An exponentially growing cyber threat

Stéphane Hurtaud
Partner
Governance, Risk & Compliance
Deloitte

Maxime Verac
Senior Manager
Governance, Risk & Compliance
Deloitte

Yasser Aboukir
Senior Consultant
Governance, Risk & Compliance
Deloitte

Nowadays, organizations are in a race to improve the state of their cyber risk programs and the maturity of their security capabilities. Meanwhile, cybercriminals are continuously advancing their methods of generating revenue. One such threat that is growing exponentially is ransomware.

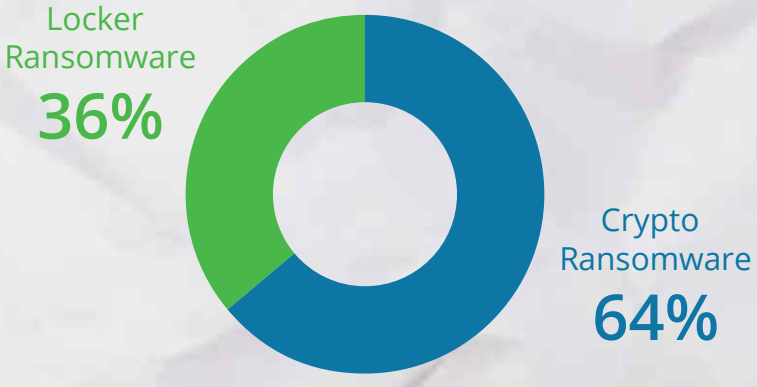
Ransom-what?

Many companies have already heard about Locky, TeslaCrypt, CTB-Locker, and other ransomware that have been in the headlines during the last months. Ransomware is a type of malicious software that restricts or limits users of a targeted organization from accessing their IT systems (servers, workstations, mobile devices, etc.) or their data, until a ransom is paid. There are two types of ransomware:

- **Crypto Ransomware:** Targets the data and file systems on the device itself, so the computer is functional except the ability to access the encrypted files
- **Locker Ransomware:** Prevents the victim from using the system by locking components or all of the system

A typical method of infection is an email containing a malicious attachment that will download the ransomware. Users may encounter this threat through a variety of means, but ransomware is often distributed as attachments to a series of phishing campaigns. Ransomware can also be downloaded by unwitting users who visit malicious or compromised websites, or it can arrive as a payload, dropped or downloaded by other malware. The most prevelent versions of the malware are TeslaCrypt and Locky, which encrypt files on a computer's hard drive and any external/shared drives, then direct to a payment page that requests a ransom amount.

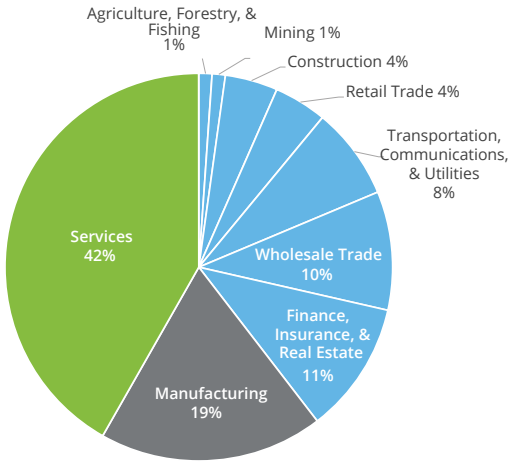
Ransomware can harm an organization's reputation, especially if intellectual property or other relevant information is compromised. It can also affect an organization financially, especially if the business activities are disrupted and the ransom amount is paid.



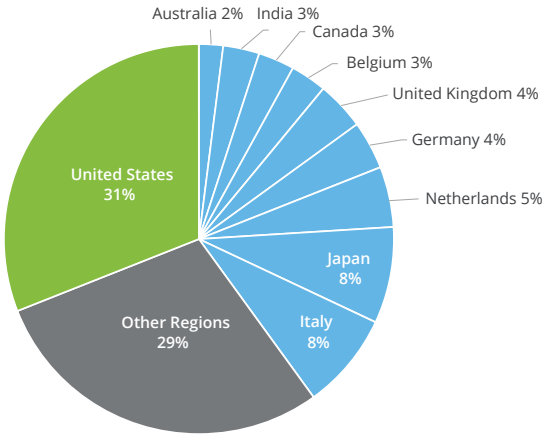
Source: Symantec 2014-2015 Ransomware Detection

Figure 1 - Symantec - Ransomware and Businesses 2016 (Statistics from January 2015 to April 2016)

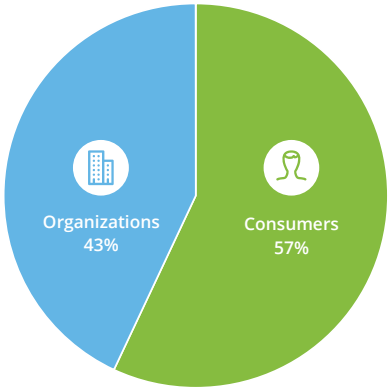
Ransomware infections by organization sector



Ransomware infections by region



Consumer vs. organization ransomware



Who are the victims?

