Ransomware.
A Victim's Perspective

A study on US and European Internet Users

Bitdefender

Contents

Executive Summary 3

A Victim's Perspective on Ransomware 3

Americans, More Willing to Pay 4

Photos of High Value 5

Brits Pay More Cash 6

The Fear of Spam Emails 6

A Look into Ransomware 7

Known Types 7

Ransomware Developments and 2016 Evolution 9

Android Ransomware 9

Browser-Based Ransomware 10

Linux Ransomware 10

Encryption Developments 10

The Ransomware Business Model 10

Ransomware to Cripple Businesses 11

Protection for End-Users and Companies 11

Authors

Liviu Arsene - Senior E-Threat Analyst
Alexandra Gheorghe - Security Specialist

Executive Summary

Biological viruses try to adapt to their surroundings to survive. Some fail, but some thrive, even spreading to become an epic epidemic. Cyber-threats are no different. In 2015, ransomware caused $350 million in damage, living up to its reputation as the most significant menace targeting Internet users and organizations to date.

A study Bitdefender conducted in November 2015 on 3,009 Internet users from the US, France, Germany, Denmark, the UK and Romania offers a victim's perspective on data loss through crypto-ransomware. *What motivates victims to pay up? How much do they value their data? What role does antivirus protection play in the problem-solving equation?*

Key findings

- 50% of users can't accurately identify ransomware as a type of threat that prevents or limits access to computer data.
- Half of victims are willing to pay up to $500 to recover encrypted data.
- Personal documents rank first among user priorities.
- UK consumers would pay most to retrieve files
- US users are the main target for ransomware.

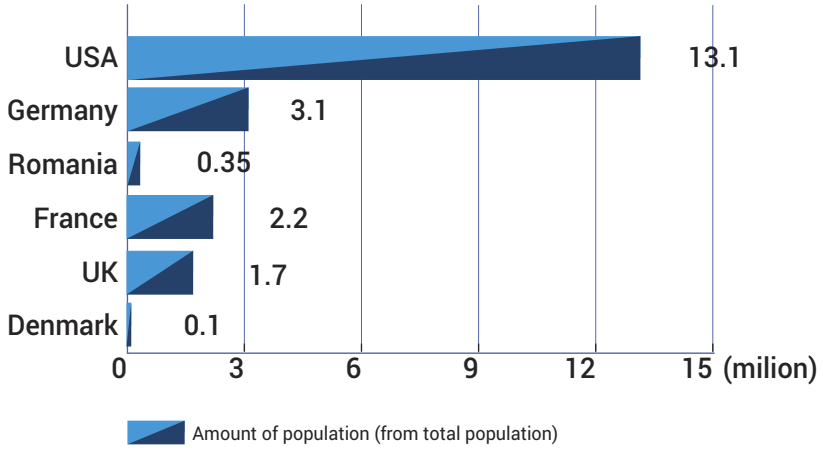
PART I
A Victim's Perspective on Ransomware

A Bitdefender study revealed that less than half of users can't accurately identify ransomware as a type of malware that prevents or limits access to computer data, but two thirds are aware that it can harm computers. The November 2015 study was conducted by iSense Solutions covering 3,009 respondents from Romania, the United States, the United Kingdom, France, Germany and Denmark.

This extortion-based malware has been indiscriminately targeting Internet connect users, including 4.1 percent of the U.S. population, amounting to almost 13.1 million people, according to the study.

32% of users unaffected by ransomware think it is improbable or very improbable they will get infected.

Although Germany, Romania, France, the UK, and Denmark have slightly lower percentages[1] in terms of ransomware victims – 3.8 percent, 3.4 percent, 3.3 percent, 2.6 percent and 2 percent – victims number in the millions. Germany stands out, with 3.1 million potential victims, followed by France with 2.2 million, the United Kingdom with 1.7 million, Romania with 350,000 and 100,000 potential victims in Denmark.



