Avoid Having to Run Somewhere From Ransomware, Part 1

Understanding Ransomware and the Criminals Who Spread It

An average of 4,000 ransomware incidents occur daily in the United States at an annual cost of US$1 billion.[1] The number of ransomware attacks more than doubled in 2019, with the average payment per incident coming in at US$41,198[2] (up from US$6,733 in 2018[3]). Insurance companies are forecasting that ransomware will soon account for the highest percentage of cyberinsurance claims.[4]

To effectively deal with this growing worldwide phenomenon, it is essential to understand what it is, what its objectives are, the most common attack vectors used to infiltrate enterprises and how to mitigate the risk of becoming the next victim.

What Is Ransomware?

Malware is any malicious software program; it is generally designed to disrupt, damage or gain unauthorized access to a specific computer or larger system. Ransomware is revenue-generating malware; it is specifically designed to deny access to a victim's files, using complex encryption, until a ransom is paid. Not all ransomware programs are created equal. There are close to 800 known variants to accommodate the various attack vectors that can be used to enter a system. Hackers typically require that payment be made in cryptocurrency to take advantage of the decentralized construct of blockchains, which generally mask transaction sources and destinations.

Case Studies

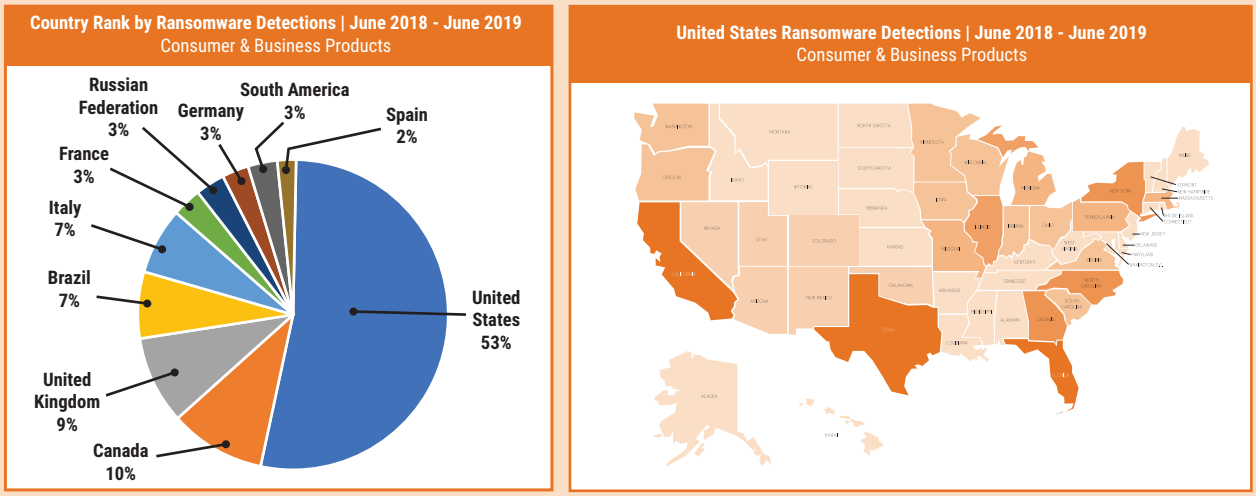
As it has become easier to purchase exploit kits, leverage automation and take advantage of payment anonymity in an environment of inconsistent cyberhygiene, criminal cohorts and state-backed hacking groups have amplified their efforts to wreak havoc on enterprises and individuals around the world. **Figure 1** shows that between June 2018 and June 2019, the country most affected by ransomware attacks was the United States, accounting for 53 percent of all attacks. Canada came in second at 10 percent, and the United Kingdom was third at 9 percent.[5] The map shows that within the United States,

Syed Ishaq, CISA, CRISC, CCISO
Has 15 years of information security experience serving Fortune 50 and government organizations. He advises chief information security officers (CISOs) on behalf of ControlPoints, a high-growth cyberrisk consulting firm. He can be reached at syed@controlpoints.com.

Faizan Mahmood, CISSP, PMP
Is a former CISO with more than 10 years of hands-on experience, much of that time spent as a data center and cloud architect. He is currently a senior member of the Security Test and Evaluation team at the US Federal Communications Commission (FCC). He can be reached at mahmoofx@gmail.com.

© 2020 ISACA. All rights reserved. *www.isaca.org*

Figure 1—International and US Ransomware Detection



Source: Malwarebytes. Reprinted with permission.

ransomware attacks were most prevalent in the US states of Texas and California, but affected all 50 states (note that the darker the shading, the more ransomware detected).

