Give me the loot, but in crypto: How ransomware has evolved overtime, and how to prevent the possibility of becoming a victim

Shikerra J. Collick, M.S. Candidate in Cyber Forensics

University of Baltimore

All inquiries concerning this journal should be directed to Shikerra J. Collick, College of Professional Studies, Cyber Forensics Program, University of Baltimore, 1420 N. Charles St., Baltimore, MD 21201.

Email: shikerra.collick@ubalt.edu

Abstract

Ransomware has become a widely popularized cybercrime as it is a means for financial gain; a way to acquire valuable information that could potentially be sold; or a combination of both. During the worldwide COVID-19 lockdowns, the restrictions mandated by different governments incited an increase for bad actors to prey on and expose the vulnerabilities present within the network security of organizations that may not have kept up with important updates that would secure their protection. The need to re-evaluate business continuity and incident response plans became a priority for those victims that suffered great loss. This paper will begin with what exactly ransomware is, then, its different forms and examples of different attacks, and conclude with how to protect yourself or your organization from becoming a victim of an attack.

Keywords: ransomware, malware, social engineering, security, prevention

Introduction

Ransom malware, or ransomware, is an attack that restricts access through the use of malware that is planted on a victim's computer system through a trojan, or any other type of malware. A message is typically displayed on the victim's screen demanding a ransom in order for their system to be restored. There is no guarantee of a system to be restored after a ransom is paid, and it could be a continued process of demands of money if one does pay. Ribeiro (2022) states that a successful attack depends on the unfeasibility of the victim to recover data. The means by which the ransom is collected has evolved overtime from requested payment be sent via mail to now where cryptocurrency is the preferred means due to the lack of traceability to the accounts used. A trend was seen where there was a rise in ransomware during the COVID-19 pandemic, but was the rise in attacks solely due to a means to make up from the lost wages or did ransomware become the most profitable means in the world of cybercrime?

The ways in which the ransomware occurs have also evolved, but social engineering seems to be effective in gaining information on a target, or even getting someone to provide their credentials under the guise that the attacker is support personnel. These instances exposed how vulnerable places such as hospitals or governments on local and state levels are due to lack of updating patches or a lack of solid security training for staff. But first, we must start from the beginning in order to find the best remedies.

Literature Review and Research

The first reported ransomware incident was in 1989 through the use of the Acquired Immunodeficiency Syndrome Trojan that was written by Dr. Joseph Popp. This was executed through a floppy disk, and the Trojan monitored the number of times the system was powered on/off, and after the threshold was met, all the files on the system were encrypted and could only be accessed again if the $189 ransom was paid. The ransom was to be paid by sending the money to a P.O. Box in Panama (Kapoor, et al., 2021; Zakaria, et al., 2017). The first attempt was one of its kind at the time, and years in 2005, ransomware reemerged in the form of the Trojan.Gpcoder, or GP code, and was developed by Russian criminals who attached spam through emails. This was the birth of what we see today (spam mail). The main fallacy with the GP Coder was that it was easily decryptable at the time, but it was reused and made stronger in latter ransomware, and its variants have been a lot more difficult to decrypt (Giri, et.al., 2006; Chesti, et al., 2020).

Majority of the literature on ransomware divides it into two main types: Locker ransomware “lockerware” and encryption ransomware, “cryptoware”. With lockerware, the display is locked only showing the message the hacker wants to be displayed, and all other functions are disabled. There is a way to unlock the lockerware, and that is by rebooting a computer system in safe mode or using a virus scanner. Also, lockerware is less damaging in its effects as the files are not encrypted (Beaman, et al., 2021; Ribeiro, 2022). On Chinese social networks, Android- lockerware has been rampant in its attacks. Android allows for users to download applications from third-party sources whereas Apple only lets you download applications that are on their App Store. Many attackers in the Chinese market use a program called AIDE to develop ransomware and hide them in apps that appeal to users who unknowingly download the fake app. As a result of the download the users phone becomes disabled and they cannot unlock it or tap anything on their screen (Su, et al., 2018).

With cryptoware, the files on a computer system are encrypted, and the ransom is demanded to be delivered in cryptocurrency, which makes it easier to launder profits. Cryptoware has been recognized as the most profitable type of ransomware and contributes to a multi-million-dollar dark web industry (Oerlemans, 2020; Morato, et al., 2018). In 2019, the

LockerGoga ransomware was developed and targeted manufacturing firms and industries. Files were encrypted and a ransom was demanded for the key. Norse Hydro was a company that fell victim to this ransomware, and it spread throughout the business companies due to it traveling over the network system. Devices had to be removed from the network system to prevent further infection, and total of $40 million was requested as ransom (Chesti, et al., 2020).

