Ransomware: What Is Ransomware, and How to Prevent It

Brandon Chambers
Old Dominion University

Ransomware: What Is Ransomware, and How to Prevent It

Brandon Chambers

Cybersecurity at Old Dominion University

Cova CCI Undergraduate Research Program Spring 2023

Abstract

This research paper answers the question, “What is Ransomware, and How to prevent it?”. This paper will discuss what ransomware is, its history about ransomware, how ransomware attacks Windows systems, how to prevent ransomware, how to handle ransomware once it is already on the network, ideas for training professionals to avoid ransomware, and how anti-virus helps defend against ransomware. Many different articles, case studies, and professional blogs will be used to complete the research on this topic.

Introduction: What is Ransomware?

Ransomware is a new hot topic within cybersecurity nowadays. Within the last decade, ransomware has become much more of a problem for cybersecurity professionals and much more popular for hackers to use in their attacks. Ransomware is a type of malware used by hackers to extort money from victims. It works by exploiting an existing vulnerability on your computer and then infecting your computer with ransomware. There are two categories of ransomware: locker ransomware and crypto-ransomware. Crypto ransomware encrypts either specific files, while locker ransomware encrypts the entire operating system or services that are critical to the machine running (What is ransomware). The easiest way to decrypt the files or operating system might be to pay out the ransom being demanded by the hackers. Typically, the hackers ask for bitcoin to be sent to a specific address, and once the bitcoin (the ransom) is sent, they will send you the decryption key in return. Sometimes, the hackers program the ransomware to encrypt your system and they don't offer a decryption key once you pay the ransom; so, once you pay the ransom your files or operating system is still encrypted and useless.

Significant Ransomware Attacks

Some of my favorite ransomware to read and talk about are Wannacry, Petya, and NotPetya. Wannacry ransomware is significant because of its impact on the United Kingdom's National Health Service. Wannacry ransomware is a worm that spreads using EternalBlue, an exploit that was leaked by the national security agency (Rosencrance, 2021). At the time of the leak, EternalBlue was a zero-day vulnerability that targeted Windows computers, specifically the server message block protocol (Rosencrance, 2021). The wannacry ransomware attacks began on May 12, 2017, and it affected hundreds of thousands of computers in 150 countries, including the

National Health Services of the U.K., Scotland, FedEx, and Honda (Rosencrance, 2021). Britain's National Health Services reported that computers, MRI scanners, blood storage refrigerators, and operating room equipment were all impacted by the wannacry ransomware (Ehrenfeld, 2017). Because of the amount of equipment that was under attack, the National Health Service was unable to care for non-critical emergencies and was forced to use traditional methods of health care that did not use technologies (Ehrenfeld, 2017). Wannacry was asking for a ransom payment varying from $300 to $600 in Bitcoin within three days to decrypt the files; but, even after paying the ransom on time, most victims never received a decryption key (Rosencrance, 2021). The wannacry ransomware could have easily been prevented by simply applying the patch that Microsoft released in March 2017 that fixed the SMB protocol vulnerability that EternalBlue exploited (Ehrenfeld, 2017).

Critical infrastructure is one of the most popular targets to hackers when using ransomware because the infrastructure is important to keeping society happily running. In June 2017, NotPetya surfaced in the world, becoming one of the most expensive and destructive cyberattacks in history (Nakashima, 2018). NotPetya is a dub of famous ransomware called Petya that was introduced in 2016 (What are Petya and NotPetya). The Petya malware was spread through phishing emails carrying a malicious PDF file functioning as a Trojan horse (What are Petya and NotPetya). As soon as the target opened the PDF file, the malware went to work. Petya gained administrative privileges and began by rebooting the computer and on the restart, rewriting the master boot record (MBR) to encrypt the hard drive (What are Petya and NotPetya). Once the hard drive was encrypted, it would begin to ask the user to pay the ransom (in bitcoin) in order to restore the hard drive (What are Petya and NotPetya). Although NotPetya technically is not ransomware, it is still generally referred to as ransomware and is a great