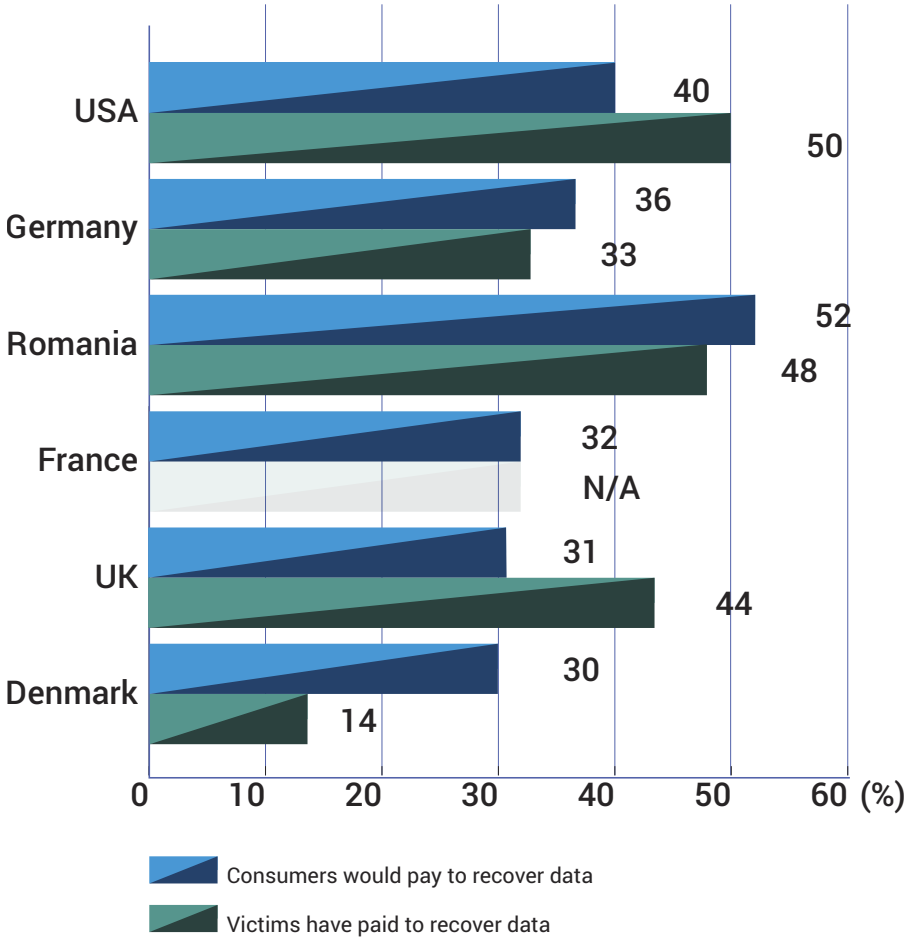
Half of victims are willing to pay up to $500 to recover their data even though there's no guarantee they'll actually receive the decryption key. This brings the ransomware business staggering amounts of money that further fuels cybercriminal activity.

1 All percentages include respondents that can correctly identify ransomware.

Americans, More Willing to Pay

In the United States alone, more than 50 percent of ransomware victims have actually paid the extortionists – at least some of the affected data was important to the users if they were willing to risk paying a criminal to retrieve it.