Another type of ransomware has been mentioned called “scareware” which uses pop-up ads to make a user believe they have to download software to protect their computer and exploits on the user’s fear rather than locking down their computer (Beaman, et al., 2021). Leakware is another type that has been mentioned, and this kind entails malware for the purpose of collecting personal information on the victim’s computer system, and then later they blackmail the victim with the information collected. If the victims refuses to succumb to their demands, the attacker threatens to leak the information online (Anghel & Racautanu, 2019).

Methods of delivering ransomware, or their sources, have even been recorded and categorized. As we commonly see today, spam emails are sent which contain a fraudulent link or fraudulent information that has malicious files embedded within. Removable media devices, for example, the floppy disk with the first recorded ransomware attack, can contain malicious files that can be downloaded upon connection to a device (Kapoor, et al., 2021). Malicious advertising, “malvertising,” is another source of delivering ransomware as the redirection feature on pop-up ads is used to redirect user to what they think is a legitimate site but is actually a fictitious domain. Unbeknownst to the user, they end up downloading software that contains malware. (Kapoor, et al., 2021, Sood, 2011). The use of social media and SMS is another method to deliver ransomware users are encouraged to follow a link which then downloads malware. There was a time on Facebook where bogus links were sent to users encouraging them to click the link to view a video, but instead of a video they were downloading malware and fell victim to ransomware. Ransomware as a Service (RaaS) is another ransomware delivery method where ransomware services are purchased by attackers who are not savvy with creating their own ransomware through the dark web, and part of the profit made from a successful ransomware attack is given to the ransomware service provider (Kapoor, et al., 2021). Meland, et al. (2020) found that during this RaaS process, a custom-made ransomware is made dependent on the target, and the service provider collects a 20-30% fee from the ransom. RaaS also allows for source code to be compiled by the customer, and then the victim information is given to the provider.

Salvi (2016) states that there are five stages a ransomware attack goes through which are: installation, contacting headquarters, handshake and keys, encryption, and extortion. The installation phase is where the initial infection of the victim's computer system takes place. After successful takeover, the attacker is notified, and the ransomware determines what type of system the victim's computer is. Then, the handshake process begins, and a key is on the victim computer and another on the attacker's server. Contact with the command servers lets the attacker know what files should be targeted, and when the encryption of those files should be done. Afterwards, the files on the victim's computer and encrypted and all access to same is denied because they do not have the key. The ransom message is displayed and the victim them has the option of paying the ransom with no certainty of actually regaining their files, or to take the loss (Meland, et. al, 2020; Anghel & Racautanu, 2019).

Now that we have a better understanding of ransomware, its types, and how its transmitted, lets view real-world examples such as those like CryptoLocker, CryptoWall, or Jigsaw. One of the largest and most financially damaging ransomware attacks known today is the

WannaCry ransomware attack in 2017 which preyed on a Samba vulnerability and was commanded through the Onion Network (Anghel & Racautanu, 2019). WannaCry was a cryptoware type of ransomware, and it encrypted its victim's files except for the few that instructed the user on what they should do in order to decrypt the program. Payment was demanded in the cryptocurrency called Bitcoin. WannaCry caused over 4 billion dollars' worth of damage to computer systems all over the world. Some of the companies and organizations affected included: FedEx, Nissan, German and Russian railways, colleges in China, and telecommunications companies (Mohurle & Patil, 2017; Tiu & Zolkipli, 2021; Kamil, et al., 2022).

The COVID-19 pandemic, and months of shutdowns led to a rise in the amount of ransomware attacks, and many governmental agencies, school systems, and healthcare systems fell victim to attackers who sought a large payout for their high-level of disruption. CONTI is the latest ransomware that has wreaked havoc. The process of this ransomware begins with phishing emails, and if the victim opens the email, malware called "Trickbot" is downloaded. Network scans are also done to gain access to other systems. The victim's computer is then connected to the attacker's server, who has now created a botnet, and the files are uploaded to a cloud server. The Trickbot malware also has the ability to access passwords and other sensitive data. After the sought information is taken, the files on the victim's computer system are encrypted, and a ransom is demanded. If the request goes ignored, a threat to leak the gained information is given, or the attacker may post pieces of files accessed on the dark web to prove their point. CONTI has amassed millions of dollars in profit as a result of its attacks (Moran, et al., 2021). For example, on May 14, 2021, the CONTI ransomware affected Ireland's healthcare systems who were targeted due to their lack of security and necessity of the data on their network. Harvey, et al.,

(2022) conducted a study on CONTI's effects on clinical trials at 10 different hospital systems, and the study was conducted during and after the attack. The results showed that out of the initial 273 patients referred for screening an 85% drop in referrals occurred after the attack, and a 55% drop in recruitment to trials.