Ransomware attacks have besieged practically every industry, from legal services to trucking. The five most targeted industries in the third quarter of 2019 were professional services, the public sector, healthcare, software services and retail.[6] The following are a few notable recent attacks and their impact.

In May 2019, the city of Baltimore, Maryland, USA, was hit with a strain of the RobbinHood ransomware that encrypted a majority of the city's servers and some government applications. The damage extended to city employees' email and voice message systems; online payment services for water bills, property taxes and traffic citations; and real estate transactions. Hackers demanded 13 Bitcoins, worth US$76,000 on the day of the attack, but city officials refused to pay the ransom because there was no guarantee that services would be restored after payment (and to discourage this type of bad behavior). But that decision proved costly. The city was forced to reallocate US$6 million from a fund for parks and public facilities to cover the costs of "remediation and hardening." The total cost of recovery eventually exceeded US$18 million.[7]

Since 2013, at least 169 county, city and state government systems in the United States have experienced ransomware attacks.[8] Yet, nearly 60 percent of taxpayers are against their local governments using tax dollars to pay ransoms. Instead, they would prefer to allocate the money toward the larger recovery costs.[9]

> "THE IMPACT OF AN ATTACK DOES NOT END WITH PAYMENT OF THE RANSOM."

Alabama-based DCH Health Systems was hit with a ransomware attack in October 2019 that disrupted access to computer systems at all three of its medical centers. For 10 days, the healthcare provider, with a combined 848 patient beds, had to implement manual paper-based workarounds and divert ambulances carrying patients to other hospitals. It instructed new patients "who have non-emergency medical needs to seek assistance from other providers while DCH works to restore our systems."[10] Complicating matters, DCH had to issue a public warning: "We are hearing reports that people claiming to be from DCH may be calling or emailing community members in an attempt to get personal information. Please know that DCH will

© 2020 ISACA. All rights reserved. www.isaca.org

never call or email patients asking for their personal information."[11] The hospital eventually decided to pay the ransom, believing it to be in the best interest of its patients.

The impact of an attack does not end with payment of the ransom, however. New research finds that when hospitals experience a data breach or ransomware attack, the death rate among heart attack patients increases in the months and years afterward. As many as 36 additional deaths per 10,000 heart attacks occurred annually at the hundreds of hospitals examined.[12] The reason: As new IT controls are implemented to protect electronic medical records, doctors, nurses and other health professionals are inevitably slowed down by the new processes. The research found that the time to administer an electrocardiogram increased by as much as 2.7 minutes after a data breach, and this lag remained as high as 2 minutes even after three to four years. For patients requiring emergency cardiac care, every second counts.

Preferred Attack Vectors

Any number of surfaces can be exploited to gain access to a system's files. Most people intuitively believe that email is the most likely method used to infect machines, but an analysis of attacks that occurred in the third quarter of 2019 found Remote Desktop Protocol (RDP) to be the most common exploitation method by a significant margin (50.6 percent). Email (39.0 percent) and software vulnerability (8.1 percent) were the second and third most common attack methods, respectively.[13]

RDP

First rolled out by Microsoft in 1996, RDP is employed by many enterprises, making it a primary target for hackers. It utilizes Standard TCP Port 3389 to allow easy remote access to virtual workstations or servers over a network.

The problem is that if it is compromised, RDP provides an easy pathway into a corporate network because it is connected to other devices. An exploited RDP attack vector allows a malicious actor to move throughout the network to perform reconnaissance, espionage or personally identifiable information (PII) exfiltration; orchestrate account takeovers; install hidden backdoors for illicit connections; add remote-access Trojans (RATs) for future attacks; or sell access to other attackers (Ransomware-as-a-Service). For this reason, ransomware threats can spread quickly from low-priority files to extremely sensitive ones, and before an organization knows it, it has become the victim of an attack.

The Dharma ransomware was the most common malware employed in 2019 because it specifically exploits open or poorly secured RDP ports.[14] Ransomware such as WannaCry, SamSam and CrySIS has also been known to spread via RDP.

> "WHEN HOSPITALS EXPERIENCE A DATA BREACH OR RANSOMWARE ATTACK, THE DEATH RATE AMONG HEART ATTACK PATIENTS INCREASES IN THE MONTHS AND YEARS AFTERWARD."

