Ransom where?
Holding data hostage with ransomware
May 2019
With the evolution of digitization and increased interconnectivity, the cyberthreat landscape has transformed from merely a security and privacy concern to a danger much more insidious by nature — ransomware. Ransomware is a type of malware that is designed to encrypt, destroy or shut down networks in exchange for a paid ransom. Through the deployment of ransomware, cybercriminals are no longer just seeking to steal credit card information and other sensitive personally identifiable information (PII). Instead, they have upped their games to manipulate organizations into paying large sums of money in exchange for the safe release of their data and control of their systems. While there are some business sectors in which the presence of this cyberexposure is overt, cybercriminals are broadening their scopes of potential victims to include targets of opportunity\(^1\) across a multitude of industries.

This paper will provide insight into how ransomware evolved as a cyberextortion instrument, identify notorious strains and explain how companies can protect themselves.

\(^1\) WIRED. “Meet LockerGoga, the Ransomware Crippling Industrial Firms” March 25, 2019; https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/
A brief history of ransomware

The first signs of ransomware appeared in 1989 in the healthcare industry. An attacker used infected floppy disks to encrypt computer files, claiming that the user was in “breach of a licensing agreement,” and demanded $189 for a decryption key. While the attempt to extort was unsuccessful, this attack became commonly known as PC Cyborg and set the archetype in motion for future attacks. Over the next few years, ransomware attacks were present but not yet a significant problem because cybercriminals were missing three key elements:

1. A clear strategy to either unencrypt or destroy the files and data they demanded money for.

2. The ability to communicate anonymously.

3. An untraceable method for the victim to pay the ransom.

With those limitations, cybercriminals settled for leveraging exploitable vulnerabilities in software and human error to install malware onto devices through anti-virus scams to steal sensitive credentials and personal information to sell for profit. Then in 2006, the Archiveus Trojan changed the realm of ransomware. When downloaded, it encrypted all files found in the “My Documents” folder of the user’s computer. To regain access to these files, victims were directed to specific websites to make purchases, thus paying the ransom.

The introduction of bitcoin in 2008 was a significant turning point in the world of cyberextortion. This new digital currency enabled cybercriminals to carry out attacks and receive virtually untraceable ransom payments. Now cybercriminals had the freedom to get creative with their attacks and up the ante. After several iterations of ransomware strains, CTB-Locker or CryptoLocker in 2013 fulfilled the other two missing elements. Cybercriminals could now execute powerful ransomware extortion plots. The CTB stands for “Curve, TOR and Bitcoin,” which provided “fast secure encryption of file content, a means for anonymous communication through ‘The Onion Routing’ (TOR) protocol, and bitcoin enabled secure, untraceable crypto-cash transactions.”

With organizations’ and supply chains’ increased reliance on networks and connected devices, the scale and effect that a ransomware attack poses can elevate any organization to the level of a potential target.

---


The prevalence of ransomware

The FBI launched the Internet Crime Complaint Center (IC3) to track cybercrime and ransomware attacks and provide information to people and organizations about how to protect themselves against these crimes. Since launching in 2000, IC3 has received reports of over 4 million cybercrime events, with cyberextortion on the rise. In 2018, ransomware attacks reported directly to the IC3 accounted for roughly $3.6 million in losses for the targeted organizations. While the financial loss reported may seem low, it is important to note that it is common for many organizations to pay ransoms and not report that they have fallen victim to ransomware attacks.

Ransomware attacks are becoming more aggressive as well. Cybercriminals are doubling and even tripling the demand if the ransom isn’t paid within the specified time frame. This method of cyberextortion has evolved into a multimillion-dollar enterprise for cybercriminals, with global ransomware costs expected to reach roughly $12 billion by the end of 2019 and $20 billion by 2021.

These attacks are increasing at such a fast pace that researchers at Cybersecurity Ventures predict that “a new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021.”

Source: Cybersecurity Ventures for global ransomware damage costs data.

What role does cyber insurance play?

Organizations need to have appropriate protection in place to guard against ransomware attacks. This extends further than implementing anti-virus, anti-malware software and backups to securing the longevity of the entity. Phishing scenarios are highly leveraged to initiate ransomware attacks and are commonly “designed to trick a user into providing Office 365 account credentials” to breach a system. These attacks go beyond demanding ransoms and often come with several damages and associated expenses, including:

“damage and destruction (or loss) of data, downtime, lost productivity, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hostage data and systems, reputational harm, and employee training in direct response to the ransomware attacks.”