The City of Baltimore was the victim of a ransomware called "RobbinHood." The attack was discovered on May 7, 2019, by Baltimore City's Office of Information Technology. Critical files needed for city functions where encrypted, and a demand for 13 bitcoin ($76,000) to be paid was given. Baltimore City chose not to pay the ransom, and instead hired IT consultants to recover the files which cost them millions of dollars compared to the 13-bitcoin ransom. This attack is heavily recognized when talking about weighing the costs and future losses when dealing with a ransomware attack (Farion-Melnyk, et al., 2021; Marett & Nabors, 2021). We must also note that guarantee of the files being released after paying the initial ransom was a factor to consider and could have turned into prolonged blackmail.

Key Findings and Recommendations

Gallegos-Segovia, et al. (2017) explains that social engineering entails a mix of psychological and social skills, and through persuasion or influence, people give out their personal or business information in order for an attacker to gain network access. The first line of defense in an organization is its employees, and they have a duty to protect their own credentials or personal data, and this is essential to the security of an organization. Social engineering has proved to be the kryptonite for this line of defense, and this was exhibited during the COVID shut downs when many organizations were forced to operate remotely. Phishing is the main source, and the vicitms that take the bait unkowingly give out their personal information, or access to their devices and/or credentials. In fact, Kara & Aydos (2022) mention that even images, or advertisements should not be clicked on as it redirects to a harmful site.

Sone preventative measures organizations should adopt are: better training for all employees on social enginneering that empahasizes the importance of not giving out any personal details; to not click any suspicious links within an email; and to always confirm with a supervisor about actions they are unsure of. When creating a plan for security awareness training, organizations should adopt a plan that adheres to the organization's mission, includes frequent training (such as interative modules or informational videos with follow-up questions), and includes fake phising tests to be done by an in-house or contractual I.T team to monitor the effectiveness of the training.

Lack of updates or keeping up with patches is common vulnerability that creates a potential ransomware target. Many individuals and organizations alike depend on antivirus software to keep their devices safe. We always hear about how a ransomware is carried out due to preying on a vulnerability within in a specific program, or how an attacker decides to test how strong a security system through brute force. If software, or an operating system is out-of-date, it can no longer effectively protect against the various forms of ransomware that emerges. When patches are released for antivirus programs, the specific names of malware should be included to be clocked, and checking logs to make sure they are known is a key step for prevention (Saxena & Soni, 2018).

A business continuity plan highlights the key information that needs to be accessible in case of any unplanned event. When an attack occurs, access to clean file backups seems to be an issue in a lot of cases, or it is discovered that backups were not done as frequently as they should. Badhwar (2021) discusses prevention techniques in regard to secure backups. He recommends daily/weekly backups stored on a separate network that is not the same one as the network housing data. Access to backup data should be restricted to authorized personnel, and even their credentials should be protected and require a multi-factor authentication for access. Badhwar then goes on to recommend backups be encrypted with the keys stored in a hardware security module. This practice should be considered as it can provide access in case of any disaster, and not just in cases of ransomware.

Lack of effective measures to detect a ransomware is a common factor of whether or not a person or organization becomes a target. The signature-based approach is widely used in malware detection, and it detects unique patterns specific to known ransomware, and it also produces a low false-positive ratio (Alshaikh, et al., 2020). A fallicy of signature-based detection schemes is defending against ransomware variants that use USB input as their mode of attack. Most programs are solely focused on attacks to a network, and overlook directly installed ransomware. Scaife, et al., (2016) developed the idea of CryptoDrop which is an early warning program for ransomware that studies a user's data and behaviors. Their study focused on identifying the operations, classifying the ransomware into categories, and then developing indicators based on the collected information. They tested their program against 492 ransomware samples and found that few files were lost, and there was a 100% detection rate. It must be noted that benign programs may create a false positive as they are overlooked. Early detection programs similar to, or better developed than CryptoDrop would help prevent future victims of attacks.

Ransomware insurance has been discussed as a possible solution to protect victims of ransomware, granted this cost fits within an organization's budget or business plan. More often than not, huge financial losses are faced after a ransomware attack occurs, and in some cases, can permenantly cripple an organization. An insurance policy can provide protection for losses, and would operate as any other insurance policy would, where a premium is paid and documentation has to be provided to redeem coverage for losses. The downfall of this plan that researchers have found that it could lead to more criminal activity in an attempt for fraud, and attackers may continue to target the same companies due to them knowing about insurance covrerage (Tiu & Zolkipli, (2021).

Conclusion

Ransomware has now become more popularized as a means for income or destruction throughout the dark industry, and for lone attackers. Ransomware as a Service has emerged as a result of the growing industry. Ransomwares are often reused and morphed into more powerful versions of previous ransomware. Social engineering has proved to be the key method for attackers to collect information on their target, and even gain access to their network systems by using phishing emails. Effective prevention is the best way to lessen the chance of becoming a victim, so keeping up with patches, effective security training, and early detection software are essential practices an individual or organization should adopt. Due to the fact that ransomware consistently morphs, consistent research on new attacks or ransomware is necessary for security officers of organizations because most antivirus programs pickup on known malware. The future of ransomware will include more insurance plans related to attacks, or better developed detection software.