Email

Web-based email is exploited by sending a seemingly innocuous email message that contains nefarious links and/or attachments encoded within it. If a link is clicked or an attachment opened, the attack can quickly lock the local systems and/or encrypt files. Depending on the type of infection, it can spread rapidly throughout the network.

Software Vulnerability

The most common software vulnerability used to infect systems with ransomware involves macros embedded within trusted applications (e.g., Microsoft Word, Excel, PowerPoint). Macros are essentially bits of computer code used to automate repetitive tasks. An end user can write macros using the Visual Basic for Applications (VBA) programming language, but so can malicious attackers who use macros to automate functions such as deleting files or automatically starting a malicious program whenever Word is opened.

© 2020 ISACA. All rights reserved. *www.isaca.org*

But there are other ways to exploit software. For example, malicious websites (often via Domain Name System [DNS] masking) use the facade of a trusted site to tempt users to click on an infected link. **Figure 2** is from a fake PayPal site that promised 3 to 5 percent cash back on purchases but, in reality, was depositing a cashback.exe ransomware file onto the victim's PC.

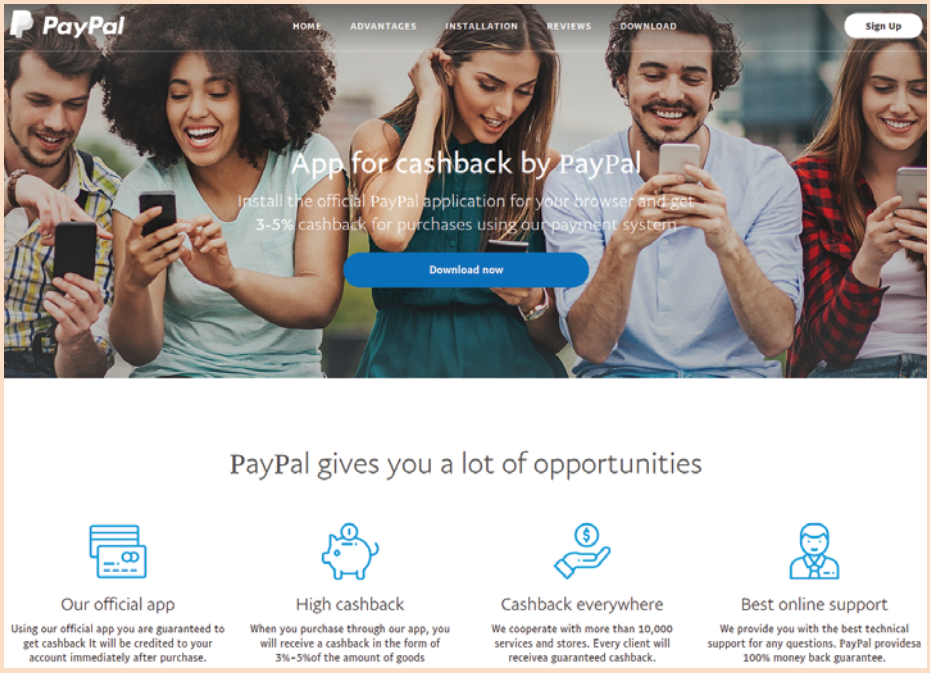
Lab tests on the cashback.exe ransomware found that only 36 of 68 antivirus engines could detect its executable file. This ransomware also has a location-based element. The executable file first checks whether an infected computer is located in Belarus, Kazakhstan, Russia, Tajikistan or Ukraine. If it is, the ransomware's file-encrypting function does not deploy. For all others, it launches the attack.[15]

The Maze ransomware provides an example of how unpatched software vulnerabilities can elevate risk. Attackers purchase advertisements that direct visitors to a fake site camouflaged as a legitimate cryptocurrency exchange application. When a potential victim arrives at the landing page, the Spelevo exploit kit is activated in the background and attempts to exploit Flash players' critical vulnerability Common Vulnerabilities and Exposures (CVE)-2018-15982. If this is successful, the kit automatically downloads and installs the Maze ransomware, then begins executing code to scan for certain file extensions (e.g., documents, photos, databases) to encrypt. The code generates a ransom note in each of the scanned folders, with instructions to open a specific website hosted on the Tor network (which cannot be blocked by countries) for further instructions on how to make payment and obtain the private key to decrypt the files. The site even provides a live chat to support the victim through the payment and decryption process.[16]

Motivating Factors: Following the Money Trail

Cybercriminals' motivation for launching a ransomware attack is simple: extortion. Precious data will be held hostage until something of value is exchanged.