example of how ransomware works and spreads. NotPetya is an improved version of Petya, NotPetya had an improved way to propagate across networks, had an improved method for encryption, and when a computer was infected with NotPetya, there is no way to decrypt the files or hard drive (What are Petya and NotPetya). Once NotPetya got access to the computer, it propagated onto other computers on the network by using backdoor exploits like EternalBlue (What are Petya and NotPetya). Where Petya encrypted the master boot record, NotPetya encrypted files and damaged drivers without needing administrative privileges (What are Petya and NotPetya). Although it has been suspected that NotPetya's main target was Ukraine, the malware spread across Europe, North America, and Asia (What are Petya and NotPetya). Over the course of time, it has continued to prove the difficulty of containing a self-propagating cyberattack. NetPetya attacked governments, transportation, energy, and financial sectors (What are Petya and NotPetya). Attacks on infrastructure that is critical to society like energy and transportation always have harsh consequences on the hackers and the victims.

How Ransomware Attacks Windows Systems

Wannacry is a great example to use when explaining how ransomware attacks Windows systems because it is tailored specifically for Windows. Wannacry exploits a vulnerability in Microsoft's SMBv1 network resource-sharing protocol, allowing an attacker to transmit crafted packets to any system that accepts data from the public internet on port 445 (Rosencrance, 2021). Once the malware is on one system in the network, it does a port scan and finds all systems running port 445, and initiates a connection (Rosencrance, 2021). Then, a buffer overflow is used to take control of the target system and install the ransomware (Rosencrance, 2021). The malware continues to run this process and propagate across the network, also making the ransomware a worm. Petya and NotPetya ransomware are other great examples of how

ransomware attacks Windows systems. The Petya and NotPetya ransomware gained access to a system by using phishing emails that include a malicious PDF file functioning as a Trojan horse (What are Petya and NotPetya). Ransomware typically uses either an existing vulnerability or a phishing attack to gain access to a Windows system, but sometimes hackers will find exposed credentials on a network and just install the ransomware onto the network themselves.

How to Handle Ransomware on the Network

Once ransomware has already infected the network, possibly the simplest way to get rid of it is to pay the ransom; but this makes you a new target for the hackers because they know you are willing to pay. It is best to quarantine the infected systems away from the rest of the network to minimize the risk of other systems being infected. In a situation where you are unsure of how far the ransomware traveled down the network, it may be best to disconnect the entire network. Once you are sure that the infected systems are off the network, you should investigate the ransomware by reverse engineering it to find how the malware gained access and fix the root of the problem. Reverse engineering the ransomware will also allow the user to see where the malware is saved on the system, so you can check on other non-infected systems and ensure that the ransomware is not dormant on other systems. After investigation, it would be best to sanitize the system to be sure the ransomware is completely gone and reinstall the operating; and make sure to reset all credentials on the network just in case the ransomware harvested credentials.

Training Employees to Prevent Ransomware

Ransomware will continue to be a problem in our society because companies still used outdated and unsupported operating systems such as Windows XP (Ehrenfeld, 2017). There also comes the issue of companies running a service that is dependent on another service that if the

service is updated, the dependent service with no longer work properly for the needs of the company. This is where companies must add more security measures, such as segmenting the network or leaving part of the network off the internet, to avoid problems. Also, ransomware often comes onto a network through phishing attacks. Since not everybody is accustomed to identifying phishing emails, it is surprisingly common for people to get phished and accidentally download malware like ransomware onto their network.

Training professionals to identify when they are being phished and report it to the security team. Training professionals in a more technical manner is important as well, professionals should make it a habit to update their computers with the recently released security patches whenever those security patches are dropped. Network administrators should be educated properly on the dangers of malware and have knowledge of the potential consequences of having malware like ransomware on a network in order to ensure there are backups nearby just in case the network must be wiped and re-downloaded; in a case in NotPetya, this would be the only way to recover the encrypted files. Some of the best ways to prevent ransomware are to just not be an easy target. You can do so by keeping your software updated with the latest security patches, blocking known malicious ports, and educating users on social engineering attacks. It is important to be aware of risky emails and web pop-ups that lead to malware downloading. Aside from the user being aware of risky emails, it is smart for companies to filter through the emails being sent to the email servers. Emails that are sent to an employee from outside of the company should be notified that the sender is not a part of the company and to look out for phishing emails. Also, it helps the email filter to look at files sent through email to determine if the file is malicious or not. Other ways to prevent ransomware consist of having good anti-virus software on your computer and doing vulnerability assessments to ensure that

there are no known holes in your system. BitDefender, TotalAV, and Norton Anti-virus are some of the most recommended anti-virus software with ransomware protection (Best ransomware protection in 2023). It is also best to use a multi-layered approach to network security; using antivirus, firewalls, intrusion prevention systems, etc, can help prevent ransomware from getting onto the network. Another best practice is to segment the network accordingly so that in the case that ransomware does infect a system, it will stop the spread from infecting the entire network. Once ransomware has infected the network, the systems that are infected should be quarantined and analyzed, the investigators should figure out what exactly is encrypted, whether it is the hard drive or files, and figure out the best option for recovering the data.