References

Alshaikh, H., Ramadan, N., & Hefny, H. A. (2020). Ransomware prevention and mitigation techniques. *Int J Comput Appl*, *117*, 31-39.

Anghel, M., & Racautanu, A. (2019). A note on different types of ransomware attacks. *Cryptology ePrint Archive*.

Badhwar, R. (2021). *The CISO'S Next Frontier: AI, Post-quantum Cryptography and Advanced Security Paradigms* (pp. 165-171). Springer.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490.

Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. Z. (2020, October). Evolution, mitigation, and prevention of ransomware. In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-6). IEEE.

Farion-Melnyk, A., Rozheliuk, V., Slipchenko, T., Banakh, S., Farion, M., & Bilan, O. (2021, September). Ransomware Attacks: Risks, Protection and Prevention Measures. In *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 473-478). IEEE.

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017, October). Social engineering as an attack vector for ransomware. In *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)* (pp. 1-6). IEEE.

Giri, B. N., Jyoti, N., & Avert, M. (2006). The emergence of ransomware. AVAR, Auckland.

Harvey, H., Amberger-Murphy, V., Ballot, J., O'Grady, M., O'Hare, D., Lawler, G., ... & O'Reilly, S. (2022). Impact of Conti ransomware attack on cancer trials Ireland sites.

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105-117.

Kamil, S., Norul, H. S. A. S., Firdaus, A., & Usman, O. L. (2022, February). The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges. In *2022 International Conference on Business Analytics for Technology and Security (ICBATS)* (pp. 1-7). IEEE.

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. *Sustainability*, *14*(1), 8.

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications*, *190*, 116198.

Jimada, S., Nguyen, T. D. L., Sanda, J., & Vududala, S. K. (2021). Analysis of ransomware, methodologies used by attackers and mitigation techniques. In *Research in Intelligent and Computing in Engineering* (pp. 379-387). Springer, Singapore.

Marett, K., & Nabors, M. (2021). Local learning from municipal ransomware attacks: A geographically weighted analysis. *Information & Management*, *58*(7), 103482

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, *92*, 101762.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940.

Moran Stritch, M., Winterburn, M., & Houghton, F. (2021). The Conti Ransomware Attack on Healthcare in Ireland: Exploring the impacts of a Cybersecurity Breach from a Nursing Perspective. *Canadian Journal of Nursing Informatics*, *16*(3-4).

Morato, D., Berrueta, E., Magaña, E., & Izal, M. (2018). Ransomware early detection by the analysis of file sharing traffic. Journal of Network and Computer Applications, 124, 14-32.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016, June). Cryptolock (and drop it): stopping ransomware attacks on user data. In *2016 IEEE 36th international conference on distributed computing systems (ICDCS)* (pp. 303-312). IEEE.

Oerlemans, J. J. (2020). Laundering the Profits of Ransomware. CRIMINAL JUSTICE, 28, 121-152.

Ribeiro, J. V. A. (2022). A brief overview of ransomware behavior analysis challenges. *Brazilian Journal of Development*, *8*(5), 38275-38280.

Salvi, M. H. U., & Kerkar, M. R. V. (2016). Ransomware: A cyber extortion. *Asian Journal for Convergence in Technology* (AJCT) ISSN-2350-1146, 2.

Saxena, S., & Soni, H. K. (2018, February). Strategies for ransomware removal and prevention. In *2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)* (pp. 1-4). IEEE.

Sood, A. K., & Enbody, R. J. (2011). Malvertising–exploiting web advertising. *Computer Fraud & Security*, *2011*(4), 11-16.

Su, D., Liu, J., Wang, X., & Wang, W. (2018). Detecting Android locker-ransomware on chinese social networks. *IEEE Access*, *7*, 20381-20393.

Tiu, Y. L., & Zolkipli, M. F. (2021). Study on Prevention and Solution of Ransomware Attack. *Journal of IT in Asia*, *9*(1), 133-139.

Triplett, W. (2022). Ransomware Attacks on the Healthcare Industry. *Journal of Business, Technology and Leadership*, *4*(1), 1-13.

Urooj, U., Maarof, M. A. B., & Al-rimy, B. A. S. (2021, January). A proposed adaptive pre-encryption crypto-ransomware early detection model. In *2021 3rd International Cyber Resilience Conference (CRC)* (pp. 1-6). IEEE.

Zakaria, W. Z. A., Abdollah, M. F., Mohd, O., & Ariffin, A. F. M. (2017, December). The rise of ransomware. In *Proceedings of the 2017 International Conference on Software and e-Business* (pp. 66-70).