OUR Journal: ODU Undergraduate Research Journal

Volume 7 *Special Issue: Interdisciplinary Cybersecurity Research*

Article 2

2020

Understanding the Use of Malware and Encryption

Eva M. Castillo
Old Dominion University

Recommended Citation

Castillo, Eva M. (2020) "Understanding the Use of Malware and Encryption," *OUR Journal: ODU Undergraduate Research Journal*: Vol. 7 , Article 2.
DOI: 10.25778/ttj9-sr29
Available at: https://digitalcommons.odu.edu/ourj/vol7/iss1/2

Understanding the Use of Malware and Encryption

Cover Page Footnote

This research is supported in part under NSF grant DGE-1723635.

UNDERSTANDING OF THE USE OF MALWARE AND ENCRYPTION

By Eva Castillo[*]

I. INTRODUCTION

Malware is a term used to described different types of programs with the intent to cause harm to the server. Some types of malware this research intends to focus on are ransomware, backdoors, and stealers. Ransomware programs deny users access to a file until a requested fee is paid. Backdoors are programs used remotely where users can access a system from a separate system and move 'laterally'. Lastly, stealers are simply programs or people whose main objective is to steal files, information, data, and in some cases passwords. Malware is typically released into a system using one of these methods, thus encrypting the victim of the attack's data. In the case of a ransomware attack, once the system is no longer under the control of the primary user, ciphertext will often appear to alert the user that their system has been hacked and they must pay a ransom. In other cases, the victim isn't even aware of the attack. The growing issue of malware attacks is an important one to understand as threat actors and attackers seem to always be one step ahead. One way to combat and decrease chances for more attacks is to understand and be informed of what to look for as red flags when browsing the internet safely.

[*] This research is supported in part under NSF grant DGE-1723635.

II. BACKGROUND

The increase in the use of malware in cyber attacks has grown exponentially in the past decade due to the poorly managed encryption technologies from cyber security professionals and organizations. In a survey through *Cyberscoop*, 1,023 Informational Technology professionals have stated that, “encryption is allowing for some malware to surpass cybersecurity measures.” The measures to which these professionals are referring to include firewalls, secure web gateways, and anti-malware software. Hackers are able to surpass these measures by masking their malware in plain sight or typical internet traffic so that it will go unsuspected in transit. The way to make this malware go undetected is to mask it with encryption, more specifically, Secure Sockets Layer, or SSL, encryption. This type of encryption provides a link between an online server and an internet browser, or just two machines. The link between these machines allows data passed between the two to be private, and therefore, undetected. The activation of an SSL certificate on a browser will then create two cryptographic keys, a public and private key, thus making it an asymmetric algorithm. An asymmetric algorithm is any program that relies on the use of two different cryptographic keys. Private keys are used for the encryption of files and require a password in order to operate or decrypt these encrypted files. The use of a private key can only be detected is by auditing authentication logs and searching for abnormal activity.

While SSL encryption can be very useful to companies, it has also become a handy weapon in cyber attacks online, as it hides malware from cyber security tools and programs. It has been discovered that companies are actually unaware of a majority of the malware being sent to their employees. There has been some progress made in the problem of the use of SSL encryption. An inspection tool was created by A10 Networks to inspect the use of SSL malware encryption online, and thus making internet traffic slightly more secure. Still, the encryption technology being used by these cyber criminals is allowing sensitive data and intel to be transmitted between each other without a trace. Also, a company called "Zscaler" created a cloud platform that inspects the use of SSL certificates within the internet traffic of their company. In 2018, 1.7 billion SSL threats were mitigated. This detection was caught by catching newly registered domains, botnet callback attempts, and hidden phishing attacks within emails and files sent to the employees of this company. This encryption is also being used to target people and organizations for intel and money, which will be discussed in this paper.

III. RANSOMWARE ATTACKS

As mentioned previously, ransomware is the use of malware that only allows the restoration of the user's access to their system through the payment of a fee at the request of the attacker. Ransomware is basically the combination of cryptography and malware. This field of study is also typically referred to as "crypto virology." Ransomware is installed on to a user's system through a method used by attackers called phishing. Phishing is when attackers use fraudulent methods of communication to get the user to share their personal information. These attackers then use the personal information acquired to hack into the host's system which can then be infected by malicious code. This encrypts the user's data making the targeted files inaccessible to the computer's owner. The only way for the owner or victim to regain access to their files is to then pay the ransom requested. The form of encryption used on the files is most often extremely high level and can only be decrypted with a key the victim must attain from the attackers.

