Understanding Ransomware Trends

Ransomware Attack Methods Alter as Threat Actors Grow in Sophistication

CyberCube

www.cybcube.com
The ransomware threat has evolved significantly over the past few years, as attackers grow in confidence and explore different approaches.

Since WannaCry in 2017, the sophistication of cyber threat actors has dramatically increased and ransomware attacks will continue to proliferate. Analysis of ransomware activity over the last three years shows some clear trends. These include:

- Specific target sectors are emerging. These include entities engaged in public services such as municipalities, schools and healthcare providers.

- A range of more advanced ransomware campaigns have been developed, where data is exfiltrated before being encrypted on the target organization’s network, such as the Maze ransomware strain.

- Perpetrators have published this confidential information when their demands were not met. This has led to dramatic consequences, potentially leading to the need for crisis communications and may result in regulatory penalties.

- The nature of attacks is changing, with more focus on enterprises (rather than individual consumers), larger payment demands and more targeted approaches deployed. The aggression of the attackers and the value of the impact on businesses is also more pronounced.

The emergence of Ransomware as a Service (RaaS) is enabling scaling of ransomware services through the dark web, empowering new users to deploy these resources. This has led to the emergence of a supply chain of ransomware developers who earn a proportion of the ransoms charged by the perpetrators actually delivering the attacks.

- Socially-engineered email and social media attacks will often rely on topical events (such as the recent Coronavirus outbreak) to fool unsuspecting recipients into clicking on links or attachments that trigger a ransomware attack.

CyberCube has researched ransomware attacks over the past few years to evaluate the changing behaviour pattern of threat actors. This reflects factors such as the vast amounts of data collected, the obligation to disclose an attack and governments’ limited resources for defence systems against cyber attacks. The sources of financial loss include the cost of paying the ransomware itself, legal and related forensic investigation costs, as well as the clean-up and potential rebuild costs in the event that the decryption keys are not effective to regain access to the encrypted files. The financial cost is only one aspect of the impact of ransomware - the disruption to services and operations can be very significant, and it can take weeks or months to fully recover.

Government organizations are key targets for ransomware attacks including schools, libraries and courts. One of the biggest cyber attacks to make headlines in 2019 featured the Baltimore City government. The city’s computer system was hit with a ransomware infection in May 2019 that crippled the government for more than a month.
Estimates put the recovery cost at over $18 million dollars, although the cybercriminal behind the malware demanded $75,000 worth of Bitcoin. The attack reportedly impacted vaccine production, ATMs, airports and hospitals.

Attacker are increasingly focused on targets that provide valuable or commercial services, for example, healthcare, utilities and services providers. In late November 2019, it emerged Allied Universal, a facility services company offering security systems, janitorial services, and staffing, had become infected with Maze ransomware. The attackers demanded a ransom of 300 bitcoins (~$2.3 million at the time).

Criminals are starting to realize that ransom demands of millions of dollars are achievable when the target becomes “the corporation”, rather than “the consumer”. Historically, ransom demands were seen in the $200-1,000 range (a price that many individuals are able to pay).

This trend towards “Enterprise Ransomware” is seen clearly in statistics published last year. According to Symantec, 69% of the ransomware attacks seen in 2016 were focused on the consumer. In 2018, this number was only 19% (with the remaining 81% of attacks detected being focused on corporations. Most consumers now spend the majority of their “IT time” on mobile devices with their critical files backed up automatically to the cloud, and their data tends to be of somewhat limited value (e.g. credit cards can be changed). Corporations, on the other hand, still rely heavily on Microsoft Windows (a much more vulnerable attack surface than an iPhone, for example). In addition, businesses stand to lose more, including (but not limited to) intellectual property, customer data and larger sums of money.

The New Kids on the Block

Today, a proliferating range of ransomware exploits have been developed. Some of the major ransomware participants are BitPaymer, Cerber, CryptoLocker, CryptoMix, CryptoWall, Dharma, GandCrab, Global 3, hAnt, HDDCryptor, Hermes, iEncrypt, LeChiffre, LockCrypt, Matrix, Maze, Megacode, Nymain, PewCrypt, RobinHood, Ryuk, SamSam, Scarab, SODINOKIBI and TeslaCrypt.

The past year has shown that the lion’s share of this “market” is divided into two main approaches:

- The “big-game hunting” camp consists of sophisticated actors who develop and deploy their own ransomware, as has been observed with the Ryuk ransomware, whose continued fame lies in their strategy - performing highly-targeted attacks (i.e. select and infect targets likely to pay) with high ransom demands.

