Ransomware: The Landscape Is Shifting --*A Concise Report-*

Ronny Richardson
Management, Entrepreneurship and Hospitality
Coles College of Business, Kennesaw State University, GA, USA

Max M. North
Information Systems Department
Coles College of Business, Kennesaw State University, USA

David Garofalo
Department of Physics
College of Science and Mathematics, Kennesaw State University, USA

[Abstract] Ransomware continues to be a growing threat to the data files of individuals and businesses. While ransomware attacks against corporations, government, and critical infrastructure, entries are growing rapidly, attacks against individual consumers are shrinking. Not only have the ransomed attacks become more frequent, they have become more severe. New versions of the malware appear frequently and are empowered to avoid antivirus and intrusion detection methods. In this concise report, we extend our original ransomware evolution, mitigation, and prevention article by presenting a few highlights of the recent growth and shifting target. Furthermore, COVID-19, an unexpected threat, and brief prevention sections are presented.

[Keywords] malware, ransomware, ransom

Background and Framework

The basic and practical description of ransomware was presented in our recent preliminary report: "Ransomware is a growing threat to the data files of individuals, businesses and government agencies. It encrypts files on an infected computer and holds the key to decrypt the files until the victim pays a ransom" (Richardson & North, 2017). This malware is liable for millions of dollars of losses annually and is rapidly increasing. Consequently, new versions of ransomware are frequently created and appear in varieties of businesses and government sectors, allowing them to avoid antivirus software and other intrusion detection methods. A complete primary report is included in an article entitled "Ransomware: Evolution, Mitigation and Prevention" (Richardson & North, 2017). In this concise report, we extend our original ransomware evolution, mitigation, and prevention article by presenting a few highlights of the recent growth and shifting target. Furthermore, COVID-19, an unexpected threat, and brief prevention sections are presented.

Growth and Shifting Targets

Since that 2017 article, ransomware attacks have grown substantially. In both 2018 and 2019, the growth rate for insurance claims related to ransomware grew at rates exceeding 100 percent (Motta, 2020; Kauflin, FORBES, 2019). Not only have the attacks become more frequent, they have become more severe. Early strains (including SamSam and Dharma) averaged demands of less than $10,000. By 2019, later strains (including Bitpaymer, Ryuk, Sodinokobi) had demands that exceeded $100,000 (Motta, 2020). According to the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019 (Federal Bureau of Investigation Internet Crime Complaint Center, 2019). While ransomware attacks against businesses and government entries are growing rapidly, attacks against individual consumers are shrinking. In August 2020, INTERPOL issued a warning that, "An INTERPOL assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure" (INTERPOL, 2020).

By 2018-2019, organizational attacks accounted for 81 percent of all ransomware infections. The major reason is that "Consumers are more trouble than they are worth," says Dick O'Brien, principal editor at Symantec, a leading antivirus company. A related reason is that consumers are rarely willing to pay more than $1,000, while organizations are willing to pay much more (Lemos, 2019). Malwarebytes Labs, another antivirus firm, found that organizational attacks increased 365 percent from Q2 of 2018 to Q2 of 2019, but consumer attacks declined during the same period (Constantin, 2020).

Ransomware is even micro-targeting within the organizational sector. It hits manufacturing companies the most with these receiving almost a quarter of the attacks IBM responds to. The next two largest sectors are professional services and government. This suggests that ransomware gangs are targeting organizations with a low tolerance for downtime (Ranger, 2020). Ransomware is also beginning to shift to blended "extortion-and-ransomware" attacks. Here, in addition to encrypting local files, the ransomware steals copies of sensitive files and the gang threatens to make the documents public unless the ransom is paid. When the ransom has not been paid, some firms have seen their data auctioned on the dark web with prices ranging from $5,000 to over $20 million (Ranger, 2020). According to IBM, the ransomware gangs are targeting the ransomware amounts to the specific firm. Known ransoms range~~s~~ from 0.08 percent of annual revenues to as high as 9.1 percent (Ranger, 2020).

