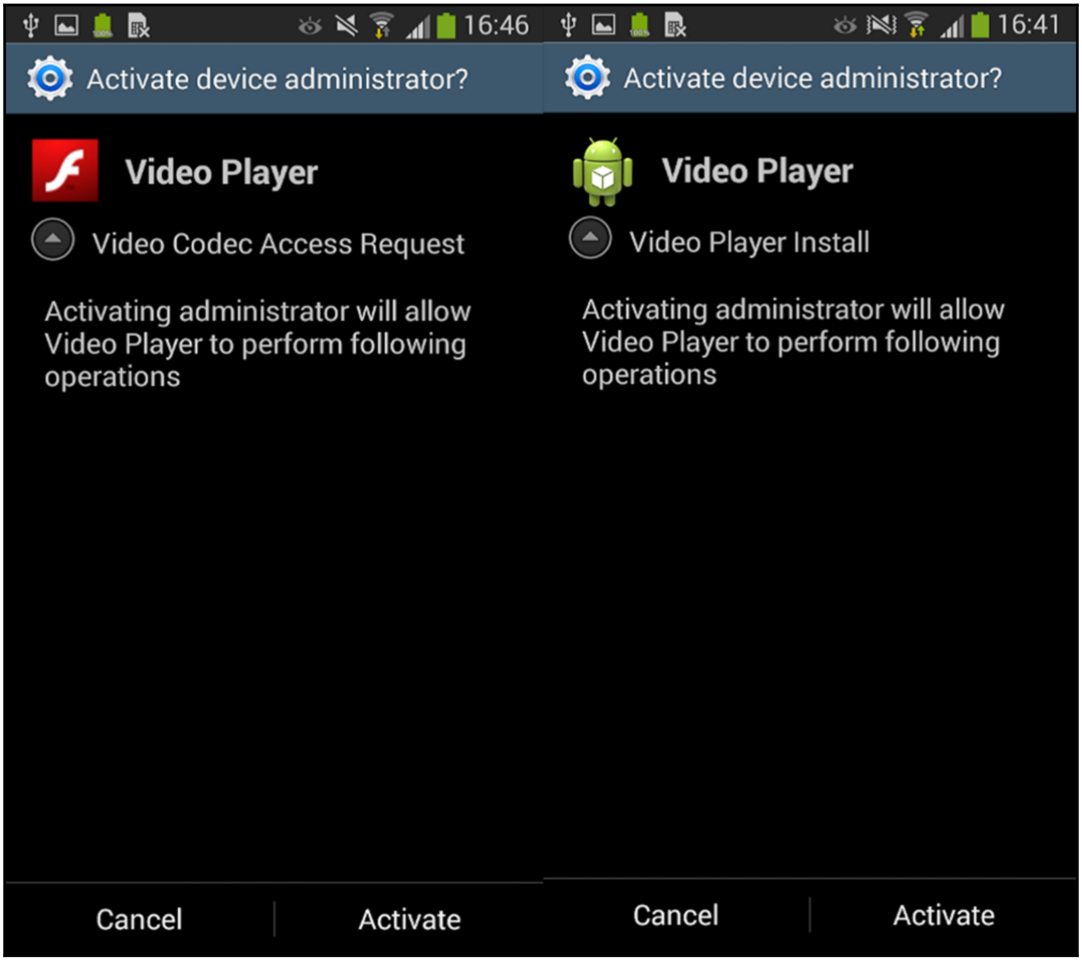
- Executing or invoking an arbitrary URL in the phone's browser
- Sending an SMS message to infected phone's contacts with malicious links
- Locking and unlocking the device
- Copying contacts
- Displaying a ransom message in the local language as per the location of the device
- Enabling or disabling mobile data/Wi-Fi

In mobile platforms the most typical communication protocol used is HTTP and in certain cases malware has been identified communicating via Google Cloud Messaging to its Command and Control center. The Google Cloud messaging service generally provisions users/developers to traverse data (inflow and outflow/receive and send) to and from the application on the supported devices (predominantly Android). Some of the other malware use Tor, Baidu, and XMPP-Jabber protocols and services. Malware targeting Android mobile platforms have also been seen communicating using the built-in SMS services for sending or receiving commands to the relevant Command and Control center.

Malware self-protection

Infecting a device with malware is not a minor task for cybercriminals since even if users don't have any anti-malware protection in place there are defensive measures provided by the corresponding mobile platforms. Once such measures are overcome, the prime focus of the malware author/operator is to make certain that their malicious code/application remain in the device persistently. To force this, malware authors embed/define multiple self defense mechanisms and techniques within the application code for instance identifying and killing processes that show anti malware application behavior. This technique was seen in multiple malware such as Lockerpin for Android mobile platform.

Amongst all, one of the primary techniques that most of the malware across mobile device platforms focuses on achieving is obtaining administrative privileges of such devices. It is important to understand that the administrative privileges for the device are not the same as the device root access (which is even more dangerous if attained by the corresponding malware), but it provides basic crucial privileges for the malware to act and control the device.



Activate device administrator?

Video Player

Video Codec Access Request

Activating administrator will allow Video Player to perform following operations

Activate device administrator?

Video Player

Video Player Install

Activating administrator will allow Video Player to perform following operations

Instances of malware asking for device administrator privileges

Such privileges are used by utilities and system-related applications for security-related activities. In contrast malware utilizes such capabilities to defend itself against intended uninstallations. This also signifies that before such applications are to be uninstalled, corresponding device administrator privileges needs to be revoked first. For example, renowned malware such as Lockerpin use exclusive device administrative privileges to set or alter the lock screen PIN.

Analysis of mobile malware sample - SMS Zombie

In this section, we will focus on analyzing a sample mobile malware to decompose the malware life cycle.

Tools utilized:

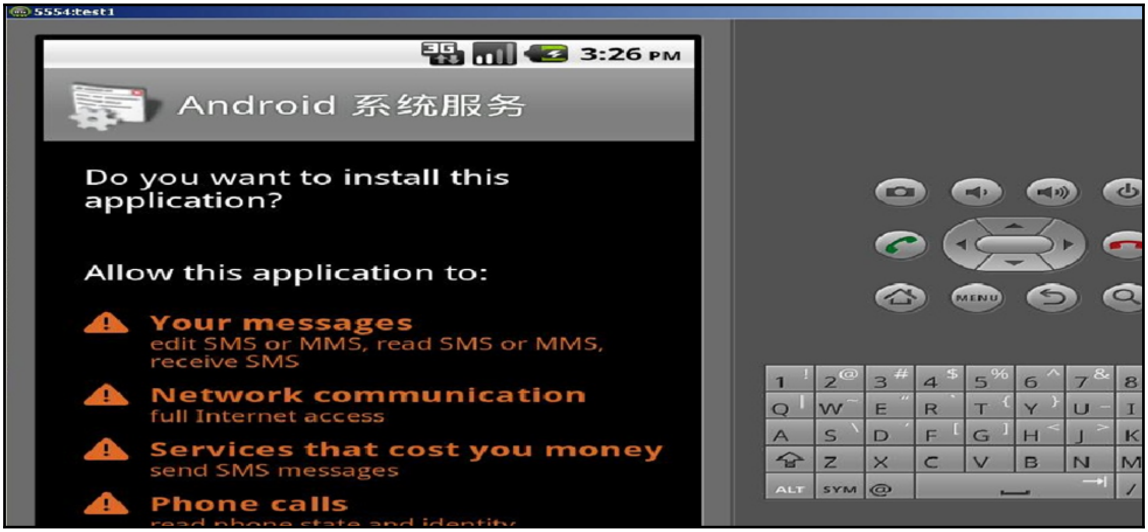
Dex2jar, JAD, Android SDK, and Dalvik Debugger Monitor

Platform affected:

Android

Malware:

SMS Zombie



5554:test1

3:26 PM

Android 系统服务

Do you want to install this application?

Allow this application to:

Your messages
edit SMS or MMS, read SMS or MMS, receive SMS

Network communication
full Internet access

Services that cost you money
send SMS messages

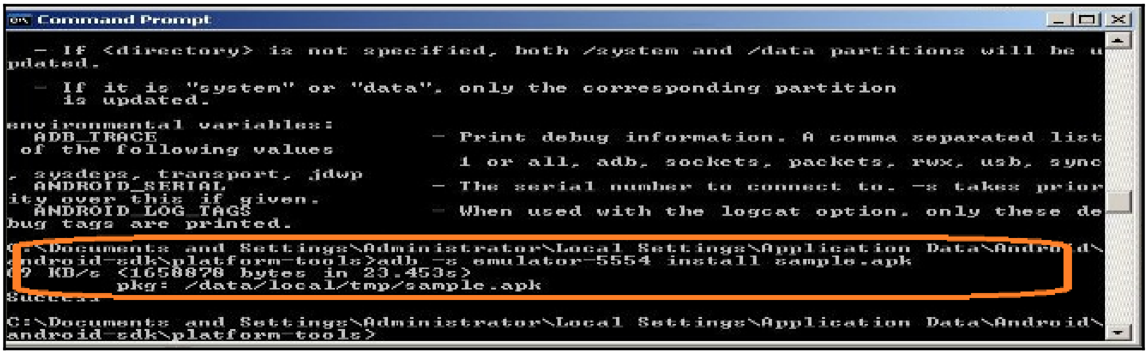
Phone calls
read phone state and identity

Sample installation of the application

Analysis observations

The following observations can be seen from the analysis:

- Once installed, malware gains permission to edit/read/receive SMS, and read incoming and outgoing calls
- **Dalvik Debugger Monitor** (**DDM**) was used to observe the changes done to log files, file permissions being given to the malware, and payloads being deployed on the Android device
- Through DDM, it was observed that two files named `android.phone.com` and `com.xqxmn18.pic` were being added to the data files of the Android device.
- While opening these files, it was observed that they contain other `.apk` files, which in turn contain `.xml` files having the phone number of the malware author to which the payload deployed on the Android device sends trapped information to.

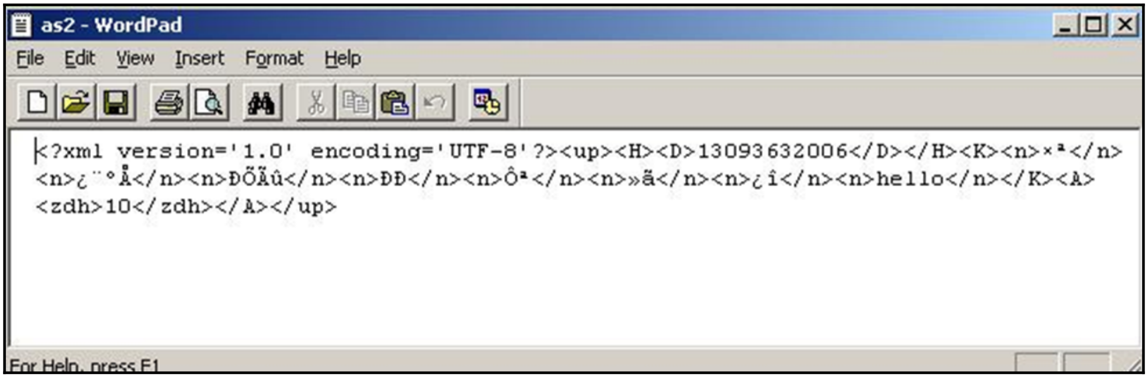


```
  - If <directory> is not specified, both /system and /data partitions will be u
pdated.

  - If it is "system" or "data", only the corresponding partition
    is updated.

environmental variables:
  ADB_TRACE                    - Print debug information. A comma separated list
 of the following values
                                 1 or all, adb, sockets, packets, rwx, usb, sync
, sysdeps, transport, jdwp
  ANDROID_SERIAL               - The serial number to connect to. -s takes prior
ity over this if given.
  ANDROID_LOG_TAGS             - When used with the logcat option, only these de
bug tags are printed.

C:\Documents and Settings\Administrator\Local Settings\Application Data\Android\
android-sdk\platform-tools>adb -s emulator-5554 install sample.apk
69 KB/s (1658070 bytes in 23.453s)
        pkg: /data/local/tmp/sample.apk
Success

C:\Documents and Settings\Administrator\Local Settings\Application Data\Android\
android-sdk\platform-tools>
```

Analysis of the malware

Static analysis

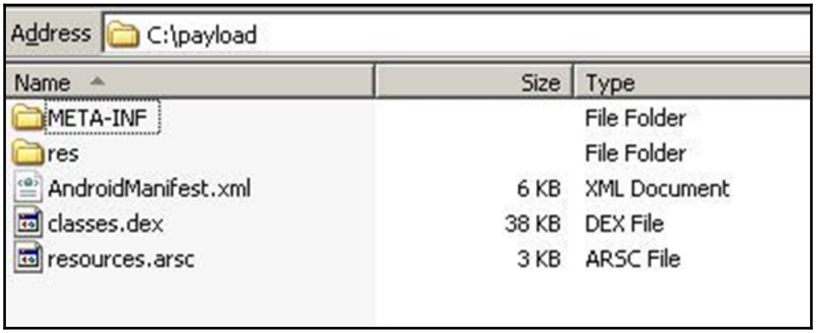
The following section demonstrates the static analysis on the mobile malware:



```
<?xml version='1.0' encoding='UTF-8'?><up><H><D>13093632006</D></H><K><n>×ª</n>
<n>¿¨°Å</n><n>ĐÕÃû</n><n>ĐĐ</n><n>Ôª</n><n>»ã</n><n>¿î</n><n>hello</n></K><A>
<zdh>10</zdh></A></up>
```

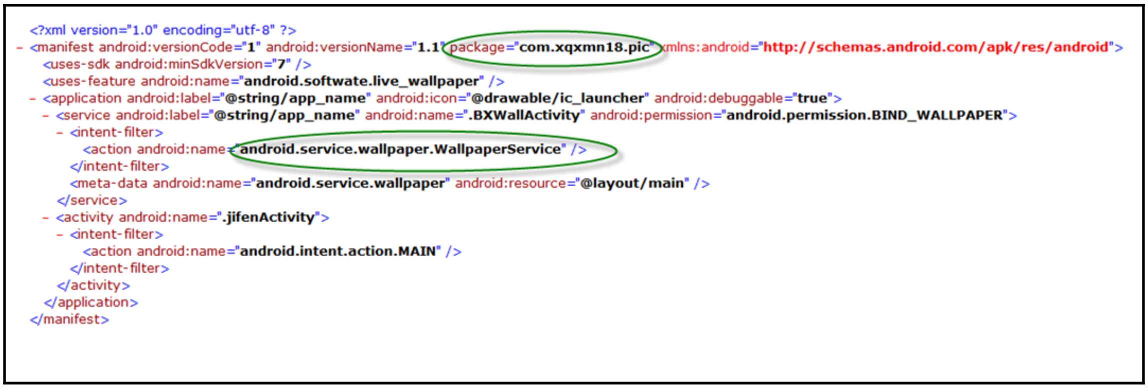
Android manifest

- While performing the dynamic analysis, it was observed that the payload was being deployed in the device by the malware. It consists of other `.apk` files consisting of an `AndroidManifest.xml` file:



Name	Size	Type
META-INF		File Folder
res		File Folder
AndroidManifest.xml	6 KB	XML Document
classes.dex	38 KB	DEX File
resources.arsc	3 KB	ARSC File

- Converting the binary XML file to human readable XML format using Apktool, it was observed that the `AndroidManifest.xml` file in turn calls the `com.xqxmn18.pic` package and send an SMS to the malware author.
- Using the Dex2jar tool to convert the `.dex` files to a `.jar` file and then decompiling the `.jar` file using the JAD tool (Java decompiler) to the `.java` file to perform the complete code analysis:



```
  <?xml version="1.0" encoding="utf-8" ?>
- <manifest android:versionCode="1" android:versionName="1.1" package="com.xqxmn18.pic" xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="7" />
    <uses-feature android:name="android.softwate.live_wallpaper" />
  - <application android:label="@string/app_name" android:icon="@drawable/ic_launcher" android:debuggable="true">
    - <service android:label="@string/app_name" android:name=".BXWallActivity" android:permission="android.permission.BIND_WALLPAPER">
      - <intent-filter>
          <action android:name="android.service.wallpaper.WallpaperService" />
        </intent-filter>
        <meta-data android:name="android.service.wallpaper" android:resource="@layout/main" />
      </service>
    - <activity android:name=".jifenActivity">
      - <intent-filter>
          <action android:name="android.intent.action.MAIN" />
        </intent-filter>
      </activity>
    </application>
  </manifest>
```

Static Analysis of the file

Possible infection vectors of mobile malware include:

- E-mails/Spam
- Suspicious applications
- SMS
- Compromised sites
- Malicious websites

Impact of mobile malware primarily includes:

- **Infiltration**: A successful attack can potentially bypass the credentials and access the target system
- **Information theft, information disclosure**: A successful attack can potentially lead to disclosure of enterprises sensitive data
- **Brand reputation damage:** Malware authors may target different vulnerabilities in mobile computing platforms
- **Business operation disruption**: Malware can potentially exploit security hole/vulnerability that may affect the availability of services from the enterprise
- **Exploitation**: Malware can potentially exploit software vulnerability in an enterprise to gain information access/control of the target system

Ransomware timeline

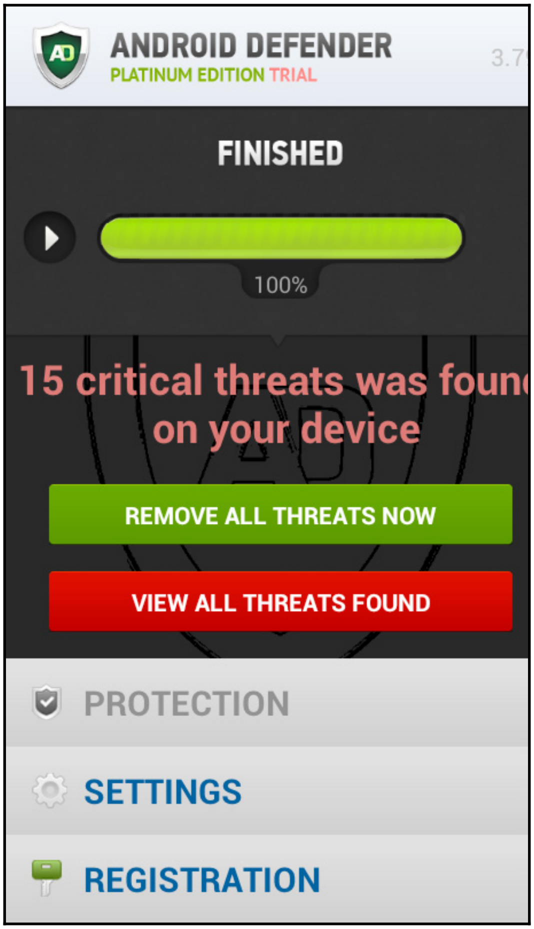
Initial presence of ransomware on mobile devices were mainly scenarios wherein extortion functionality was added to fake anti viruses (impersonating a legitimate anti-virus application). Fake AV's have existed for a long time and they are available on mobile platforms from as early as 2011 and on desktop environments since 2004. These malwares primarily imitate an antivirus scan across all the files and folders of the mobile device, and then ask users for money to eliminate all the threats from the infected files. Such malware is also called Scareware due to the reason that they extort money from infected victims after giving them a fake alarm making them believe that their device is infected with multiple malware.

Fake AVs may or may not be considered as ransomware. It depends upon the key characteristics of the application. Some Fake AVs target to trick infected victims to pay to show the false alarms of malware persisting on the device, whereas on the other hand, some of them have ransomware built into it and force the user to pay for unlocking the device.

Ransomware and extortion attempts were primarily seen with lock screen malware on Windows with multiple tricky messages supposedly representing law enforcement agencies, FBI, and local polices used to scare the infected users and as penalty asked them for payments.

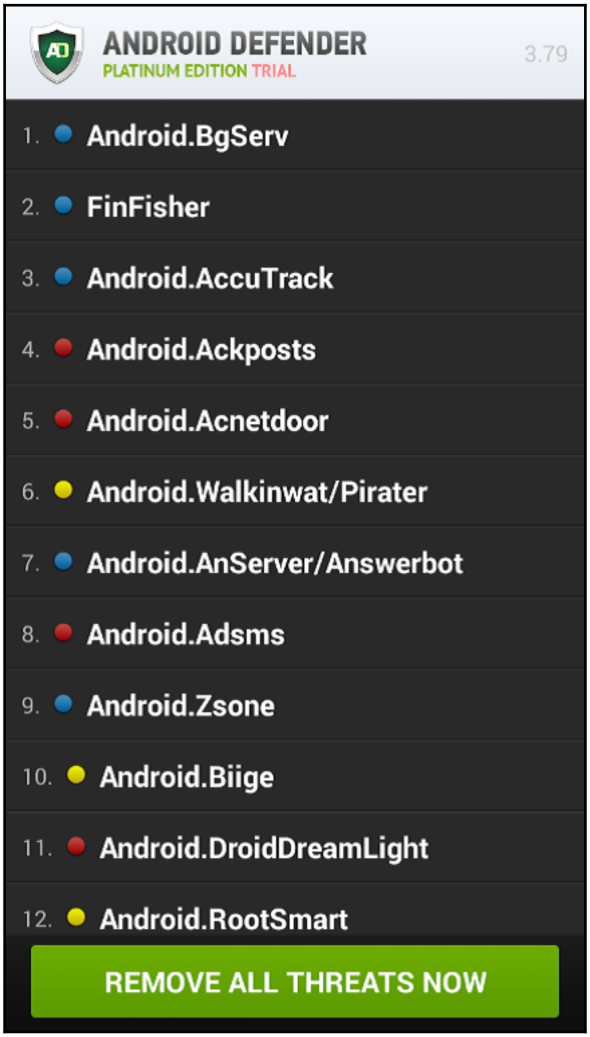
Android Defender

Defender, an instance of fake antivirus can perhaps be called the first ransomware that targeted Android-based mobile devices. It was initially identified in late 2012 - mid 2013. The following screenshot shows the GUI of the application that tricks the user to believe that the application is a legitimate anti-virus application with similar behavior. It also shows the multiple stages of the application.



15 critical threats was foun
on your device

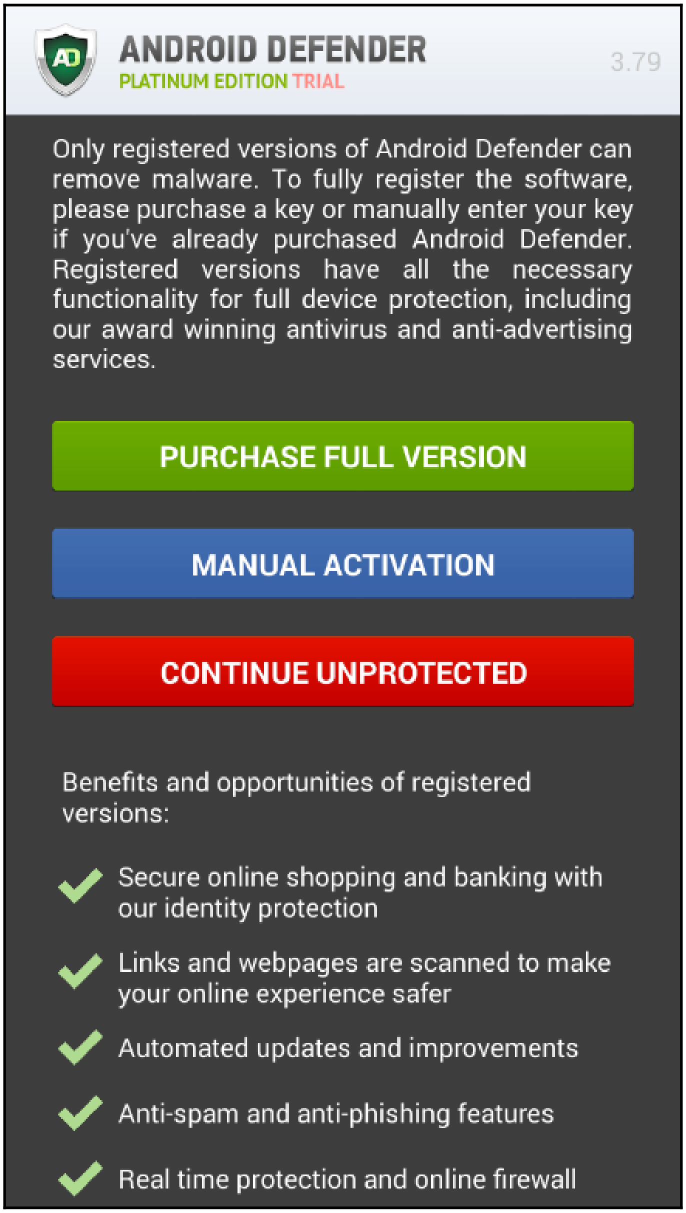
This is one of those malware that displays the name of different types of malware (which actually exist) including actual files and folders existing on the mobile device and memory card tricking its users to assume the application as legitimate.



1. Android.BgServ
2. FinFisher
3. Android.AccuTrack
4. Android.Ackposts
5. Android.Acnetdoor
6. Android.Walkinwat/Pirater
7. Android.AnServer/Answerbot
8. Android.Adsms
9. Android.Zsone
10. Android.Biige
11. Android.DroidDreamLight
12. Android.RootSmart

Fake AV

The good thing about the application is that the user still has control of whether they would like to continue using the application, leaving their devices unprotected.

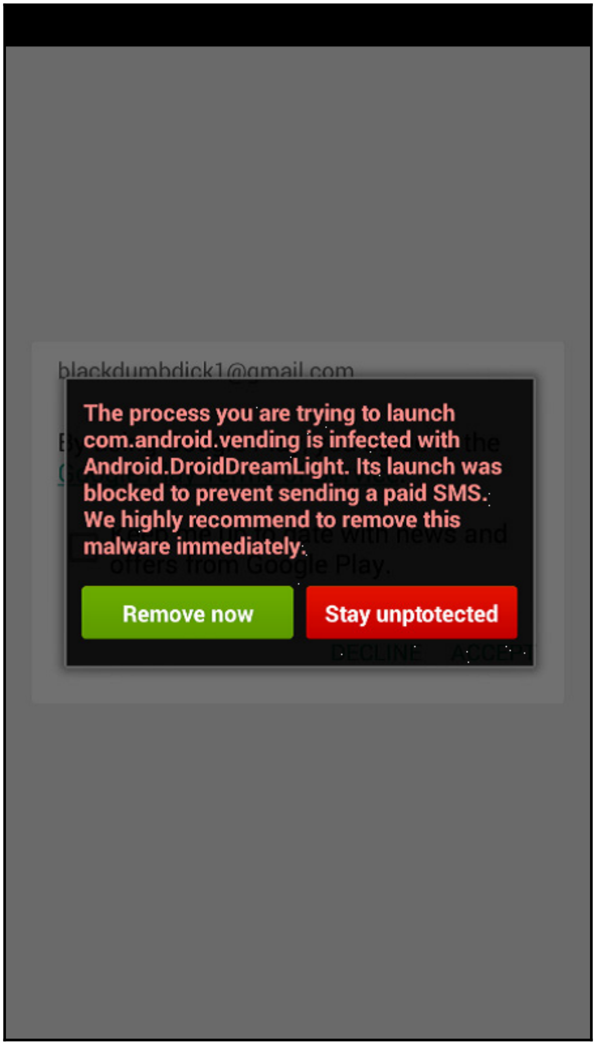


Only registered versions of Android Defender can remove malware. To fully register the software, please purchase a key or manually enter your key if you've already purchased Android Defender. Registered versions have all the necessary functionality for full device protection, including our award winning antivirus and anti-advertising services.

Benefits and opportunities of registered versions:

- ✓ Secure online shopping and banking with our identity protection
- ✓ Links and webpages are scanned to make your online experience safer
- ✓ Automated updates and improvements
- ✓ Anti-spam and anti-phishing features
- ✓ Real time protection and online firewall

Nonetheless, on the other side - the application makes the device unusable by displaying popups and multiple notifications every time the user clicks on any application. If the users click on the red button, it dismisses the notification popup, but generates another popup disrupting the user's experience.



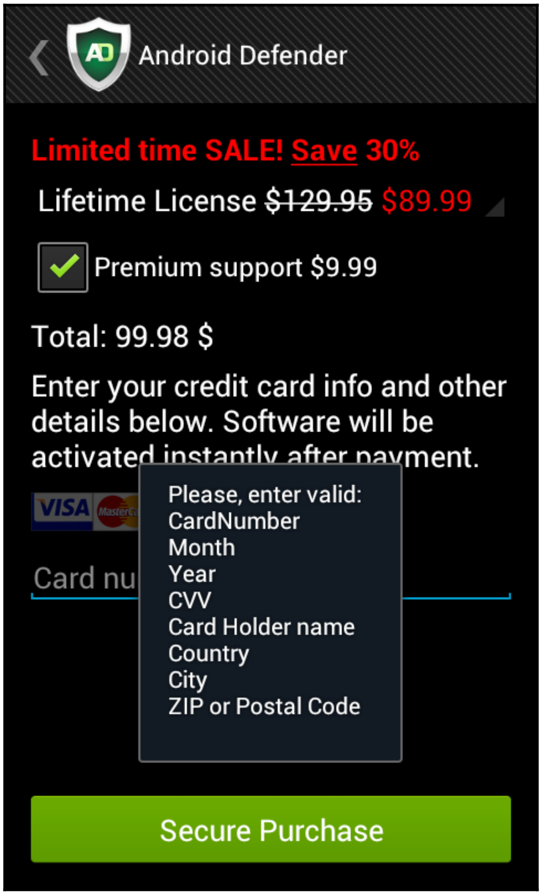
blackdumbdick1@gmail.com

The process you are trying to launch com.android.vending is infected with Android.DroidDreamLight. Its launch was blocked to prevent sending a paid SMS. We highly recommend to remove this malware immediately.