Figure 2—Spoofed PayPal Site



Source: Ilascu, I; "Fake PayPal Site Spreads Nemty Ransomware," Bleeping Computer, 8 September 2019, *https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware*. Reprinted with permission.

© 2020 ISACA. All rights reserved. *www.isaca.org*

Value is in the eye of the beholder. Consider the interesting conundrum posed by the Popcorn Time ransomware. The unfortunate person who gets hit with this malware has a dilemma: pay the attacker right away to get the files unencrypted or unceremoniously forward a ransomware referral code to contacts and infect their devices. If at least two of the victim's contacts pay the ransom to have their files unlocked, the attacker gladly provides the person at the top of the pyramid the decryption key for free.[17]

Some ransomware is designed purely to wreak havoc. The group behind the 2017 NotPetya attack, for example, had no interest in receiving payments. Instead, the ransom motivation was destruction. The malware irreversibly encrypted an infected computer system's master boot records, the deep-seated part of the machine that tells it where to find its own operating system. The attack started in Ukraine and within hours had spread around the world, crippling companies such as Maersk, Merck and FedEx and causing US$10 billion in damage.[18] No decryption keys existed. Similarly, the 2019 GermanWiper ransomware rewrites the content within the files of an infected system, rendering them useless.

The majority of attacks, however, are motivated by money, and it is now possible to get a picture of the economics for both attackers and victims. A quarter of business executives would be willing to pay between US$20,000 and US$50,000 to regain access to encrypted data.[19] Nearly 40 percent of ransomware victims pay the ransom.[20] As of the third quarter of 2019, the average ransom paid was US$41,198, an increase of 13 percent compared with the second quarter and a nearly sixfold increase from the third quarter of 2018.[21] As many as 98 percent of enterprises that paid the ransom received a decryption tool from the hackers.[22] But 17 percent that paid the ransom never recovered their data because decryption success depends on the type of ransomware.[23] For example, Dharma ransomware variants were often unreliable after the ransom was paid, whereas GrandGrab TOR almost always delivered a successful decryption tool after payment was received.[24] Approximately 98 percent of ransomware payments were made in Bitcoin.[25]

McAfee's Advanced Threat Research (ATR) team set out to investigate the path ransom payments take from victim to attacker. The team reviewed the Sodinokibi ransomware and linked underground forum posts with Bitcoin transfer traces on its blockchain to understand key touch points. The ATR team observed that Sodinokibi attackers generate a unique Bitcoin wallet for each victim and utilize a prominent mixing service called Bitmix.biz to obfuscate the origin of the transaction (the infection site of the victim) from the cash-out wallet. Attackers employ affiliates (middlemen) to set up additional wallets to further mask transactions.

The ATR team learned that the average Sodinokibi ransom request is between US$2,500 and US$5,000. After a victim sends payment, an average of two to three transactions occur before it reaches the final destination. An average of 30 to 40 percent of each payout goes to the attacker, and 60 to 70 percent is divided among the affiliates. A total of 41 active affiliates were spotted; one particular affiliate's wallet contained US$4.5 million worth of Bitcoin.[26]

Consistent with RDP being the attack vector of choice, compromised RDP server prices have increased since 2017 on the dark web.[27] In 2017, for example, a compromised RDP from any country could be bought for about US$10 on the dark web,[28] but in 2019, this price jumped to US$26 on average, a 160 percent increase.

Conclusion

As ransomware continues to spread like wildfire, a macro-level risk profile begins to emerge. Public and private organizations in Canada, the United Kingdom and the United States are most likely to be under attack and their unsecured RDP, employees (via email) and software vulnerabilities more than likely to be exploited. Most victims are unprepared to effectively respond to an attack.

Ransomware criminals will demand on average US$42,000 paid in Bitcoin to release their decryption keys, which will not work 17 percent of the time. Read part two in this series to understand how to mitigate the risk of becoming the next victim.

Enjoying this article?

- Read *State of Cybersecurity 2019, Part 2: Current Trends in Attacks, Awareness and Governance. www.isaca.org/state-of-cybersecurity-2019*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

© 2020 ISACA. All rights reserved. *www.isaca.org*

> AS RANSOMWARE CONTINUES TO SPREAD LIKE WILDFIRE, A MACRO-LEVEL RISK PROFILE BEGINS TO EMERGE.