The threat agents behind ransomware are continuously evolving, and have become more focused and selective when launching their ransomware attack campaigns. Initially, ransomware attacks have been non-targeted, i.e., they mostly spread through large email phishing campaigns and demanded small payments (~1-5 Bitcoins) from individual users. However, threat actors have evolved to target specific organizations instead, hoping to land a bigger payday. Consumers are still the most likely victims of ransomware (accounting for 57 percent of all infections between January 2015 and April 2016[1]), but realizing the potential for higher profits, cybercriminals are increasingly targeting the business space with organizations.

New ransomware knows where you live: Threat agents are now taking geographical location into account when targeting victims, especially to focus on wealthier countries, likely because victims in those countries are more able or willing to pay (as illustrated in Figure 2, the vast majority of infections occur in the USA and Europe). Another objective with those geo-targeted ransomware is to develop elaborate attacks integrating local specificities (local language, local currency, etc.) and to spoof local institutions like the regional postal service or law enforcement agency, luring the targeted organization to open the attachment and download the ransomware.

In Luxembourg, the Computer Incident Response Center Luxembourg (CIRCL) receives four to five reports of ransomware infections per week. CIRCL has stated, based on its operating Malware Information Sharing Platform (MISP), that Locky and TeslaCrypt[2] ransomware are the evolving ransomware varieties targeting the Grand Duchy right now.

1 Symantec - Ransomware and Businesses 2016

2 In May 2016, the developers of TeslaCrypt released the master decryption key and shut down the ransomware, thus ending the ransomware

A very attractive business model

Ransomware is considered to be a major and exponentially growing threat in 2016, based increasingly on anonymizing payment methods (e.g., Bitcoin digital currency) and anonymous networks (e.g., Tor anonymity network).[3] The Cyber Threat Alliance estimates that the group behind the CryptoWall ransomware attacks caused US$325 million in damages, after infecting hundreds of thousands of computers across the world.[4]

The popularity of ransomware attack is growing continuously. The FBI has reported a 33 percent increase in the number of complaints filed involving ransomware.[5]

- In 2014, over 1,800 complaints were filed
- In 2015, more than 2,400 complaints were filed, with a reported loss of more than US$24 million
- In the first quarter of 2016, US$209 million was paid to ransomware criminals

The popularity of ransomware among cybercriminals can be attributed to three main advantages:

- It is a low-maintenance operation for threat actors, and tools have become more advanced and much cheaper.
- It provides the opportunity to target on a wide scale, allowing a higher return on investment.
- It offers a quick path to monetization, since the users pay adversaries directly in cryptocurrencies. Furthermore, the relatively low initial ransom cost (if compared to the high value of victim's data) complemented by the gradual increase scheme (the sooner you pay, the cheaper it is), is a strong incentive for victims to pay the ransom.

In other words, the return on investment is faster than with most types of malware because there is no middleman involved, and there is no need to resell anything such as personal data; it's a cash deal only. The simplicity of the business model is a compelling attraction for the criminal elements.

3 McAfee Labs - 2016 Threats Predictions. URL: http://www.mcafee.com/us/resources/misc/infographic-threats-predictions-2016.pdf

4 Cyber Threat Alliance: Lucrative Ransomware Attacks - Analysis of the CryptoWall version 3 Threat.: URL: http://cyberthreatalliance.org/cryptowall-report.pdf

5 FBI - Ransomware: Latest Cyber Extortion Tool, April 26, 2016. URL: https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool

Anatomy of a ransomware attack and delivery models

A ransomware attack is a multi-step process. If the proper defenses are in place at the various steps of the attack, the impact can be greatly reduced.

Figure 2 - Anatomy of a ransomware attack

As illustrated in Figure 2 above, the initial step in a ransomware attack is to deliver the ransomware—or in other words, infecting the victim. The most common delivery methods are:

- **Phishing:** Nearly all phishing emails now contain ransomware. Phishing consists of a fraudulent email that appears to be from an official source, such as a supervisor, bank, or partner organization. The email includes an attachment that, once downloaded, infects the target computer. Once embedded in the computer, the malware typically spreads itself across the network. A recent wave of ransomware phishing emails targeted HR teams since they often receive unsolicited email from job applicants.
- **Drive-by Download:** A drive-by download occurs when compromised software or a website "pushes" a download to a target computer without the user's consent. This kind of attack has become less common over the years as more web browsers use proactive security to prevent unauthorized downloads and alert users. That said, it remains important to maintain up-to-date versions of your web browsers and other critical software. Organizations should have patch management in place to quickly apply security fixes.
- **Corrupted Software:** Software should only be downloaded directly from the home page of known software vendors. Although some legitimate free software sites do exist, even these tend to include unwanted commercial "bloatware" that may serve ads or change your browser settings without consent. Those changes in turn can make it more likely that you will be exposed to compromised websites. Free software on unknown sites is often a "Trojan", disguising malware or other viruses.

