THE RAPID EVOLUTION OF THE RANSOMWARE INDUSTRY

By Patrick Vibert, Senior Consultant, Cyber Threat Intelligence, Control Risks.

The ransomware industry is exploding. For cybercriminals, it's profitable, low-risk, and easily accessible. For CEOs, it's a nightmare that conjures images of down networks, lost productivity, bad press and angry calls from board members. Every day there seems to be a story of a new ransomware victim or variant. Hardly a week goes by without hearing about a new attack from an affected client, or from someone in our personal lives who has become infected by this weapon of mass extortion.

Ransomware is a type of malware that blocks a user's access to their data or programs until a ransom payment is made to cybercriminals. Control Risks, Dell, Symantec, and Forcepoint all rank ransomware among their top cyber threats for 2016.[1] [2] [3] [4] In May, the US Computer Emergency Readiness Team (US-CERT) and the Canadian Cyber Incident Response Centre (CIRCC) released a joint warning on the increasing danger of ransomware to businesses and individuals.[5] Further, in Q1 of 2015 McAfee Labs saw a 165% increase in ransomware. Due to its prevalence and profitability, ransomware is becoming unavoidable.

As the title of this piece indicates, ransomware is an industry. Like any industry, there are profits, customers, and competitors. As a result, ransomware operators seek to maximise their return on investment (ROI), successfully engage their customers, and win market share. This paper will examine the rise of the ransomware industry through a business lens. It will also provide mitigation strategies, summarise major developments and look at where the threat might be going.

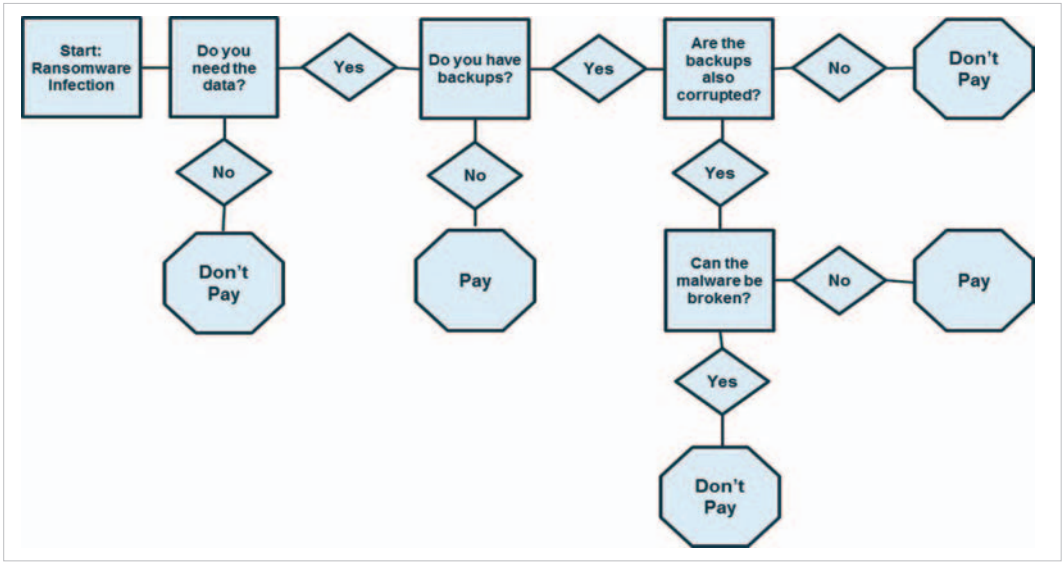

Figure 1.

BACKGROUND INFORMATION

Devices become infected with ransomware when a user unknowingly visits an infected website, or opens a malicious email attachment. Payment is typically demanded in Bitcoin, with ransoms ranging from $300-$500 for individuals and much higher for businesses and other organisations.

There are two main types of ransomware: locking and encrypting. Locking ransomware simply blocks access to files and applications, while encrypting ransomware applies a cipher algorithm to scramble the data, making it unusable without the decryption key.

Once a device is infected, a message appears instructing the user to make a payment for the release of their data. At this point, the panicked user enters the following painful decision-making process (see Figure 1).

Sometimes a victim will have a data backup system, only to find that it hasn't been updated in over a year or, worse, is also corrupted with ransomware. As a result, the key to mitigating this threat is to have current, secure backups that are updated regularly, but are not persistently attached to the network where they could become infected.

Many of today's ransomware operators are likely the same people behind the pharma spam epidemic of the early 2000s, when spammers clogged email inboxes with pharmaceutical offers.[6] These (mostly former Soviet) cybercriminals were experts at spamming and social engineering, which are two important skills for the large phishing campaigns that are critical to successful ransomware operations.

To combat the pharma spam menace, law enforcement officials targeted so-called bulletproof hosting services, dodgy pharmaceutical suppliers and worldwide payment processing systems. But the rise of Bitcoin and Tor makes that almost impossible. There is now no way to stop the flow of money, and it is very difficult to identify where illicit services are hosted to shut them down.