COVID-19 and Ransomware

There are two concerns surrounding COVID-19 and ransomware. The first is phishing. Recently, researchers at Proofpoint have seen a major increase in ransomware being distributed by COVID-related emails with hundreds of thousands of these emails going out daily (Palmer, *Ransomware: Attacks that start with phishing emails are suddenly back in fashion again*, 2020). From January to April 2020, INTERPOL found "some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs – all related to COVID-19 – detected by one of INTERPOL's private sector partners." (INTERPOL, 2020).

The largest attacks are by a new ransomware strain called Avaddon. During one week in June 2020, the gang behind it sent out over one million phishing emails, mainly targeting US organizations (Palmer, 2020). This is in keeping with the shift away from individual attacks to organizational attacks.

The second (and larger) COVID-related concerns are attacks against COVID research firms, firms manufacturing the vaccine, and healthcare facilities treating sick individuals. The risk is great. Interpol issued a warning about the ransomware gangs using disruptive malware against the healthcare institution due to the high impact and possibility of high ransoms (INTERPOL, 2020). "Hackers are very financially motivated and healthcare institutions and hospitals are extremely vulnerable and willing to pay right now because they can't afford to be shut down when they're at capacity and overflowing with coronavirus patients," says Charity Wright, cyber-threat intelligence advisor at IntSights (Palmer, 2020).

Some ransomware gangs have announced that they are avoiding directly targeting medical facilities during the pandemic. However, this does not eliminate the risk for the healthcare industry. The healthcare industry has a large supply chain that is still at risk, and an attack on firms in this supply chain could be just as devastating as a direct attack against the healthcare facility itself (Palmer, 2020).

An Unexpected Ransomware Threat

Often, the first debate after a ransomware attack is to pay or not to pay. Law enforcement and security personnel generally advise against paying the ransom~~.~~ (Goodin, 2020). If the decision is made to pay the ransom, the concerns are if the ransomware gang will decrypt the files and, where applicable, not release the data publicly. However, paying the ransom entails a risk that is seldom considered.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. For example, SamSam ransomware attacks started in late 2015 and frequently targeted government institutions. In November 2018, OFAC designated two Iranians as providing material support to a malicious cyber activity. Additionally, a 2017 ransomware attack called WannaCry 2.0 was linked to the Lazarus Group, a cybercriminal organization sponsored by North Korea (Department of the Treasury, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 2020).

"Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA), U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is also prohibited" (Department of the Treasury, 2020) Thus, paying a ransom could cause your firm to be in violation of Treasury Department sanctions and open the firm up to enforcement actions.

Ransomware Prevention

A number of specific techniques and methods have been researched and recommended for detection, identification, and prevention of ransomware attacks (Ahmed, Koçer, Huda, Al-rimy & Hassan 2020; Bansal, Deligiannis, Maddila & Rao, 2020; Bajpai & Enbody, 2020; Hwang, Kim, Lee & Kim, 2020; Margarov & Mitrofanova, 2020; Yaqoob, Ahmed, ur Rehman, Ahmed, Al-garadi, Imran & Guizani, 2017). Experts recommend a multi-prone approach to avoiding ransomware and then dealing with it if you are unlucky enough to become infected. Motta (2020) has comprehensively provided precise steps that we briefly provide in this section.

The first step is to make your organization less open to attack since more ransomware attacks are targets of opportunity. The two most common attack vectors are phishing and remote network access points. The most common of these is Microsoft Remote Desktop Protocol (RDP). Avoiding using RDP or limiting its use can prevent you from becoming a target (Motta, 2020).

The second step is to be vigilant, watching for a phishing attempt, a user enabling macros, or suspicious activity on your network. The average time between infection and activation is 30 days with a range of 30 minutes to one year (Motta, 2020). In many cases, this gives vigilant organizations time to recover from a ransomware attack before its payload is triggered.

The third step is to eliminate remote access and administration interfaces that connect to your primary network environment. If you must use them, limit their use and use multi-factor authentication. Basic hygiene, like regular patching and limiting administrator access, are also important (Motta, 2020).

