CHUBB®

Cyber InFocus

October 2019

Adapting to the new realities of Cyber Risks

Malware cyber attacks, known as ransomware, rose at an alarming rate during the first half of 2019, bypassing the total number of ransomware claims Chubb saw in 2018. This statistic proves that the trend is continuing, as Chubb also saw an 84% increase in ransomware attacks from 2017 to 2018. With ransom demands growing, some in the six- to seven-figure range, it's more important than ever to understand their function, the increased sophistication in who they target, and how to protect your business, regardless of the industry.

Visit Chubb Cyber Index℠ to learn about data-driven trends.

> "Chubb also saw an **84%** increase in ransomware attacks from 2017 to 2018."

What is ransomware and why is it such a problem?

What it is.

Ransomware is a type of malicious software that typically encrypts a victim's data or network accessibility to data so that the victim can't use it for their ongoing business and operational functions. To decrypt the data or environment, the bad actor usually makes a ransom demand in the form of a cryptocurrency, such as bitcoin, in exchange for a decryption tool.

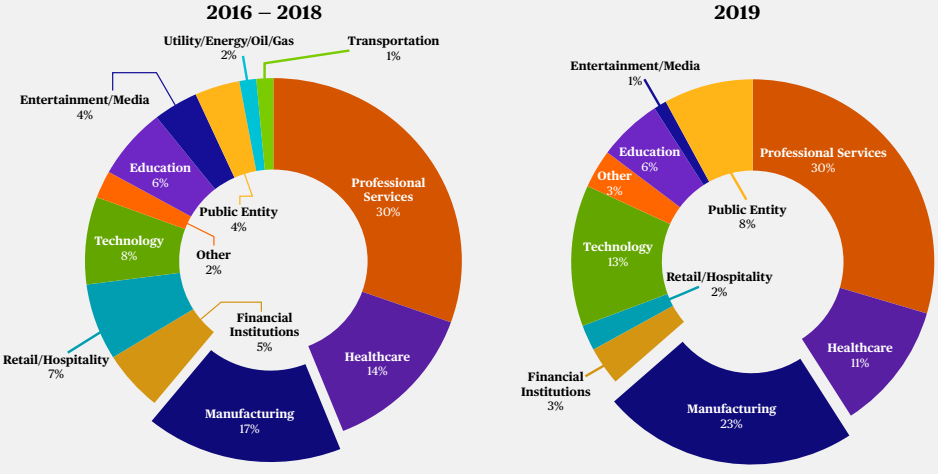
How it works.

Ransomware attacks are typically carried out through email phishing. Malware is deployed into a victim's computer system through a malicious attachment or embedded link within an email. Once deployed, the ransomware moves quickly throughout the computer system, identifying key system components and data files, including any available backup files on the computer system, and encrypting those files to prevent access and cause business disruption.

Business interruption loss trend

Because ransomware encrypts data and can render a company's systems inoperable, the victim may have to consider paying the ransom to recover their data and restore business operations. This scenario is leading to a significant increase in both cyber extortion and business interruption losses.

Ransomware – Industry%



Industries Affected by Ransomware

Ransomware can affect any company or public entity, regardless of size or industry. However, the industries we see affected the most are manufacturing and professional services.

- Manufacturers are likely targets of ransomware attacks because they have more incentive to pay the ransom to restore operations quickly.
- Professional service firms are often affected because they are an email based business with more opportunities to click on malicious links.

Bad actors are becoming more sophisticated with targeted ransomware strains.

Bitpaymer & Ryuk

Ryuk accounts for 50% of known variants we have seen in 2019.

Bitpaymer and Ryuk are two strains of ransomware that have been impacting computer systems since 2018. Unlike earlier variants, these attacks are not random, but target victims that have the financial ability to pay higher ransoms, generally in the six- to seven-figure range.

How they work.

A "banking Trojan" type of malware, like TrickBot or Emotet, infiltrates the victim's system through an open remote desktop protocol (RDP) access point or a phishing email. The malware then allows the bad actor to see sensitive information in the victim's system such as financial statements, which demonstrate the victim's ability to pay the ransom.

Sodinokibi: Evolution in Ransomware

What it is.

Sodinokibi appears to be the evolution of Bitpaymer and Ryuk and emerged in April/May 2019. Like the earlier variants of ransomware, Sodinokibi specifically targets its victims and demands larger-than-average ransoms.

How it works.

Sodinokibi is unique in that it targets Managed Service Providers (MSPs), which provide IT services to various other organizations.

This type of ransomware infects its victims through mass phishing campaigns with malicious links or attachments, open remote desktop protocols, as well as using compromised system credentials. Once inside the MSP's system, the bad actor drops the malware into the victim's network infrastructure, infecting its customers' systems as well.

Chubb Insight – What can be done?

Detecting phishing emails

Bad actors are continuously changing their attack techniques and increasing the complexity of the ransomware to cause as much disruption as possible. Thus, it is imperative that all entities implement multiple layers of preventative measures to mitigate the potential of future incidents and have a business continuity plan in place in the event the organization is affected by a ransomware attack.

Some useful best practices include:

Keep your backup process consistent and up-to-date.

A majority of ransomware attacks can be traced back to email phishing where login credentials are compromised or a malicious link is clicked. Therefore, it is vital that employees are trained on how to detect phishing emails and why it's so important to never click on a link or attachment they do not recognize.

Useful detection tools

Computer system backups can be used to recover data after a ransomware attack and avoid the payment of a ransom demand. However, if backups are outdated, not properly labeled, or the backup practice is inconsistent across the systems, the backups may not be useful.

Make sure there is a consistent backup process in place across all systems, that all backups are properly labeled (segregate labels to avoid encryption), and that no matter what form of backup is used, it is segregated from the main system to avoid deletion or encryption by the bad actor.

Because bad actors are becoming more sophisticated and able to bypass traditional antivirus software, next-generation antivirus (NGAV) protection, which includes endpoint detection and response, can be a useful tool to detect credential-stealing banking Trojans, which are often a precursor to Ryuk and BitPaymer ransomware.

To learn more about cyber trends, please visit www.chubb.com/cyber