Malware popups

The application also has a more aggressive mode that invokes after six hours once the application is launched. It then shows a full screen with adult images that cannot be closed until the time the infected user pays up the amount demanded.

The following screenshot shows the sample wherein $99.98 USD is being charged and the user is asked to provide lot of critical data representing their credit cards, personal information, and so on. The infected user's credit data once shared could also be used for further misuse.



Limited time SALE! Save 30%

Lifetime License ~~$129.95~~ $89.99

☑ Premium support $9.99

Total: 99.98 $

Enter your credit card info and other details below. Software will be activated instantly after payment.

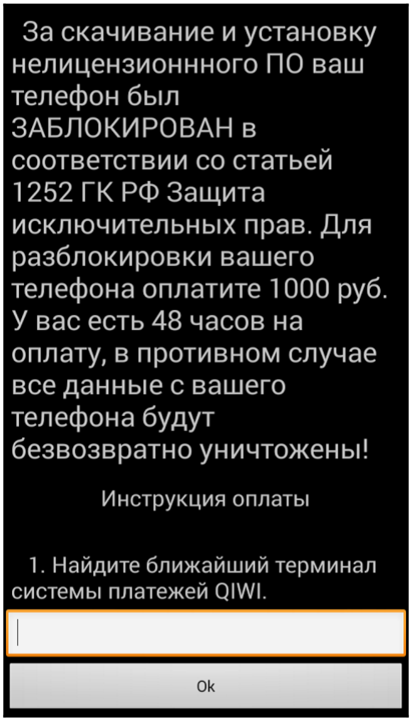
Please, enter valid:
CardNumber
Month
Year
CVV
Card Holder name
Country
City
ZIP or Postal Code

Purchase options

Police ransomware

We have discussed a lot of malwares having Lock screen as one of the themes across multiple variants. Some lock screens gave the impression as a **Blue Screen of Death** (**BSOD**) and some showed the windows activating message. The most predominantly used lock screen was the notification screen impersonating messages of FBI or police claiming that the infected users system is locked due to illegal activity being traced from their systems.

Reveton is one of the known variants. The ransom messages that get notified also at time quote relevant Criminal Code, but they do mention that the user can get away paying a fee. One of the interesting aspects is that the malware uses IP-based geolocation capabilities to customize the ransom messages and the locking screen as per the law relevant to the local region.



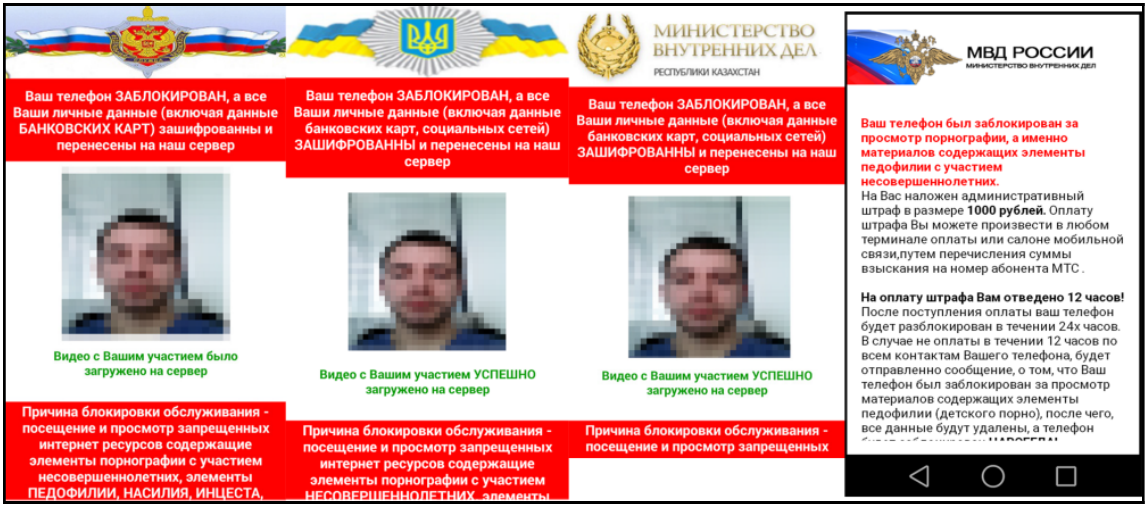
За скачивание и установку нелицензионнного ПО ваш телефон был ЗАБЛОКИРОВАН в соответствии со статьей 1252 ГК РФ Защита исключительных прав. Для разблокировки вашего телефона оплатите 1000 руб. У вас есть 48 часов на оплату, в противном случае все данные с вашего телефона будут безвозвратно уничтожены!

Инструкция оплаты

1. Найдите ближайший терминал системы платежей QIWI.

Initial malware variants targeting Russian speaking users

The initial samples of this type of ransomware on mobile devices were seen in the first half of 2014 and they were targeting Russian speaking mobile users. Though it was not long until English variants came into the picture with location aware malware being introduced targeting global mobile users.



Ваш телефон ЗАБЛОКИРОВАН, а все Ваши личные данные (включая данные БАНКОВСКИХ КАРТ) зашифрованны и перенесены на наш сервер

Видео с Вашим участием было загружено на сервер

Причина блокировки обслуживания - посещение и просмотр запрещенных интернет ресурсов содержащие элементы порнографии с участием несовершеннолетних, элементы ПЕДОФИЛИИ, НАСИЛИЯ, ИНЦЕСТА,

Ваш телефон ЗАБЛОКИРОВАН, а все Ваши личные данные (включая данные банковских карт, социальных сетей) ЗАШИФРОВАННЫ и перенесены на наш сервер

Видео с Вашим участием УСПЕШНО загружено на сервер

Причина блокировки обслуживания - посещение и просмотр запрещенных интернет ресурсов содержащие элементы порнографии с участием

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

Ваш телефон ЗАБЛОКИРОВАН, а все Ваши личные данные (включая данные банковских карт, социальных сетей) ЗАШИФРОВАННЫ и перенесены на наш сервер

Видео с Вашим участием УСПЕШНО загружено на сервер

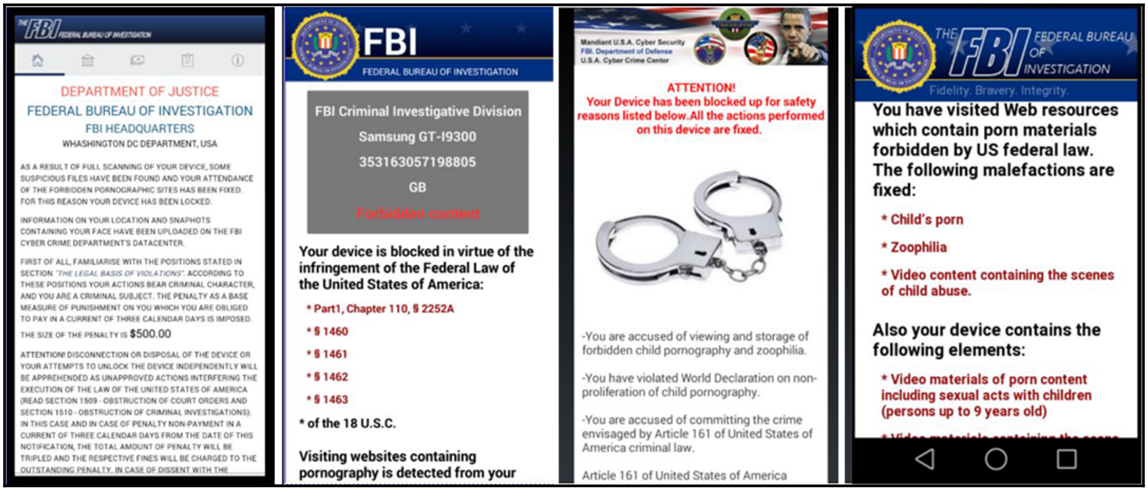
Причина блокировки обслуживания - посещение и просмотр запрещенных

МВД РОССИИ
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ

Ваш телефон был заблокирован за просмотр порнографии, а именно материалов содержащих элементы педофилии с участием несовершеннолетних.
На Вас наложен административный штраф в размере **1000 рублей.** Оплату штрафа Вы можете произвести в любом терминале оплаты или салоне мобильной связи,путем перечисления суммы взыскания на номер абонента МТС .

На оплату штрафа Вам отведено 12 часов!
После поступления оплаты ваш телефон будет разблокирован в течении 24х часов. В случае не оплаты в течении 12 часов по всем контактам Вашего телефона, будет отправленно сообщение, о том, что Ваш телефон был заблокирован за просмотр материалов содержащих элементы педофилии (детского порно), после чего, все данные будут удалены, а телефон

Locker malware variants also showing a camera shot with messages in multiple languages example shows Russian, Ukrainian, and Kazakh banners



THE FBI FEDERAL BUREAU OF INVESTIGATION

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WHASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION *"THE LEGAL BASIS OF VIOLATIONS"*. ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED. THE SIZE OF THE PENALTY IS $500.00

ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS NOTIFICATION, THE TOTAL AMOUNT OF PENALTY WILL BE TRIPLED AND THE RESPECTIVE FINES WILL BE CHARGED TO THE OUTSTANDING PENALTY. IN CASE OF DISSENT WITH THE

FBI
FEDERAL BUREAU OF INVESTIGATION

FBI Criminal Investigative Division
Samsung GT-I9300
353163057198805
GB
Forbidden content

Your device is blocked in virtue of the infringement of the Federal Law of the United States of America:

* Part1, Chapter 110, § 2252A
* § 1460
* § 1461
* § 1462
* § 1463

* of the 18 U.S.C.

Visiting websites containing pornography is detected from your

Mandiant U.S.A. Cyber Security
FBI. Department of Defense
U.S.A. Cyber Crime Center

ATTENTION!
Your Device has been blocked up for safety reasons listed below.All the actions performed on this device are fixed.

-You are accused of viewing and storage of forbidden child pornography and zoophilia.

-You have violated World Declaration on non-proliferation of child pornography.

-You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.

Article 161 of United States of America

THE FBI FEDERAL BUREAU OF INVESTIGATION
Fidelity. Bravery. Integrity.

You have visited Web resources which contain porn materials forbidden by US federal law. The following malefactions are fixed:

* Child's porn

* Zoophilia

* Video content containing the scenes of child abuse.

Also your device contains the following elements:

* Video materials of porn content including sexual acts with children (persons up to 9 years old)

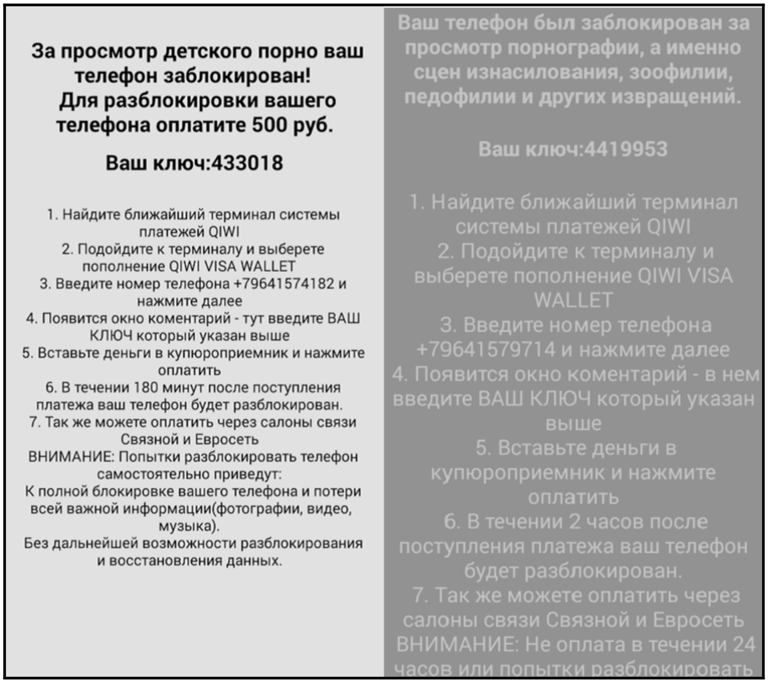
Malware variants transforming with change in English language

Simplocker

In the second quarter of 2014 multiple file encryption ransomwares were identified for mobile devices. It was during this time that such types of malware were seen massively infecting Windows users (Cryptolocker, CTB-Locker, and Crypto Wall being some of the renounced ones) across the globe. Once the malware is launched, it displays a ransom message as shown in the trailing figure (Figure 14) and in a background process it initiates to encrypt files.

Simplocker primarily scans the mobile devices and the SD card for files with multiple image file extensions (such as `.jpg`, `.png`, and so on), document file formats (such as PDF, DOC, and so on), media format (such as MP4, AVI, and so on), and get them encrypted with AES cipher (which is one of the strong variants of encryption).

It was also identified that the encryption key was hardcoded inside the application binary (in plain text) unlike the conventional crypto ransomware variants targeting Windows operating system. This also signifies that the earlier versions of the malware were prematured and were in early development or proof of concept stage.



За просмотр детского порно ваш телефон заблокирован!
Для разблокировки вашего телефона оплатите 500 руб.

Ваш ключ:433018

1. Найдите ближайший терминал системы платежей QIWI
2. Подойдите к терминалу и выберете пополнение QIWI VISA WALLET
3. Введите номер телефона +79641574182 и нажмите далее
4. Появится окно коментарий - тут введите ВАШ КЛЮЧ который указан выше
5. Вставьте деньги в купюроприемник и нажмите оплатить
6. В течении 180 минут после поступления платежа ваш телефон будет разблокирован.
7. Так же можете оплатить через салоны связи Связной и Евросеть

ВНИМАНИЕ: Попытки разблокировать телефон самостоятельно приведут:
К полной блокировке вашего телефона и потери всей важной информации(фотографии, видео, музыка).
Без дальнейшей возможности разблокирования и восстановления данных.

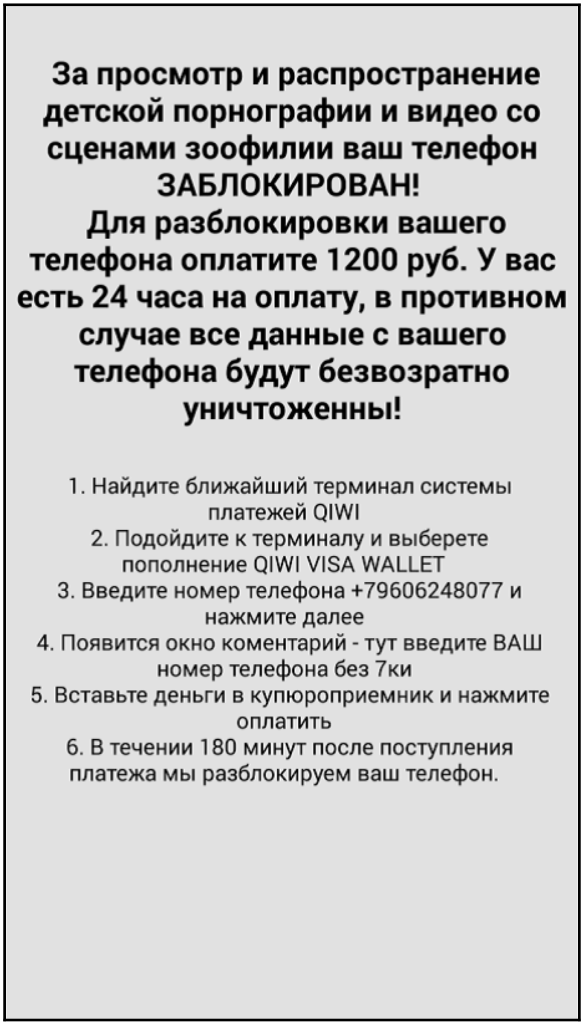
Ваш телефон был заблокирован за просмотр порнографии, а именно сцен изнасилования, зоофилии, педофилии и других извращений.

Ваш ключ:4419953

1. Найдите ближайший терминал системы платежей QIWI
2. Подойдите к терминалу и выберете пополнение QIWI VISA WALLET
3. Введите номер телефона +79641579714 и нажмите далее
4. Появится окно коментарий - в нем введите ВАШ КЛЮЧ который указан выше
5. Вставьте деньги в купюроприемник и нажмите оплатить
6. В течении 2 часов после поступления платежа ваш телефон будет разблокирован.
7. Так же можете оплатить через салоны связи Связной и Евросеть

ВНИМАНИЕ: Не оплата в течении 24 часов или попытки разблокировать

The majority of the ransom messages were in Russian and the payment demanded remained in Ukrainian Hryvnias. The malware authors also instructed the infected users to make payments via prepaid money vouchers, for instance MoneXy or QiWi, since these were not traceable compared to credit cards.

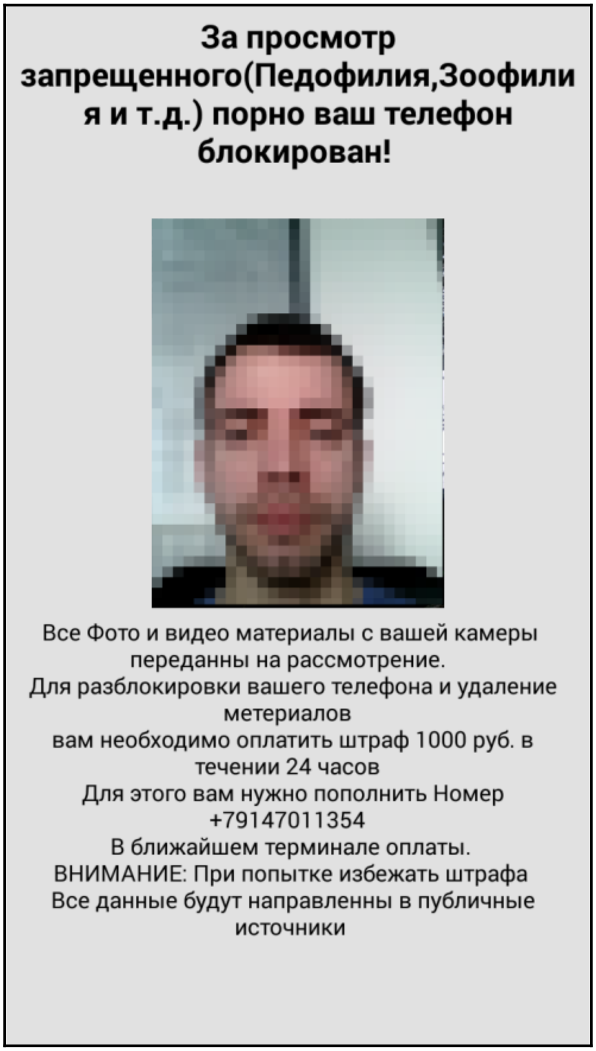


За просмотр и распространение детской порнографии и видео со сценами зоофилии ваш телефон ЗАБЛОКИРОВАН!
Для разблокировки вашего телефона оплатите 1200 руб. У вас есть 24 часа на оплату, в противном случае все данные с вашего телефона будут безвозратно уничтоженны!

1. Найдите ближайший терминал системы платежей QIWI
2. Подойдите к терминалу и выберете пополнение QIWI VISA WALLET
3. Введите номер телефона +79606248077 и нажмите далее
4. Появится окно коментарий - тут введите ВАШ номер телефона без 7ки
5. Вставьте деньги в купюроприемник и нажмите оплатить
6. В течении 180 минут после поступления платежа мы разблокируем ваш телефон.

Ransom requests

When the malware notified the users, via the language and payment methods it could be derived that the malware author was targeting mobile users in Ukraine.



За просмотр запрещенного(Педофилия,Зоофилия и т.д.) порно ваш телефон блокирован!

Все Фото и видео материалы с вашей камеры переданны на рассмотрение.
Для разблокировки вашего телефона и удаление метериалов
вам необходимо оплатить штраф 1000 руб. в течении 24 часов
Для этого вам нужно пополнить Номер +79147011354
В ближайшем терминале оплаты.
ВНИМАНИЕ: При попытке избежать штрафа
Все данные будут направленны в публичные источники

Malware using the front camera

Some variants of the malware also used to take the picture of the victim through the mobile device camera and displayed it to increase the overall impact.

Simplocker distribution vectors

This malware, as other malware targeting mobile device platforms, generally tricks a user into downloading and deploying the application by disguising itself as a legitimate application. It generally targets brands across adult applications (applications for viewing adult videos), gaming applications (such as Grand Theft Auto - GTA, and so on), and common utility applications (such as Flash, and so on). They also spread through trojan downloaders. Trojan downloaders are not that common in the mobile device space, but their evolution is transcending. Trojan downloaders are applications whose sole focus is to download other malicious malware.

Applications such as Trojan downloader have a much greater possibility of getting in application stores such as Google Play, and so on, due to multiple reasons:

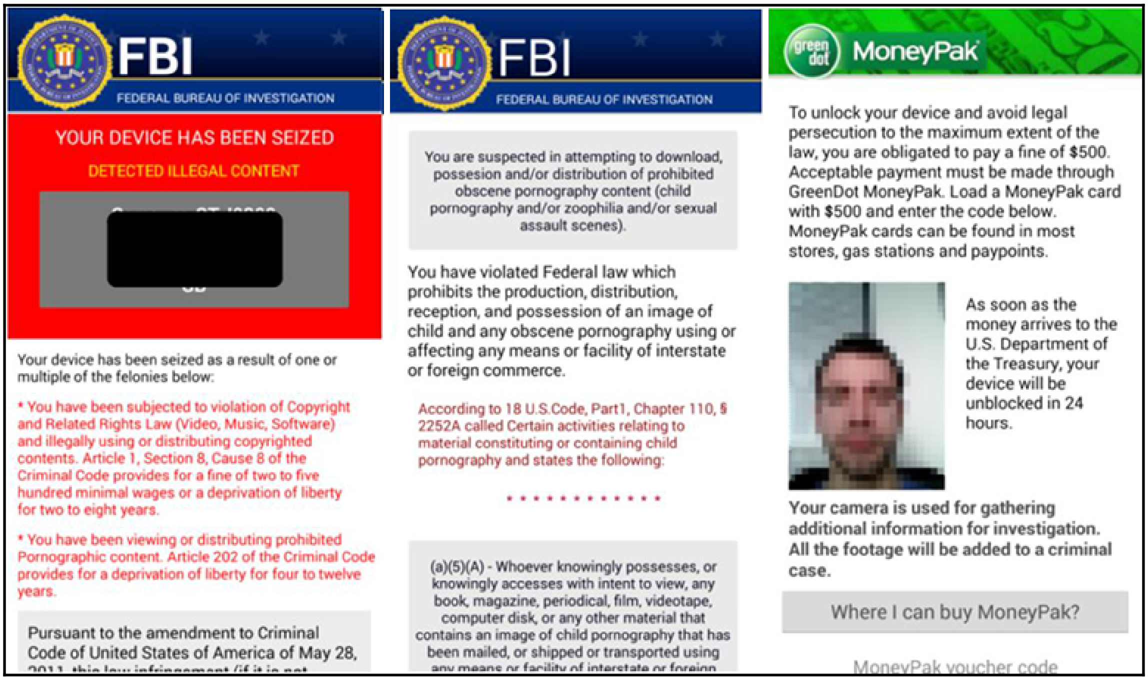
- In case the only activity that the application performs is opening a URL outside the application. This activity cannot be qualified as a malicious behavior.
- There are no permissions requested, which can be called as malicious thus allowing any application to get installed and request privileges from the user.

It also has been noticed that the URL contained within the applications in most cases do not point to any malicious package. The malicious packages are served once the user reaches the redirected URL and then again gets redirected from that server or instance that is under the cybercriminal's control.

Simplocker has not been seen spreading via the official Google store at any point in time.

Simplocker in English

Soon after the initial sample of Simplocker was observed, it was detected that new variants of the malware were spreading across markets with multiple improvements. The most evident change was the language. Now the malware authors were also using English instead of Russian. The message intent was similar to the ones earlier, that is, victims were made to accept it due to the trace of illegal activity via their systems (such as piracy, pornography, and so on). Their devices are then blocked by the law enforcement agency. Furthermore, it was observed that the ransom was asked to be paid using a MoneyPal voucher and was now in the range of USD $200 to $500. Like some of its earlier variants, this malware presented the camera feeds to the infected user too.



YOUR DEVICE HAS BEEN SEIZED

DETECTED ILLEGAL CONTENT

[redacted]

Your device has been seized as a result of one or multiple of the felonies below:

* You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents. Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

* You have been viewing or distributing prohibited Pornographic content. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not

You are suspected in attempting to download, possesion and/or distribution of prohibited obscene pornography content (child pornography and/or zoophilia and/or sexual assault scenes).

You have violated Federal law which prohibits the production, distribution, reception, and possession of an image of child and any obscene pornography using or affecting any means or facility of interstate or foreign commerce.

According to 18 U.S.Code, Part1, Chapter 110, § 2252A called Certain activities relating to material constituting or containing child pornography and states the following:

• • • • • • • • • • • •

(a)(5)(A) - Whoever knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign

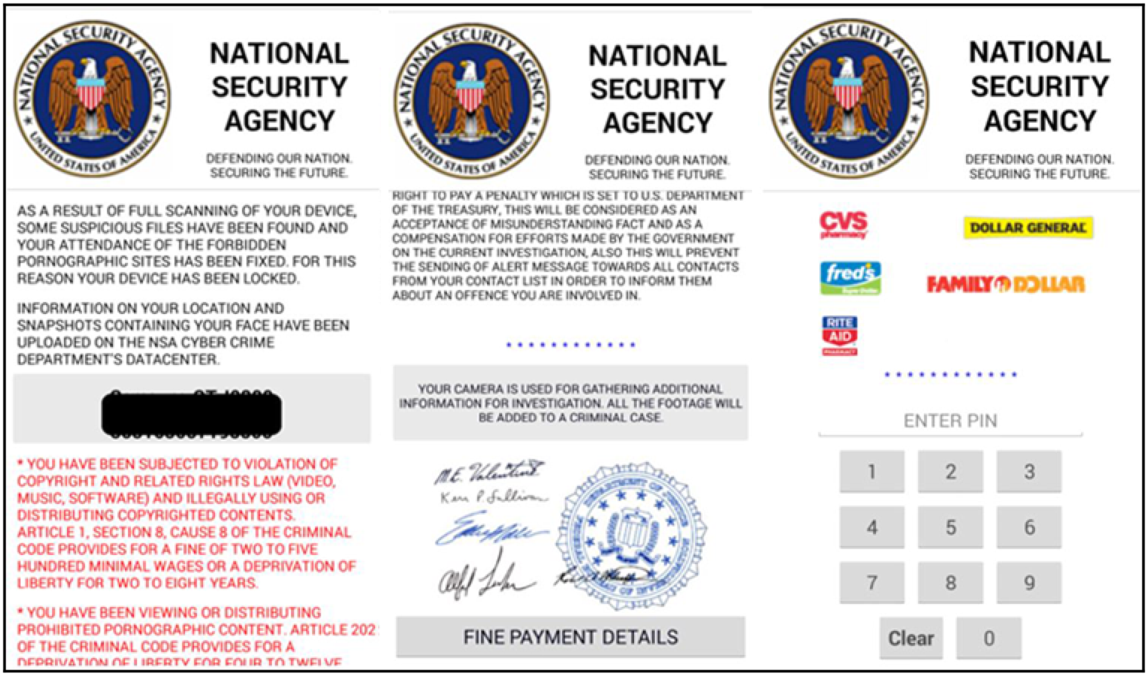
To unlock your device and avoid legal persecution to the maximum extent of the law, you are obligated to pay a fine of $500. Acceptable payment must be made through GreenDot MoneyPak. Load a MoneyPak card with $500 and enter the code below. MoneyPak cards can be found in most stores, gas stations and paypoints.

As soon as the money arrives to the U.S. Department of the Treasury, your device will be unblocked in 24 hours.

Your camera is used for gathering additional information for investigation. All the footage will be added to a criminal case.

Ransom messages in English

The newer variants of the malware also transformed with time, most notably the visuals and design of ransom requests. From the FBI they started using NASA with the same type of messages accusing victims of visiting pornographic sites and asking for a fine of $500 USD.



AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE NSA CYBER CRIME DEPARTMENT'S DATACENTER.

[redacted]

* YOU HAVE BEEN SUBJECTED TO VIOLATION OF COPYRIGHT AND RELATED RIGHTS LAW (VIDEO, MUSIC, SOFTWARE) AND ILLEGALLY USING OR DISTRIBUTING COPYRIGHTED CONTENTS. ARTICLE 1, SECTION 8, CAUSE 8 OF THE CRIMINAL CODE PROVIDES FOR A FINE OF TWO TO FIVE HUNDRED MINIMAL WAGES OR A DEPRIVATION OF LIBERTY FOR TWO TO EIGHT YEARS.