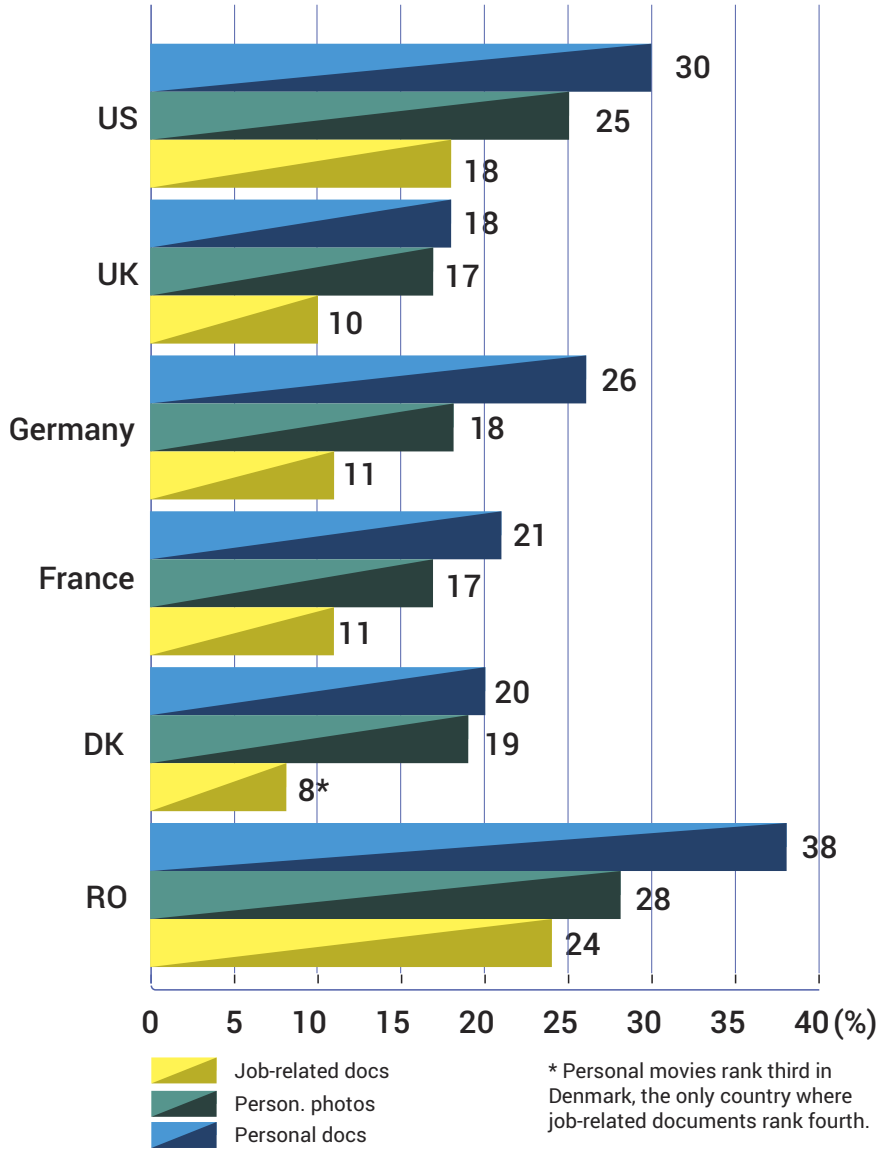
Romania and the UK follow the same behavior, as 48 percent and 44 percent of victims, respectively, paid the ransom following an infection. More skeptical are Germany and Denmark where 33 percent and 14 percent, respectively, to pay the requested fees.



Photos of High Value

Asked to rank data by its importance, US respondents said they value personal documents and personal photos more. Some 30 percent would pay to recover personal documents and 25 percent for photos, while only 18 percent would pay to recover job-related documents.

The perception that some data is more important than other data holds true for all respondents. The same prioritization was observed for the UK, Germany, France, Denmark and Romania, which only differed in percentages. For instance, 18 percent of UK respondents would pay for personal documents, 17 percent for personal photos and only 10 percent for job-related documents.



With 26 percent of German users willing to pay for personal documents, only 18 percent would hand over cash for personal photos, and 11 percent for work-related documents.

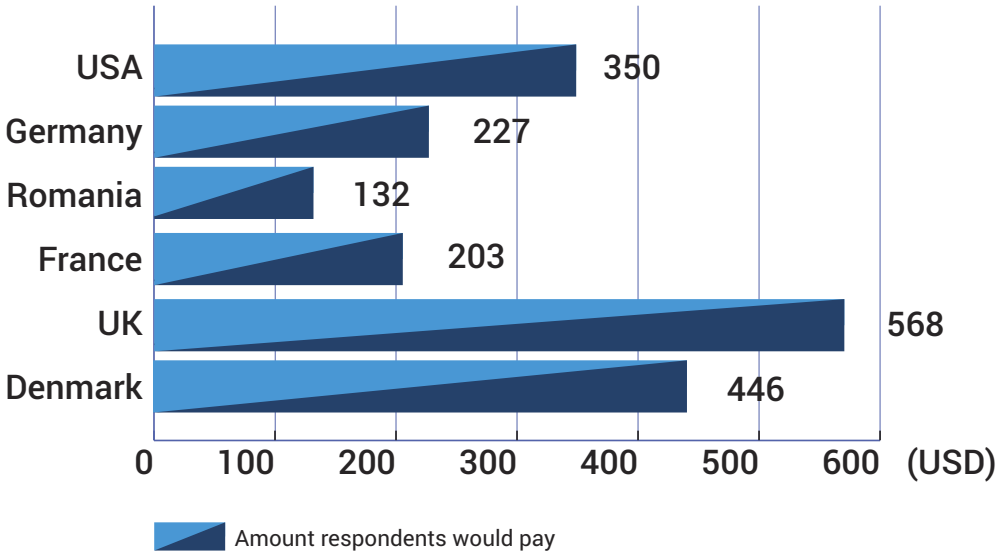
In France, Denmark and Romania, 21 percent, 20 percent and 38 percent of respondents consider personal documents of utmost importance and would pay to regain access to them.