The fourth step is to have good backups, something we strongly advocated for in our original article (Richardson-& North, 2017). Offline backups (sometimes called a cold site backup) are important since this prevents the ransomware from encrypting the backup (Motta, 2020). Of course, having a strong backup will not protect you completely from an extortion-and-ransomware infection since the ransomware gang can still release your data.

The fifth step is, should you find yourself infected with no means to recover your data, hire an experienced, dispassionate, third-party expert to manage negotiating with the ransomware gang. If you have cyber insurance that covers ransomware, this is likely part of your policy (Motta, 2020).

References

Ahmed, Y. A., Koçer, B., Huda, S., Al-rimy, B. A. S., & Hassan, M. M. (2020). A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. *Journal of Network and Computer Applications, 167*, 102753.

Bajpai, P., & Enbody, R. (2020). Attacking key management in ransomware. *IT Professional, 22*(2), 21-27.

Bansal, C., Deligiannis, P., Maddila, C., & Rao, N. (2020). *Studying Ransomware Attacks Using Web Search Logs*. arXiv preprint arXiv:2005.00517.

Constantin, Lucian, (2020). *More targeted, sophisticated and costly: Why ransomware might be your biggest threat.* Retrieved from https://www.csoonline.com/article/3518864/more-targeted-sophisticated-and-costly-why-ransomware-might-be-your-biggest-threat.html

Department of the Treasury Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Washington, D.C. Department of the Treasury, National Cyber Awareness System. Retrieved from https://us-cert.cisa.gov/ncas/current-activity/2020/10/02/department-treasury-releases-advisory-potential-sanctions-risks

Federal Bureau of Investigation Internet Crime Complaint Center. (2018-2019). I*nternet Crime Report Washington, D.C. Federal Bureau of Investigations*. Retrieved from https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219

Goodin, D. (2020). *Paying ransomware demands could land you in hot water with the feds*. Retrieved on 11/18/2020 from https://arstechnica.com/tech-policy/2020/10/paying-ransomware-demands-could-land-you-in-hot-water-with-the-feds/

Hwang, J., Kim, J., Lee, S., & Kim, K. (2020). Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. *Wireless Personal Communications, 112*(4), 2597-2609.

INTERPOL, INTERPOL report shows alarming rate of cyberattacks during COVID-19. (2019). Retrieved from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19#:~:text=INTERPOL%20report%20shows%20alarming%20rate%20of%20cyberattacks%20during%20COVID%2D19,-4%20August%202020&text=In%20one%20four%2Dmonth%20period,of%20INTERPOL's%20private%20sector%20partners.

Kauflin, j., (2020). *FORBES, Ransomware Has Catapulted This Insurtech Startup To $100 Million In Revenue.* Retrieved from https://www.forbes.com/sites/jeffkauflin/2020/11/24/ransomware-has-catapulted-this-insurtech-startup-to-100-million-in-revenue/?sh=537206ed4fab

Lemos, R., (2019). Ransomware Moves Away from Consumers Retrieved from https://symantec-enterprise-blogs.security.com/blogs/feature-stories/ransomware-moves-away-consumers

Margarov, G., & Mitrofanova, E. (2020). Management of Ransomware Detection and Prevention in Multilevel Environmental Monitoring Information System. In F*unctional Nanostructures and Sensors for CBRN Defense and Environmental Safety and Security* (pp. 125-131). Springer, Dordrecht.

Motta, M. (2020). *How to Avoid Ransomware and How to recover if you're victimized.* Retrieved from https://researchexchange.iaao.org/conference2020/IAAO2020/schedule/56/

Palmer, D. (2020). *Ransomware: Attacks that start with phishing emails are suddenly back in fashion again.* Retrieved from https://www.zdnet.com/article/ransomware-attacks-that-start-with-phishing-emails-are-suddenly-back-in-fashion-again/

Ranger, S. (2020). *Ransomware gangs are changing targets again. That could make them even more of a threat.* Retrieved from https://www.zdnet.com/article/ransomware-gangs-are-shifting-targets-and-upping-their-ransom-demands/

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review, 13*(1), 10.

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks, 129*, 444-458.