* YOU HAVE BEEN VIEWING OR DISTRIBUTING PROHIBITED PORNOGRAPHIC CONTENT. ARTICLE 202 OF THE CRIMINAL CODE PROVIDES FOR A DEPRIVATION OF LIBERTY FOR FOUR TO TWELVE

RIGHT TO PAY A PENALTY WHICH IS SET TO U.S. DEPARTMENT OF THE TREASURY, THIS WILL BE CONSIDERED AS AN ACCEPTANCE OF MISUNDERSTANDING FACT AND AS A COMPENSATION FOR EFFORTS MADE BY THE GOVERNMENT ON THE CURRENT INVESTIGATION, ALSO THIS WILL PREVENT THE SENDING OF ALERT MESSAGE TOWARDS ALL CONTACTS FROM YOUR CONTACT LIST IN ORDER TO INFORM THEM ABOUT AN OFFENCE YOU ARE INVOLVED IN.

YOUR CAMERA IS USED FOR GATHERING ADDITIONAL INFORMATION FOR INVESTIGATION. ALL THE FOOTAGE WILL BE ADDED TO A CRIMINAL CASE.

NSA ransom messages

Unlike earlier variants that emphasize on encrypting documents, images, and video formats, the malware now also encrypts archive files such as ZIP, 7z, and RAR formats. Potentially the impact of this add-on is enormous since Android file backup solutions store the backups as archive files, which signifies if a potential user gets infected with the malware all the backup will also be encrypted.

Advanced variants of the malware also tricks users into giving the malware device administrator rights. Once these rights are granted, it makes the removal process of the malware more complicated since the user then would require to primarily revoke the applications prior to uninstalling them. This is quite challenging especially when the ransomware is locking the screen disrupting all the activities of the user.

Another key aspect was the updated communication protocol for communication with its Command and Control Center, which now was **Extensible Messaging and Presence Protocol** (**XMPP**). With XMPP it gets more complex to detect than other protocols used. These protocols are used to share the details of the infected device to the server and to execute the commands by the malware operator.

One of the most crucial aspects in this malware's evolution is the encryption keys that are utilized by the malware for encrypting the victims file. After the initial version of the malware it was observed that the new malware variants used unique cipher keys that were generated and sent by the associated Command and Control center. Thus, now with new variants it was no longer possible to decrypt the hijacked files easily.

Lockerpin

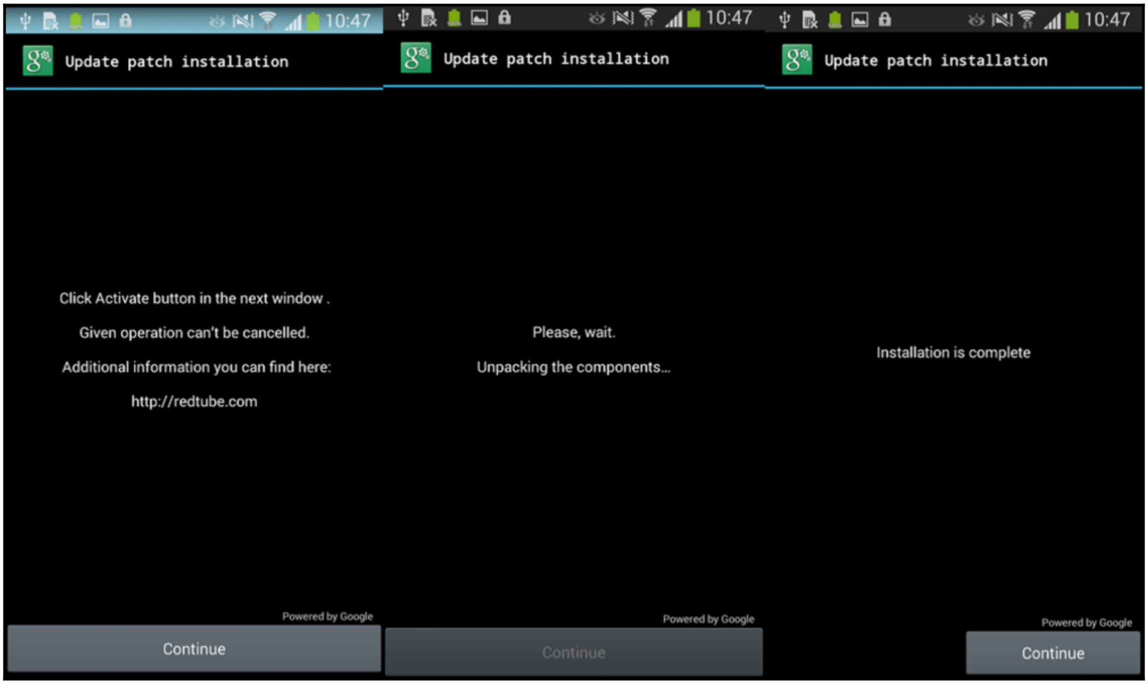
If we observe malware that previously had the screen locking functionality - it was done by invoking the ransom window in an infinite loop. Even though multiple self-defense techniques were implemented to keep the device user locked out, it wasn't complex to unlock the device via disabling device administrator rights and removing the malicious application in safe mode.

Unfortunately, with this malware in place, which was discovered in mid-2015, it was identified that malware operators have transformed their approach. In this case if a user is infected with the malware, one of the sole ways to remove the screen lock was if the device was previously rooted or if there has been an MDM solution that is capable of resetting the PIN. The last resort was to do a factory reset that deleted all the data existing in the device.

The key mechanism used by this malware was quite straight forward, that is, it leveraged the built-in Android screen locking mechanism if was able to set a pin on the device or modify it if the PIN was already set. It was able to do so provided if the targeted user had granted the rogue application device administrator privileges.

As per the statistics provided by multiple security vendors it was noted that most of the infected mobile devices were in the USA. As per the malware trends it was observed that the malware authors were shifting their targeted users from Russian, Ukrainian, to United States wide mobile user bases - noticeably due to the fact that was it was potential for higher profit.

Most of the malware infecting Android devices rely on the elevated privileges provisioned by end mobile users. Most malware these days use covert techniques such as displaying multiple windows for instance with an overlaid message such as "Patch Installation", which triggers the underlying window representing Device Admin activation. Thus, when a user clicks on the legitimate looking button, assuming it to be installing patches for the application, it actually intentionally activates the underlying device admin privileges.



Click Activate button in the next window .

Given operation can't be cancelled.

Additional information you can find here:

http://redtube.com

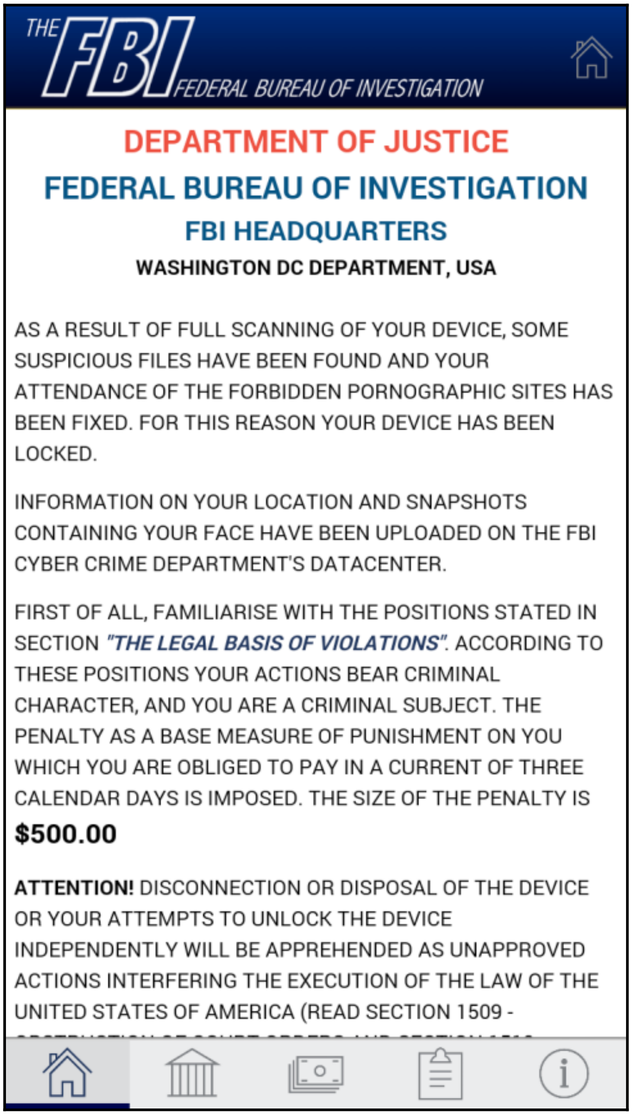
Please, wait.

Unpacking the components...

Installation is complete

Malware stealthily obtaining Device Administrator rights

Once the malware is installed as with other ransomware variants, a bogus message representing the FBI tricking the users to pay a ransom of USD $500 is displayed.



THE FBI FEDERAL BUREAU OF INVESTIGATION

DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

FBI HEADQUARTERS

WASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

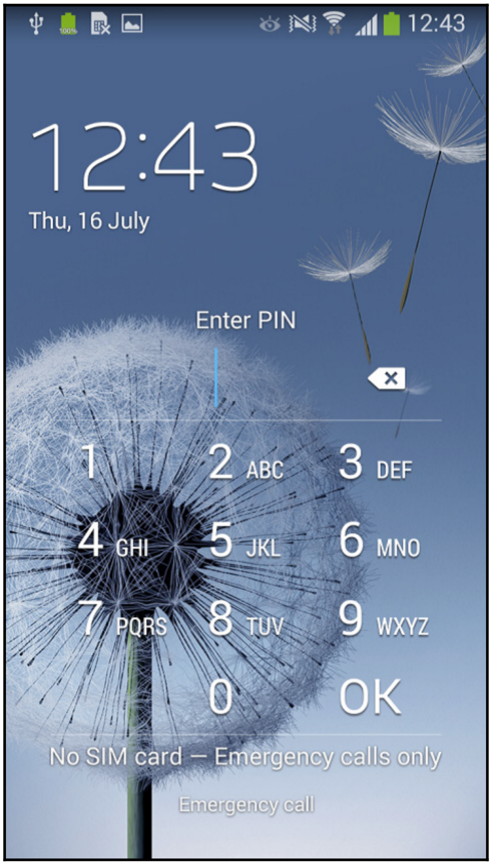
INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION ***"THE LEGAL BASIS OF VIOLATIONS"***. ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED. THE SIZE OF THE PENALTY IS **$500.00**

ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 -

Ransom message

Subsequently after some time once the ransom message is displayed, the PIN of the mobile device is automatically set/changed to a number that is randomly generated by the malware. In some of the variants it has been observed that the malware removes the PIN of the device resetting it to a `0` value.



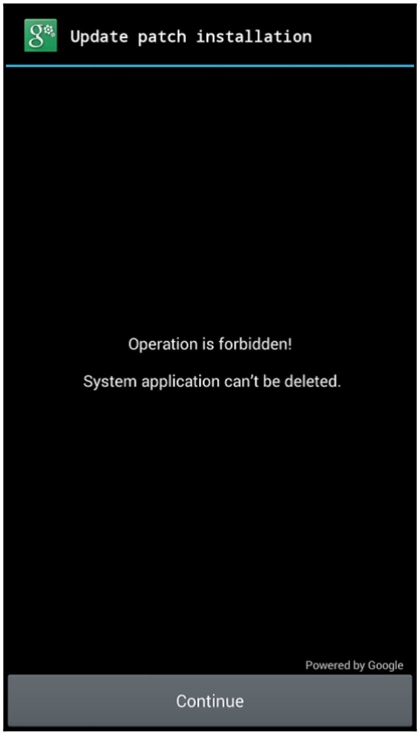
No SIM card – Emergency calls only

Device locked by Lockerpin

Lockerpin's aggressive self-defense

Lockerpin also customizes multiple self-defense techniques to make sure the malware is not removed from the mobile device. Any form of efforts to disable the device admin privilege for the application fails generally due to the fact that the malware registers a callback function for reactivating the privileges as soon as any event gets triggered for removing the privilege.

Like the way how the device admin privileges were forcefully provisioned by the user whenever a removal attempt is made by the user, the malware reactivates the privileges with a bogus message window over the device admin privilege permission approval window.



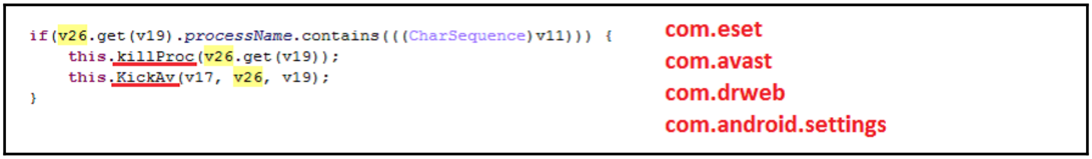
Update patch installation

Operation is forbidden!

System application can't be deleted.

Malware blocking efforts to revoke high level privileges

One of the self-protection mechanisms is to kill the currently running anti-virus/anti-malware processes when the AV comes into play. As per the following screenshot, the malware attempts to protect itself from Avast, Dr. Web, and ESET mobile security solutions:



```
if(v26.get(v19).processName.contains(((CharSequence)v11))) {
    this.killProc(v26.get(v19));
    this.KickAv(v17, v26, v19);
}
```

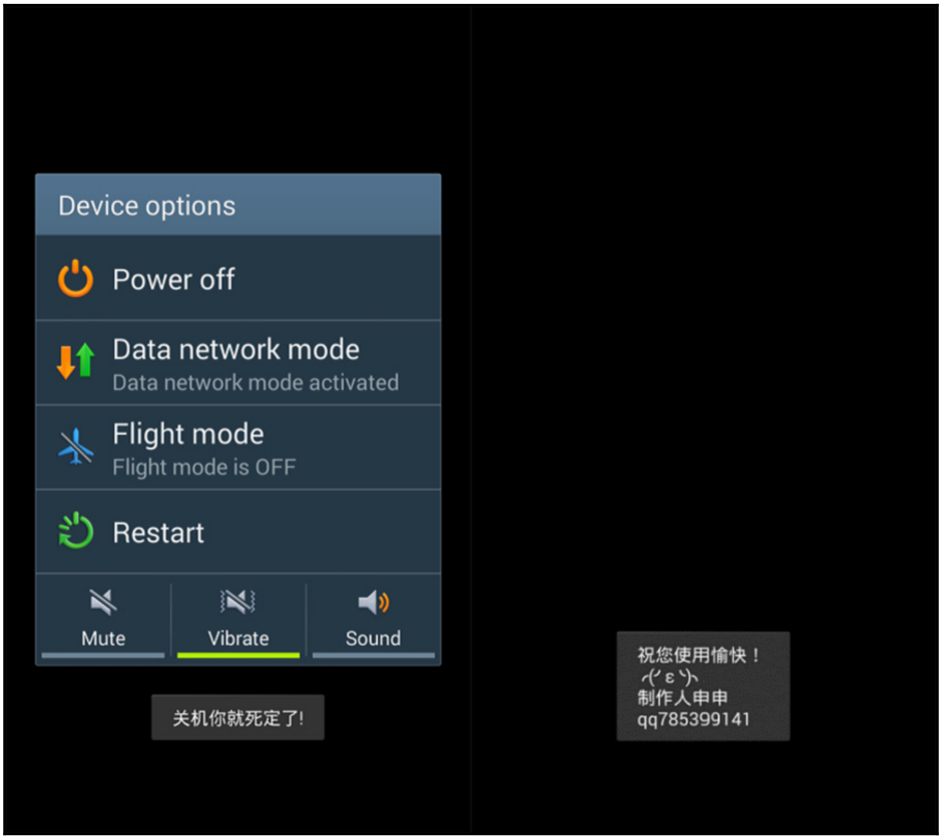
com.eset
com.avast
com.drweb
com.android.settings

Malware making an attempt to kill running AV processes

Jisut

This is a malware that can be considered as quite unusual compared to others in this chapter. All the other malware samples termed in this book primarily have financial gain as the motivation; Jisut gives the impression of being created as a practical joke. This malware is mostly identified in China and seems to be the work of novice cyber criminals.

Initially this malware appeared in the first half of 2014. Since then multiple variants have been observed with some modifications across messages, templates, and so on. This malware has a behavior of having a full screen (only a black background) overlay above all the mobile activities, which tricks users in believing that the device is locked or switched off. If the user tries to get the menu to **Power off/Restart** the device a joke is displayed:

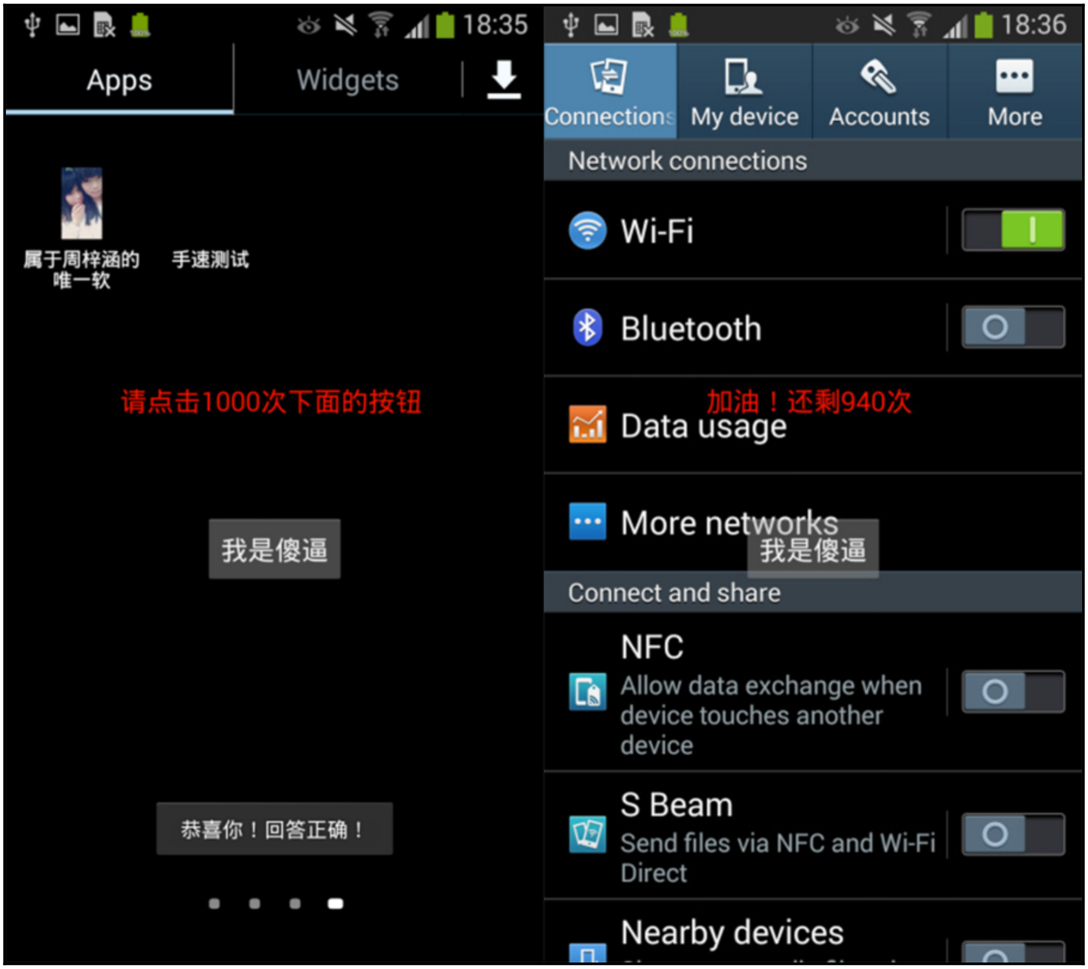


关机你就死定了!

祝您使用愉快！
╭(′ε`)╮
制作人申申
qq785399141

Joke messages: Left joke says - "Off, you are dead!" and the right joke says "I hope you have fun!"

Some other variants of the malware require infected users to click on a message that reads "I am an idiot". These actions are just meant to frustrate users.



请点击1000次下面的按钮

我是傻逼

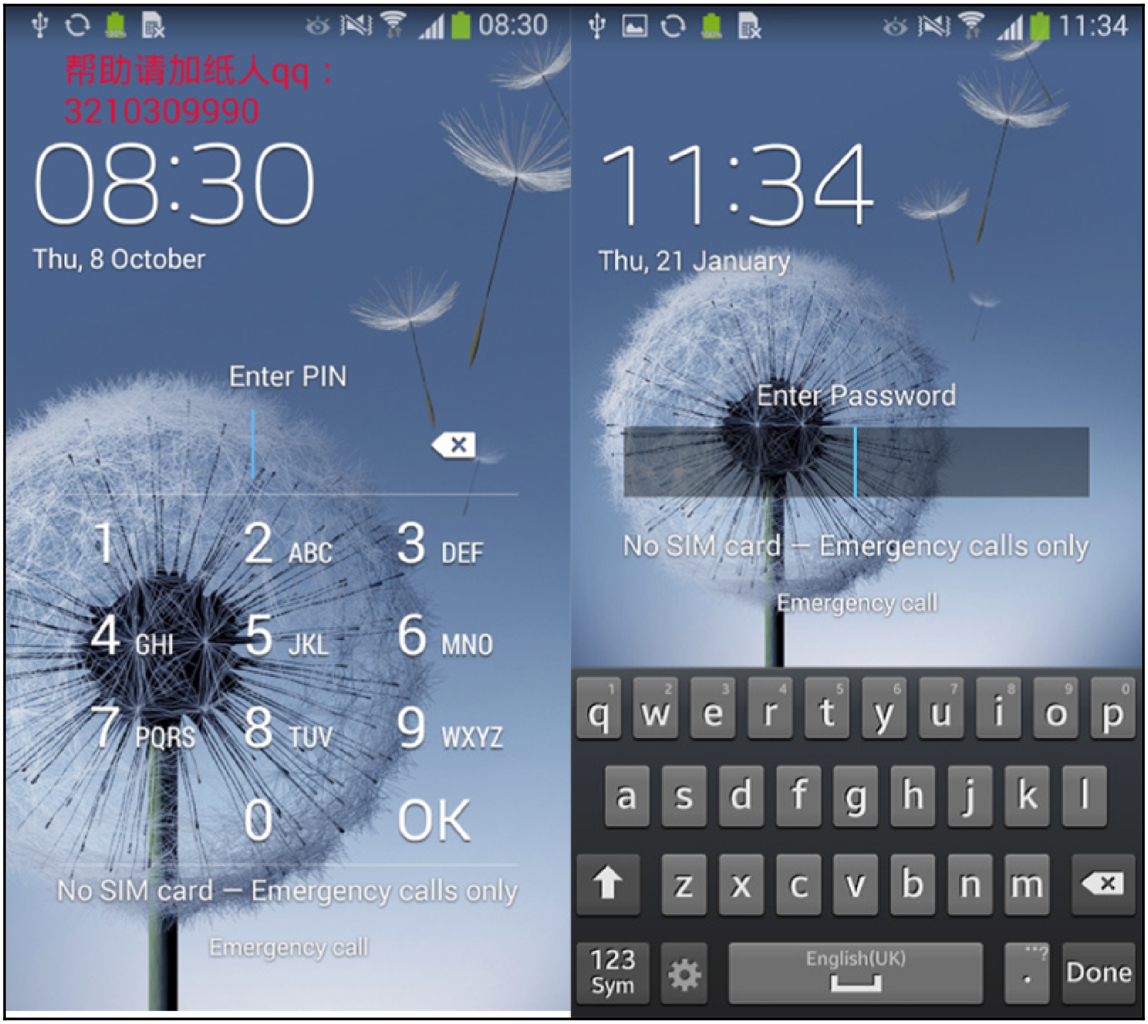
恭喜你！回答正确！

加油！还剩940次

我是傻逼

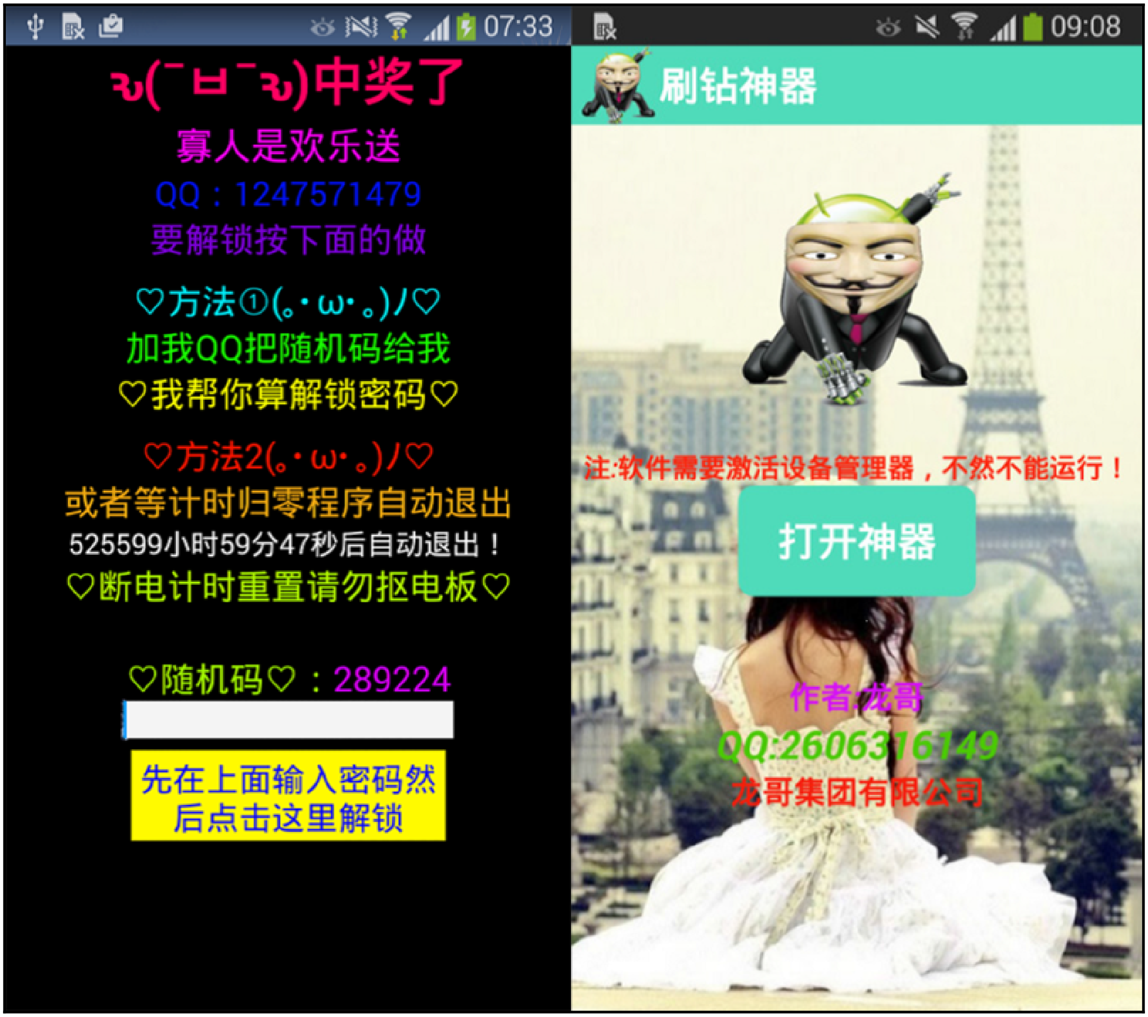
The message says "Please click the button below 1000 times"

Like other malware discussed in this chapter, some variants of this malware are able to set or modify the mobile device lock screen and password.



帮助请加纸人qq：
3210309990

A mobile device locked with a PIN and password by the malware.



ჳ(¯ㅂ¯ჳ)中奖了

寡人是欢乐送

QQ：1247571479

要解锁按下面的做

♡方法①(｡･ω･｡)ﾉ♡

加我QQ把随机码给我

♡我帮你算解锁密码♡

♡方法2(｡･ω･｡)ﾉ♡

或者等计时归零程序自动退出

525599小时59分47秒后自动退出！

♡断电计时重置请勿抠电板♡

♡随机码♡：289224

注:软件需要激活设备管理器，不然不能运行！

作者:龙哥

QQ:2606316149

龙哥集团有限公司

Custom lock screens

Protecting your mobile phone

It is crucial for mobile users to be aware of the potential ransomware threats existing across environments and the importance taking preventive measures. One of the key focuses that all individuals should consider is to avoid unofficial applications being installed on the device either via any third-party portal or malicious app store. Furthermore, it's essential to have a backup of all the sensitive data from the device.

If the users take applicable measures against malware, they may never face any request for ransom. If a user gets infected with a malware there are multiple options for eliminating it based on the ransomware variant:

- In most cases, boot the device in Safe Mode so that third-party applications do not execute. In such cases, the user can manually remove the malicious application.
- If a malware is locked with adequate high level privileges, those should be revoked prior to the application being uninstalled. If the enterprise device has a **Mobile Device Management** (**MDM**) solution deployed, it will be able to reset the lock as per the user's requirement. Google Device manager is also another solution if the user is able to use the functionality.
- A factory reset can be used as the last resort in case none of the solutions work.
- In case the crypto ransomware is based on the malware, variant decryption may or may not be possible. It is recommended to not pay the ransom since there's no certainty that the malware authors would decrypt the files if the victim decide to pay the ransom.