Personal photos rank second in importance in France, Denmark and Romania, with 17 percent, 19 percent, and 28 percent of respondents stating their willingness to recover them. Job-related documents rank third for the same countries, with only 11 percent, 8 percent and 24 percent of respondents, respectively, expressing willingness to pay for their recovery. Only the Danes ranked personal movies third.

Brits Pay More Cash

UK consumers are willing to pay most to recover personal documents, photos and job-related documents, handing out twice as much as the French. Brits are willing to pay as much as £400 to decrypt their files. The French would be willing to dispense as much as €188 to recover their data, while Germans would part with about €211.

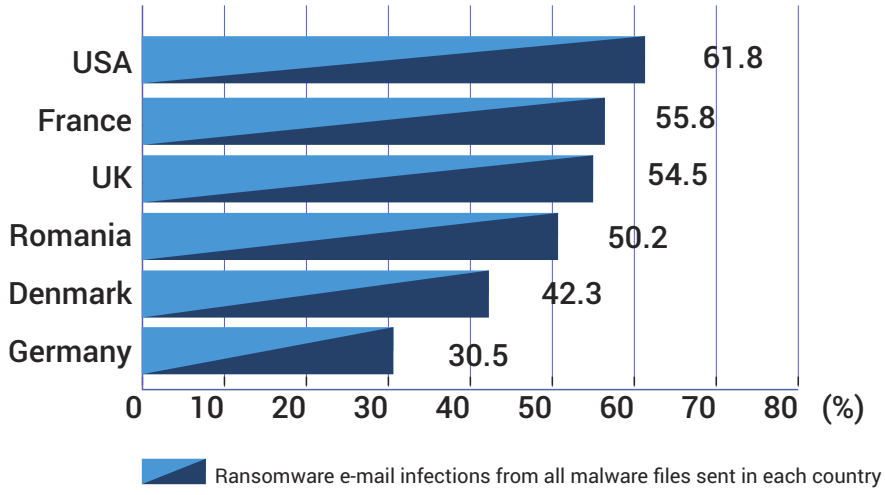
U.S. and Danish respondents would spend as much as $350, and €311, while Romanians would go no higher than €122.



The Fear of Spam Emails

American users are the most sought-after targets. Bitdefender internal reports show 61.8 percent of all malware files distributed via email targeting US Internet users contained some form of ransomware threat. France ranks second with 55.8 percent, while the UK, Romania, Denmark and Germany had 54.5 percent, 50.2 percent, 42.3 percent and 30.5 percent, respectively.

While emails also contain other threats, such as banking Trojans, spyware and other info-stealers, it seems that they are also the most common delivery method for ransomware infections. To pique the user's curiosity, messages range from "Please see attached file" to "Please find your invoice attached" or "Here's your package tracking info."



Another interesting aspect is that 21.21 percent of all ransomware-infected emails sent globally target the US, with the UK and France coming second and third, with 9.1 percent and 3.85 percent.

Romania, Germany and Denmark account for 3.46 percent, 3.41 percent and 0.10 percent of global ransomware-infected emails, possibly because cybercriminals believe US users are more willing to pay.

9 out of 10 users of social networks say the attacks can happen anytime, not just around a certain holiday

Note:

The study was conducted in November 2015 on 3009 respondents from Romania, United States, United Kingdom and Northern Ireland, France, Germany, and Denmark. The margin of error for the U.K. is of ± 4.38 percent. The margin of error for Denmark, Germany, and U.S. is of ± 3.1 percent, while the margin of error for France and Romania is of ± 6.88 percent. The confidence interval was set for 95%.

In most countries surveyed, the majority of respondents are men (52%), 36-55 years of age. In the UK and France there are slightly more female respondents, while in Germany and Denmark the number of men and women is identical. Half of respondents are business managers, with a Bachelor degree education and married with children.