Cyber insurance can reduce the likelihood of a company exhausting all of its resources to investigate and recover from an attack. In the event of a ransomware attack, cyber insurance would cover the ransom demand and extra expenses, including forensics and investigation, up to the specified cyber policy limit. The value that cyber insurance provides is demonstrated through the extensive core insuring agreements and enhancements available in the marketplace, such as:

- Network security liability.
- Privacy regulatory proceeding.
- Breach response costs.
- Cyberextortion reimbursement.
- Hardware replacement (bricking).
- Data recovery.
- Business interruption and extra expense.
- Dependent business interruption.
- Reputational harm.

Coverage enhancements like dependent business interruption offer coverage to companies for damages caused by third-party vendors because of a cyber event like ransomware. Lockton sees firsthand the value that cyber insurance affords our clients against damages and costs incurred due to ransomware attacks, like Ryuk and WannaCry, providing coverage for expenses reaching upward of $4.5 million cumulatively. Lockton has secured exclusive amendatory endorsements with many of the large cyber insurance carriers to ensure that our clients receive optimal coverage options.

Ransomware attacks come with hefty price tags and considerable business interruption. For the past 30 years, ransomware has adapted to defensive strategies time and time again, with cybercriminals exploiting numerous avenues to carry out attacks. From social engineering and phishing attempts to infected websites, the threat becomes more sophisticated by the minute. Its advancement is impacting a growing number of industries, shifting the likelihood of an attack from an “if” to a matter of “when.” Organizations should shift their focus from a recovery stance to a proactive one to develop the appropriate prevention and contingency plans.

---


---

Lockton Companies
## TIMELINE

**BIGGEST RANSOMWARE AND MALWARE ATTACKS TO DATE**

<table>
<thead>
<tr>
<th>DATE</th>
<th>STRAIN</th>
<th>EVENT</th>
<th>INDUSTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Reveton</td>
<td>Trojan that fraudulently claimed to be law enforcement and shut users out of their devices until the demand or “fine” was paid.</td>
<td>PUBLIC SECTOR — Metropolitan Police Service (London)</td>
</tr>
<tr>
<td>September 2013</td>
<td>CryptoLocker</td>
<td>Trojan used to target devices running Microsoft Windows, using the Gameover Zeus virus delivered through spam messages. The virus managed to infect roughly 500,000 computers around the world. Cybercriminals were able to extort roughly $1 million within a six-month period.</td>
<td>AEROSPACE AND DEFENSE — NASA GOVERNMENT — Health and Human Services</td>
</tr>
<tr>
<td>February 2015</td>
<td>TeslaCrypt</td>
<td>A CryptoLocker variant, notorious for infecting computer gamers, downloaded from an infected HTML webpage and not only encrypted the gamers’ data and ancillary files but also other files found on their devices in exchange for ransom. Extortion payments totaled roughly $76,522.</td>
<td>COMPUTER GAMING AND SOFTWARE</td>
</tr>
<tr>
<td>2015</td>
<td>SimpleLocker</td>
<td>Targeted Google Android OS device users to encrypt the SD cards under the guise that the user had committed a crime. The virus demanded payment in exchange for access to the user’s data as well as not reporting the user to the authorities.</td>
<td>COMMUNICATION SERVICES — Google</td>
</tr>
<tr>
<td>February 2016</td>
<td>Locky</td>
<td>A targeted attack that delivered malicious code through a phishing email with a Microsoft Word document or JavaScript attachment. Once downloaded, it aggressively attacked critical backup systems and files, thus making it more difficult for data recovery methods to be successful. The virus encrypted the entire system and demanded a ransom for the hospital’s computer files to be returned and regain access to systems.</td>
<td>HEALTHCARE — Hollywood Presbyterian Medical Center</td>
</tr>
<tr>
<td>November 2016</td>
<td>HDDCryptor</td>
<td>Encrypted the entire local and networked drives through modifying the master boot records (MBRs) of an entire transportation system. This left train station gates open and ticket machines out of order, even displaying messages that passengers could ride for free.</td>
<td>MUNICIPAL TRANSPORTATION — San Francisco Municipal Transportation Authority</td>
</tr>
</tbody>
</table>
| May 2017   | WannaCry     | Exploited a code developed by the NSA called EternalBlue and gaps in the Server Message Block (SMB) Protocol (used for printers, file sharing and remote access) patching for devices running Windows 7 OS. The ransomware was circulated via email, and once in the system, the virus encrypted files on the hard drive, preventing user access on that device and any other device connected to the network in exchange for ransom to be paid in bitcoin. This attack managed to hit more than 300,000 computers in total and is believed to have been linked to the Lazarus Group — with connections to the North Korean government. | HEALTHCARE — Britain’s National Health Service
AEROSPACE AND DEFENSE — Boeing
TELECOMMUNICATIONS — MegaFon in Russia
AIR FREIGHT AND LOGISTICS — FedEx
AUTOMOBILE MANUFACTURERS — Nissan, Renault
EDUCATION — Universities in China
PUBLIC SECTOR — Police Authorities in India, China
GOVERNMENT AGENCIES — Russian Interior Ministry
ELECTRONICS |
<table>
<thead>
<tr>
<th>DATE</th>
<th>STRAIN</th>
<th>EVENT</th>
<th>INDUSTRY</th>
</tr>
</thead>
</table>
| June 2017 | NotPetya* | An iteration of a previous version, Petya, that was released in March 2016 and encrypted the hard drive and data on the targeted computer running Windows OS. The virus displayed a message to the user explaining that they needed to pay a ransom to access their data. The virus was delivered through an attachment in an email under the guise of a résumé to get the user to click on it, open the PDF and agree to the subsequent Window User Access Control prompt. The virus got its name from the 1995 James Bond film, GoldenEye. NotPetya, a new, more powerful version of Petya, aimed to encrypt everything, not just the hard drive on the device. This virus spread without the assistance of spam or social engineering attempts. The virus overwrote the master boot record, successfully locking the users out of their devices. This is believed to be a targeted attack by Russia and is known as a “watering hole attack,” which infected a website used with a common accounting software used in the Ukraine in combination with EternalBlue. This attack is notable for the following reasons:  
  - Not only did it encrypt the entire device, but it destroyed the data and hardware as well, thus leaving the hardware “bricked.”  
  - While a ransom was demanded, there was no tangible way to pay the ransom.  
  - Biggest malware attack by impact. Total damages to date are estimated at $10 billion or more. |
| September 2017 | Bad Rabbit | Like NotPetya, this was considered a “watering hole attack” where the virus used a fake Adobe Flash installer update that downloaded from infected websites that users commonly visit. Once users launched the download, the virus locked the user out of the device and demanded that the ransom be paid within 40 hours. |
| January 2018 | SamSam    | Exploited vulnerabilities in the Remote Desktop Protocol (RDP) or Java-based File Transfer Protocol (FTP) servers on devices running Windows OS to gain access to the network and run malware on the system. This strain encrypted systems and files and demanded a ransom to regain access to patient files, warrants and pending court cases. Essentially, the criminals behind SamSam purchased credentials off the darknet to gain access to systems through RDP or FTP. This ransomware attack has managed to collect roughly $850,000 in extortion payments and created damages expected to exceed $30 million. |