- In the Ransomware-as-a-Service (RaaS) “business model”, a number of affiliates are in charge of deploying the ransomware on victim networks. If payment is submitted, a portion of this payment goes to the ransomware developers with the rest being paid out to the affiliate. This specialization allows sophisticated ransomware developers to focus on developing the malware while offloading the work (and risk) of finding and infecting targets to others (who may also be more specialized in this type of work).

The big-game hunting method targets very prominent victims that have resources and stand a lot to lose from these attacks. This may cause fewer infections but is offset with larger payouts.
The RaaS approach demonstrates ransomware has become more than a cottage industry with ransomware developers and hackers teaming up to attack companies and then divide the spoils. The focus of some new groups of software developers is not about developing ransomware with a view to distributing it themselves, which has risk attached, but to sell it to third parties for specific targets. Such services can be sold on the dark web where other third parties are deploying it on a target. Once that service becomes more readily available, it does not take a highly sophisticated user to use these resources.

In both big-game hunting and RaaS, the victim faces pressure to submit payment, which could be due to a number of factors such as the high costs of response and remediation, the victim’s industry, function and urgency to be back online, or to prevent loss of critical documents.

Many ransomware victims feel pressurised to pay as it is perceived to be the quickest and least expensive way for business to return to usual. Certain industries, which provide critical infrastructure to many physical locations that are dependent on them, place a premium on their ability to get back to business as usual.

There is risk associated with simply paying the ransom immediately as there are cases where the decryption keys have not fully restored the files to the state prior to the attack. The case of National Ink and Stitch is an interesting one, as after suffering a ransomware attack in December 2016, the initial ransom was paid. An additional ransom was then demanded, which the company refused to pay and brought in computer experts to restore their systems. It was subsequently determined that remnants of ransomware were still in the system, causing slower computing performance and ongoing financial costs.

An Evolving Business Model

As entire industries move to mitigate the potential effects of a ransomware attack by boosting defences and increasingly backing up data in multiple secure locations, cybercriminals have turned to other ways to pressure victims into payment, namely by threatening to leak, or actually leaking a downloaded copy of victims’ files.

Attackers engaging in data theft aim to increase pressure on the ransom target to pay. The scaling of this approach is very dramatic and can increase corporate costs. This can include crisis communications consequences for a company that has been attacked and has potential legal liability associated with it, as well as regulatory implications for anyone holding personally identifiable information either in the US under data breach notification laws, or under the European General Data Protection Regulation (GDPR).
An Evolving Business Model (contd.)

Organizations following the new laws introduced in 2018 must be aware of the added impact it poses in the event of an attack.

Threat actor groups are conducting campaigns and adjusting their business models to extract greater value from a smaller number of incidents. More recently, some very sophisticated and aggressive organized criminal groups conducted carefully-targeted ransomware attacks, which is a move away from the traditional high volume low-value method approach.

The employment of a more specific approach is particularly significant for large corporate businesses as ransomware groups study fresh potential targets to assess vulnerabilities. Their goal is also to design attacks targeting supply chains that extract much higher ransoms more efficiently.

With WannaCry, the typical ransom was more than $1,000 per customer while for Travelex it reached $6 million (see panel From WannaCry to Travelex). Given the numerous conversations, negotiations, delays, threats, counter-threats and amounts of money to be transferred, targeted attacks potentially yield a higher return for the ransomware criminal. Targeted attacks are more likely to have a higher success rate in the same way that more personalised methods employed in modern marketing techniques tend to be more effective than a traditional “billboard” approach.

From WannaCry to Travelex
From WannaCry to Travelex

The WannaCry attack of 2017 marked the first time the term “ransomware” entered the public’s consciousness and lexicon. WannaCry had a major impact on the UK’s National Health Service (NHS) as well as other institutions and public entities, causing widespread disruption that received attention from both traditional and social media platforms.

WannaCry was a scattergun attack that did not target any specific entity or individual. The primary source of financial gain was a lot of small-dollar amounts from exploiting downtime and systems recovery vulnerabilities. It combined the payload of ransomware with the self-replicating nature of a virus to spread rapidly throughout and between organizations.