PART II
A Look into Ransomware

Modern-day ransomware is a type of malware that locks and usually encrypts an operating system until the user pays to regain access. The malware can enter a system through a malicious downloaded file, a vulnerability in a network service or a text message.

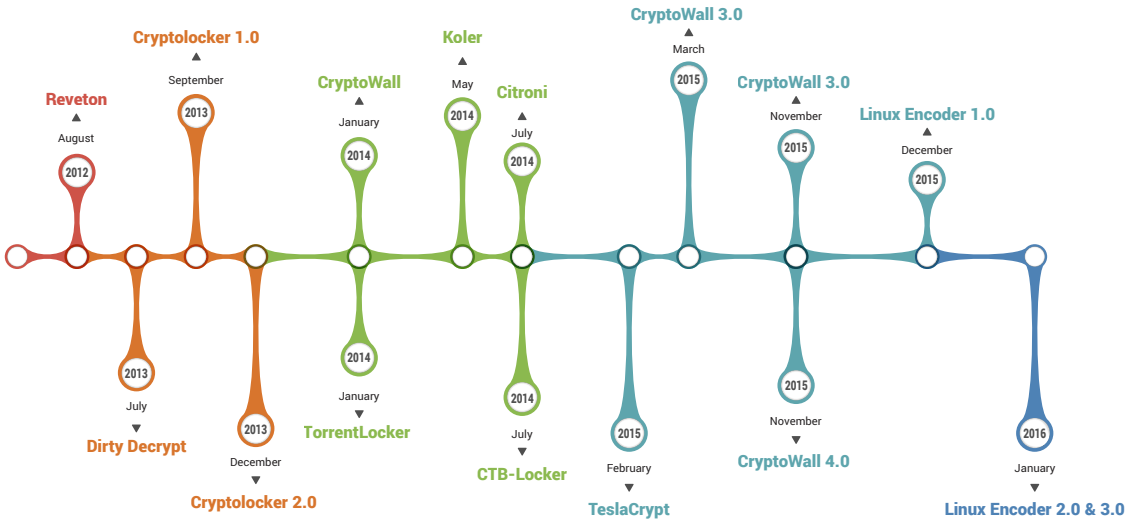
Why is it different from traditional malware?

- It doesn't steal victims' information, but rather encrypts it
- It doesn't try to hide itself after files are encrypted because detection won't restore the lost data
- It demands a ransom, usually in a virtual currency
- It's relatively easy to produce—there are a number of well-documented crypto-libraries

Known Types

Extortion is an age-old crime, but it showed its digital face in the early 2000s with a fake spyware removal tool. They exaggerated the impact of computer issues, such as unused registry entries and corrupt files, and claimed to resolve them if the user paid between US$30 and US$90 for a license. The next milestone occurred between 2008 and 2009, when cybercriminals started creating fake antivirus programs, a more aggressive subcategory of misleading applications.

In 2011, attackers transitioned from fake antivirus tools to a more sophisticated form of extortion: file-encrypting viruses.