**TRANSPORTATION AND LOGISTICS** — Maersk  
**PHARMACEUTICALS** — Merck  
**CONSTRUCTION** — Saint-Gobain  
**FOOD PRODUCTS** — Mondelez International, Inc.  
**AIR FREIGHT AND LOGISTICS** — TNT Express (FedEx)  
**NUCLEAR ENERGY** — Chernobyl Nuclear Power Plant  
**MANUFACTURING**  
**PROFESSIONAL SERVICES**  

**MEDIA OUTLETS** — Interfax News Agency (Russia)  
**HEALTHCARE** — Allied Physicians of Michiana, Hancock Health, Allscripts Healthcare Solutions  
**MUNICIPALITIES** — City of Atlanta
August 2018  Ryuk  Tailored attack primarily in the United States, unique because of how it was deployed. Cybercriminals sat within the network of organizations for as long as a year to gather the information necessary to execute their attack. The virus used the Emotet and Trickbot Trojans to deliver the malware through a phishing email. This email contained a Microsoft Office document attached that contained malicious code. Once opened, the code executed and downloaded the Emotet Trojan. This Trojan spread throughout the network and downloaded the Trickbot Trojan, which attacked the memory and stole credentials.

This virus strain encrypted the network drives, wiped shadow copies on the endpoint and disabled the Windows System Restore option for the end user. This attack is notable for the highest ransom demand in history in the amount of $145,000 in bitcoin, approximately $700 million in USD. More victims are being discovered as information about this strain develops.

The actors behind the attack have garnered roughly $4 million in ransom payments.

January 2019  LockerGoga  While information on how the virus has spread is still developing, this strain encrypted all devices on the network, disconnected them, changed user and admin passwords, and locked down the devices. The virus attacked the Windows Boot Manager, responsible for starting the device’s operating system, and has been used to halt manufacturing operations. With this strain, there is currently no known way of decrypting systems and files, and the variants “do not allow an infected system to function well enough for the victim to pay the ransom or use a decryption tool.” The full extent of the damage this strain has created is ongoing, but it has already created nearly $40 million in damages.

*This strain is not defined as ransomware and is instead identified as wipeware; however, this strain is notable for its scale and impact.

---

WHITE PAPER SOURCES


Hampton, Nikolai, and Zubair Baig. 2015. “Ransomware: Emergence of the Cyber-Extortion Menace.”


TIMELINE SOURCES