Using Anti-Virus and Reverse Engineering to Prevent Ransomware

Using anti-virus software is great to prevent ransomware because it uses artificial intelligence and machine learning technology. Artificial intelligence and machine learning do not automatically detect malware, but they can create a model of good and bad behavior on a system and can create a consistent method to prevent bad behavior, such as malware being, downloaded onto a system (Vigna, 2019). Artificial intelligence and machine learning find the bad behavior and add the signature of the malware into a database where the next time the malware attempts to install itself on a system, it can be denied. Machine learning can take into account how many resources get used by a piece of software like CPU or memory, connections to hosts/communications, data transfer, unusual logins, and network exploitation tools to determine if a piece of software is malicious and then take further action (Vigna, 2019). It helps keep anti-virus updated to keep up with all of the new malware being released to the world and reduces the work on humans to improve the anti-malware software because humans are not required to audit every piece of software and how it affects the performance of a system. In addition to artificial

intelligence, physical developers, and cybersecurity professionals help defend and improve anti-malware by finding the ransomware and reverse engineering it in order to find exactly what the ransomware does, what it attacks, and the entire source of the problem. Reverse engineering ransomware gives professionals an idea of how to prevent malware because they can figure out the vulnerability being exploited and find a way to fix the vulnerability as well as locate the exact location of the malware and remove it. It also allows cybersecurity professionals the ability to find out who the attackers are to charge them accordingly and figure out the intentions of the malware. Professionals can reverse engineer ransomware without infecting their systems/network by using a sandbox environment like Cuckoo to analyze and inspect the malware.

Conclusion

Since ransomware was so profitable in 2022, Emma McGowan from Avast predicts that ransomware will continue to be a serious problem in the future. I side with McGowan on this point of view and I believe that hackers will continue to use scamming and using extortion methods through social engineering toward people, companies, and governments in the future. History has proved that ransomware works for criminals and is effective to extort money and information from organizations or individuals. Professionals need to constantly improve their networks, take precautions, and use anti-malware in order to do their best to prevent ransomware. The ransomware problem is far from ending. The best we can do is offer awareness to everybody in hopes that people can avoid this problem.

References

Best ransomware protection in 2023 | cybernews. CyberNews. (2023, January 11). Retrieved February 8, 2023, from https://cybernews.com/best-antivirus-software/best-ransomware-protection/

Ehrenfeld, J. M. (2017, May 24). *Wannacry, Cybersecurity and Health Information Technology: A Time to act - Journal of Medical Systems*. SpringerLink. Retrieved February 15, 2023, from https://link.springer.com/article/10.1007/s10916-017-0752-1

Nakashima, E. (2018, January 13). *Russian military was behind 'Notpetya' cyberattack in Ukraine, CIA concludes*. The Washington Post. Retrieved March 13, 2023, from https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

McGowan, E. (2022, December 9). *3 major cybersecurity predictions for the New Year*. 2023: 3 major cybersecurity predictions for the new year. Retrieved March 14, 2023, from https://blog.avast.com/2023-predictions

Rosencrance, L. (2021, September 27). *What is WannaCry ransomware?* TechTarget. Retrieved February 15, 2023, from https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware

Vigna, G. (2019, January 22). *How ai will help in the fight against malware*. TechBeacon. Retrieved March 26, 2023, from https://techbeacon.com/security/how-ai-will-help-fight-against-malware

What are Petya and Notpetya ransomware? Malwarebytes. (n.d.). Retrieved March 13, 2023, from https://www.malwarebytes.com/petya-and-notpetya

What is ransomware? www.kaspersky.com. (2022, February 18). Retrieved January 31, 2023, from https://www.kaspersky.com/resource-center/threats/ransomware