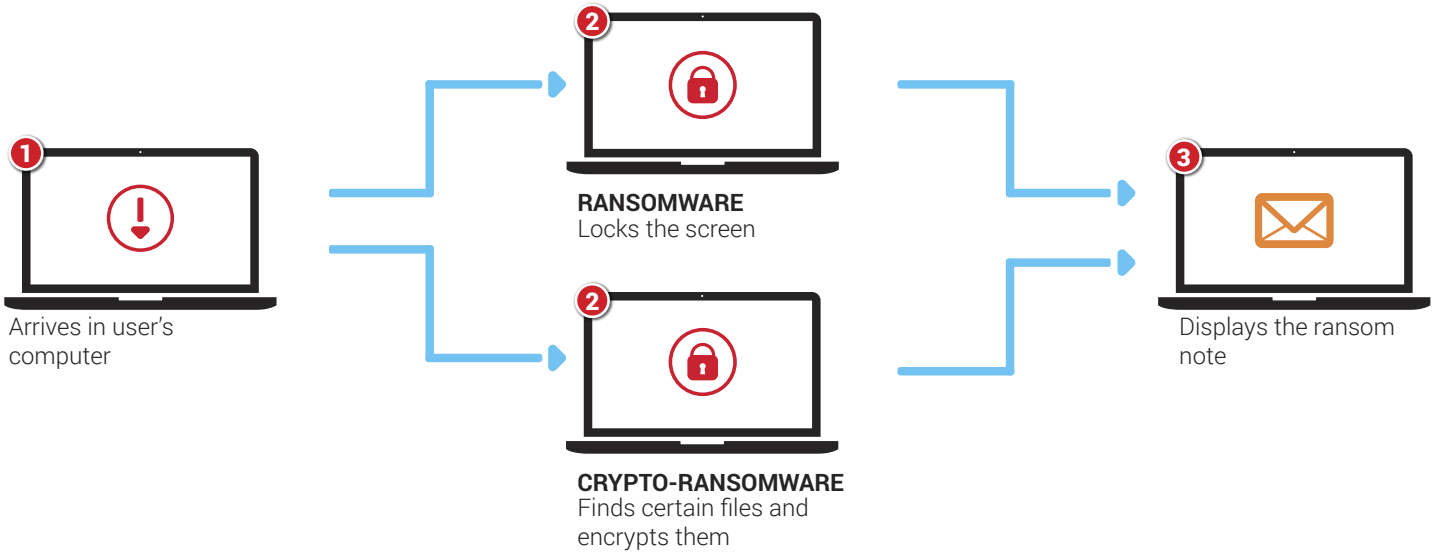


Two main forms of ransomware are circulating today.

Device lockers. This type of early ransomware locks the device screen and displays a full-screen image that blocks access to the device. The message demands payment, but personal files are not encrypted. This type of ransomware is often presented as a message from police and threatens to fine users for alleged online indiscretions or criminal activities.

Crypto-ransomware. File-encryptors are more evolved than lockers, boasting irreversible encryption of personal files and folders such as documents, spreadsheets, pictures and videos.

Both types of malware deny access to computer resources, but lockers can be dismantled through various system restore techniques and tools while encryptions can't be easily deciphered, making them more destructive by nature.



How the Infection Chain Works

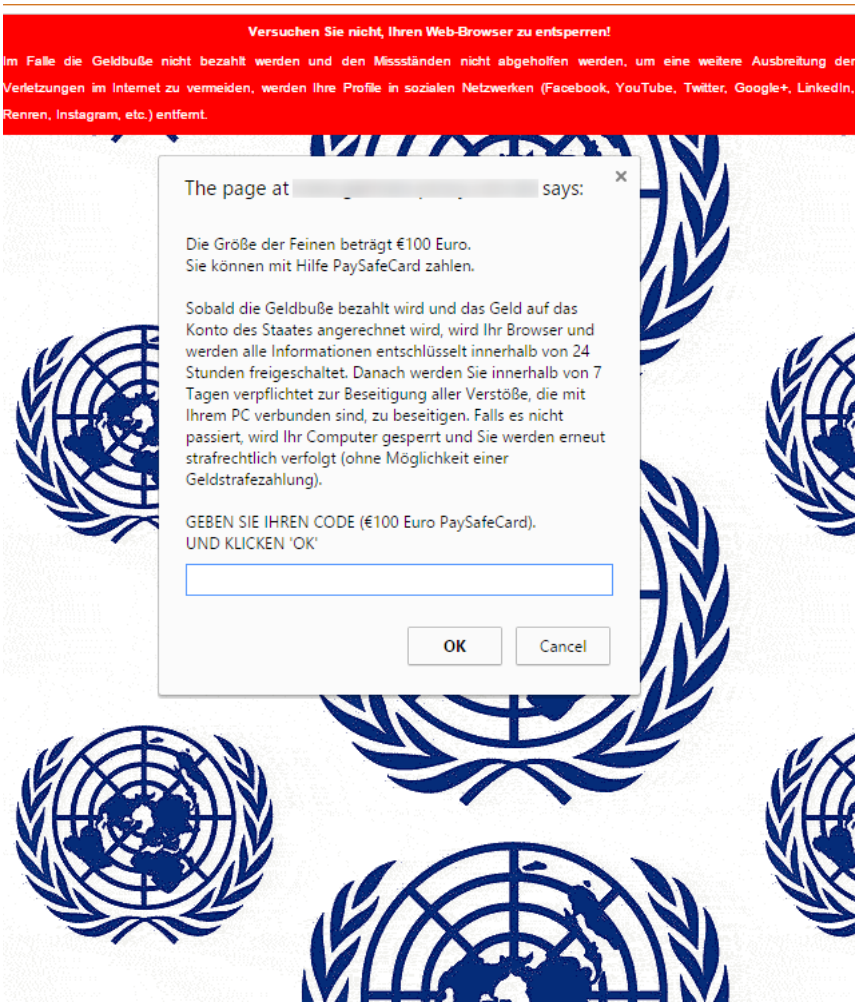
Ransomware proliferates through these main attack vectors:

- Spam/Social engineering
- Direct drive-by-download
- Drive-by-download through malvertising
- Malware installation tools and botnets

After infiltrating the machine, crypto-ransomware connects to randomly generated domains to download an encryption key. It starts looking for user-defined content such as documents (.doc, .xls), presentations (.pdf, .ppt), photos (.jpg) and other files extensions. For instance, CryptoLocker begins encrypting more than 70 types of files that might be on the victim's device. After identifying the targeted files, a key will be generated for each file and used to cypher the data, according to more or less complex encryption algorithms. The process renders the data unusable.

The malware displays a message telling victims how to recover data and requesting urgent payment through virtual currencies or a pre-paid cash voucher, before a specific deadline. The victim transfers the money and sends proof of payment. Once the transaction is complete, the attackers send decryption information to the victim.

Sometimes, cyber-criminals localize the screen-blocking message.



Ransomware Developments and 2016 Evolution

Android Ransomware

While ransomware has plagued the Windows operating system for a couple of years, its developers have expanded their horizon to new platforms. The Android operating system was deemed a likely candidate for the new generation of mobile ransomware, not only because of its staggering 82.2 percent market share in Q2 2015, according to IDC, but also because it has more than 1.4 billion 30-day active users globally, according to Google CEO Sundar Pichai.

Android ransomware samples usually lock out users and demand payment to unlock devices, although no actual file encryption takes place. While some may encrypt information on SD cards, 2015 ransomware variants focused more on simply scaring users into giving in to their demands.

One sample changed the lock screen PIN of the infected device and tried to kill the process of the on-device security solution that could have detected and removed the threat. This is pretty much the same type of behavior we've seen from PC threats, meaning that 2016 will probably bring new functionalities.

As for infection vectors, one of the most common methods for delivering Android ransomware has been through malvertising. In this process, malware developers poison ads on legitimate websites by purchasing advertising space. When clicked, these ads either redirect users to fake marketplaces or trick them into downloading seemingly innocuous video players or system updates that end up infecting devices.

As Google has allowed code obfuscation by introducing ProGuard, all Android malware, including ransomware, will become a lot tougher to spot and analyze, potentially even touching GooglePlay, in addition to third-party marketplaces.

Bitdefender's own Android statistics show that the Android SLocker ransomware family has grabbed 4.35 percent of all mobile malware reported by infected devices in Q3 2015, and 3.08 percent in Q4 2015.

Browser-Based Ransomware

Browser ransomware, although scarce in 2015, is an effective method to scare victims into paying. One of the simplest types of ransomware, it prevents users from switching browser tabs while displaying a fake fine for surfing pornography illegally.

Because no actual malware is installed on the device, but rather a couple of JavaScript tricks that prevent users from closing the browser tab, the browser ransomware is fairly simple to remove. Because it's just a JavaScript, it means that it can affect PC, Mac OS X and Android users alike as long as they use a browser with JavaScripts enabled.

Linux Ransomware

The newest development in ransomware has been its attack on the Linux operating system. Its developers have been gravitating towards this platform because Linux-enabled webservers are at the heart of the Internet, many of them even hosting dozens of websites. Successful infection could affect more than one victim, so ransom payout could also increase.

So far, attempts to create a truly persistent form of Linux ransomware have failed as Bitdefender researchers were able to find cracks in the encryption algorithms used to lock the files and to provide a free decryption tool to recover the Linux.Encoder-encrypted files.

Mostly exploiting vulnerabilities in Joomla or various unpatched Linux components, a truly working Linux ransomware would be quite devastating to the Internet, as webservers that make up a vast majority of the internet rely on Linux to serve webpages to millions of users. One of our 2016 predictions actually involves the evolution of Linux ransomware, marking it one the most serious threats to date.