NOTABLE RANSOMWARE CASES

In 2014, cybercriminals attempted to extort the city of Detroit for $800,000. City officials deemed the files non-critical and refused to pay.[7]

Police departments also appear to be attractive targets for ransomware operations, with police in Illinois, Maine, Massachusetts and Tennessee all

falling victim over the last two years.[8] In 2015, local police departments in Illinois and Massachusetts were forced to pay ransoms when their data was taken over by CryptoLocker and Cryptoware respectively (the police department in Massachusetts had assistance from the FBI, Department of Homeland Security, and two separate cyber security consulting companies).[9] In both cases, the backups were corrupted as well.[10]

This year, a South Carolina school district paid $10,000 in Bitcoin to regain access to their servers after they were infected with ransomware.[11] Meanwhile, an exemplary school district in New Jersey declined to pay their cyber extortionists after becoming infected with ransomware, as they were able to restore their servers from backups.[12] These two cases illustrate the importance of maintaining secure, offline backups.

Also this year, we have seen several high-profile ransomware attacks on medical centres.[13] No loss of life was reported as a result of the attacks, but the targeting of such a critical industry resonated with the public. The stories were widely reported in the press, and politicians began speaking out against the attacks. However, as ransomware-as-a-service (RaaS) increases, more people will be able to engage in ransomware operations and it is only a matter of time until serious real-world consequences occur from a ransomware infection.

THE RANSOMWARE INDUSTRY

As Control Risks has pointed out in the past, the cybercrime sector evolves in a similar manner to legitimate industries. It is a business driven by economics; operators are profit-driven and face stiff competition. As such, we've seen cybercriminals diversify their operations, segment their target markets and improve their customer service to win more business.

Payment is usually demanded in Bitcoin, which most people have never used. As a result, cyber extortionists provide explicit step-by-step instructions to guide victims through the process, with one operation even offering a live-chat option.[14] Cyber extortionists tend to view their victims almost as customers, so the better customer service provided, the more likely their victims are to pay the ransoms.

Ransomware operations are highly profitable. A 2015 report by IT security company Trustwave estimated a

1,425% return on investment (ROI) for ransomware operations.[15] With the average ransom demand hovering around $300-$500 it doesn't take much to break even. Profitability relies on the number of people willing to pay ransoms, and pay they do – particularly in wealthier Western countries, where victims are far more likely to send criminals money to regain access to their data.

A recent survey by Romanian security company Bitdefender found 33% of German ransomware victims paid attackers to recover their data, compared with 44% in the UK and 50% in the US.[16] McAfee puts the worldwide figure much lower, with about 7% of victims paying.[17] The true rate of payment is probably somewhere in the middle, but in any case it's easy to understand why ransomware operations are so attractive to cybercriminals.

The rapid evolution of ransomware operations indicates an increasing level of innovation by cybercriminals keen to find new ways to profit from these attacks. To this end, the ransomware-as-a-Service (RaaS) market began to emerge in 2015, with multiple variants issued for sale in cybercriminal forums. The decreasing cost of deploying ransomware attacks will likely lead to an expanding selection of targets, as cybercriminals diversify their operations to increase their likelihood of success.

As the ransomware market matures, it will likely continue to segment. Along with widespread 'spray and pray' attacks aimed at infecting as many devices as possible, we should see an increase in more focused attacks. To achieve this goal, attackers will need to research individual victims to identify vulnerable targets with higher potential ROI.

RANSOMWARE-AS-A-SERVICE

Although the frequency of attacks has exploded over the last three years, ransomware has been around for over a decade, mostly targeting developed nations where businesses and individuals are more likely to pay higher ransoms.

While targeting has changed and the level of sophistication has increased, the biggest recent development is the emergence of ransomware-as-a-service (RaaS). Sold on dark web cybercriminal forums, RaaS attacks are customisable, offering the capability to select targets and set ransom terms. This

enables cybercriminals who do not have the requisite skills to develop their own ransomware operations tailored to their needs.

MITIGATION

While ransomware attacks are increasing in sophistication that does not mean victims are powerless. This section describes steps that people and organisations can take to mitigate the threat, starting with securely backing up your critical data.

If the data is not securely backed up, ransomware victims are generally given two choices: pay the ransom, or lose your data. However, there are rare cases where the ransomware's encryption keys have been broken. In 2014, the encryption of the infamous Cryptolocker malware was broken by security researchers, who provided decryption keys to many relieved victims.[18] More recently, the Petya ransomware, which encrypts a computer's boot record (rendering the device useless), was broken by a security researcher who developed applications that could crack the malware password and retrieve the decryption keys.[19]

Still, assuming a solution will be available in the event of an infection is a very risky bet. Aside from not getting infected in the first place, your best course of action is to have your data securely backed up. In addition, companies are advised to use application whitelisting, to update all software patches and antivirus definitions, and to restrict users' network access and ability to install unwanted (potentially malicious) programs. These are the best methods to protect you against ransomware in its current state.

WHERE IS THE RANSOMWARE INDUSTRY HEADING?