Surrendering to the malware authors demands primarily increases the overall problem. Enterprises can address the mobile security risks by:

- Reviewing and updating governance framework, policies, and procedures to include mobile environment specific requirements including legal, regulatory, and corporate.
- Access to different zones should be provided based on security posture demonstrated by end-device. The following are the sample host posture controls that may be considered while providing the access:
    - Jail-broken or rooted devices
    - Compliance with corporate policy
    - User roles
- Implementing security controls in enterprise applications to demonstrate acceptable security posture and resist malicious activities.

- Implementing endpoint security solutions that align with enterprise security policy.
- Implementing OS and mobile app patches in accordance with enterprise patch management policy.

Future predictions

As we see massive sophisticated attacks increasing across the environment utilizing technologies such as IoT, and so on. The following are the key predictions out of which most of them can be seen gaining momentum in today's date:

- **Cross platform attacks** : Malware may potentially gain the ability to infect different mobile device platforms with small variations in the code.
- **Targeted attacks** : Malware authors may potentially target security hole/vulnerability within an enterprise and compromise target systems.
- **Advanced social engineering attacks :** Malware attacks under the disguise of legitimate applications can potentially target mobile platforms.
- **Mobile botnets :** Mobile botnet may potentially gain access to the device and its contents. It takes advantage of unpatched exploits to provide attackers with root permissions over the compromised mobile device, enabling attackers to send e-mails or text messages.

Summary

In this chapter, we focused on covering most of the common mobile ransomware and the next chapter will concentrate on describing the next steps ahead once the user is infected and money is transferred via such ransomware schemes, taking you deep into the cybercrime world to help you understand how the digital currency receives flows in various types of extortion.

In the next chapter, *we will look deep into the cybercriminal world to help us understand digital currency in detail and how the money flows in various types of extortion.*

7

Follow the Money

Extortion is all about money. Now after successful multiple extortion campaigns across the globe by means of multiple attack vectors, the profits can be seen and the idea is proven. This is motivating more cybercriminals to enter the scene and replicate the concept (and more than a few times even other assaulter's names).

This chapter will take you deep into the cybercriminal world to help you understand the digital currency in details and how the money flows in various types of extortion. We will look at why it is so hard to catch the cyber extortionists and in future why such extortionists can't hide behind crypto currencies such as Bitcoin. We will also look at ransomware as a service, which is designed to be so user-friendly that it could be deployed by anyone with little cyber know-how, which makes it important for protection to be solid.

The chapter will end with some take away for the reader on defense side based on how the money flows.

We will cover the following topics:

- Cryptocurrency
- Blockchain
- Bitcoins
- Why is it difficult to catch attackers?
- Ransomware as a service (RaaS)

Cryptocurrency

Whether it be **Distributed Denial of Service** (**DDoS**) attacks to take down a service or ransomware to abstract or steal data—cyber extortionists extorting organizations of all sizes for money is growing and cryptocurrency plays one of the major roles.

During ancient times, multiple items have been utilized as a stock for value and medium of exchange such as coins, cowrie shells, clay tablets, and now paper and plastic money.

> In the early 18th century, countries progressively used valuable metals such as gold and silver to back their plastic money, forming a monetary/fiscal system called the gold standard. This made it essential for governments to hold and embrace these valuable metal reserves to support their currency. As the economy worldwide became more composite/multifaceted in the latter half of the 20th century, most countries in due course moved away from the gold standard, creating flat currencies constructed on laws and trust in corresponding government.

As the evolution of money—as a store of value, norm of exchange, and unit of account has matured, so have the methods and modes of exchanging it. From this perspective the exchange of money has constantly been a function of the skill and technology available. We transformed from valuable metals to coins to paper and plastic money prior to inventing checks, and then credit cards, which by the way were not created for Internet era.

If we see holistically, it has merely improved to meet the need of trades, and consumers operating in a networked and digital world.

Cryptocurrency thus is fundamentally use of cryptography and hashing algorithms leveraged to establish a distributed system of economy:

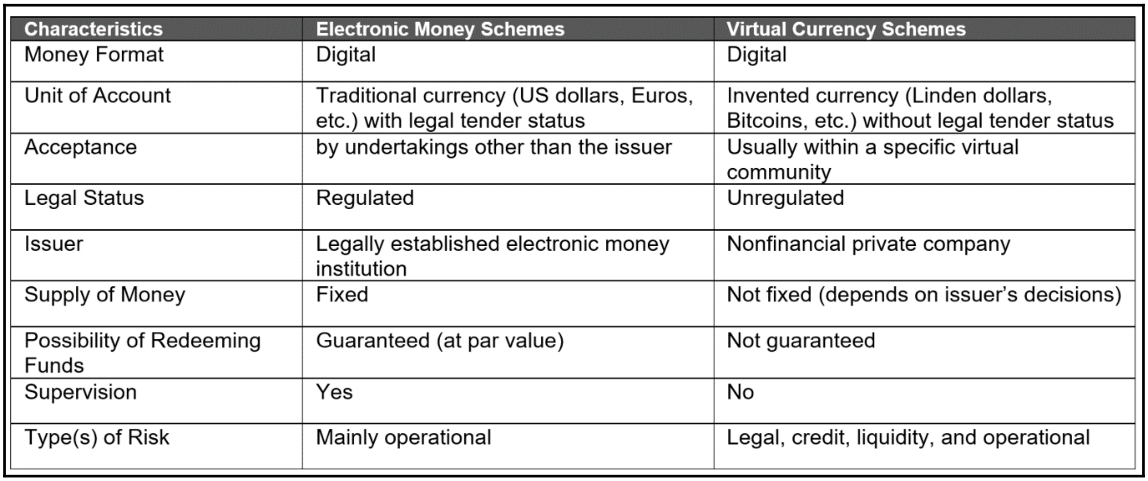
- The currency is just in the form of numbers inside text files that are cryptographically secured.
- Transactions are basically "Pseudonymous" and the currency allows for a decentralized governance model where a distributed ledger keeps track of transactions.
- Cryptocurrency transactions are potentially performed by computers processing at high speeds thus yielding a better throughput.
- Digital operation eliminates the chances of typically encountered human errors. Thus, it is near to impossible to abuse money production rate as it is mathematically controlled.
- Fraudsters, cybercriminals, and cyber extortionists thus find it more profitable to follow the rules than to breach them and try to benefit.

Bitcoin can be called as the first successful implementation of the Distributed cryptocurrency. The increasing propagation of virtual and crypto currencies transcends the availability of tools and services that are essential to carry out cyber crime. Unfortunately, this in turns increases the cyber crime rate and other forms of disruption. Furthermore, as per multiple reports from McAfee, such currencies do face a challenge of using them for money laundering—with a propensity to target attacks on financial institutions and exchanges and digital wallets.

Today, if we speak of the term "cryptocurrency" or "virtual currency", in the eyes of most people Bitcoin is the first thing that they think about. It's indeed one of the widespread currency schemes among a plethora of existing currency schemes. As per the European Central Bank, digital currencies are categorized into varied two categories:

- Electronic money schemes (wherein units are the traditional currency for instance US Dollars, Pound, and so on)
- Virtual currency (whose units are "invented currency")

The characteristics between each of the preceding categories, as defined by the European Central Bank, are depicted in the following table:



Characteristics	Electronic Money Schemes	Virtual Currency Schemes
Money Format	Digital	Digital
Unit of Account	Traditional currency (US dollars, Euros, etc.) with legal tender status	Invented currency (Linden dollars, Bitcoins, etc.) without legal tender status
Acceptance	by undertakings other than the issuer	Usually within a specific virtual community
Legal Status	Regulated	Unregulated
Issuer	Legally established electronic money institution	Nonfinancial private company
Supply of Money	Fixed	Not fixed (depends on issuer's decisions)
Possibility of Redeeming Funds	Guaranteed (at par value)	Not guaranteed
Supervision	Yes	No
Type(s) of Risk	Mainly operational	Legal, credit, liquidity, and operational

Blockchain

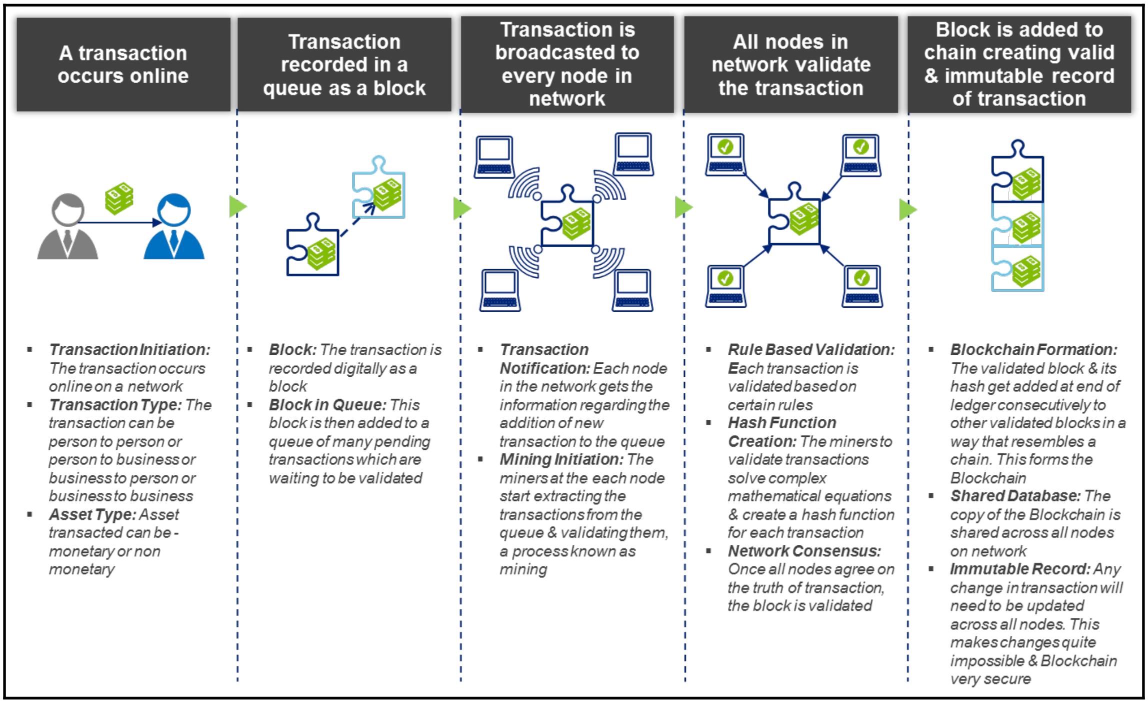
Blockchain is a digital public ledger or a database where transactions are verified and securely stored on a network of connected blocks without a governing central authority.

The blockchain has several unique and valuable characteristics that are transforming multiple ranges of industries. Some of the primary ones include:

- **Distributed Ledger**: The ledger is shared across all the nodes of the network and keeps an updated record of all transactions
- **Decentralized network**: The database is maintained and governed in a decentralized manner by network participants without any central authority
- **Immutable transactions**: Consensus requirement of all nodes on status of ledger at any time makes changes highly difficult as those would need to be done at all nodes
- **No third party validation**: All transactions are validated by independent data miners at all nodes and unknown identities of participants makes processes free from biases
- **Real time recording**: Copies of the ledger get updated across all nodes instantly

How does a blockchain transaction work

The following diagram illustrates the working of a blockchain transaction:



A transaction occurs online

- ***Transaction Initiation:*** *The transaction occurs online on a network*
- ***Transaction Type:*** *The transaction can be person to person or person to business or business to person or business to business*
- ***Asset Type:*** *Asset transacted can be - monetary or non monetary*

Transaction recorded in a queue as a block

- ***Block:*** *The transaction is recorded digitally as a block*
- ***Block in Queue:*** *This block is then added to a queue of many pending transactions which are waiting to be validated*

Transaction is broadcasted to every node in network

- ***Transaction Notification:*** *Each node in the network gets the information regarding the addition of new transaction to the queue*
- ***Mining Initiation:*** *The miners at the each node start extracting the transactions from the queue & validating them, a process known as mining*

All nodes in network validate the transaction

- ***Rule Based Validation:*** *Each transaction is validated based on certain rules*
- ***Hash Function Creation:*** *The miners to validate transactions solve complex mathematical equations & create a hash function for each transaction*
- ***Network Consensus:*** *Once all nodes agree on the truth of transaction, the block is validated*

Block is added to chain creating valid & immutable record of transaction

- ***Blockchain Formation:*** *The validated block & its hash get added at end of ledger consecutively to other validated blocks in a way that resembles a chain. This forms the Blockchain*
- ***Shared Database:*** *The copy of the Blockchain is shared across all nodes on network*
- ***Immutable Record:*** *Any change in transaction will need to be updated across all nodes. This makes changes quite impossible & Blockchain very secure*

The preceding figure describes the working flow of blockchain across the following key five areas providing insight about the key elements involved in each phase:

1. Initializing a transaction.
2. Recording of the transaction.
3. Transaction broadcasting.
4. Validation of the transactions.
5. Overriding blocks.

Common misconceptions about blockchain technology

The following key areas can be considered as the most common misconceptions regarding this technology:

- Blockchain enables Finance to eliminate FTE costs: Although blockchain is a technological innovation, it does not aim to "replace" humans with technology. Blockchain would help companies automate many processes thereby reducing (and not eliminating) reliance on Finance talent. Blockchain indeed creates the role for accountants, and other specialists in its area.
- Blockchain is a flexible technology that can improve every business function: In its current form, blockchain comes with its own limitations and considerations that it is not suited for all business functions. The blockchain framework is an effective approach to validate scenarios where blockchain would work best.
- Blockchain is just a hype and a mere upgrade to the current ERP and Reporting systems: Though it is still early days for blockchain, it is not a hype anymore. Blockchain is not an ERP or system upgrade, but a "radical shift" in technology and a "leap forward" change in current processes.
- Going for blockchain is an IT decision and not a business decision: Blockchain is much more than just a new technology as it fundamentally changes the existing business models and the processes. Blockchain needs to be supported by a shared vision between business, finance, and IT.
- Blockchain is a solution to all finance problems: Blockchain makes sense when businesses are brought together with distributed consensus technology. Without building business collaboration, Blockchain misses its essence and the promised benefits in terms of speed, efficiency, security, and cost reduction are not fully realized.

- Blockchain can store all of the company's information: In using blockchain for business applications with a high volume of information, the amount of stored blockchain data adds up quickly. This is because the blockchain tends to replicate itself with every node that is added. This makes blockchain "too heavy", impacting its speed and efficiency.
- Blockchain is protected from user mistakes: Although blockchain is based on a complex mathematical algorithm, its nodes are only referenced by public key hash, which makes them susceptible to human error. A few other examples of user mistakes may include fat-fingering an extra zero; or copying and pasting a completely different address string
- Blockchain is a store-all for the endless amount of data that would limit cloud usage: Although the database on a blockchain can hold reliably all the needed information, it may become too complex with the addition of other necessary features that help analyze that information. As a result, blockchain cannot be used for large-scale database applications.

Bitcoins

Bitcoin protocol is slightly different from other crypto currencies and the following are a few characteristics of the protocol:

- Cryptography—Elliptic Curve Digital Signature Algorithm (ECDSA).
- Hash Function—Double SHA256 Hashing or SHA256 and RIPEMD-160.
- Addressing individual users in the Peer-to-Peer network:
    - Key Hash = Version of BTC + RIPEMD-160 (SHA-256(Public key)).
    - Checksum = First four bytes of SHA-256(SHA-256(Key Hash)).
    - Bitcoin Address = Base58Encode (Key Hash + Checksum).
- Block Header - Every block has a special Block Header section that contains information about the version, timestamp, pointer to previous block in the form of the previous block hash, Merkle root hash, proof-of-work nonce, and transaction count.
- Proof-of-Work - Proof-of-Work involves finding a nonce that when hashed along with the block header results in a hash that is less than a target value of hash. The target can be adjusted based on difficulty level required, which is actually related to the time required for validating every block.

- Incentive - For every block validated, a process known as mining, 50 BTC are given as the incentive. This value halves every four years. Current incentive is 25 BTC for every block mined out.
- Currency Generation - Mining introduces a new currency to the system. Transactions that begin with mined currency are called **Coin base transactions.**

Quick facts about Bitcoin

Let us look at some interesting facts about Bitcoin:

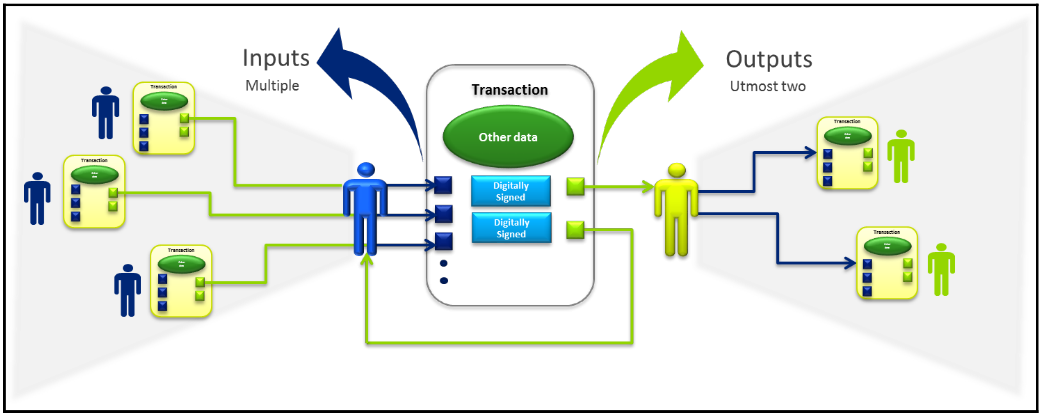
- Bitcoin and the concept of cryptocurrency were first mentioned in a 2008 paper published under a presumably pseudonymous identity, Satoshi Nakamoto.
- The currency code for Bitcoin is BTC. At the moment, it is unofficial.
- Least denomination—Satoshi = 10^{-8} BTC.
- Exchange rates over time—$1 = 1309.03 BTC in October, 2009. 1 BTC = $1250 in November, 2013.
- Biggest wallet balance that was seized by the FBI—1FfmbHfnpaZjKFvyi1okTjJJusN455paPH 144,341.51959292 BTC = $142 million.
- Current Bitcoin rate—$502.83.
- Magic: The Gathering Online Exchange - Mt. GOX, a Tokyo based Bitcoin exchange was launched in July 2010. By 2013 they were handling 70% of all transactions. It was suspended in 2014 because of bankruptcy.
- World's first Bitcoin ATM—Robocoin, introduced in Vancouver, Canada in October 2013.
- More than 100 Bitcoin ATMS are operational worldwide.

Currency denomination

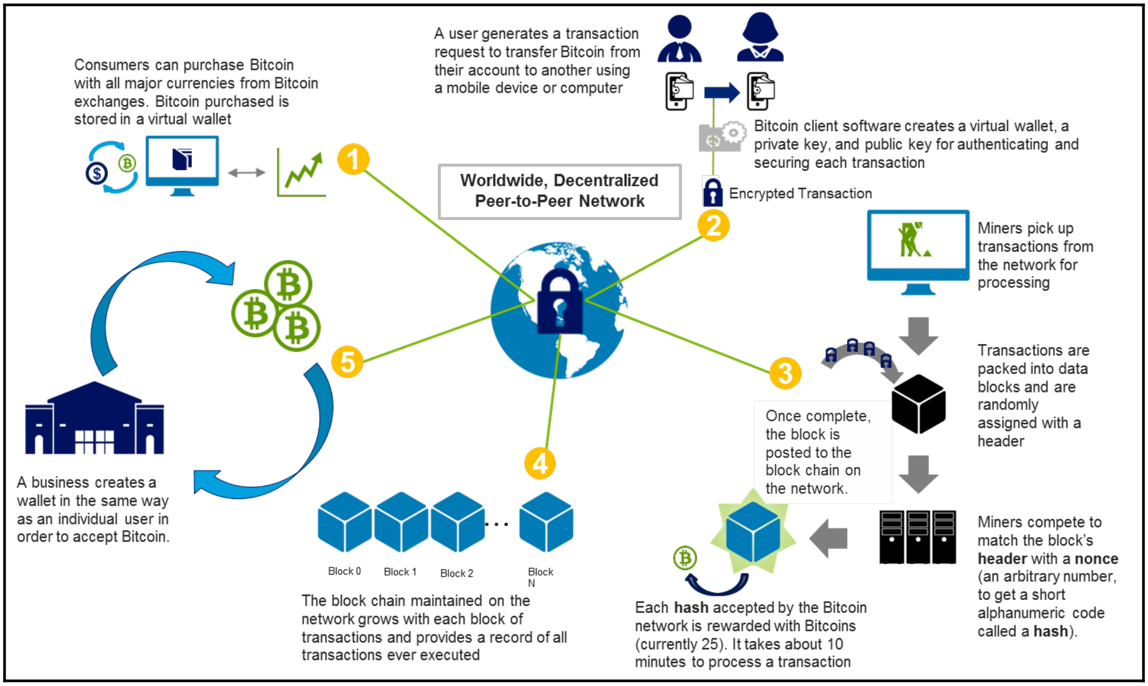
Creating a transaction for every Satoshi/ Bitcoin will be infeasible and impractical to even keep track of all Bitcoins from multiple transactions. Bitcoin protocol uses a special piping process using multiple inputs and multiple outputs in a transaction.

Each transaction will have multiple inputs that can refer to outputs of previous transactions. The accumulated input sum will go to the outputs that are directed at the payee's.

Any extra sum can be redirected back to the payer by using another output. If the input sum is greater than the output sum, the difference will be paid as a transaction fee to whosoever mines the block containing the transaction.



The following figure on the Bitcoin lifecycle illustrates the overall process involved in Bitcoin transactions:



Consumers can purchase Bitcoin with all major currencies from Bitcoin exchanges. Bitcoin purchased is stored in a virtual wallet

A user generates a transaction request to transfer Bitcoin from their account to another using a mobile device or computer

Bitcoin client software creates a virtual wallet, a private key, and public key for authenticating and securing each transaction

Encrypted Transaction

Miners pick up transactions from the network for processing

Transactions are packed into data blocks and are randomly assigned with a header

Once complete, the block is posted to the block chain on the network.

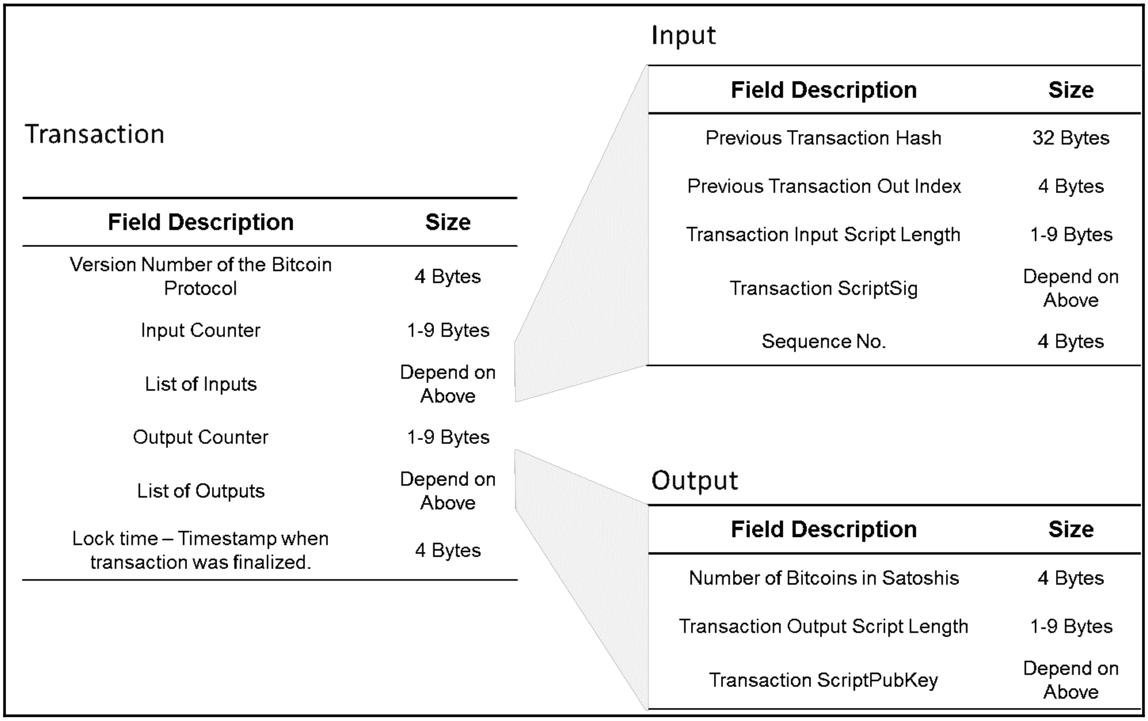
Miners compete to match the block's **header** with a **nonce** (an arbitrary number, to get a short alphanumeric code called a **hash**).

Each **hash** accepted by the Bitcoin network is rewarded with Bitcoins (currently 25). It takes about 10 minutes to process a transaction

The block chain maintained on the network grows with each block of transactions and provides a record of all transactions ever executed

A business creates a wallet in the same way as an individual user in order to accept Bitcoin.