The form of payment most frequently used in the act is cryptocurrency, usually Bitcoin. There are other methods of payment and cryptocurrencies such as the following:

- Bitcoin: Bitcoin is the oldest and most popular form of cryptocurrency. It is the most popular cryptocurrency used in ransomware attacks because of its most simple access to victims of attacks. The ease of purchasing bitcoin increases the chance for attackers to be paid.
- Ethereum: Ethereum is the second largest market of cryptocurrency and popularity. Ethereum, specifically, is popular in ransomware attacks because of its privacy features making it harder to track down the attackers and convict them for their crimes.
- Monero: Cybercriminals are slowly making their ways to using Monero more in cyberattacks because of how private the features of this currency are.

IV. How Ransomware Works

To begin the process of attacking a system using ransomware, the attacker must first create a key that will be released along with the malware upon the attack. Next, the malware in the infected system will create a random key which is the actual part of the malware that encrypts the victim's data and files. The random key is also used to inactivate the key within the encryption to decrypt the code that is making the data inaccessible. After this, the message with directions to pay the ransom will appear and the victim will send the 'e-money' to the attacker. Once the attacker receives the payment, this will then activate the decryption key within the malware allowing the victim to regain access to their files.

A. Tips on Avoiding Attack

To combat attacks, a very helpful tip to follow is to download antivirus software to avoid cyber malware attacks. This should and can be done on all devices as it is the best opportunity to not suffer from these attacks. Also, it is very important to keep your operating system software up to date or to turn on automatic updates. The longer you wait to update devices, the more vulnerable they are left for attack. This is why users should regularly update applications and programs on devices. For extra safety insurance, it is also vital that, while online, users should not click on any links in spam or unverified emails. When storing documents, files, and information on your devices, try to backup all files in two different media forms. For example, make a copy of a Microsoft Word document in a PDF form.

B. Applications and Real-Life Examples

A real life past examples of a cyber attack is WannaCry or WCry—a cyber ransomware attack that occurred in May of 2017. This was also many people's first run-in with bitcoin. Many machines all around the world were affected by this cyber attack. The United Kingdom's National Health Services, LG Electronics, and Deutsche Bahn and others where all affected. Attackers of this incident were requesting somewhere between 300 to 600 USD for each computer infected. The total amount of money received from this ransom attack was approximately totaling to 241,000 USD.

V. ENCRYPTING A SYSTEM

Using the information attained on how ransomware attacks are carried out, this student will be thoroughly walking through the skeletal procedure for a simulated ransomware attack. The necessary materials for this attack would be two computers with Microsoft Word, encrypting software, a static IP address on all of the computers used, and a static DNS name to simplify the network. It is important to not use a router between computer HOST1 and computer HOST2 because they should solely be running their own network.

A. Procedure

To begin this simulated attack, from the HOST1 computer, the attacker would send a phishing email with an attacked file that is already infected with a virus. The document will be in a Microsoft Word document format so that the HOST2 victim can receive this email in their Outlook. The subject line of this email should contain an urgent message to get the victim to follow the steps in the email so that the attack can be carried out. If an email like this is sent to a school or company email address, they will usually have software within their servers to send emails like this one to the victim’s spam folder as to prevent these attacks from happening. Once the victim has opened the email, an error message will be displayed, making them think that the program crashed and that they must force close or exit the program. When this happens, what is actually happening to the victim is that the code within the encrypted file is being released, and thus, infecting the victim’s computer. This can be verified by having the victim check their files and seeing that the names of some of them have changed. Also, while the original copies of their files are the same, an encrypted copy is made, and the originals are deleted. When the victim eventually goes to try and open their files, a message will be displayed to their screen informing them as to what has happened to their files. In order for them to regain access to their files, they will need a private key for the decryption of their locked files. This private key, however, will only be provided once the ransom is paid.