Encryption Developments

Windows ransomware has gone through various transformations, as law enforcement and security companies hammered down on some of the most popular and prolific variants, such as CryptoLocker, TorLocker, BitLocker and others.

Not only have malware developers included various polymorphism and obfuscation mechanisms to their variants, but encryption mechanisms have also evolved to make it difficult to decrypt files without the decryption key and hide the location of their command and control severs.

To this end, the first ransomware samples used asymmetric encryption (RSA), requiring public and private keys for data verification and decryption. Of course, decryption keys were stored on remote servers - command and control servers – and sent to victims only after they agreed to pay the ransom.

Subsequent attempts to make identification of command and control servers even more difficult involved using the Tor (which stands for The Onion Router) network, to anonymize the domain address of the C&C server. While the Tor network was purposely build to ensure anonymous internet surfing for everyone, those who wanted to avoid being tracked (e.g. by cybercriminals or cyberterrorist) quickly adopted it.

Infected Windows computers would send encrypted data back to the malicious server with the .onion domain address, making it extremely difficult for law enforcement and security companies to take down the entire operation.

Ransomware made an interesting move when it started to target the Linux operating system, effectively encrypting files stored on webservers, such as webpages. While the first three variants of Linux.Encoder allowed Bitdefender researchers to easily guess the encryption key and provide a free decryption tool for victims, it's becoming clear that its developers are trying to strengthen their encryption to counter this.

The Ransomware Business Model

The elusive dark web has been associated with criminal, cybercriminal and terrorist activities, nurturing the distribution of illicit goods and services ranging from drugs and guns to assassinations and cybercriminal activities. Hacker and malware coders have openly offered their knowledge and services to the highest bidder, developing custom malware for serous money – usually using the Bitcoin cryptocurrency.

The term "malware-as-a-service" has been attributed to such activities, which have gone so far as to distribute ransomware kits that enabled even non-tech-savvy individuals to purchase, deploy and monetize the malware for as little as $3,000. Considering the return on investment is usually stellar – provided a large enough network of victims – the price is a bargain for someone willing to break the law.
The CryptoLocker/Cryptowall ransomware kit was spotted on sale for such an amount. Its developer even offered business models ranging from affiliation – where both the customer and the developer split the earning 50/50 – to partnerships that could span to other cybercriminal activities.
Besides purchasing the full source code of the malware and the ability to endlessly generate new samples, the developer also offered free 24/7 support.

Cybercriminal activities in the Dark Web have been constantly adapting and thriving, with malware-as-a-service business reaching the same complexity, scale and management as a legit outsourcing business.

Ransomware to Cripple Businesses

Bitdefender predicts ransomware will intensify attacks against small and medium businesses. By encrypting data and threatening to post it online, attackers will likely aim at SMBs to generate more revenue than ever.

Besides file-encrypting capabilities, ransomware may come packing worm-like functionalities, allowing it to spread to entire networks once an endpoint is compromised. Everything from desktop and laptops to file sharing servers could be affected, causing significant data losses or even completely crippling a small business.

Ransomware's platform-agnostic capabilities will be used against companies, as they're far more likely to pay for data recovery than end-users. Monetization and profitability has always been the main focus of ransomware developers and in 2016 they'll probably reach stellar conversion rates from successfully targeting small and medium businesses.

Protection for End-Users and Companies

A major component in security of both end users and companies is the use of an endpoint security solution that can quickly identify threats and mitigate infections that might break free.

2 out of 10 of men believe that an antivirus program will surely prevent an infection.

Here are a couple of steps that could help users stay safe from ransomware:

- Use a known, award-winning security suite
- Patch or update your software to avoid known vulnerabilities from being exploited and used to infect your system
- Back up your data
- Enable the "Show hidden file extension" option. This will help identify suspicious files that have been named ".ZIP.EXE" and prevent their execution

Companies, on the other hand, are strongly encouraged to:

- Use an endpoint security solution
- Patch or update all endpoint software and webservers
- Deploy a backup solution
- Disable files from running in locations such as "AppData/LocalAppData" and deploy policies that restrict users from executing malware
- Limit users from accessing mapped network drives
- Protect email servers with content filtering solutions
- Educate employees on identifying spear-phishing emails and other social engineering techniques.

Publication Date: January 2016

Bitdefender

BD-NGZ-Feb.01.2016-TK# 86847