Demand ransom

Users attempt to access files and are alerted that the data has been encrypted

Decrypt

Decryption keys will eventually be provided upon payment of a ransom

- **Malvertising:** Malvertising is any form of advertising intended to spread malware through the internet. This often happens when legitimate advertising is compromised by a malware. Illegitimate ads created by hackers can spread malware directly using malicious scripts, causing "drive-by downloads". They might entice users to click the fake ad and potentially download ransomware. Most malvertising can be prevented through common ad blocking software.

- **Social Engineering and Self-Propagation:** Social engineering can take place in two ways. Some ransomware passes itself off as a "fine" from a government agency, which can confuse the end user and make them take actions that spread the infection. Once a computer is infected, the other form of social engineering takes place: The infected user's email contacts and other data are used to spread the infection to other users. The new group of targets unthinkingly accesses the message, believing it to be from their colleague—a prime example of self-propagation.

The new trends of ransomware

The first versions of ransomware were basic, and often used poor encryption, making it relatively simple to recover encrypted files. However, the threat agents behind ransomware are continuously learning from their mistakes, and have become more sophisticated in their latest variants. According to the latest cyber threat reports, the ransomware threat landscape is evolving in the following ways:

- Ransomware has primarily plagued Windows platforms. Recent platform-agnostic capabilities have been developed and targets have expanded to other operating systems (such as Linux, Android, OS X, etc.)
- More data extortion techniques. At the end of 2015, a Chimera crypto-ransomware was discovered with three disturbing capabilities: (i) encrypting files, (ii) doxing, and (iii) extortion. After encrypting files, if the ransom is not paid, attackers claim to make those files public over the internet. This trick, in most cases, pressures the victim into paying the ransom, despite having a data backup.
- Increased adoption of IP address anonymizing services for ransomware delivery (e.g., Tor anonymity network). These services can complicate the profiling of the threat actor behind a ransomware campaign.
- Increased adoption of cryptographic key provisioning. This process ensures unbreakable cryptographic communication between hosts. When cryptography is implemented correctly, the encrypted files are impossible to recover without a key.
- Wide variety of technical sophistication. Some types of ransomware depend on links to third party libraries, making them easy to detect. However, other types of ransomware use different techniques (e.g., thread injection, process replacement, etc.) to avoid detection. For instance, CTB-Locker uses more advanced techniques (e.g., position-independent code wrapper) that make it almost impossible to detect using traditional signature-based methods.
- "Ransomware as a Service" or RaaS. This is an evolution discovered in mid-2015, in which the creation of ransomware has been commoditized, allowing attackers to develop and distribute customized ransomware. This also gives uninitiated cybercriminals a foothold in ransomware business.
- Ransomware uses every possible attack vector to get into victims' machines. In some ransomware versions, complex obfuscation and covert launch techniques are used. These allow them to evade detection in the early stages of infection. In addition, cybercriminals are seeding legitimate websites with malicious code to distribute ransomware.
- Exponential deletion. Increased use of time-based motivation techniques, in an effort to maximize criminal actors' revenues (e.g., encrypted files are gradually deleted permanently).

The popularity of ransomware attack is growing continuously. The FBI has reported a 33 percent increase in the number of complaints filed involving ransomware.

Protect your business and your intellectual property from ransomware

Ransomware is not new to the world of crime-ware. However, newer more sophisticated methods of delivery, detection, and monetarization, means ransomware continues to be a highly profitable business for cybercriminals. Ransomware promises to be more threatening, and organizations should be proactive in developing and maintaining their readiness and resilience against it. Although the initial cost may be perceived as high, investing in cybersecurity can pay huge dividends in the long term.

The following preventive and detective controls can help your organization be prepared for ransomware threats:

- Implement an effective backup and recovery strategy (offline backups, storage in a secure/separate location, retain backups at multiple points in time, etc.)
- Develop awareness programs for your users
- Implement robust vulnerability and patch management processes
- Manage the use of privileged accounts and configure access controls correctly
- Consider recourse to whitelist filtering to prevent execution of unknown programs
- Implement content filtering to filter out emails and web content
- Harden the security configuration of your devices (including mobile devices)
- Assess the readiness of your IT infrastructure and incident response processes by performing ransomware attack simulations