Roll forward to today and the problems experienced by foreign exchange company Travelex are just a foretaste of future cyber crime. In late December 2019, Travelex announced it faced an attack which shut down its website and its foreign exchange ordering services for more than two weeks. The attack was notable for two distinctive features. The first was the scale of ambition shown by the attackers who demanded a $6 million payment - a significant increase compared to past ransomware campaigns. This is likely to be an indicator of the increased aggression of actors, particularly against large organizations going forward. It should be noted that there is no evidence the ransom was paid, particularly in light of the length and cost of disruption which followed.

The second aspect of note was the depth of business interruption that Travelex suffered. All of the company’s operations around the globe were impacted, as well as other financial services companies such as Sainsbury’s Bank, Virgin Money and First Direct, owned by HSBC. Travelex has estimated its first-quarter underlying core earnings will be hit by £25 million ($32 million).
Technique & Motivations

A huge percentage of ransomware attacks to date have relied on the delivery of malicious code through email attachments and embedded URL links. Training users to be appropriately cautious about email attachments can have a profound effect on attack success rates.

Criminals have also learned to “live off of the land” in their attack strategies. Use of tools that many of us have on our computer systems and that we use every day such as email, spreadsheets and basic programming applications (such as Microsoft’s Powershell) can now be used against us. This saves the criminal time and money (as there is no need to develop new tools) and makes attacks extremely hard to detect through traditional “anti-virus” (signature-based) methods.

Some Predictions

CyberCube predicts that ransomware and, in particular, “Enterprise Ransomware” is here to stay and likely to grow as an attack vector. In 2020 and 2021, it is expected that:

1. Ransom demands will be calibrated with company performance, data assets and other measurables.
2. Criteria for targets will get interesting. Expect to see the “reconnaissance” phase of a ransomware attack to target individuals in senior positions of authority, particularly those who have access to company bank accounts.
3. Social engineering will be powered by Artificial Intelligence (AI) at scale.

Criminals will construct algorithms that will be extremely powerful in the context of hunting for individual targets and deciding “which buttons to press” to make these targets act in a manner that suits the criminal. Criminals are good at social engineering, AI will be much better.

The Role of the Insurance Industry

After an attack takes place, businesses can use a SWOT approach to understand what happened, whether systems can be renewed, what backups are in place, and how quickly they can be restored. This is a retrospective analysis using Strengths, Weaknesses, Opportunities and Threats of the situation to learn lessons from the experience. From an insurance perspective, cyber policies typically include business interruption costs, forensics expenses, legal liability, data breach notification costs, the costs of technology to replace software, the compensation of the ransom itself, regulatory fines in a particular jurisdiction (where insurable) and investigative costs.
Insurers are assessing how the ransomware threat is evolving. Taking a forward-looking view of risk can help insurers to anticipate how attackers are evolving their techniques in order to create widespread impact. CyberCube is investing in research and development to understand how threats are evolving and what that means for large-scale attacks in particular. The potential for systemic risks to occur from common vulnerabilities drives the need for constant awareness of how the threat is evolving.

Harnessing a wide array of data and expertise can help insurers reduce the uncertainty exposed to these very large and very complex risk exposures. This helps insurers not only reduce their uncertainty but creates a more sustainable basis for innovating and creating new solutions to cyber risk.

The amount of ransomware cases that have been paid and make the public domain is only the tip of the iceberg - many incidents are only reported if they involve sensitive proprietary information and reputational damage. Incidents that tend to be reported are under SEC disclosure, such as in healthcare, and those with government reporting structures. However, calls for greater transparency are likely to grow across both the public and private sectors.

The evolution of ransomware tactics that target the enterprise and the emergence of more sophisticated groups means that this type of cyber risk is (or will rapidly become) a strategic issue for every business. CyberCube expects the nature of ransomware to continue to develop and play an important part in the tool kit for cyber attackers. It offers the potential for systemic and high severity risk of many types including Business Interruption, Contingent Business Interruption, Financial Loss, Regulatory Penalties and more. CyberCube is proud to be bringing expertise, data and tools to the fight to help insurers take an active role in protecting business from this element of the digital threat landscape.
Authors
Darren Thomson, Head of Cyber Security Strategy
Oli Brew, Head of Client Services
Yvette Essen, Head of Research & Communications

United States
CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108
Email: info@cybcube.com

United Kingdom
CyberCube Analytics
51 Eastcheap
1st Floor
London EC3M 1JP

Estonia
CyberCube Analytics
Metro Plaza
Viru Väljak 2
3rd floor
10111 Tallinn

www.cybcube.com