The ransomware industry has evolved rapidly over the last three years. The combination of high profitability, low risk and low barriers to entry will likely cause a growing number of players to enter the market. This will lead to increased competition among cyber extortionists for targets, and encourage cybercriminals to adapt their operations (improved customer service, harder-to-detect malware) and targeting (more focused attacks asking for more money, expansion into new sectors).

It's also helpful to understand ransomware in the context of its enabling technologies. Just as YouTube's explosive growth would not have been possible without the advent of widespread broadband internet, the rise of ransomware would arguably not be possible without Bitcoin making it difficult to trace the funds and Tor making it nearly impossible to identify the perpetrators.

In terms of targeting, PCs were originally the primary victims of ransomware. Later, we started seeing infected phones and servers. In 2015, cyber extortionists started locking people out of websites by encrypting page files, images and directories until a ransom was paid.[20] Projecting further into the future, the rapid expansion of the Internet of Things (IoT) could lead to cyber extortionists locking people out of their cars, homes or refrigerators. In addition, we should also begin to see cyber activists using ransomware operations to further political agendas.

While much has been written about the cost to victims of ransomware attacks, understanding the cost to attackers is the key to addressing this threat. Although there have been a handful of high-profile arrests in the Netherlands, Spain, the UK and the US, cyber extortionists have so far been highly effective at eluding capture and prosecution.[21,22,23]

Due to the low-cost, high-reward and low-risk nature of establishing a successful ransomware scheme, the laws of economics dictate that criminals will increasingly engage in this activity, as profitable ransomware operations invite copycats. Finally, with the rise of RaaS, the barriers to entry into this market are lower than ever.

New dimensions of the ransomware industry are discovered each week, and the situation continues to evolve rapidly. Recently, a new ransomware marketplace surfaced that helps facilitate Bitcoin payments between attackers and victims.[24] Like any profitable market with low barriers to entry, the competitive ransomware industry is driving innovation. As long as the trends outlined above persist, the ransomware industry will continue to be a major cyber security challenge. ■

REFERENCES

1. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
2. https://www.forcepoint.com/content/2015-ws-threat-report
3. https://powermore.dell.com/technology/top-5-security-threats-2016/
4. https://www.controlrisks.com/webcasts/studio/2015-GENERAL/Riskmap-2016/RM-2016-report-PDFs/2015-11-27-RM-REPORT-2016-LR.pdf
5. https://www.us-cert.gov/ncas/alerts/TA16-091A
6. Krebs, B. (2014). Spam nation: The inside story of organized cybercrime – from global epidemic to your front door. Naperville, Illinois: Sourcebooks.
7. http://www.detroitnews.com/story/news/politics/michigan/2014/11/17/north-american-international-cyber-summit/19162001/
8. http://www.govtech.com/security/Ransomware-Poses-Tremendous-Threat-to-Police-Departments.html
9. http://www.networkworld.com/article/2906983/security0/massachusetts-police-department-pays-500-cryptolocker-ransom.html
10. http://www.darkreading.com/attacks-breaches/police-pay-off-ransomware-operators-again/d/d-id/1319918
11. http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/
12. http://www.networkworld.com/article/2901527/microsoft-subnet/crypto-ransomware-attack-hit-new-jersey-school-district-locked-up-entire-network.html
13. http://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/
14. http://www.webroot.com/blog/2016/02/18/new-ransomware-padcrypt-first-live-chat-support/
15. https://www.trustwave.com/Resources/Trustwave-Blog/What-You-Can-Learn-from-the-Ridiculous-Money-That-Cybercriminals-Make/
16. http://www.bitdefender.com/media/materials/white-papers/en/Bitdefender_Ransomware_A_Victim_Perspective.pdf
17. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf
18. http://www.theregister.co.uk/2014/08/06/decryptolocker/
19. https://threatpost.com/password-generator-tool-breaks-petya-ransomware-encryption/117315/
20. http://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/
21. http://www.kaspersky.com/about/news/virus/2015/Collaboration-between-the-Dutch-police-and-Kaspersky-Lab-leads-to-the-arrest-of-suspects-behind-the-CoinVault-ransomware-attacks
22. http://thehackernews.com/2013/02/group-behind-largest-ransomware.html
23. https://threatpost.com/dutch-police-arrest-alleged-coinvault-ransomware-authors/114707/
24. http://www.darkreading.com/endpoint/crowdsourcing-the-dark-web-a-one-stop-ran$om-shop/a/d-id/1325265

ABOUT THE AUTHOR

Patrick Vibert is a Senior Consultant on Control Risks' Cyber Threat Intelligence (CTI) team, serving the Americas. He has extensive experience providing cyber intelligence solutions to Global 500 companies in a variety of sectors. His responsibilities at Control Risks include conducting cyber threat research and analysis, and working closely with clients to help them understand and navigate their threat landscape.

Previously, Patrick worked for a major U.S. defence contractor as a Senior Cyber Threat Intelligence Analyst. He holds a B.S. in Business Administration, an M.A. in International Relations, and has lived in eight different countries around the world. This unique background enables him to understand cyber threat risks from a truly global business perspective.