Data structure (transaction and block) of Bitcoins is illustrated here:



Transaction

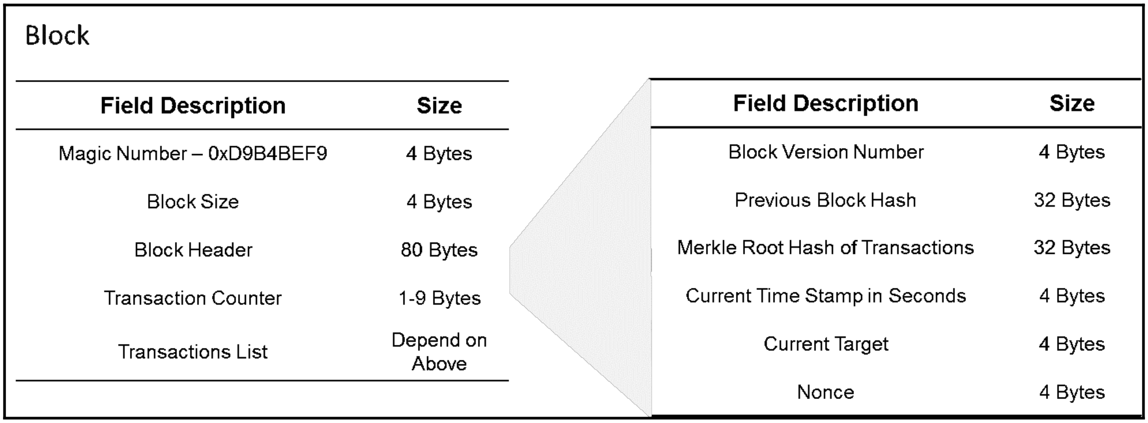
Field Description	Size
Version Number of the Bitcoin Protocol	4 Bytes
Input Counter	1-9 Bytes
List of Inputs	Depend on Above
Output Counter	1-9 Bytes
List of Outputs	Depend on Above
Lock time – Timestamp when transaction was finalized.	4 Bytes

Input

Field Description	Size
Previous Transaction Hash	32 Bytes
Previous Transaction Out Index	4 Bytes
Transaction Input Script Length	1-9 Bytes
Transaction ScriptSig	Depend on Above
Sequence No.	4 Bytes

Output

Field Description	Size
Number of Bitcoins in Satoshis	4 Bytes
Transaction Output Script Length	1-9 Bytes
Transaction ScriptPubKey	Depend on Above



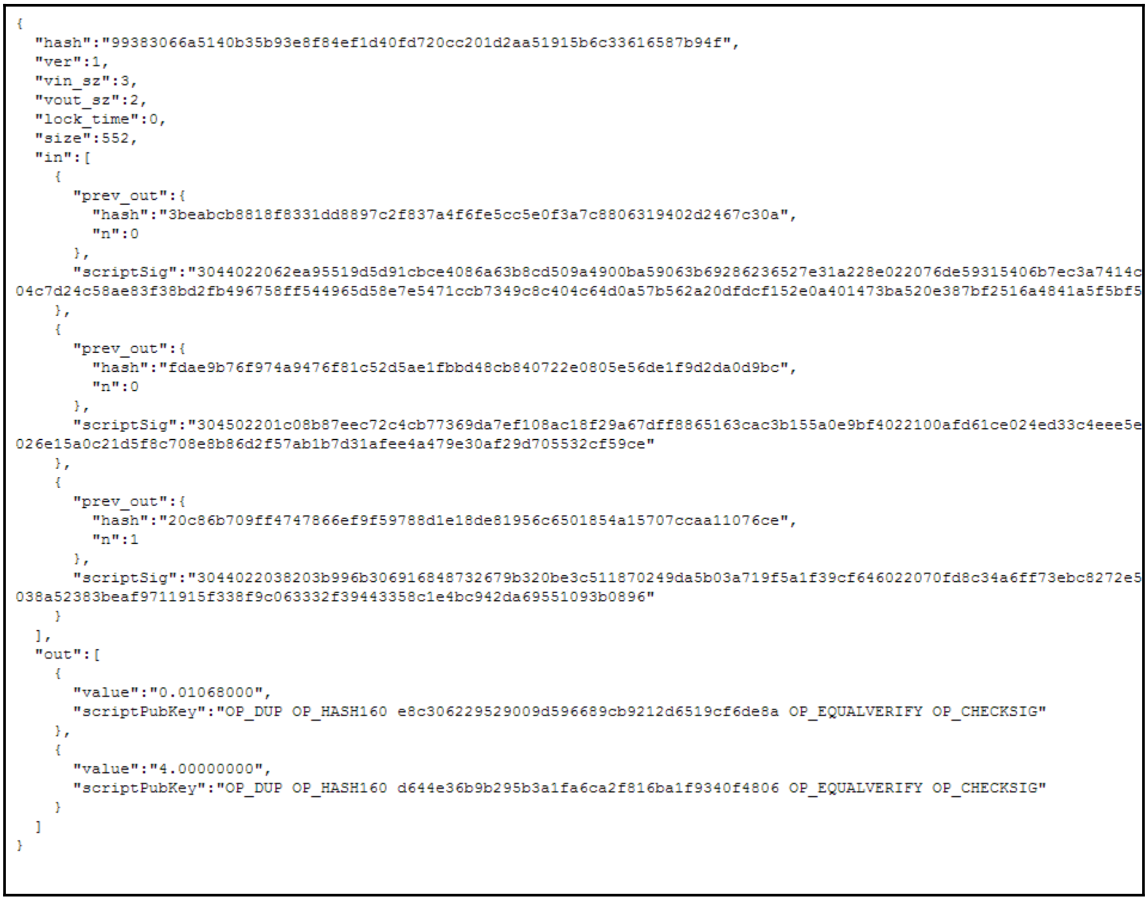
Block

Field Description	Size
Magic Number – 0xD9B4BEF9	4 Bytes
Block Size	4 Bytes
Block Header	80 Bytes
Transaction Counter	1-9 Bytes
Transactions List	Depend on Above

Field Description	Size
Block Version Number	4 Bytes
Previous Block Hash	32 Bytes
Merkle Root Hash of Transactions	32 Bytes
Current Time Stamp in Seconds	4 Bytes
Current Target	4 Bytes
Nonce	4 Bytes

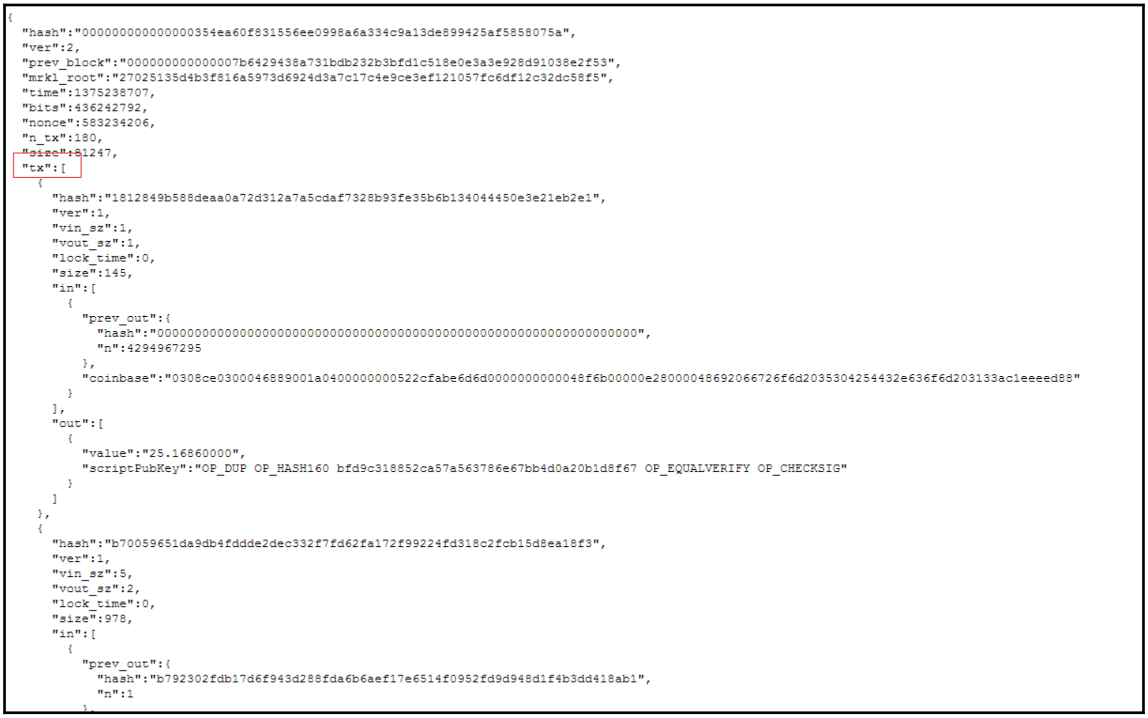
Samples of transactions and blocks

The following screenshot an example of sample raw transaction:



```
{
  "hash":"99383066a5140b35b93e8f84ef1d40fd720cc201d2aa51915b6c33616587b94f",
  "ver":1,
  "vin_sz":3,
  "vout_sz":2,
  "lock_time":0,
  "size":552,
  "in":[
    {
      "prev_out":{
        "hash":"3beabcb8818f8331dd8897c2f837a4f6fe5cc5e0f3a7c8806319402d2467c30a",
        "n":0
      },
      "scriptSig":"3044022062ea95519d5d91cbce4086a63b8cd509a4900ba59063b69286236527e31a228e022076de59315406b7ec3a7414c
04c7d24c58ae83f38bd2fb496758ff544965d58e7e5471ccb7349c8c404c64d0a57b562a20dfdcf152e0a401473ba520e387bf2516a4841a5f5bf5
    },
    {
      "prev_out":{
        "hash":"fdae9b76f974a9476f81c52d5ae1fbbd48cb840722e0805e56de1f9d2da0d9bc",
        "n":0
      },
      "scriptSig":"304502201c08b87eec72c4cb77369da7ef108ac18f29a67dff8865163cac3b155a0e9bf4022100afd61ce024ed33c4eee5e
026e15a0c21d5f8c708e8b86d2f57ab1b7d31afee4a479e30af29d705532cf59ce"
    },
    {
      "prev_out":{
        "hash":"20c86b709ff4747866ef9f59788d1e18de81956c6501854a15707ccaa11076ce",
        "n":1
      },
      "scriptSig":"3044022038203b996b306916848732679b320be3c511870249da5b03a719f5a1f39cf646022070fd8c34a6ff73ebc8272e5
038a52383beaf9711915f338f9c063332f39443358c1e4bc942da69551093b0896"
    }
  ],
  "out":[
    {
      "value":"0.01068000",
      "scriptPubKey":"OP_DUP OP_HASH160 e8c306229529009d596689cb9212d6519cf6de8a OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value":"4.00000000",
      "scriptPubKey":"OP_DUP OP_HASH160 d644e36b9b295b3a1fa6ca2f816ba1f9340f4806 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

The following screenshot an example of sample raw block:



```
{
  "hash":"000000000000000354ea60f831556ee0998a6a334c9a13de899425af5858075a",
  "ver":2,
  "prev_block":"000000000000007b6429438a731bdb232b3bfd1c518e0e3a3e928d91038e2f53",
  "mrkl_root":"27025135d4b3f816a5973d6924d3a7c17c4e9ce3ef121057fc6df12c32dc58f5",
  "time":1375238707,
  "bits":436242792,
  "nonce":583234206,
  "n_tx":180,
  "size":81247,
  "tx":[
    {
      "hash":"1812849b588deaa0a72d312a7a5cdaf7328b93fe35b6b134044450e3e21eb2e1",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":145,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"0308ce0300046889001a0400000000522cfabe6d6d000000000000048f6b00000e2800004869206672 6f6d2035304254432e636f6d203133ac1eeeed88"
        }
      ],
      "out":[
        {
          "value":"25.16860000",
          "scriptPubKey":"OP_DUP OP_HASH160 bfd9c318852ca57a563786e67bb4d0a20b1d8f67 OP_EQUALVERIFY OP_CHECKSIG"
        }
      ]
    },
    {
      "hash":"b70059651da9db4fddde2dec332f7fd62fa172f99224fd318c2fcb15d8ea18f3",
      "ver":1,
      "vin_sz":5,
      "vout_sz":2,
      "lock_time":0,
      "size":978,
      "in":[
        {
          "prev_out":{
            "hash":"b792302fdb17d6f943d288fda6b6aef17e6514f0952fd9d948d1f4b3dd418ab1",
            "n":1
          },
```

Protocol weakness

The following points describe the key weaknesses observed for Bitcoin:

- Selfish Miners:
    - A mining operation can refrain from announcing the next new block for a while in order to get a head start on the next block
    - This prevents other honest miners to waste time and processing on irrelevant proof-of-work
    - The analysis shows that anyone with more than one-third of computing power can always get the strategy successfully working

- 51% Attack:
    - Miner controlling 51% of the computation power could potentially tamper with the block chain and enforce double-spending transactions
    - Although the possibility of such overpowering is very low, the concern became almost genuine when a mining power from China grew to control almost 41% of the network power
    - Later they were moderated due to community outcry
- History Tracing:
    - Since transactions are publicly logged, the flow of currency is visible to anyone on the network
    - This information alone will not be able to identify anyone, but it is possible to construct a pattern based on the history of transactions and it might be possible to work out who owns which addresses with a single clue
- Energy Consumption:
    - So many machines set out to solve proof-of-work significantly consume power
    - One of the factors that decides the value of the Bitcoin will be the power consumption
    - Cheaper energy linearly increases mining energy use

Security concerns

The following points describe the key security concerns for Bitcoin:

- Transaction Malleability:
    - Until a transaction is finalized and incorporated into a block chain the underlying data and hash can be altered.
    - This is not really a serious problem since the money intended for recipients will reach without any failure. But if the recipient is malicious, they can alter a transaction and later claim that they did not receive any. This was the issue that happened which made it suspend its operations on bankruptcy.
    - Users need to be careful while spending unconfirmed transactions.

- Malware:
    - Malware stealing Bitcoins by targeting computers with wallet programs installed. The wallet is stored unencrypted.
    - Malware creating botnets that lead to unauthorized mining by using combined computation power of the botnets.
    - Ransomware affecting users through drive-by downloads and disseminating through e-mail attachments that take hold of a machine and keep it locked until some ransom in the form of Bitcoins is paid to the malware developer.
- Denial of Service Attacks:
    - The currency network could potentially be targeted with DDoS attacks to slow down the network
    - Such attacks will not be successful in modifying the block chain because of the proof of work scheme and they may only slow down the processing of transactions
- Vulnerabilities in Client Software:
    - Vulnerabilities associated with the implementation software platform and infrastructure could potentially be targeted to steal currency or obtain computing power to overcome the block chain
    - Performing infrastructure vulnerability scans and keeping them patched up to date may help deal with such attacks
    - This will not affect the Bitcoin block chain in any way and the vulnerability is not in the protocol

Economics of Bitcoin

The following points describe the economic key features of Bitcoin:

- Price volatility:
    - Bitcoin is over seven times as volatile as gold
    - Bitcoin community claims this is due to insufficient liquidity and lack of popularity
    - Users need to be careful while spending unconfirmed transactions

- Regulation:
    - Governments could levy regulations on how the Bitcoin currency can be traded
    - **Internal Revenue Service** (**IRS**) has already started treating Bitcoin as property rather than currency and ruled that it should be treated more like a stock rather than cash and should pay taxes.
    - This makes Bitcoin not fungible
- Criminal activity:
    - Due to the anonymous nature of transactions, Bitcoins have been used for trade in underground markets and black markets for the sale of drugs and other illegal products
    - Ponzi scheme and money laundering have been suspected
- Banks' skepticism:
    - Banks have always been skeptic about Bitcoins and their reputation
    - Bitcoin companies have had problems with opening traditional bank accounts and do not share enthusiasm in investing in the currency

Bitcoin – myth busters

Before we move ahead, let's bust some myths about Bitcoins:

- **Myth 1:** Bitcoin is difficult to handle than fiat currency! It creates more problems than it solves.

  Explanation:

- Unlike precious metals such as gold/silver, Bitcoin is easy to transfer, secure, and verify
- Bitcoins are predictable and limited in supply and they are not controlled by any authority
- They are faster and cheaper to transfer than fiat currency

- **Myth 2:** The CPU processing power is the investment for Bitcoin.

  Explanation:

- It is not appropriate to say that Bitcoin is obtained for the energy put in the form of CPU power
- The currency is "Created" by processing power and is also a means of securing the network
- The value of Bitcoins is not based on the amount of CPU power or electricity that goes in to mining them

- **Myth 3:** Anybody can create Bitcoins at will. The system runs in to inflation over time.

  Explanation:

- The currency generation is controlled by the network and is impossible to be created by the nodes
- The amount of currency mined out for each block reduces by half every four years and hence reaches a saturation point
- **Myth 4:** Bitcoin is mostly used by hackers for bad activities.

  Explanation:

- Bitcoin development happened among a group of enthusiastic computer programmers.
- The form of currency exchange was widely adopted by hackers due to the very nature of anonymity. The trade of illicit goods over the black market was covertly done over Bitcoins owing to its anonymous nature.
- But today nearly 25,000 merchants across the world have started dealing over Bitcoins.
- **Myth 5:** Bitcoin developers can plan a conspiracy and dictate the software behavior.

  Explanation:

- Any modification to the software will render all the others incompatible and thus all the transactions get rejected.

- Thus Bitcoin developers have limited or no power over the behavior of the currency.
- Protocol modifications also cannot be made until all the users in the network agree upon the modification.
- Also different developers make different client software all adhering to the original Bitcoin protocol. This makes it highly difficult for other developers to modify the protocol and be successful.

Why is it so difficult to catch attackers?

Virtual currencies or Crypto currencies are becoming quite popular choices for cybercriminals and extortionists to engage in illegal activities. These currencies, especially Bitcoin, by now have already expanded with a name or reputation for facilitating the drug trade and other illicit activities through the deep web and through websites, for instance, Silk Road. Nonetheless the major risk which we foresee is of using it for extortion. Numerous characteristics of Bitcoin, which we discussed earlier in this chapter, illustrate that this cryptocurrency is prodigious for regular end users, also making it the excellent currency of choice for cybercriminals and extortionists. It is also termed as one of the most perfect and seamless extortion currencies.

We have been asked multiple times why Bitcoin extortion is becoming so popular. If we look at the overall features and physiognomies of this cryptocurrency, it is a near perfect tool for extortion. Of all the anonymity features of this cryptocurrency, its users prefer it since it makes it quite tough for regulatory and legal authorities to trace the flow of payments. It is a boon for most cybercriminals and extortionists to execute multiple widely treacherous extortion schemes.

Bitcoin automates and makes all the functions of traditional currency quite easy. In addition, it is quite difficult to trace the location or identity of people using the crypto currencies transactions, especially if more security measures are considered while transacting. Thus, cybercriminals prefer cryptocurrency, which can be exchanged in the dark web with 100% anonymity.

For most cases, it is due to the anonymity and decentralization of the cryptocurrency that Bitcoin is the prime choice for cybercriminals, but there's another view to it. Bitcoin as we have seen has no specific barriers to enter. Anyone and everyone can set up a free and unrestricted Bitcoin wallet address without needing any approval from financial institution, regulations, or dealing with providing evidence and proofs of identity, taxation, evidence of residence, and so on. This signifies that anybody can leap in for the cyber ransom game and could cash out until they want without any interference from regulations or laws.