Endnotes

1 US Federal Bureau of Investigation, "How to Protect Your Networks From Ransomware," *https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view*

2 Schwartz, M.; "Ransomware: Average Ransom Payout Increases to $41,000," Bank Info Security, 1 November 2019, *https://www.bankinfosecurity.com/ransomware-average-ransom-payout-increases-to-41198-a-13333*

3 Palmer, D.; "Ransomware: The Cost of Rescuing Your Files Is Going up as Attackers Get More Sophisticated," ZDNet, 16 April 2019, *https://www.zdnet.com/article/ransomware-the-cost-of-rescuing-your-files-is-going-up-as-attackers-get-more-sophisticated/*

4 Cimpanu, C.; "BEC Overtakes Ransomware and Data Breaches in Cyber-Insurance Claims," *ZDNet*, 2 September 2019, *https://www.zdnet.com/article/bec-overtakes-ransomware-and-data-breaches-in-cyber-insurance-claims*

5 Malwarebytes, "Cybercrime Tactics and Techniques: Ransomware Retrospective," August 2019, *https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-ransomware-retrospective/*

6 *Op cit* Schwartz

7 Duncan, I.; "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts," *The Baltimore Sun*, 29 May 2019, *https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html*

8 Liska, A.; "Early Findings: Review of State and Local Government Ransomware Attacks," Recorded Future, 10 May 2019, *https://www.recordedfuture.com/state-local-government-ransomware-attacks/*

9 IBM, "IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks," 5 September 2019, *https://newsroom.ibm.com/2019-09-05-IBM-Security-Study-Taxpayers-Oppose-Local-Governments-Paying-Hackers-in-Ransomware-Attacks*

10 DCH Health System, "Patient and Community Information Regarding Attack on DCH Computer Frequently Asked Questions," 2 October 2019, *https://www.dchsystem.com/Articles/patient_and_community_information_regarding_attack_on_dch_computer.aspx*

11 DCH Health System, "DCH Ongoing Response to Cyberattack and IT System Outage," 7 October 2019, *https://www.dchsystem.com/Articles/dch_ongoing_response_to_cyberattack_and_it_system_outage.aspx*

12 Akpan, N.; "Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks," PBS News Hour, 24 October 2019, *https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks*

13 Coverware, "Ransom Payments Rise as Public Sector Is Targeted, New Variants Enter the Market," 1 November 2019, *https://www.coveware.com/blog/q3-ransomware-marketplace-report*

14 Palmer, D.; "Ransomware: These Are the Most Common Attacks Targeting You Right Now," *ZDNet*, 16 October 2019, *https://www.zdnet.com/article/ransomware-these-are-the-most-common-attacks-targeting-you-right-now/*

15 Ilascu, I; "Fake PayPal Site Spreads Nemty Ransomware," Bleeping Computer, 8 September 2019, *https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware*

© 2020 ISACA. All rights reserved. *www.isaca.org*

16 Gatlan, S.; "Maze Ransomware Now Delivered by Spelevo Exploit Kit," Bleeping Computer, 18 October 2019, *https://www.bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit/*
17 Newman, L.; "Devious Ransomware Frees You if You Infect Two Other People," *Wired*, 13 December 2016, *https://www.wired.com/2016/12/popcorn-time-ransomware/*
18 Greenberg, A.; "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 August 2018, *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*
19 IBM, "IBM Study: Businesses More Likely to Pay Ransomware than Consumers," 14 December 2016, *https://www-03.ibm.com/press/us/en/pressr. lease/51230.wss*
20 Malwarebytes, "Understanding the Depth of the Global Ransomware Problem," *https://go.malwarebytes.com/OstermanRansomwareSurvey.html*
21 *Op cit* Schwartz
22 *Op cit* Coverware
23 Kaspersky, "Story of the Year Ransomware," 2017, *https://cdn.securelist.com/files/2017/11/KSB_Story_of_the_Year_Rans. mware_FINAL_eng.pdf*
24 *Op cit* Coverware
25 *Ibid*.
26 Fokker, J.; C. Beek; "McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service—Follow the Money," McAfee, 14 October 2019, *https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-se. vice-follow-the-money/*
27 Gray, I.; "Pricing Analysis of Goods in Cybercrime Communities," Flashpoint, 15 October 2019, *https://www.flashpoint-intel.com/wp-content/uploads/2019/10/Flashpoint-Report-Pricing-Analysis-of-Goods-in-Cybercrime-Communities.pdf*
28 Rowley, O.; "Analysis: Pricing of Goods and Services on the Deep & Dark Web," Flashpoint, 2017, *https://go.flashpoint-intel.com/docs/analysis-pricing-of-goods-and-services-on-the-ddw*

© 2020 ISACA. All rights reserved. *www.isaca.org*