B. RSA Algorithm

The files that the hacker has locked are encrypted using an RSA encryption algorithm, or Rivest Shamir Adleman encryption algorithm that uses two keys: a public key to lock the files, and a private one to unlock or decrypt them. The RSA algorithm typically involves the use of four steps:

1. Key generation
2. Key distribution
3. Encryption
4. Decryption

Key generation is the creation of the public and private keys to restore the files, while key distribution is the tricky aspect for the victim. Finding the key without paying the ransom is nearly impossible because its physical location can be anywhere in the world, even another country. Usually, the hacker will provide an ultimatum to speed up the ransom paying process by saying there is a time constraint to paying it or else the key to decrypt their files will be destroyed after a certain amount of time. They will provide an address so that the currency can be paid; typically a bitcoin address will be provided. Although, there are some cases when the hackers, even after the ransom is paid, won't provide the private key for the decryption of their files. There are other ways to clean an infected device, like with the help of professional computer service providers. If worse comes to worse in such a case, the next step for the victim of this attack to take would be to contact these professionals for assistance.

VI. Conclusion

Overall, it is clear that the use of malware and encryption online has presented cyber criminals with many backdoors and vulnerable firewalls. While IT and cyber security professionals have tried to create software to detect these infiltrations and malicious activities, these hackers have continued to advance their software also, thus making the threat today larger than ever before. The explanation of how ransomware is used was a perfect example of how these cyber attackers can go from small attacks on innocent online victims and citizens, to large and knowledgeable, defensive companies and organizations. The magnitude of this problem is presented within the facts from real life cyber attacks reported and the ease that is demonstrated in the simulated ransomware attack. The use of malware and encryption is no longer specialized for professionals. It is now a tool that is attainable for anyone with a device, browser, and server. At no additional cost, a cybercriminal is made and a lot of the time, can successfully attack a victim without a trace. Hopefully, with the knowledge of these attackers' motives and strategies, online users can avoid these attacks by taking the steps mentioned to browse safely and smartly.

Works Cited

"Annual Cybersecurity Report: The Evolution of Malware." *Annual Cybersecurity Report: The Evolution of Malware*, www.discover.cisco.com/en/us/acr/evolutionofmalware.

Bing, Chris. "Report: Hackers Increasingly Use Encryption to Hide Malware." *CyberScoop*, CyberScoop, 24 Sept. 2016, www.cyberscoop.com/report-hackers-increasingly-use-encryption-hide-malware/.

"Encryption Hiding Malware in Half of Cyber Attacks." *ComputerWeekly.com*, www.computerweekly.com/news/450303346/Encryption-hiding-malware-in-half-of-cyber-attacks.

"Encryption Offers Safe Haven for Criminals and Malware." *Dark Reading*, www.darkreading.com/threat-intelligence/encryption-offers-safe-haven-for-criminals-and-malware/d/d-id/1334016.

Help Net Security March 1, 2019. "Enterprises Are Blind to over Half of Malware Sent to Their Employees." *Help Net Security*, 1 Mar. 2019. www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/.

"Malware What It Is | How To Protect." Proofpoint, 18 Oct. 2018, www.proofpoint.com/us/threat-reference/malware.

"MITRE ATT&CK™." *MITRE ATT&CK™*, attack.mitre.org/.

"Ransomware: Facts, Threats, and Countermeasures." *CIS*, 18 May 2017. www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/.

"RSA Algorithm in Cryptography." *GeeksforGeeks*, 6 Sept. 2018, www.geeksforgeeks.org/rsa-algorithm-cryptography/-.

Tabora, Vince, and Vince Tabora. "Cryptography Malware = Ransomware." Hacker Noon, Hacker Noon, 4 June 2018, hackernoon.com/cryptography-malware-ransomware-36a8ae9eb0b9.

"The Most Popular Cryptocurrencies In Ransomware Attacks." *Cryptonews*, cryptonews.com/exclusives/the-most-popular-cryptocurrencies-in-ransomware-attacks-1712.htm.

"Threat Actor Goes on a Chrome Extension Hijacking Spree." *Proofpoint*, 27 Jan. 2019, www.proofpoint.com/us/threat-insight/post/threat-actor-goes-chrome-extension-hijacking-spree.

"What Is SSL?" *What Is SSL?*, 7 June 2005, info.ssl.com/article.aspx?id=10241.