On the flip side, the major issue with this cryptocurrency's anonymity is that all the transactions are publicly logged by design, that is, anybody and everybody can see the Bitcoin transactions or the flow of the cryptocurrency from address to address in the blockchain. The overall information widely available in the public ledger cannot by itself be used to identify a user (due to the fact that the addresses are merely random numbers), but if any of the addresses are mapped or backtracked to a real identity, it may be possible to discover who owns the corresponding addresses. There are multiple ways of deriving information specifically from network analysis or surveillance or searching public forums for Bitcoin addresses.

Cybercriminals, for the most part, to make it more complex to trace their transaction, generally use some third-party services that primarily take their Bitcoins, send them to some other address that may be used in multiple other transactions, and then send them back to some other addresses that the cybercriminal may own. This is generally called Bitcoin mixing service, and there are multiple services available like that. This choice presumes that the corresponding mixing service may not keep track of the overall lifecycle of transactions, thus anonymizing the overall transaction and not revealing any information.

Primarily due to the following reasons it is generally difficult to trace back the cybercriminals and extortionists:

- When they create and majorly utilize a new Bitcoin address for each payment request or inward payment
- When they route all Bitcoin traffic through an anonymizer
- When they associate the balance of old Bitcoin addresses into a new address to carry new transactions (payments)
- When they use money laundering services
- When they utilize the third-party eWallet service to consolidate addresses

Ransomware as a Service

Today, anyone can be a cybercriminal, and the worrying aspect is that cybercriminal's activities are getting mainstream by offering assaults - "as a service" with adequate service manuals. Ransomware being one of the most treacherous attacks has amalgamated with other illegal online campaigns by becoming a service—**Ransomware as a Service** (**RaaS**) , that is, ransomware service platforms, which accomplish all the necessary functions for the crime. In the first five months of 2016 we have seen a ~260% increase in ransomware and most of the credit for such happenings goes down to mass Ransomware as a Service campaigns.

With ransomware as a Service thriving widely over the dark web, the perturbing aspect is that this cybercriminal business model extensively lowers the barriers to entry for future cybercriminals. The ransomware supervisor's markets and recruits mass dark web forum members with multiple recruitment messages translated such as "This solution is for all of them who would want to earn money in not a very virtuous path. This model is 100% successful and does not require any fees or you to pay any advance payments."

The rationale and approach behind these forms of services primarily tend to be software distribution, which customs the proven business affiliate model. Thus, the malware supervisors are also open to recruit members who do not have any experience. The prime objective of the supervisors is to provide the affiliates with copies of the malware so they could infect multiple targets by which so ever means they select. These affiliates generally attempt to directly target victims in addition to hiring multiple criminal services, for example, hiring a botnet, spam run, and so on. Thus, the modus operandi is being renting the ransomware service platform to cybercriminals including members who don't have the technical competency to do it by themselves, getting paid potential huge commission on every successful ransom.

The malware supervisor doesn't mention or care how much ransom is demanded by the affiliate, provided the supervisor gets his share. Every malware distributor sets custom parameters for each campaign. The interesting aspect is that the ransomware doesn't generally rely on standard malware C&C servers. Once a victim gets infected by the affiliate, it drops an e-mail or message to the victim with adequate instructions to contact the malware supervisor for resolution. Once the ransom has been paid by the victim (in crypto-currency, that is, Bitcoins) the malware supervisor send 40$ of the revenue to the affiliate as their cut.

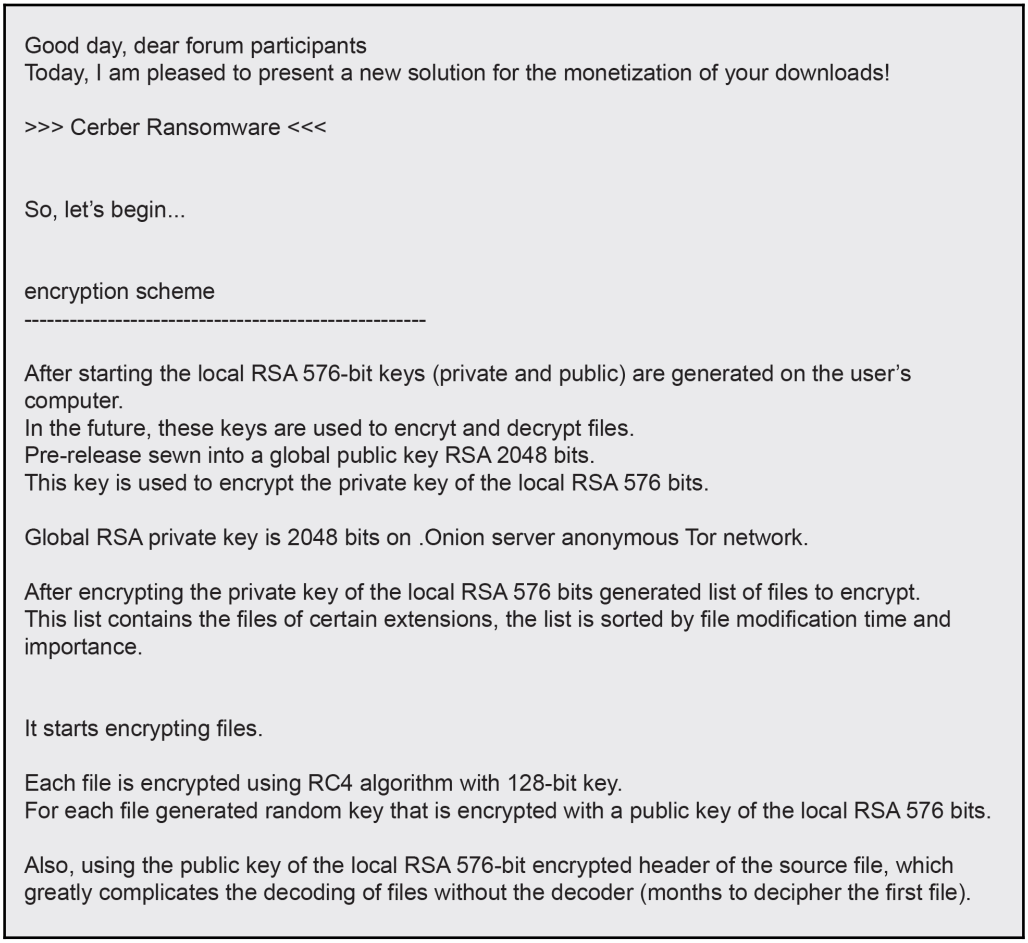
Dissecting RaaS with Cerber

Some of the high profiled campaigns include Ginx, Ranstone, and Cerber.

Cerber ransomware is one of the top ransomware variants existing in the wild with multiple new versions and campaigns affecting victims. It demonstrates every single aspect of an evolving ransomware-as-a-service operation. With Cerber, cybercriminals have unleashed the notion of easy and flexible RaaS, which could be customized, managed, and executed by untrained actors without any required technical knowledge. In multiple deep web forums, these affiliates and unskillful actors can connect with developers of the malware to get suitable instructions. In this case of Cerber, with an insignificant payment, the affiliates and to-be attackers get a variant of this ransomware. With this, they can effortlessly manage their ransomware campaigns by means of a basic web interface.

As per the data gathered by McAfee, Cerber affiliates at one point in time ran more than 160 ransomware campaigns active in nature, infecting more than 150,000 victims across the globe, with an estimated profit of approx. $195,000 during the second quarter of 2016 alone. What's interesting is that all campaigns ran separately by means of a dissimilar distribution method and unique packer.

McAfee initially discovered this ransomware's ecosystem through an advertisement in the deep web by a cybercriminal named "crbr", providing potential forum members the opportunity to join the Cerber affiliates program. The advertisement included a detailed and accurate description of the malware and its components to be managed including the landing pages, the affiliate program through which it is traded, and the relevant estimated profit.



Good day, dear forum participants
Today, I am pleased to present a new solution for the monetization of your downloads!

>>> Cerber Ransomware <<<

So, let’s begin...

encryption scheme

After starting the local RSA 576-bit keys (private and public) are generated on the user’s computer.
In the future, these keys are used to encryt and decrypt files.
Pre-release sewn into a global public key RSA 2048 bits.
This key is used to encrypt the private key of the local RSA 576 bits.

Global RSA private key is 2048 bits on .Onion server anonymous Tor network.

After encrypting the private key of the local RSA 576 bits generated list of files to encrypt.
This list contains the files of certain extensions, the list is sorted by file modification time and importance.

It starts encrypting files.

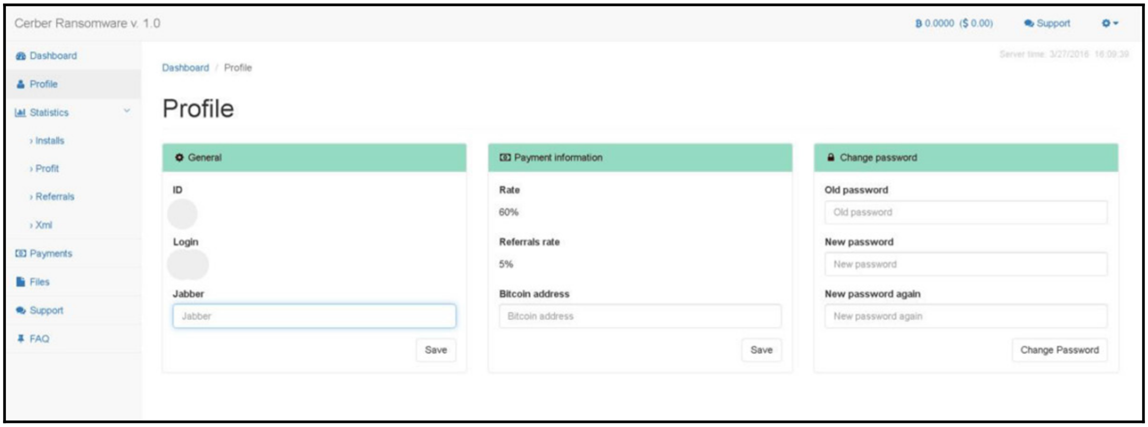
Each file is encrypted using RC4 algorithm with 128-bit key.
For each file generated random key that is encrypted with a public key of the local RSA 576 bits.

Also, using the public key of the local RSA 576-bit encrypted header of the source file, which greatly complicates the decoding of files without the decoder (months to decipher the first file).

As per multiple research and analysis conducted by McAfee, it was accepted that Cerber was originated in Russia as most of its advertisement appeared in Russian. In addition, while analyzing its configuration, it was revealed that there are a certain number of countries wherein the ransomware does not infect the potential targets. This is assumed to be the approach for avoiding legal or regulatory consequences in those countries by their corresponding law enforcement agencies.

For this corresponding ransomware, the ransomware supervisors advertised that the participating actors who are enthusiastic and keen to distribute the ransomware by any means to a large target base, would receive a part of the overall profit. In this particular instance those who would distribute the ransomware would earn 60% of the overall profit and the rest would go to the developers of the ransomware. In addition, 5% of the profit was also to be shared with the affiliates if they recruit new members to this business model.

As per the overall campaign, a unique Bitcoin would be created for each potential target/victim. Flexibility for a lot of customizations was also available for affiliates who can, for instance, adjust the ransom and create a rule to double after some number of days if the ransom is not paid in full. As per the campaign, once the payment is made by the victim they would be provided a link to the decryption tool for that system. For the affiliates, even an all-inclusive support service exists with a comprehensive ticketing system in the ransomware management panel.



Profile

General

ID

Login

Jabber

Jabber

Payment information

Rate

60%

Referrals rate

5%

Bitcoin address

Bitcoin address

Change password

Old password

Old password

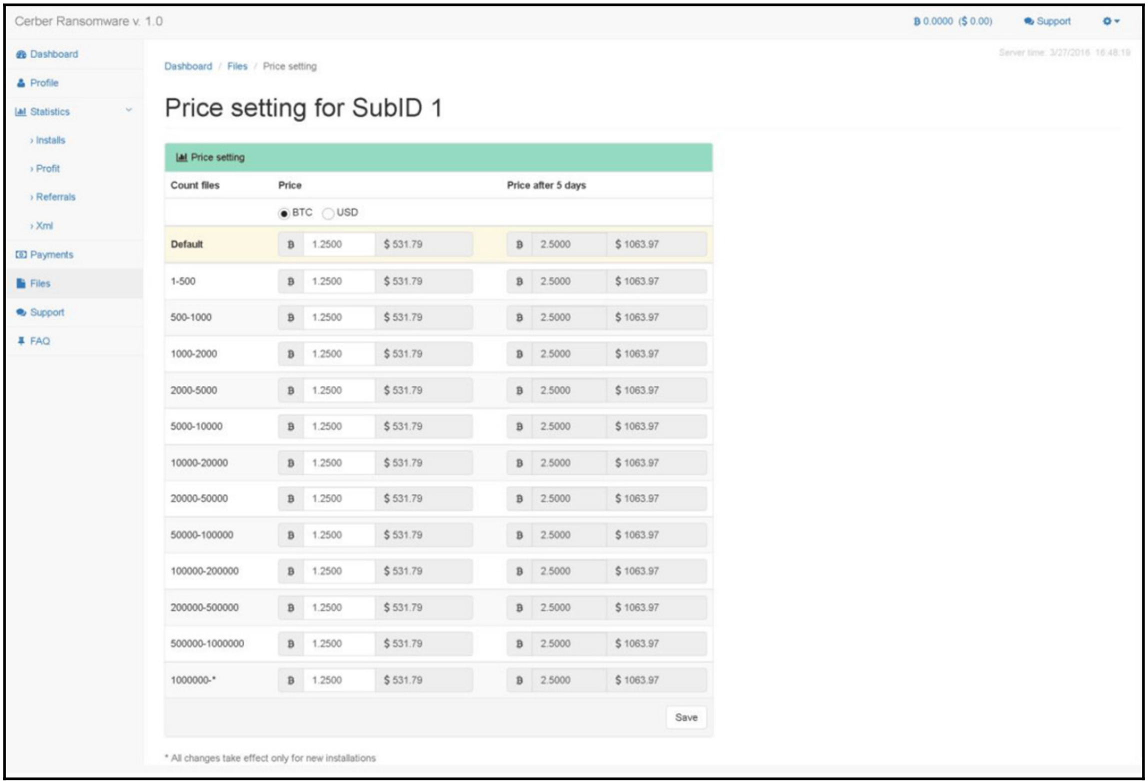
New password

New password

New password again

New password again

Profile page of ransomware in discussion (Cerber)



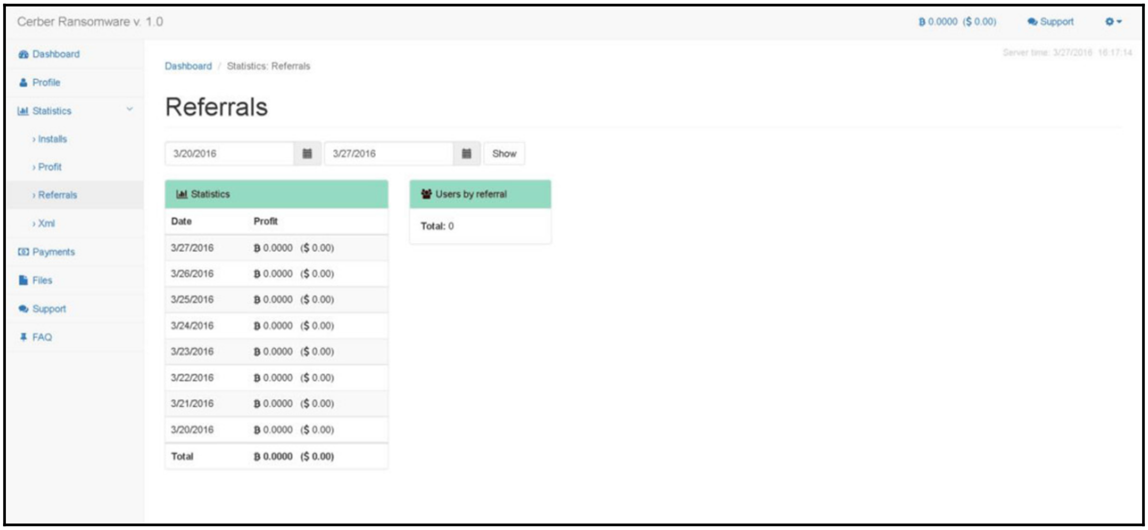
Price setting for SubID 1

Price setting

Count files	Price			Price after 5 days		
	● BTC ○ USD					
Default	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
1-500	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
500-1000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
1000-2000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
2000-5000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
5000-10000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
10000-20000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
20000-50000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
50000-100000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
100000-200000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
200000-500000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
500000-1000000	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97
1000000-*	Ƀ	1.2500	$ 531.79	Ƀ	2.5000	$ 1063.97

* All changes take effect only for new installations

The preceding screenshot shows the spots where the malware operator can define the ransom amount based on the targeted systems.



Server time: 3/27/2016 16:17:14

Dashboard / Statistics: Referrals

Referrals

3/20/2016 3/27/2016

Statistics

Date	Profit
3/27/2016	฿ 0.0000 ($ 0.00)
3/26/2016	฿ 0.0000 ($ 0.00)
3/25/2016	฿ 0.0000 ($ 0.00)
3/24/2016	฿ 0.0000 ($ 0.00)
3/23/2016	฿ 0.0000 ($ 0.00)
3/22/2016	฿ 0.0000 ($ 0.00)
3/21/2016	฿ 0.0000 ($ 0.00)
3/20/2016	฿ 0.0000 ($ 0.00)
Total	**฿ 0.0000 ($ 0.00)**

Users by referral

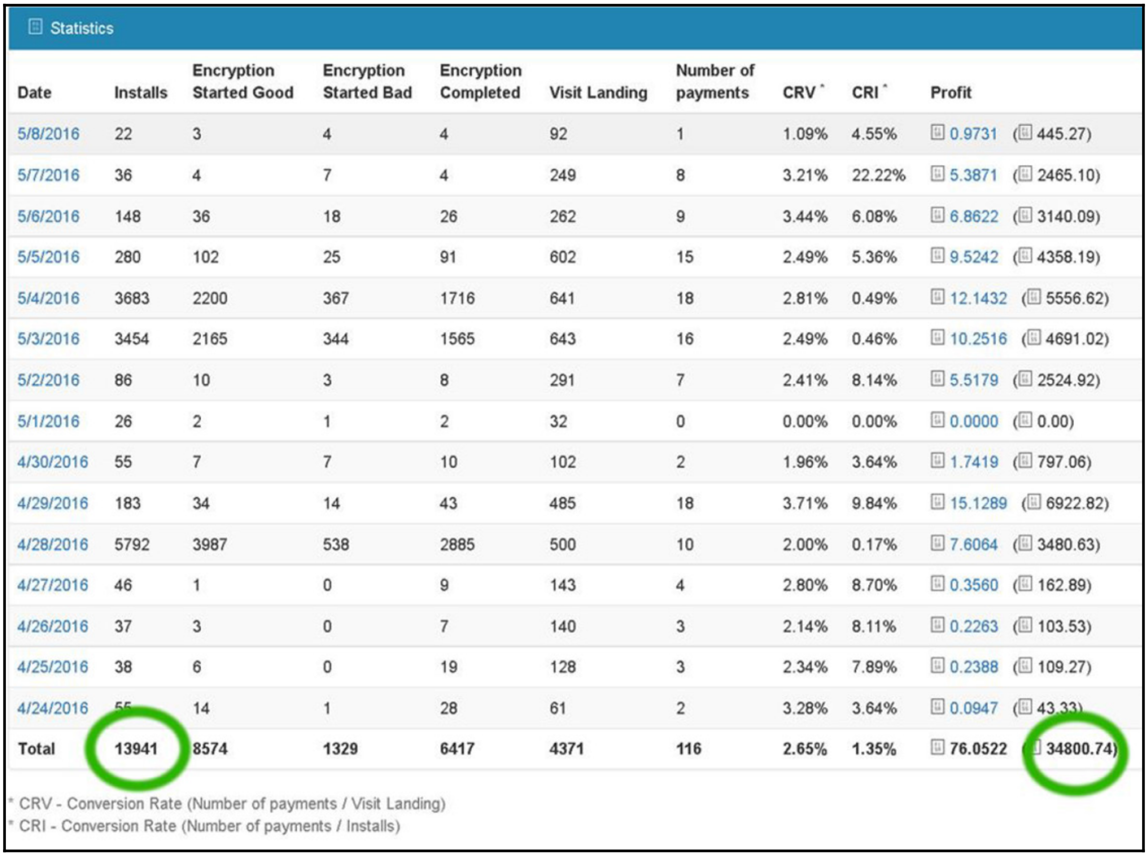
Total: 0

Referral statistics with placeholders for defining the referral amount

The ransomware supervisor provides the referrals statistics along with the affiliates projected profit. As per the observation and analysis of such campaigns, approximately 3% of the campaign victims do procure the decoder. Certainly, this proportion of procurement varies based on the campaign method and the country, but holistically the percentage of victims infected through spam e-mail as a medium to send ransomware is higher.

As per multiple sources the average amount paid by the victims is approximately $500. As per McAfee, most of the decoders for the infected systems are purchased by victims in France, Germany, Italy, Great Britain, US, and India.

The following screenshot illustrates 13491 installations of the ransomware and 116 ransom payments that earned the campaign owners approximately $34,800 during the second quarter of 2016.

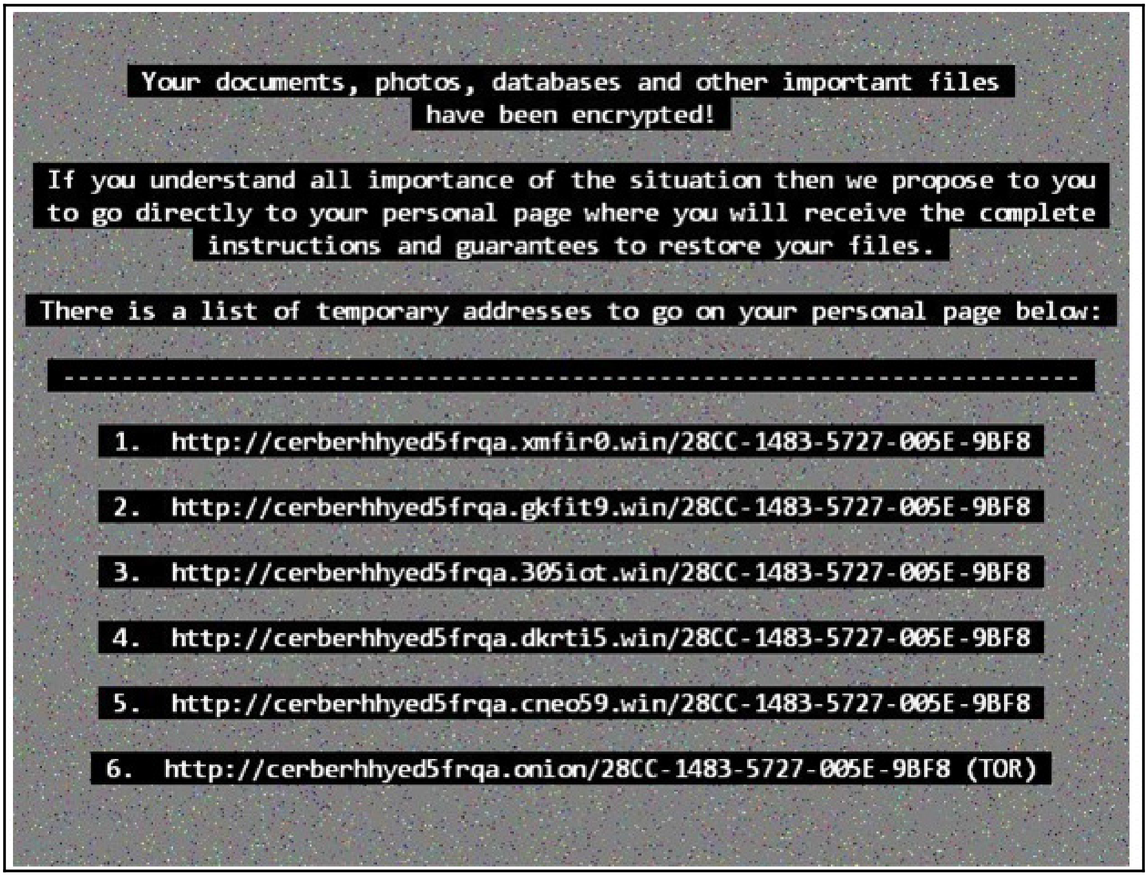


□ Statistics

Date	Installs	Encryption Started Good	Encryption Started Bad	Encryption Completed	Visit Landing	Number of payments	CRV *	CRI *	Profit
5/8/2016	22	3	4	4	92	1	1.09%	4.55%	□ 0.9731 (□ 445.27)
5/7/2016	36	4	7	4	249	8	3.21%	22.22%	□ 5.3871 (□ 2465.10)
5/6/2016	148	36	18	26	262	9	3.44%	6.08%	□ 6.8622 (□ 3140.09)
5/5/2016	280	102	25	91	602	15	2.49%	5.36%	□ 9.5242 (□ 4358.19)
5/4/2016	3683	2200	367	1716	641	18	2.81%	0.49%	□ 12.1432 (□ 5556.62)
5/3/2016	3454	2165	344	1565	643	16	2.49%	0.46%	□ 10.2516 (□ 4691.02)
5/2/2016	86	10	3	8	291	7	2.41%	8.14%	□ 5.5179 (□ 2524.92)
5/1/2016	26	2	1	2	32	0	0.00%	0.00%	□ 0.0000 (□ 0.00)
4/30/2016	55	7	7	10	102	2	1.96%	3.64%	□ 1.7419 (□ 797.06)
4/29/2016	183	34	14	43	485	18	3.71%	9.84%	□ 15.1289 (□ 6922.82)
4/28/2016	5792	3987	538	2885	500	10	2.00%	0.17%	□ 7.6064 (□ 3480.63)
4/27/2016	46	1	0	9	143	4	2.80%	8.70%	□ 0.3560 (□ 162.89)
4/26/2016	37	3	0	7	140	3	2.14%	8.11%	□ 0.2263 (□ 103.53)
4/25/2016	38	6	0	19	128	3	2.34%	7.89%	□ 0.2388 (□ 109.27)
4/24/2016	55	14	1	28	61	2	3.28%	3.64%	□ 0.0947 (□ 43.33)
Total	**13941**	**8574**	**1329**	**6417**	**4371**	**116**	**2.65%**	**1.35%**	□ **76.0522** (□ **34800.74**)

* CRV - Conversion Rate (Number of payments / Visit Landing)
* CRI - Conversion Rate (Number of payments / Installs)

One of the most interesting aspects of this ransomware as it operates is that it doesn't require a C&C - Command and Control connection for encrypting the machines of victims. Nevertheless it does reports to a node that is used to monitor the performance, productivity, and effectiveness of the ransomware through gathering information of victims infected by the ransomware, payments made, and corresponding details of the campaigns. One of the most fascinating elements created by Cerber's developers to evade discovery of this server is to broadcast all the messages to an extensive IP range over UDP (thus not requiring any form of response from the server).



```
Your documents, photos, databases and other important files
have been encrypted!

If you understand all importance of the situation then we propose to you
to go directly to your personal page where you will receive the complete
instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

-----------------------------------------------------------------

1.  http://cerberhhyed5frqa.xmfir0.win/28CC-1483-5727-005E-9BF8

2.  http://cerberhhyed5frqa.gkfit9.win/28CC-1483-5727-005E-9BF8

3.  http://cerberhhyed5frqa.305iot.win/28CC-1483-5727-005E-9BF8

4.  http://cerberhhyed5frqa.dkrti5.win/28CC-1483-5727-005E-9BF8

5.  http://cerberhhyed5frqa.cneo59.win/28CC-1483-5727-005E-9BF8

6.  http://cerberhhyed5frqa.onion/28CC-1483-5727-005E-9BF8 (TOR)
```

Tracing the flow of money

As we understand Cerber ransomware creates an exclusive and lone Bitcoin wallet for each prospective victim to receive funds. This wallet usually appears on the landing page, which is displayed to the victim, denoted as an encoded string.

The highest number of Cerber's infections and payments was in South Korea. The United States ranked second as per McAfee reports to have provided the cybercriminals with the highest number of payments. Even the malware developers and supervisors over forums claimed that the United States is one of the leading countries with various ransom paying users.

Once the ransom is paid by the victims and the Bitcoin transaction occurs, what happens further? Most of the major inquiries revolved around whether the money goes straight to the ransomware's author or to a vast Bitcoin account that further transmits the amount as appropriate. This indeed was one of the logical assumptions against how ransom payments were handled until the reality was recognized.

After analyzing a lot of Bitcoin transactions, it was identified that most ransomware's used a Bitcoin mixing service as part of the ransom flow or the flow of the money to make the transactions as anonymous as possible. As we discussed earlier, Bitcoin mixing service is one of the most constructive ways identified by cybercriminals and extortionists to make the money flow untraceable while making purchases or carrying out other business transactions.

As we have seen, wallets are anonymous or unspecific (as they cannot be associated with any specific user), but on the other hand all the Bitcoin transactions and corresponding actions are logged and exist publicly via blockchain—which keeps a record of each and every individual transaction made using this cryptocurrency. There are multiple third-party services available for Bitcoin, which enables you to trace such records when required.

Wallets that frequently hold a high number of the cryptocurrency and through which numerous daily transactions occur generally draw the attention of law enforcement agencies and third-party security services. This could potentially lead to recognizing or detecting multiple accounts associated with ransomware as well as those of the prospects involved with the ransomware affiliate business model eventually discovering their personal accounts.

Bitcoin mixing services do assist the attackers by transferring money between wallets that could not be linked with the original holder. These services generally charge a fraction of the transfer fee and mix transactions using hundreds of Bitcoin wallets, making it near to impossible to track them individually. In addition to the mixing service, the potential customer using the services could also split the total amount across various Bitcoin wallet once the mixing process is complete. This service is thus one of the least flawless and seamless tools for cybercriminals and extortionists to rotate funds gained through illegal businesses.

As per McAfee's analysis of multiple Bitcoin wallets created for Cerber ransomware, each victim sends the ransom amount to the unique Bitcoin wallets created for them (ransomware developer wallets). The ransomware developer then utilizes a Bitcoin mixing service, which exchanges the cryptocurrency for others and then transfers the exchanged Bitcoins to quite a lot of new and distinct Bitcoin wallets.

The ransom transfers from the designated victim Bitcoin wallets to the ransomware author's wallets. The author then uses a Bitcoin mixing service, exchanging the Bitcoins for others, paying the transfer fee, and then transferring the swapped Bitcoins to several new and completely unrelated Bitcoin wallets.

Summary

We have discussed multiple areas in this chapter that detailed how money flows across multiple areas with a deep insight on the technologies used today. We also dissected an entire ransomware campaign to show a practical insight of the ecosystem.

In the next chapter, we will discuss "the next steps"—once a user is victimized by ransomware.

8
Held Hostage – What Now?

We have discussed cyber extortion and its realms in earlier chapters, primarily it's the act wherein a victim is demanded to pay a ransom so to avoid the effects of the malicious event.

Ransomware is the most common method via which cyber extortion is transcending day by day. With such attacks going mainstream in 2016 wherein the targeted system and corresponding information are locked or encrypted with an ultimatum of paying a ransom to unlock or decrypt the system, it is no wonder why the trend looks to increase in upcoming years.

With such assaults and campaigns increasing, crypto currencies such as Bitcoin are under the radar from governments and financial regulators. Once a victim is trapped with the ransomware, as per the demand from malware authors or operators, the decryption key is sent to the victim only after the ransom is paid by the victim. One of the things to note is that even though in many cases the victims have paid the ransom as per the instructions by the malware author or operator, it doesn't provide assurance of being attacked again.

In this chapter, we will see what options there are and if the system has been compromised starting first with To pay or Not to Pay. We will also discuss the world of cyber insurance as well as how to analyze the attack and what to do for future attacks.

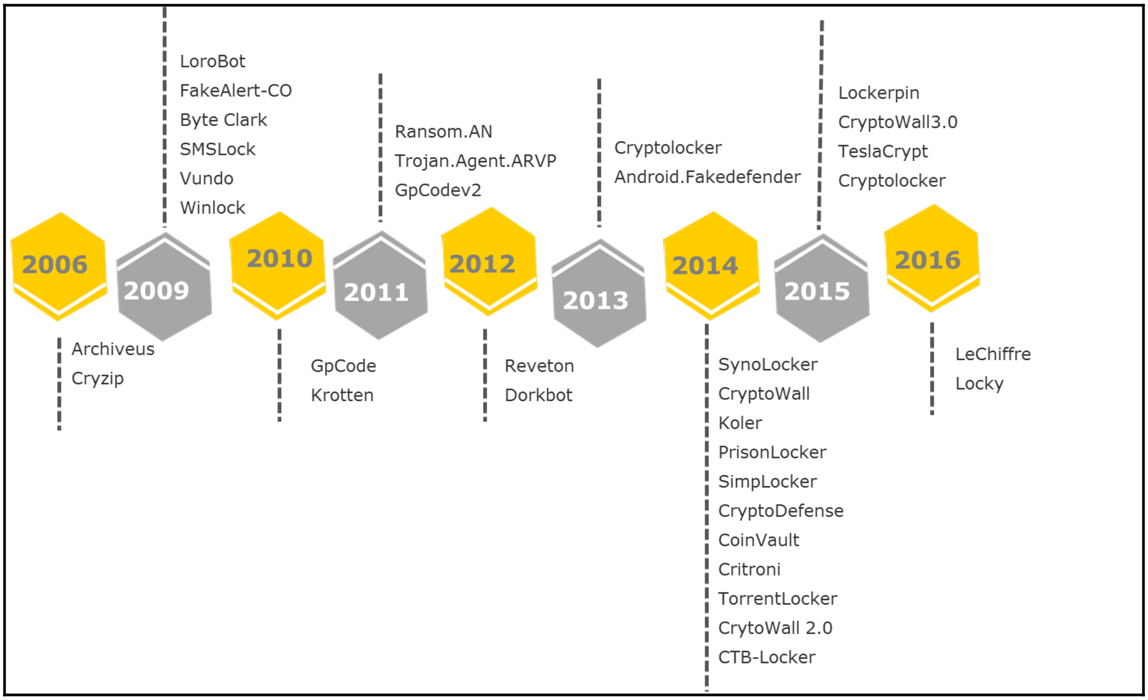
The topics covered in this chapter are as follows:

- To pay or not to pay
- Cyber insurance
- Analyze and respond
- The moral dilemma of malware

To pay or not to pay

When an organization or a user gets hit with such malware it is quite complex for the victim to choose if they should pay or not pay the ransom as per the ultimatum provided by the malware operators to get their system or files back. In the case of a large organization, where data is critical for business operations, not agreeing to the demands may have a massive impact, for instance - losing customer's valuable data, halting business for some time/days, and so on.

The following figure outlines the key malware outbreaks seen in the last decade:



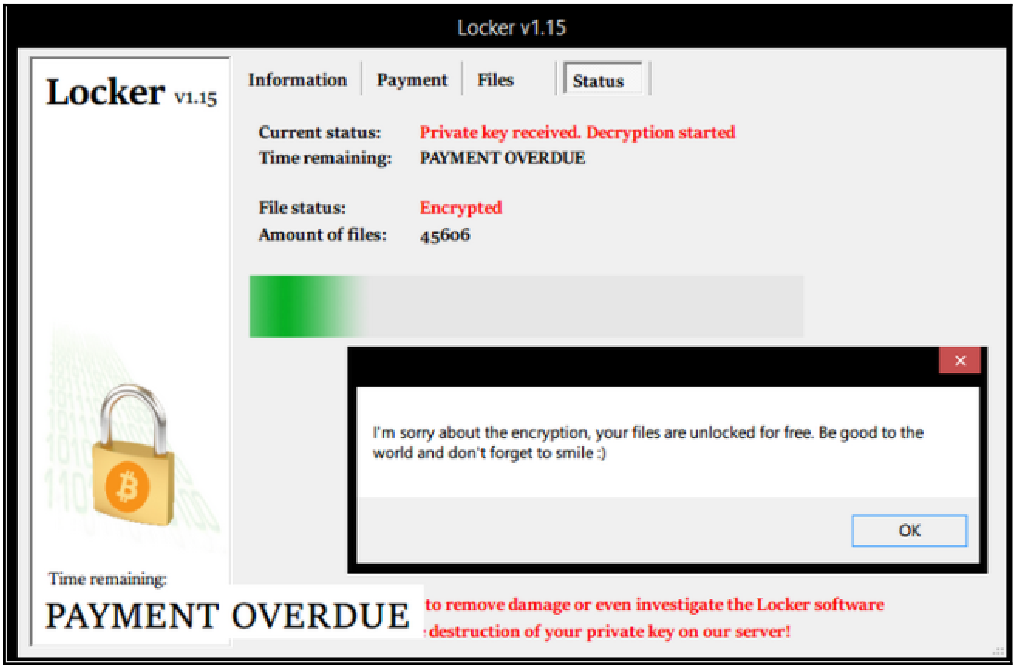
Ransomware variants

If we look at the other side, if victims agree to the demands and pay the ransom every time - this would raise the spirits of malware operators and more sophisticated campaigns may originate. Even though law enforcement agencies recommend not to pay the ransom, there have been numerous instances wherein they themselves have agreed to the demands of cybercriminals to get their files back. Midlothian's police force, the city of Detroit, and a Tennessee sheriff's office include the few government agencies who have fallen victim to such cyber crimes.

Undoubtedly there has always been a question of whether we can trust such malware operators to actually unlock the files once they are encrypted. Many cybercriminals have the business acumen to understand that their reputations play a major role in the whole campaign. Thus as a part of the campaign they set in certain approaches to gain the reputation, demonstrating the ability to decrypt limited files (such as one-five) free of charge. CTB-Locker provides such provisions wherein the victims can try to decrypt the files before they pay the ransom. CTB-Locker makes options available to decrypt one—five random files for free. This provides an assurance and possibility that the malware operators have the ability to decrypt and could decrypt the files once the ransom is paid.

There have been cases, where:

- The security researchers (pretending to be the malware infected victims) and cybercriminals have been involved in negotiating the demand posed by the malware operators (so to make it more affordable)
- The malware operators decided to return, decrypting the files - even when the victim didn't pay as per the dates provided on the ultimatum *(Figure 1)*



Current status: Private key received. Decryption started
Time remaining: PAYMENT OVERDUE

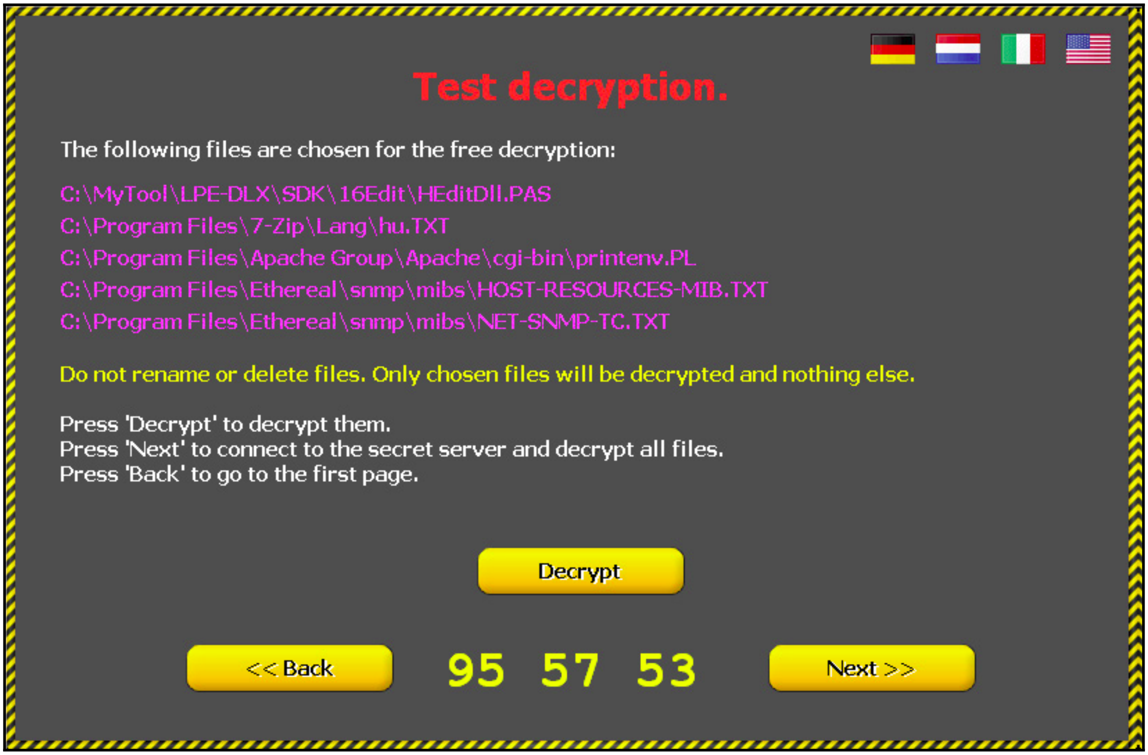
File status: Encrypted
Amount of files: 45606

I'm sorry about the encryption, your files are unlocked for free. Be good to the world and don't forget to smile :)

Time remaining:
PAYMENT OVERDUE

to remove damage or even investigate the Locker software
:destruction of your private key on our server!

Decryption message



Test decryption.

The following files are chosen for the free decryption:

C:\MyTool\LPE-DLX\SDK\16Edit\HEditDll.PAS
C:\Program Files\7-Zip\Lang\hu.TXT
C:\Program Files\Apache Group\Apache\cgi-bin\printenv.PL
C:\Program Files\Ethereal\snmp\mibs\HOST-RESOURCES-MIB.TXT
C:\Program Files\Ethereal\snmp\mibs\NET-SNMP-TC.TXT

Do not rename or delete files. Only chosen files will be decrypted and nothing else.

Press 'Decrypt' to decrypt them.
Press 'Next' to connect to the secret server and decrypt all files.
Press 'Back' to go to the first page.

CTBLocker offering a test decryption

It is only possible to cease such form of business models if none of the victims paid the ransom. Nevertheless, due to several reasons, an individual or business affected by the ransomware tend not to be in a position wherein such thinking can be applied (of not paying the ransom) - primarily due to the sensitivity of data and system being encrypted. The other crucial reason is not having adequate contingency measures to protect against such malicious threats.

On the other hand, there is no certainty that once the ransom is paid by the victim, the files would be decrypted—either due to the fact that the malware operator does not intend to decrypt the files or the decryption fails. In a minority of cases, interacting with the malware operators did result in lowering the ransom costs, but this may not be the case at all times.

As with multiple forms of digital extortion, it cannot be guaranteed that the infected system's data would be decrypted or revived back in its steady state and neither can it also be assured that they would not be targeted again.

Hollywood Presbyterian medical center – Impact based scenario

Possibly one of the most acknowledged and covered malware extortion incidents was the one befallen on Hollywood Presbyterian Medical Center. During the first quarter of 2016, the medical center's employees weren't able to access their systems and network and eventually realized that cybercriminals had seized control of the environment with a malware variant (Locky Ransomware) via the most predominant method of infection—e-mail. As with most Locky campaigns, the e-mails were masqueraded as an invoice and one of the potential victims enabled macros, which further downloaded and executed the malware. Users were presented with the ransom message when they attempted to access the network and the corresponding system.

In this particular case, cybercriminals demanded 40 Bitcoins at that point in time. Medical center management was not prepared for such assaults on their environment and thus approximately for a week their environment stayed offline. Some of the patients were diverted to other medical centers and 911 were called for patients that required intensive care. Eventually, the medical center's administration understood that paying the ransom to the malware operators was the only way out to get operations stabilized and thus, they paid the ransom. The medical center received the decrypter for the ransomware, which further brought the network back online.

The prestigious Hollywood Presbyterian Medical Center infected with malware

Analyzing and responding

Even though with the best potential security readiness with an exceptional security plan and rigorous mitigation procedures in place, cyber attacks potentially targeting all the key sensitive areas in an environment will occur and in some cases compromises may occur. Responding to such forms of malware and extortions is more of a situational challenge. When identified mitigation falls across places, it is crucial for organizations to consider potential options for responding to the cyber attack, and in some cases, interacting directly with malware operators.

It is recommended to avoid communicating with the cybercriminals directly up until the condition or current state of affairs is comprehensively evaluated. Since cybercriminals often provide victims a time limit, it is often essential to have a systematized and controlled response ensuring balanced and rational decision making. This precisely depends on the following factors, including, but not limited to:

- The risk acceptance of an organization
- Impact of the malware to the organization's critical asset
- Impact of business operations and continuity
- High availability of the environment (actively available redundancy)

Preference 1 – situation being controlled by the Incident Response (IR) team

The **Incident response** (**IR**) team should be spontaneous to take control of the environment. The response to such malware should more or less be the same as followed for any **Advanced Persistent Threat attacks** (**APT**). As soon as the assault is reported the incident response stage initiates and the procedures defined by the information security team should be followed. Information Security teams generally provide procedures to be followed in the event of a ransomware assault.

This also signifies that information security teams are an important element in the overall organization structure. It is crucial and without the security team in an organization, it can be quite challenging to face such assaults. This would also give enough liberty to cybercriminals to target such organizations with any trouble.

The IR team should control the case initially by informing the relevant authorities and law enforcement bodies. The executives within an organization tend to be generally reluctant reporting such assaults due to the fear of potential reputation damage. Thus, a security team along with an IR team should be in a position to evaluate the situation and provide feedback to executives on whether the environment held hostage may well potentially have a much greater harm to the business than the reputation part.

A potentially competent and trained information security team should create a plan of action, which should include all the critical parameters to be followed by the IR team. It should also be aligned with the organization's disaster recovery plan, which classifies the **Recovery Time Objective** (**RTO**) and **Recovery Point Objective** (**RPO**) in the case of cyber assaults. These are a few of the key aspects that form an important element to derive the best course of action.

It is also recommended to have a backup of the infected systems for forensic evidence of the cyber attack - which should be preserved for action from law enforcement. Once such IR activities are achieved, the affected systems must be reverted from the back copies of the environment. If no redundant systems are available for the business critical assets, then the respective security teams should implement a vendor solution (decryption tool) if available.

Preference 2 – implementing a security solution (without an Information Security team)

There are multiple scenarios wherein organizations do not have an information security team. Users thus need to be aware of high level remediation strategies and an incident respondent should be aware of vendor security solutions and decryption tools. Respondents should also be trained in the concepts of information security to be able to understand the situation and remove the malware.

According to *ICIT The Ransomware Report,* if a victim organization does not have an information security team, then a respondent will have to assume those roles and responsibilities. Knowledgeable users can implement some vendor solutions and decryption tools; however, without training in information security or computer systems, the victim might not be able to remove the ransomware. In multiple cases, files may not be decrypted completely or might have got moderately corrupted or may still have been infected with the malware. Thus, awareness is an important aspect of the overall remediation. Without user awareness the potential risk of getting the systems compromised increases in general.

For more information, check out the following link:
`http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf`

Preference 3 – trying to recover the data

Recovering data from backups is primarily the sole assured way out for systems infected with malware. If the infected systems have a backup that is not infected the recovery is easy and it is just a matter of restoring back to a point in time.

If the infected systems in the environment have been backed up and are reliable, then victims can ignore the demands from the cybercriminals and clean and restore the system via the backup.

The other way is to recover data via a file recovery tool or via shadow copies. Unfortunately, most modern ransomware remove the shadow copies and may detect third-party recovery processes and tools, which it then kills. In numerous situations, due to the system registers being infected even with recovery points the system restoration may not be possible.

Preference 4 – paying the ransom

Agreeing to the demands of the cybercriminal and paying the ransom should be the last resort. Paying the ransom alleviates the pressure on businesses. At the same time, there have been scenarios wherein the malware operators haven't provided the decryption key after the ransom payment. If a victim is at this stage where paying the ransom is the only way out, it is highly recommended to perform a background research on:

- The variant of ransomware that has infected the system
- The reputation of the malware operator (assurance that the keys for decrypting the files would be provided)

cybercriminals do understand that if they have a bad reputation of the files not being unlocked by them after the ransom is paid, then infected victims would not pay the ransom. Thus as a sign of good faith, some variants provide an option to decrypt random limited files for free.

Victims should also realize that paying the ransom once does not provide the assurance that they would not be attacked and infected again with such malicious campaigns. General users should not tend to expect honesty from cybercriminals. With the assumption that the victim is in a position to pay the ransom, the cybercriminals may attempt to target the same environment again.

If the malware operator does not decrypt the data, then based on the variant of ransomware it is challenging to recover the system to its steady state. Modern ransomware provisions algorithms are quite strong in nature such as RSA 2048 bits.

Thus, it is important to understand the situation once the environment is infected by the ransomware. In multiple cases sometimes no other options are effective. Some of them include:

- When the backup of the infected system is also compromised
- When the system outage would disrupt business operations causing a loss that is significantly more than the ransom demanded
- When hospital systems are impacted and patient's lives are at risk, and so on

If the victim has decided to pay the ransom the following elements should be considered:

- Organizations should pay the ransom in the crypto currency demanded
- Credit card and other financial information should not be shared or used to pay the ransom
- If the card or account information is used to pay the ransom, it should be closed or frozen for any activities aftermath, to avoid any further breaches

Cyber insurance review

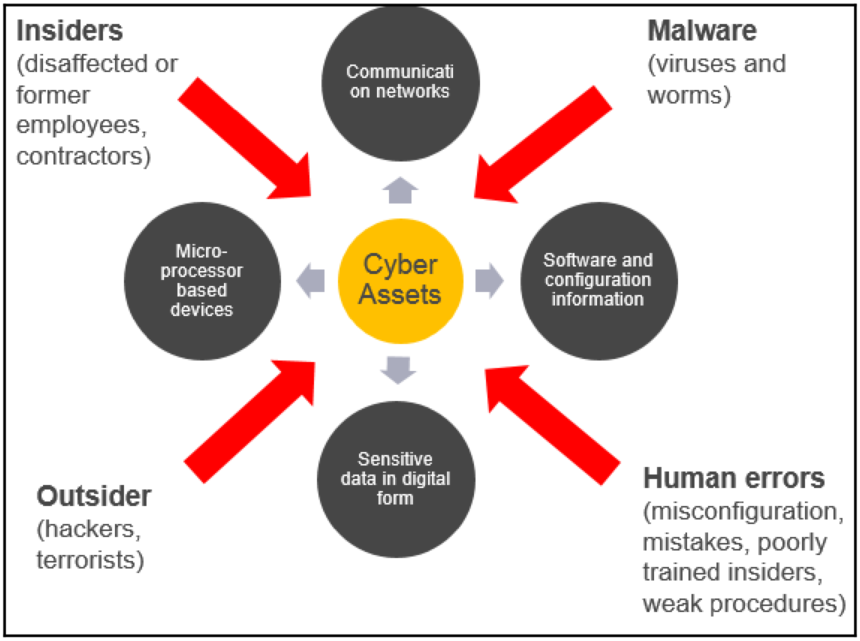
The cyber risk landscape is increasing day by day and thus cyber insurance is going mainstream. Cyber insurance allows businesses and organizations to transfer some of the risks associated with the cyber security incidents to their insurance providers.

Cyber threat landscape and the impact of cyber risk

As we have realized, with the steady increase in cyber crime, many organizations across a variety of industries are susceptible to various types of cyber incidents. Many organizations have come to the realization that a cyber attack is inevitable—not "if" but "when".

These cyber attacks have significant financial consequences that vary by geography, industry, and sophistication of attack:

- Two years back, the average cost of a data breach was between $1.1 million and $5.4 million dollars, which has increased
- Based on multiple analyst reports, the average cost per compromised record is anywhere from $150 to $277


Insiders
(disaffected or former employees, contractors)
Communicati on networks
Malware
(viruses and worms)
Micro-processor based devices
Cyber Assets
Software and configuration information
Sensitive data in digital form
Outsider
(hackers, terrorists)
Human errors
(misconfiguration, mistakes, poorly trained insiders, weak procedures)

Threat landscape

Information security programs are facing a funding shortfall and are looking towards cyber insurance to assist. In addition, other non-monetary risks such as reputational and regulatory risk may also be realized.

Cyber incidents today result in multi-million dollar losses for organizations. The average financial impact to companies in the US for one or more incidents is ~ $5.4 million. Cyber incidents are widespread and spanning across industries irrespective of the organization size. It has been identified that only 52% of data breach incidents were carried out via hacking activities, a good portion of the rest involves insiders or third-parties.

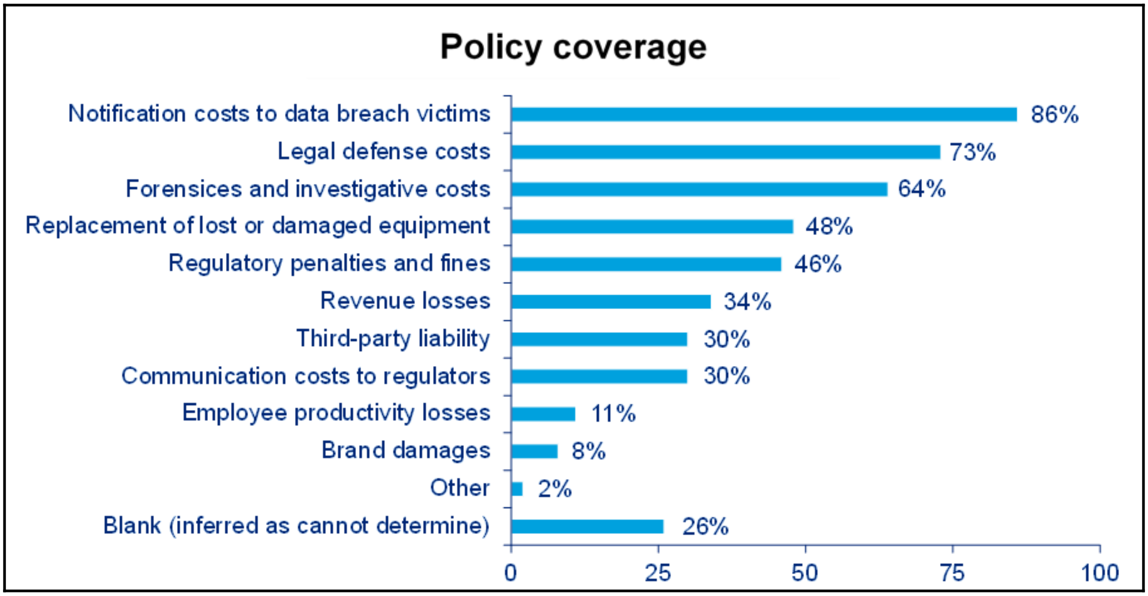
The growing need for cyber insurance

This changing cyber risk landscape is driving interest in cyber insurance, which allows organizations of all sizes to transfer some of the risk associated with their cyber incidents to their insurance provider. While cyber insurance can provide a means of addressing the unexpected, organizations are typically faced with the following challenges:

- Selecting a policy that appropriately balances the cost of premium with risk exposure
- Understanding policy complexity and exclusions
- Understanding the type of risks covered by cyber insurance and the impact of residual risks

In the wake of increased cyber risk, cyber insurance can help organizations mitigate losses from a variety of cyber risk exposures, including data breaches, loss of confidential information, and business disruption.

Cyber insurance coverage



Cyber Insurance coverage areas

Cyber insurance can be considered as an add-on security control mitigating the risks of the organizations by provisioning insurance coverage to the organization in following key areas highlighted by a paper authored by Deloitte and referenced by Harvard (`http://rmas.fad.harvard.edu/files/rmas/files/lu-cyber-insurance-cyber-risk-management-strategy-03032015.pdf`):

- Liability for loss or breach of data
- Remediation costs to respond to a breach such as forensic investigation, notification to affected parties, and so on
- Regulatory fines and penalties as well as associated settlement costs

Maturation of the cyber insurance market

The demand for cyber insurance has been increasing from the time when it was launched in the year 2000 along with an increase in the number of insurance providers. Now the market has matured and is incrementing profoundly. Despite the increase in cyber incidents, **cyber insurance adoption among organizations still remains low.** This is primarily due to:

- Lack of awareness
- Complexity associated with underwriting
- Challenge with aligning insurance coverage with risk exposure

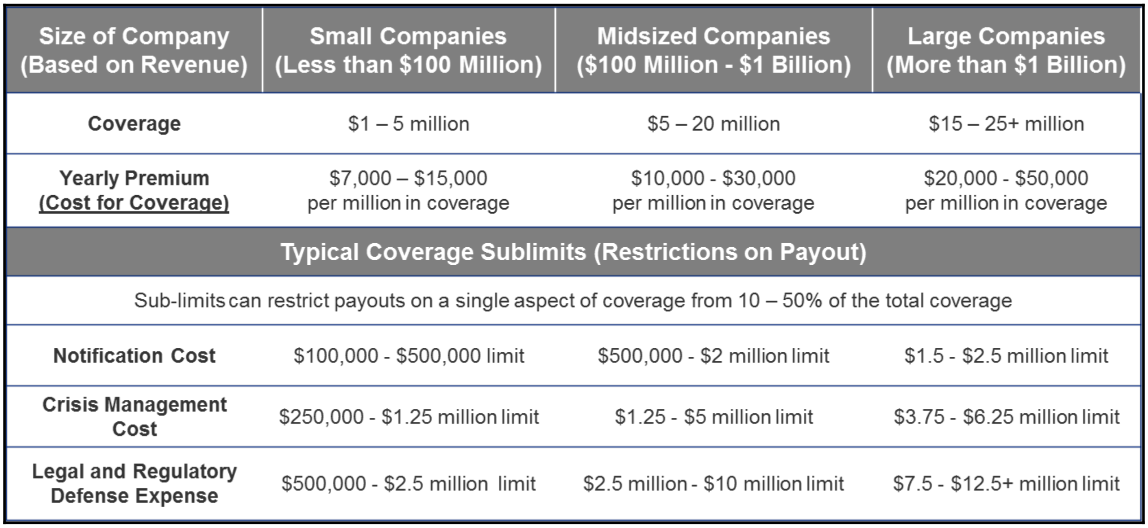
According to the "Chubb Public Company Risk Survey: Cyber," more than 65% of public companies surveyed do not purchase cyber insurance, yet 63% of decision-makers were concerned about cyber risk at a point in time.

Typical coverage provided by cyber insurance

Multiple coverage options need to be considered along with associated pre-conditions prior making an investment in cyber insurance. Some of the most typical coverage provided by insurance providers includes:

- **First Party Coverage:** It defends against losses suffered in response to a cyber security incident that can be referred to as a direct expense to the organization. It primarily includes cyber extortion (which is prevailing right now), costs associated with crisis management including notification of the cyber security incidents, disruption of business services, and so on.
- **Third Party Coverage:** It defends againstlossesrelated with third parties in response to a cyber security incident that can be referred as a cost to others. It generally includes regulatory expenses, communications, and so on.

- **Typical Coverage Exclusion:** Overall the insurance providers write an insurance matching the customer's requirement and their analysis of the customer. Thus, it may explicitly exclude and include certain clauses, coverage limits, coverage areas, and add sections to protect the insurer from much excessive risks. It may include non performance of third-party services (such as cloud, and so on), software malfunction due to errors in programming, and so on.



Size of Company (Based on Revenue)	Small Companies (Less than $100 Million)	Midsized Companies ($100 Million - $1 Billion)	Large Companies (More than $1 Billion)
Coverage	$1 – 5 million	$5 – 20 million	$15 – 25+ million
Yearly Premium **(Cost for Coverage)**	$7,000 – $15,000 per million in coverage	$10,000 - $30,000 per million in coverage	$20,000 - $50,000 per million in coverage
Typical Coverage Sublimits (Restrictions on Payout)			
Sub-limits can restrict payouts on a single aspect of coverage from 10 – 50% of the total coverage			
Notification Cost	$100,000 - $500,000 limit	$500,000 - $2 million limit	$1.5 - $2.5 million limit
Crisis Management Cost	$250,000 - $1.25 million limit	$1.25 - $5 million limit	$3.75 - $6.25 million limit
Legal and Regulatory Defense Expense	$500,000 - $2.5 million limit	$2.5 million - $10 million limit	$7.5 - $12.5+ million limit

Typical premiums associated with cyber insurance as per the Deloitte study

Typical cyber insurance underwriting process

Insurers have started to institute a more rigorous process to underwriting cyber insurance policies:

1. **Initiate and Asses**: The cyber insurance provider would direct the client to have a self assessment of their organization's information technology and security environment. As per the self assessment of the organization the insurance provider may have an independent assessment or walk-through of the environment based on the self assessment.
2. **Risk Assessment**: If the client is requesting coverage of more than $10 million - $15 million, the provider may request the client to also conduct a third-party assessment of their premises.

3. **Review and Report**: As per the results provided to the provider, the provider analyzes the recommendation made by the third party and suggests the outcome as per their own analysis.
4. **Underwriting**: Based on the overall analysis the cyber insurance provider calculates the premiums, and then defines the coverage and associated exclusions.

Considerations while selecting cyber insurance

The following items should be considered when selecting a cyber insurance policy:

- Knowledge of the enterprise risk appetite:
    - Analyze the controls implemented to identify the cyber risk coverage and evaluate the cyber insurance coverage that would be required to cover the high priority risk areas
    - After a comprehensive analysis, it would be gathered that for certain areas where there are security controls, coverage may not be required
- Rationalizing policies and associated complexities:
    - In multiple policies available in the market it is seen that some of them may require enormous underwriting processes. Thus it is advised to spend time in understanding the pre conditions of the policies that are required to be met so as to get hold of insurance.
    - Simultaneously, it is also recommended to realize that there are certain policy exclusions that need to be understood to make the coverage more effective.
- Maintain an equilibrium between cost of premium and deploying security controls:
    - Organizations should definitely conduct a cost benefit analysis once they identify their organization's risk appetite so to determine the overall suitability or relevance of an investment in coverage
    - It is urged in general – to have cyber insurance for covering those risks that are considered to be a challenge for the organization to be resolved in house
- Process for claiming insurance should be clear:
    - Not all cyber claims are treated equally – know what is going to be required to file a claim and make sure you can satisfy these requirements before purchasing insurance

When an incident happens, insurers often require organizations to execute a formal incident response process—including saving logs, e-mails, forensic scans, and other evidence—using methods that preserve the integrity of the evidence.

How third party vendors can assist

Third-party vendors can assist in executing a cyber insurance focused risk assessment to answer the following questions:

- How do you select the appropriate insurance policy?
- What type of coverage should my organization get?
- What residual risks does my organization face with our current cyber insurance?

It is highly recommended to conduct a **cyber risk insurance focused assessment, which should involve:**

- Security assessments to gauge:
    - Cyber prevention measures in place
    - Current risk exposure and potential impact on business
- Analysis of coverage requirements based on assessment results
- Comparison of different policies and coverage offered on the market
- Recommendations and opportunities to strengthen the security program by defining cyber risk management strategies and cyber prevention measures based on current capabilities and coverage requirements

Cyber insurance focused risk assessment

The following sample approach could be used to assist clients in understanding their risk exposure, evaluating insurance policies, and providing recommendations in selecting insurance as well as implementing security controls to improve risk posture. The approach has been split into four phases:

- **Phase 1:** Performing current state cyber risk assessment
- **Phase 2:** Assessing cyber insurance options
- **Phase 3**: Conducting fit-gap analysis
- **Phase 4:** Developing strategy and recommendations

Performing current state cyber risk assessment

This phase includes (at a high level) conducting a risk assessment to identify the key cyber risks, analyzing the security controls in place corresponding to the organization's cyber risks, and conducting simulation activities to understand the extent of losses associated with key cyber risks. It also includes:

- Developing risk profile: Conducting a cyber risk assessment to identify and understand the nature of key cyber risks
- Evaluating the security posture of the organization:
    - Analyzing the security controls in place corresponding to the organization’s cyber risks
    - Based on the analysis, identifying gaps
- Assessing the potential loss: presenting the threat scenarios and simulating the potential financial impacts caused by different types of breach or failure
    - Based on the simulation results, analyze the potential range and extent of losses

Assessing cyber insurance options

This phase primarily emphasizes on gaining an understanding of the organization's existing insurance coverage and identifying various cyber insurance providers—analyzing different types of policies, price and controls expectation, and conducting the review of first-party and third-party policy coverage options. It also consists of:

- Reviewing comprehensive policy options:
    - Conducting the review of first-party and third-party policy coverage options. Analyzing the organization’s existing policy and identifying gaps.
    - Understanding the policy exclusions and identifying potential gaps.
    - Evaluating claims coverage and understanding the potential triggers.
- Based on the policy analysis, identifying corresponding pros and cons
- Mapping the current capabilities and gaps against exclusions and coverage

Conducting fit-gap analysis

Based on the current state assessment, this phase emphasizes identifying potential cyber risks that require insurance, including:

- Identifying gaps in controls required to be implemented prior to insurance purchase
- Performing cost-benefit analysis of purchasing insurance and implementing internal controls

Developing strategy and recommendations

This phase identifies and prioritizes the initiatives required to address gaps in policy requirements and finalize policy purchase decision based on roadmap necessary to meet baseline requirements.

The moral dilemma of malware

Malware is generally malicious in nature by itself. Nonetheless, it is one of the key element forcing victims to consider their actions once they get infected. When a victim is under threat from malware, they don't necessarily have the time and patience to analyze the circumstances and react (or weigh) to the demands from cybercriminals. Until recently, the malware exploit trends followed more or less a similar approach and direct progressive strategy.

Such malware operators also have introduced ethics and principles into the overall equation. Accepting ransom demands from such malicious campaigns is in one way obnoxious, but a necessity in a large number of cases. In a way, it's motivating the cybercriminals—who not only broke into the victim's environment, but also stole or controlled their data. It enables malware operators to grow and plan future attacks with the potential of getting much stronger.

Such malware attacks do not only highlight the vulnerabilities across by environment, but also emphasize on the fact that there's not a clear answer of whether one should accept the ransom demand and pay. In one viewpoint, it could be argued that it's the price that the victim has to pay for having an environment that is unpatched and using outdated applications and software. It is not a surprise that there still exist multiple business units who are using outdated operating systems such as Windows XP for critical business operations, across multiple sectors including healthcare, business and financial institutions, and so on. No general computer users or businesses would prefer to get extorted or fund such criminal activities.

In multiple cases even the law enforcement agencies have suggested victims to "pay the ransom", even though officially it is discouraged—primarily due to the fact that even if victims pay, they may not get their data back. Organizations thus must look forward to having a strategy to decide the best course of action during such incidents. This may split into multiple areas, including:

- Having a timeline associated with bringing the environment back online
- Responsibilities split across stakeholders to keep the business operations up
- Safeguarding the critical assets—customers and employee's information, and so on
- Technical and strategic measures for the organization systems

These are the most critical areas and for no two organizations, it may be similar—excluding the technical measures.

At a minimum the technical measures should include:

- **Creating a defense in depth secure architecture**: Layered security or defense in depth is a crucial element for overall security and it is implemented through overlapping layers providing protection at each level. The key benefits of the defense in depth strategy is that it provides measures corresponding to:
    - Protection
    - Detection
    - Response

In many scenarios, a layered security strategy mitigates the potential weakness of one layer by the strength of other corresponding layers. Practically this strategy involves protecting an asset in a series of multiple layers - for instance at the perimeter layer (that is, the boundary between the Internet and locally managed systems and networks), a classic network security design would enable routers, firewalls, and intrusion detection (or prevention mechanisms to protect the network from cybercriminals and attackers).

In addition to the perimeter devices, further manual real-time monitoring by resources to identify anomalies in the environment and finally the third layer would inculcate automated mechanisms triggering an action in response to anomaly detection. Thus, defense in depth emphasizes on controls at every layer to provide comprehensive security.

Layered security can be related to multiple systems and services. To measure and define one's defense in depth stratagem, it is crucial to identify the key assets that need to be protected from potential threats. It would include - identifying the type of data, where it resides and what are the possible ways to reach to it. This, in turn, assists to define the approach in a more secure manner.

- **Identifying the key vulnerable areas in the environment**: There are multiple components in a computing environment that are generally vulnerable and play a crucial role in the overall system security. These primarily include:
    - Unauthorized and unpatched software's (such as browsers, messaging, social networking applications, and so on)
    - Handling data—How people handle sensitive data and where they store and log critical and sensitive information in the environment.
    - User actions—In the niche of cyber security people are the most vulnerable element in an organization. Modern crypto malware tends to exploit this vulnerability via multiple sophisticated campaigns through spear phishing, social engineering, and click baits.

- **Key actionable steps to hack proof the systems:** At a very high level the following items should be commonly followed across all stakeholders:
    - Endpoint protection
    - Hardening of system services:
        - Ports, port services, and protocols
        - Secure software installation
    - Handling information assets and private information
    - Protection from spamming and phishing
    - Protection from social engineering
    - Backup

For individuals and general computer users the following items are crucial and should be considered very seriously.

Using endpoint protection solutions

The following points should be considered at minimum while configuring an endpoint solution:

- You should scan all the data or documents downloaded from the Internet.
- New versions of the endpoint protection software should be downloaded or scheduled as new versions become available.
- Your system should be configured to be updated with new virus signatures on a daily basis. In addition, anti-virus signature files and programs shall be updated immediately when you are notified that signatures are available to counter a new virus threat.
- Real-time monitoring of files should be enabled.
- Scans of selected operating system files and files in memory should be configured automatically by the virus screening software each time the PC is booted or rebooted.
- A full virus scan of all files on the PC should be performed after every virus signature update.
- Virus scans should not be bypassed or disabled.
- You should also scan all the in-bound and out-bound e-mail messages for traces of any potential harmful malware. Any e-mail messages with virus indications must be quarantined, reviewed, and infected messages deleted.

Hardening systems

It primarily focuses on using restricted services, protocols across ports, and having secure software installation mechanisms in place.

Ports, services, and protocols

It is crucial to determine which ports, services, and protocols are unnecessary by assessing which ones are the least used and do not support a functional use. Systems should be configured so that only the necessary ports, protocols, and services are integrated into support of the organization's functional needs and level of risk tolerance.

Any unnecessary open ports and available protocols and services provide entry points for attackers attempting to attack a system. These risks are increased if there are known vulnerabilities associated with a given port, protocol, or service.

In addition, the remote connections should be provided for system users with a defined functional requirement. If remote connections are approved for use by the organization, use the security requirement guidelines to identify the security configurations for remote access.

Secure software installation

It should be determined how the installation of software should be managed. The simplest approach is establishing controls on computers that prevent any self-installations by users and require software installation to be done at the organizational level. However, this option may not be practical as per your environment. Other methods for controlling the installation of software that may be considered include:

- Whitelisting - All software should be checked and taken from original sources
- Checksums - All software is checked to make sure the code has not changed
- Certificate - You should use software with signed certificates from a trusted vendor
- File extension - Software with certain file extensions such as .bat should not be installed

The following principles are crucial for you from a software perspective:

- All installed software must be legally acquired and covered by a valid license agreement
- Illegal or pirated software must not be used

Handling information assets and private information

Information assets include information and information systems that are of value to you/your family and hence need protection. Examples of information assets include customer data, photos, videos, financial records, and electronic media.

There have been several instances of a sensitive data breach in recent history resulting in a huge financial loss, regulatory action, negative publicity, and other legal and regulatory issues.

All personnel should be respectful of the privacy in the collection, use, retention, and disclosure of personal information. You should be aware of how to prevent unauthorized or inadvertent disclosure.

Protection from spamming and phishing

Spamming refers to the act of flooding user's mailboxes with numerous unsolicited e-mails. Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking e-mail in an attempt to gather personal and financial information from recipients. Spam e-mails fill up the allocated disk space for the user and make it difficult to find the legitimate e-mails.

Phishing can cause damage ranging from denial of e-mail access to financial losses. Phishing is used to steal the identity of the person and impersonate them.

Key tips!

- Do not open attachments of e-mails sent from strangers.
- Use the spam filtering facility of e-mail clients to send spam e-mails directly to the junk folder.
- Do not reply to spam e-mails.
- Do not click on any links in suspicious e-mails especially that are from an unknown sender.
- Do not provide a company e-mail ID for registrations on websites.
- Verify the source of the e-mail before providing personal details.

Ransomware assaults against personal systems are transcending day by day. In the last quarter of 2016 multiple crypto ransomware attacks were targeted towards the general public via multiple phishing campaigns. Since these attacks and campaigns are profitable for cybercriminals with all organizations and individuals being vulnerable, it's becoming mainstream via spamming and phishing techniques.

The consequences of such malware campaigns are far broader than just the cost of the ransom. From the productivity loss in personal data to unavailability of services to general users the impact is enormous.

Protection from social engineering

Social engineering is obtaining confidential information from the user by manipulating. An attacker uses baits or other methods to persuade the user to give out information.

Social engineering relies on common characteristics of most human beings namely to seek help, to trust others, and to fear something that might affect them.

Malicious attackers sometimes impersonate themselves as legitimate personnel. By impersonating as legitimate personnel, these attackers will try to convince employees to divulge confidential information such as user ID, passwords, and so in, in order to gain understanding of your information assets and obtain user account information for data compromise

Key tips!

- Do not share your user ID and password. Avoid giving the password information to anyone electronically or over the phone.
- Do not provide confidential information to strangers.
- If you receive a call from a helpdesk or IT regarding your account, verify if the call is legitimate by asking for their name and calling them back through the company's phone system.
- If someone tries to improperly obtain confidential or proprietary information confirm with the organization that the intruder is impersonating.

Backup

Backup as we understand is the process of saving sensitive data of an organization and its systems in a safe place so it may be used for restoring the services and data in case of an unexpected catastrophe or system failures.

Why do we need backups?

The most crucial aspect of backups is that it prepares the organization to face any form of system failures providing the assurance of full restoration and backup of services. The sole objective of backups is to have the business services available to organization users and customers so to maintain the continuity of the business within a limited accepted time.

What is a recovery?

Recovery is restoration of the files from the backup in a limited amount of time:

- **Offline backup:** When a backup is done while the systems are shut down it is called offline backup, also known as cold backup. In this case an operating system utility is used for copying data and controlling files for providing the complete backup of the environment.
- **Online (or Hot) backup:** Online backup is normal backup wherein you schedule a backup while operating with your system. It is suggested to carefully back up files due to the fact that you would not prefer to have the malware infect your backup drive too. Cloud-based backup can be made using services such as Google drive, Dropbox, and so on.
- **The frequency of online backups:** It is recommended to do a backup every week at maximum or whenever drastic changes or modifications are made to the system in terms of new applications, exporting new family videos or photos, and so on.
- **Critical files**: All the files belonging to the operating system and corresponding database are important. If a media failure damages a file due to a malware while traversing files from one system to a backup drive, recovering it is generally challenging.

Summary

Ransomware assaults are incrementing day by day and are enabling script kiddies and newbies to join the criminal activities. The most effective means to mitigate such cyber attacks is having an appropriate strategy to tackle the situation along with cultivating an environment of awareness among employees.

Having a security and incident response team is of utmost importance and it should be the team who determine a comprehensive security strategy and an action plan that should include - periodic vulnerability management, crisis management principles, and procedures taking into account all known threats, applications and infrastructure patch management, auditing vendors, and so on. Consequently, such actions combined thus would limit the organization's attack surface. Based on the strategy and periodic assessment, an appropriate use case can also be created for cyber insurance.

To increase security detection and prevention capabilities across business units, organizations must seek to capitalize on a comprehensive cyber security framework that includes the key ingredients as organization strategy, talent, processes, and technical security requirements. Employers that leverage security professionals with wide experience in risk assessments and mitigation as a qualification for their team can be more confident in the skills of the employee and their understanding of evolving threats and priorities.

In the next chapter, we will close off the book with final thoughts with an eye towards the future, especially mobile and Internet Of things (IOT). We will also discuss the attacks of the future on servers as well as how machine learning will play a huge role in attacks as well as defense.

9
Extortion of the Future

The key objective of this chapter is to address our final thoughts with an eye towards the future, especially mobile, the Internet of Things, and crypto currencies. We will also discuss in detail IoT and key areas within IoT identifying areas to secure and the key attacks of the future on multiple environment including areas such as wearables and smart home appliances. We will also look at how new technologies and frameworks will play a key role in attacks as well as key areas for protection.

In this chapter, we will cover the following topics:

- What does the future hold for ransomware?
- Focus on operational security
- Ransomware everywhere
- Internet of Things (IoT) meets malware and extortion
- Transforming the business model

What does the future hold for ransomware?

It is easy to estimate how the malware landscape is going to advance in the future. The ransomware industry currently is at a matured state and via observing the pattern of its evolution, it can be speculated how it is going to be transformed in the future

The current level of maturity can be noticed by the number and variety of variants that have emerged in the last 5 years. The ransomware variants are transforming themselves as per the new technologies and security solutions so as to evade the defense systems. The ransomware operators are also transcending their business model by introducing various schemes such as Ransomware as a Service, via which they recruit multiple novice cybercriminals to distribute the respective malware to any extent possible.

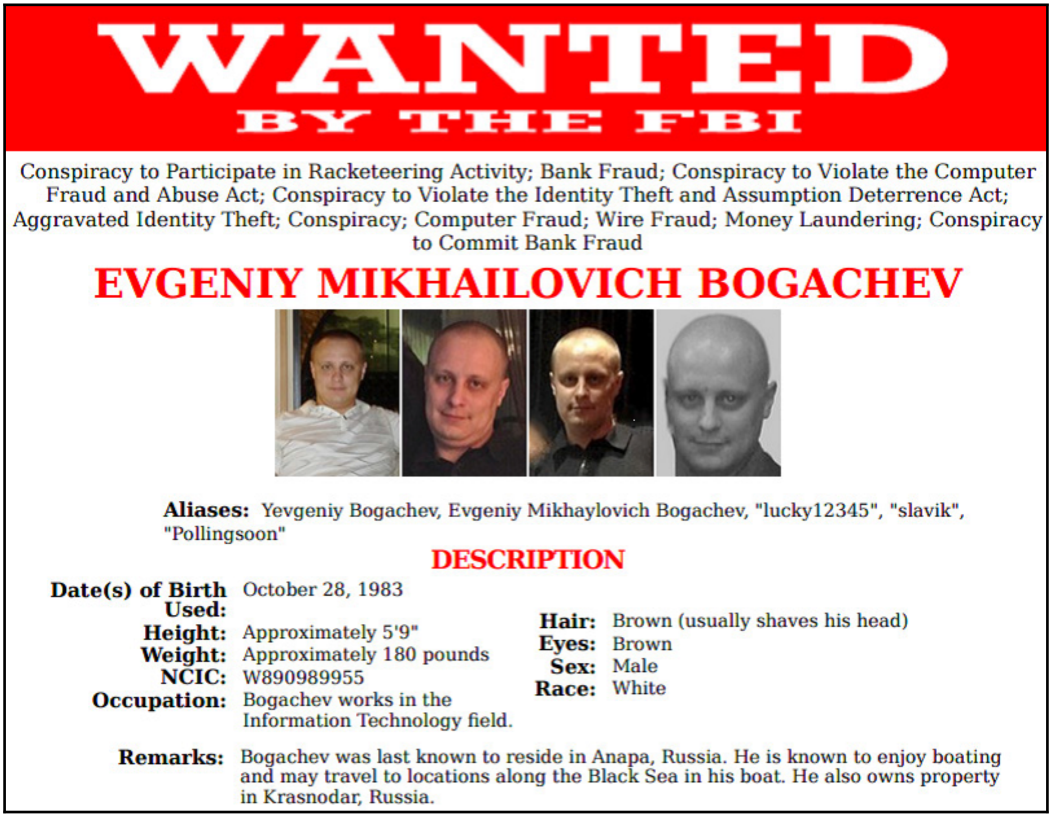
If we analyze the evolution of malware, it can be observed that every 2 to 3 years, malware authors and operators switch their modus operandi and introduce new variants of malware.

Even though the malware trends are incrementing worldwide, it is also to be noted that malware authors need to change the modus operandi periodically due to the increase in protection technologies against such malware, shutdowns from law enforcement agencies, and so on. Malware authors have been seen transforming themselves much rapidly than other cybercriminals.

Seeing the malware trend and variants across sectors, we can potentially note that the recent technological implementations from crypto currencies to sophisticated IoT deployments would share the future of malware and corresponding extortion schemes.

Focus on operational security

As law enforcement agencies are targeting malware operators to a great extent, cybercriminals are required to force themselves to innovate and transform their criminal operations. There have been multiple rewards introduced by law enforcement agencies and security vendors to individuals who will share and give leads to catch/arrest multiple malwares. For instance, the FBI proposed a reward of up to $3 million to any evidence leading to the conviction of the author and architect of the Cryptolocker ransomware.



WANTED

BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used:	October 28, 1983		
Height:	Approximately 5'9"	**Hair:**	Brown (usually shaves his head)
Weight:	Approximately 180 pounds	**Eyes:**	Brown
NCIC:	W890989955	**Sex:**	Male
Occupation:	Bogachev works in the Information Technology field.	**Race:**	White

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

Notice from FBI for Evgeniy Mikhailovich Bogachev –the Cryptolocker author

With this instance, multiple cybercriminal groups are carefully working around malware, introducing multiple services such as **Ransomware as a Service** (**RaaS**), to create a bigger scheme for concealing their identities and introducing multiple middlemen. They also have implemented stringent security processes using Tor and the **Invisible Internet Project** (**I2P**) for communicating with their group members and synchronizing their activities.

Mechanisms such as Tor and I2P provide network anonymity, which in the case of ransomware authors and operators is the most crucial aspect - since it assists them to safeguard themselves from the consistent "take down" efforts by the security solution providers and law enforcement agencies. These also conceal the location of their web portals and services via which the malware operators deal with middlemen and other operators.

In a similar manner, malware authors and operators are primarily using crypto currencies such as Litecoin and Bitcoin as a medium for victims to transfer payments, as per the ransom demands. Such setups make it complex for law enforcement agencies to track criminal trails and even their corresponding money laundering activities.

The hosting services used by the malware operators and cybercriminals are the domain and hosting services provided by another set of firms, which provision multiple avenues for cybercriminals to bypass the law. Such service providers use mixing services, which include multiple levels of redirection so to obfuscate the path of traversal and decreasing the chances of getting caught.

Other measures including wide usage of Captcha and JavaScript challenges into the key activities involved in the ransomware operations, which adds another layer making it complex for enforcement agencies to track in and out operations of the malware. Cryptolocker primarily uses such challenges to prevent automatic downloading of their malware, whereas Cryptodefense customs such challenges preventing direct access to the payment details.

Multiple blacklisting of IPs and geo location capabilities are also used to avert certain visitors from sensitive locations (such as locations where the enforcement agencies are placed or situated) to download the malware. This is also extended to restrict users and investigators from other countries other than the targeted countries. Such mechanisms used by the malware authors and operators are increasing day by day. Thus, it is expected that cybercriminals will employ crucial drivers of future technologies to block attempts to thwart their activities. Some of the key drivers include concepts of Artificial Intelligence, machine learning algorithms, and IoT.

Ransomware everywhere

Since recent times, ransomware was a matter primarily existing in the most widely used OS—Windows OSes only. Gradually malware was designed and available for other operating systems and platforms too, for instance, macOS X, Linux OS, Mobile OS, browsers, and so on. Due to the increasing market share of all other platforms, malware across all the platforms are transcending day by day targeting general users.

Seeing the evolution, malware authors are working to introduce malware into other key areas.

Ransomware was initially a problem that mainly existed for users of the Windows operating system in mostly traditional computer form factors. As Windows is by far the most widely used operating system in the world, this comes as no surprise. Ransomware specifically designed for the other major desktop operating systems such as Linux or macOS X have been thin on the ground. This is most likely due to the low market share of those operating systems, making ransomware investment in them unattractive.

Multi-platform locker ransomware such as Browlock has been created as a sort of catch-all solution to target non-core victims. However, ransomware such as Browlock has limited effectiveness, since it only targets the web browser and can be relatively easily overcome. We have already seen ransomware appear on mobile phones, but where else is ransomware likely to appear?

Malware on your wrist

IoT has a wide market with various applications across multiple industries. Smartwatches are one such area considerably significant in the wearables niche. This is a crucial area in consumer electronics that has gained momentum in recent times across multiple watch manufacturers. Currently, most watch manufacturers are also using their own OS or established mobile OS for the wearables.

Android wear is the customized mobile OS for smartwatches from Google, whereas watchOS is the mobile OS by Apple. Android wear smartwatches are more popular and widely used across the globe due to its wide community support.

With the evolution of wearables and the incrementing hype with associated technologies, it is likely to attract the attention of various malware authors and operators.

When we consider the wearables platform from a malware perspective, it doesn't seem to have any specific reason on why malware may not work on them. Wearable devices generally have a touchscreen that interacts with the underlying system via touch gestures to get the device working. In addition, they also support voice commands that have to be activated through multiple mechanisms - in the case of Android phones by saying "OK Google", and so on. Hardware buttons are generally not used by users since it has a very limited capability. Most of the features and functions can be worked upon via touch and voice commands.

Such devices also have the ability to have direct Internet connections via Wi-Fi. These devices are constructed with **system on chip** (**SoC**) hardware with built-in Wi-Fi equipment. Multiple devices also have the capability to connect with another device such as mobiles with the same platform or operating system - provisioning access to control the smartwatch and deploy custom applications for wearables. Such features on one side provide comfort to users by having mobile notifications and alerts reflecting on the wearable and on other hand it shows multiple avenues for malware authors to create customized malware for wearables or mobile devices that can further affect other devices. Currently, the features available with wearable devices can extend the functionalities of other wearables taking full advantage of the IoT ecosystem.

As per the key areas of wearables mentioned previously and known behavior of malware discussed up until now, it is easy to correlate that the most effective ransomware for wearables will be the locker ransomware. From a cybercriminal's perspective locking wearable devices seems to be an intriguing and potentially viable business model than locking the data contained within the wearable. It is not expected that users may have sensitive data stored in the wearable. Due to the limited control over the wearable hardware and potentially a few ways of interaction - such devices are vulnerable to multiple forms of malware. Even if such kinds of malware hit the devices, the viable options available to a user are either to pay the ransom as demanded by the malware author/operator or resetting the device back to factory state. At the most, such malware infections could make the device unusable.

For deploying an application on an Android wearable, the corresponding device needs to be paired with an Android phone via a Bluetooth connection. Once a device is connected, the user can control the application landscape and settings from the mobile itself. There are multiple ways of pushing an application to the wearable - for instance applications can be installed via a platform-specific application store (for example, Google Play for Android and App Store for Apple) or by directly executing a `.apk` file.

In many cases, applications which get installed over the phone and with Android wear component, would look out and automatically make changes to the Android wear without any manual effort from the user via using wireless protocols. This from the perspective of a cybercriminal also signifies that they can drive a mobile user to install applications from a malicious third-party application store or portal via spam e-mails and SMS - with links to the malicious portal.

Malware on wearables

One of the most common ways via which malware could be deployed into the device is by engaging the user to browse to a malicious web page or application store that further redirects them to download malware disguised as a useful application. Generally, most of the time, a user gets primarily tricked to believe they are installing the right application from the right source, which masquerades the original legitimate sources.

Once the application file is downloaded on the device, it is deployed on the user device and further synchronizes with the other wearable devices associated with the primary device (in which the malware was installed). Generally, it is relatively easier to execute the malware in the smart wear devices provided that the malware author repackages the malware for wearables operating system and the platform. This can be considered as a fairly easy process.

Once this is achieved, and the user executes the malicious application, both the mobile devices and associated wearables would get locked disabling all the touch gesture functionalities. Once the device gets locked any efforts to interact with the wearable or mobile device gets responded by the notification message in the local language of the malware.

Usually, if there is an application that is not required by the device user, they can uninstall the app (which would remove the application from all the devices). Unfortunately, once the device is infected with the ransomware the user cannot remove any of the applications using the general method via traversing through the menu.

This stops the device users from performing any form of interactions since every time they try to interact with the device system, the ransom message is notified to the user. All the functions are impacted, particularly functions that operate through the touch gestures or hardware button. Thus, for all the interactions malware would continuously block and interrupt the user making it unmanageable and difficult to execute any functionality including access to reset functionality.

Since there are multiple types of wearable technology and devices existing on the market, some of them have capabilities to force a cold reboot by holding the hardware button for a limited time. In such instances, users can potentially get some time to execute the factory reset functionality prior the malware gets invoked. This could potentially delete all the existing configurations and settings earlier set as per the user's convenience and provide with a fresh smartwatch. In cases wherein the malware gets invoked when the device restarts, potential recovery is uncertain.

Overall, after validating all the key possibilities of infections across multiple scenarios, in the future we can expect the following types of attacks from malware to wearable devices:

- **Cross Platform attacks** - Malware that may potentially gain the ability to infect different wearable device platforms with small variations in the code.
- **Targeted attacks** - Malware authors may potentially target security hole/vulnerability within an enterprise mobile environment and compromise target devices in layers starting with infecting mobile users.
- **Advanced Social engineering attacks -** Malware attacks under the disguise of legitimate applications can potentially target multiple wearable platforms.
- **Botnets** Mobile and smartwatch botnet's may potentially gain access to the device and its contents. It takes advantage of unpatched exploits to provide attackers with root permissions over the compromised mobile device, enabling attackers to broadcast and send e-mails or text messages to nearby devices.

Internet of Things (IoT) meets malware and extortion

One of the interesting areas where we see the next generation technology drivers emerging is IoT. IoT is one those trends that is transcending periodically with potential dynamic opportunities across all sectors.

The simplest definition for IoT is a giant network of connected things (applications, devices, and people). The information sharing and data flow between things are at the core of this technology. IoT describes the domain where just about everything can be connected and communicated in a smart manner.

Today, people across the world are heavily dependent on IoT, which is touching every facet of our lives. The various application areas for IoT include wearables, smart retail, smart home, connected health, and so on. At the end of the day, all these things need to be tested and validated to ensure the quality and the accuracy of data associated. Quality assurance in IoT, thus, refers to the validation process of various aspects associated with communication, computing, and of course the software, which remains an integral part of IoT.

According to *Gartner Inc*, the Internet of Things base will grow to approximately 26 billion units by 2020.
As per TMT predictions in 2015 by *Deloitte*, IoT and corresponding connectivity revenues are growing at about 10-20 percent annually, while the apps, the analytics, and the services are increasing even more rapidly at 40-50 percent. But very few parameters exist to check and ensure the quality of these IoT enabled devices and machines from a quality and security perspective.

The following sections will provide a comprehensive analysis of approach and methodologies that can be used for securing and testing IoT enabled devices and the various challenges and complexities involved when compared with the traditional approach.

According to *Gartner Inc*, IoT product and service suppliers will generate incremental revenue of more than $300 billion, generally in services in 2020. It will result in $1.9 trillion in global economic value-add through sales into diverse end markets. Creating a robust and reliable IoT system thus becomes an important point of focus, with an approach to test the IoT enabled systems and people focusing on applications and devices.

This extensive growth opportunity is also available for malware authors and operators. At present we can see smart home appliances such as smart TV's, smart refrigerators, smart lights, smart locks, and so on, which can commendably be connected with each other. These work on **Application Programmable Interfaces** (**APIs**), which could potentially be compromised and hijacked by cybercriminals and held for extortion. Most of the devices across industries could be vulnerable by the nature of design or the usage. For instance, **Network Attached Storage** (**NAS**) devices have already been targeted with crypto ransomware variants such as Trojan.Synolocker, which focused on Synology NAS products.

Internet of Things (IoT)

IoT has been the most pertinent word in the technology space and engineering circles over the past few years. With increasing demand for cutting edge devices such as smartphones, tablets, electric cars, and wearable devices, Internet of Things is most likely to transform and shape the technology ecosystem with many more devices for this technology in the coming years.

The concept of this technology is very simple; connect all things to the Internet. The "things" here may refer to computer-based smart devices with sensor and network communication functionality, which has devices such as smartphones, webcams, microphones, medical diagnostics devices, smartwatches, and even vacuum cleaning robots. IoT requires smart elements or units to make it run. An IoT unit is any device or system that is used for communication between systems and devices through the Internet.

> *"The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."*
>
> *Gartner.*

IoT has made great progress in the technology market of wearable devices. There is a recent trend of people getting smartwatches, health bands, and eyewear and using them in tandem to for health purposes and getting fit. There are serious talks of wide usage of smart attire and body embedded technologies as well. All this will be connected through the Internet, to give a boost to the IoT technology.

Assessing embedded and IoT devices

There is a strong need for traditional software quality assurance and security models to be evolved along with IoT. The quality assurance and security teams should start focusing more on usability testing, simulating the environment where the devices will be used, making sure information is exchanged in a secure manner, and that the performance of these devices are not affected. Today, the IoT space mainly constitutes mobile and embedded systems. Thus, the general test approach for testing has to be significantly different from the traditional way of testing desktop or web applications.

The quality assurance and security teams must create use cases and tests scenarios that go beyond the use of mouse and keyboard to interact with these embedded devices They should now take into account the body movements, voice commands, and touch and sensor utilization while designing the tests and at the same time should focus more on the usability and performance aspects of these devices. The key for quality assurance and security teams to achieve quality testing is to think in a way how the "User" interacts with mobile or embedded IoT devices. Since all of these devices actually function with us, testing how the user experiences these devices becomes imperative. If we do not test the user interaction, our assessments and decisions of quality will be lacking some of the most important information needed to determine whether or not the devices are ready to be catered securely to the customer. Why is "User experience" testing so important to IoT devices?

In general, testing should include all things physical, including sizes, shapes, and genders of the users. It should also include testing all sensory reactions including sight, sound, and touch along with orientation, or the interaction with human movement. All these are an incredibly crucial part of the test. Finally, we must consider the value and most thoroughly test in terms of the user's perceptions, mindsets, biases, and emotions when interacting with the IoT devices.

The first step towards adopting the "User Experience" approach is to understand the end user's/customer's requirements. In the case of testing a new device, one can observe contributors using the corresponding device in a prototype lab. In this setting, they can observe and focus on their reactions and possibly discuss with them regarding their feedback and response of the device. Thus, the key to following a test approach for user experience testing involves not only "field" testing, but also testing in the real environment in which the customer is present.

According to `http://www.softwaretestingclass.com`, the following are some of the test scenarios that could be created as part of IoT testing and security:

- Verify that a device is able to register to a network and data connection is made successfully
- Verify that all the devices involved in the IoT testing are able to register to the network
- Verify that devices involved in the IoT testing are able to transmit and receive data through the network
- Verify that only IoT devices with appropriate authentication and authorization are able to connect to the network
- Verify that IoT devices successfully disconnect from the network when the user asks to
- Verify that devices involved in IoT do not frequently disconnect from the network until the user specifically asks to
- Verify that if a maximum number of connections (as per the requirement) is attained, the IoT device needs to stop the attempt to link to the network until a predefined duration
- Verify that in the event when data volume surpasses that defined in requirement, the IoT device should not initiate any more transfer of data until a predefined duration
- Verify that the IoT device is able to transfer data in low power mode
- Verify threshold signal range for an IoT device and how far can the device operate from the network

IoT as of now is highly vulnerable and is not a foolproof system. An aggressive approach to IoT testing by building a framework and executing different types of testing can only help in making the ecosystem robust.

Although, being one of the most critical areas in testing IoT apps and services, security testing is often overlooked due to market pressure on companies for launching new products/releases. Also, at times there is a lack of understanding of security testing by the IoT manufacturers. Needless to say, security testing is very critical and cannot be missed as the device's behavior affects the end user's everyday life and the device can actually be configured through a wireless connection, remotely.

So one can imagine how vulnerable these devices become if these devices are wrongly configured intentionally! As an example, taking control of IoT systems of another user by cutting off its transmission can be done by an IoT system remotely. Thus, security testing assures that the system is accessed only by an authorized user and the information exchanged between the device and the system is not intercepted and modified by a hacking attack. A few security features that can be included as part of security testing in an IoT ecosystem are insufficient authentication/authorization, insecure network services, privacy concerns, insecure software/firmware, lack of transport encryption, and so on.

The common security observation

Across the industry, the following observations that are listed here, relate to people, processes, or technology and they are the most common root cause for lack of security in IoT and are summarized as follows:

- **There is no clear ownership of device security:** Though the product R&D teams are knowledgeable regarding the product design and configurations, they don't perceive themselves as the accountable parties for owning security requirements and proactively embed security into product design, development, and deployment lifecycle.
- **There are no baseline security requirements for product R&D teams to use**: For certain products, the product R&D teams are more aware of technical security capabilities especially when these products are becoming more accessible remotely. For others, there is more reliance on physical security controls of the hospital or clinical environment where devices reside.

- In general, the process is lacking in:
    - Applying security into product development lifecycle including lack of a formal security risk assessment
    - Raising awareness to smart device users (for example, calling out specific security responsibilities for hospital users to adhere to via user manuals, training, standard end user license agreements, and so on)
    - Managing security for those products that are outsourced to third parties for design and development a formalized security patch management process.
- **There is a lack of basic security controls for most of the in-scope devices**: The lack of these security capabilities (such as unique user account and password controls, anti-virus, security patching, logging and monitoring, and so on) introduce increased risk exposure, especially as these devices are moving online or becoming remotely accessible. Even for devices that are only connected to the local hospital network, the increasing threats of computer virus contamination or hacking activities (against the hospital environment) potentially make these devices more vulnerable and render physical security controls less effective.
- **A lack of technical security control capabilities in devices is beginning to impact device sales**: The use of legacy versions of Windows operating systems, the inability of customers to patch operating system vulnerabilities, and difficulties in implementing anti-virus capabilities on the devices has led customers to not select a firm's devices, or require them to go to extra efforts (for example, use of network isolation) to utilize their devices. They can also lead to regulatory compliance challenges due to the increased security risk exposure (for example, unauthorized disclosure or loss of patient information, and so on).

In a nutshell, IoT security and testing complexities go beyond devices and sensors to include added complexity that comes with a big volume of data transaction and communication (that is, huge volume, velocity, and variety), which makes testing of real-time IoT certification a major headache.

With IoT getting mainstream possibilities for cybercriminals are also endless. Some of the scenarios can be the smart house locking out its residents, a smart car being controlled by the ransomware and rejecting its normal operations such as controlling speed, and so on. There have been practical instances wherein a few security researchers remotely controlled a moving vehicle and took control of the entire vehicle. They were able to remotely control most of the vehicle's functionality such as the infotainment system (entertainment system), steering, brakes, and so on. Such kinds of attacks are not complicated to automate especially considering that connected computing technologies go beyond using machine learning and artificial intelligence frameworks.

In the past, ransomware infections did not necessarily put lives at risk. In the future, this frightening prospect may just become that bit closer to reality. Such key aspects could be intrinsic to the IoT space; their impact would obviously be quite vertically agnostic.

Transforming the business model

For rookie cybercriminals who are looking for fun and profit via cybercriminal activities there have been multiple underground marketplaces wherein malware authors and operators sell various forms of crimeware toolkits. Such tools provision easy access to the ransomware and extortion. RaaS is one of such examples wherein several malware instances were transitioned and made available via an affiliate model free of cost.

Multiple malware variants are available with access to almost all the key components to build a sophisticated malware and to hold a system hostage including a provision to create a backend C&C server (with server control plane application). Cybercriminals could procreate the malware customizing the mode of extortion message and the amount that they wish to present to the potential victim. Some of the early examples include Trojan.Ransomware.k, Trojan.Bootlock.B, and so on.

Cybercriminals are potentially seeing criminal activities as a medium to earn profits and in most cases a business venture. Thus most of the successful technological evolutions and innovations motivate cybercriminals to apply them into their potential campaigns. Malware authors primarily look to monetize their malicious solution (malware) and innovating via various affiliate models procreating technology, gives them enough **return on investment** (**ROI**). Tox and Torlocker are some of the key examples where the authors took the opportunity to transcend its operations via provisioning it "as a Service"—Ransomware as a Service. This allowed novice users to get into criminal activities and at the same time a share of the profit earned by distributing such ransomware across the globe via any means.

Given the success of such types of business models, it could be assumed that cybercriminals would look forward to innovating with current business models and increasing the complexity of malware utilizing novel innovation techniques and modernization.

Summary

Thus, extortion, malware campaigns, and multiple other cybercriminal activities are to rise tremendously in the near future with the industry leaning on multiple new technologies such as unregulated crypto currencies and devices revolutionized as a part of the IoT ecosystem. Using such technical innovations and exploiting the unregulated industry, we have seen how cybercriminals earn profits and launder money via piloting multiple sophisticated criminal activities.

Index