The Growing Influence of Ransomware

Matthew A. Mos, MD Minhaz Chowdhury

Department of Computer Science

East Stroudsburg University of Pennsylvania

East Stroudsburg, PA, USA

Email: mmos@live.esu.edu, mchowdhur1@esu.edu

Abstract—**Ransomware is a malicious cyber-attack in which a user's files are encrypted and rendered inaccessible until the attacker receives a ransomed amount in return for the decryption key. The advanced yet unsophisticated nature of the malware allows for the development of many types of ransomware; thwarting any type of long-term countermeasure from being effective. This allows both professional cyber-criminals and novice script kiddies to operate attacks with devastating potential. With the introduction of crypto-currencies most ransomware interactions can be untraceable. This paper is directed at an overview of ransomware, the stages of a typical ransomware attack, and defense mechanism against ransomware. Diving into recent attacks, using reverse engineering and methodologies to get a core idea of how all ransomware functions.**

Keywords—crypto-virus, cryptoLocker, torrentLocker, wannaCry, NotPetya, torrentLocker

I. INTRODUCTION

Traditionally, malware has been malicious code with the primary function of placing dangerous programs without the user's knowledge. However, the malware landscape has seen a paradigm shift from nuisance and destructive malware to resilient and robust crimeware [1]. Ransomware is a resilient and powerful crypto-virus which uses the latest encryption techniques to encrypt companies' important files and demands a payment "ransom" for the decryption of their files. In worse cases, once the files have been encrypted the cyber-attacker will steal the victim's files regardless of payment. For many companies like Maersk, the largest container shipping company in the world they had to reinstall over 50,000 computers after a ransomware attacked their system [1]. These ransomware attacks can cause companies to suffer continued disruptions for daily operation.

The attack strategy behind Ransomware is one of social engineering and rapid-fire attacks, where cyber-criminal organizations will use a "shotgun" approach sending companies as many phishing emails as possible. These emails appear legitimate, offering some sort of promotion or reward for a contest won, and are sent to company employees all throughout the hierarchy and aim to install the ransomware via malicious links. Other more aggressive versions of ransomware, such as NotPetya, can exploit the security vulnerabilities of networks, no longer needing to deceive an end user [3]. The goal is to encrypt and cash out on as many companies' files as possible before gaining notoriety.

In 2016 alone, ransomware activities increased by 82 percent, nearly quadrupling in rate of occurrence and cost [3]. There was an average of 4,000 attacks per day and a total cost in excess of $1 billion paid in ransoms in 2016 alone. On average an individual attack could total up to $133.000, not including residual damages. These numbers have only increased since 2016, with ransomware becoming the most prominent and devastating form of social engineering for big companies. With ransomware now targeting phones via malicious applications the threat of data compromise is rising. This has only become more dangerous as the anonymous use of crypto-currencies such as Bitcoin for payments and transactions have made the tracking of cyber criminals a mammoth battle [1].

With all that has been said, there are a few effective preventive measures for combating ransomware. The use of these measures has proven to significantly mitigate a business's risk of a ransomware attack. In this paper there will be a dive into WannaCry, one of the most devastating ransomware attacks which affected over 150 countries in a short period of time [1]. The security research and knowledge learned from such a devastating attack are what motivate the preventative measure presented in this paper. With the rapid expansion of ransomware, and the fear that as the potency of encryption increases so will the potency of ransomware knowing how to protect a company's important information is critical.

This paper is organized as follows, Section II describes the steps of ransomware and the troubles with stopping ransomware, along with any necessary background information. Section III and beyond focus on the methodology behind ransomware and investigates the Crypto Mining side of crypto-viruses. There is a delve into defense against ransomware, and a deeper dive into the companies that have been affected by large ransomware attacks. Through reverse engineering and conquered ransomwares there is evidence of how ransomware works. Lastly, Section IX concludes the presented ideas.

978-1-7281-5317-9/20/$31.00 ©2020 IEEE

II. BACKGROUND

There are several steps that take place during a ransomware attack [1].

At the first step, the ransomware infects the user, either when they open a malicious email, visit an infected website, or download a corrupt executable.

During the second step, the ransomware creates its encryption key, this can either be from contacting a command and control server (C2), or some advanced ransomware malware are able to create their own key.

Afterwards, the ransomware stealthily begins to perform deep searches across all folders on the computer, encrypting as many files as possible.

At this point the ransomware is no longer concerned about being identified, instead a ransom screen is displayed with instruction for the victim. Displayed will state that the files on their computer have been encrypted and that if the user does not wish to lose valuable information that a ransom must be paid within a given amount of time. Depending on the type of ransomware, some may even pose as official law enforcement, or corporate company.

If the ransom is paid the malware will receive a decryption key from the command and control and begins decrypting the user's files.

Early forms of ransomware used symmetric key encryption and poorly constructed cipher algorithms. This allowed every computer affected by the same ransomware program to be unlocked using one symmetric key [7]. Later, ransomware criminals began the use of public key cryptography, a system in which two keys a public key used for the encryption of the files was only able to be decrypted by a private key held onto by the criminals themselves. Along with the use of advancing cipher algorithms ransomware became a dangerous new threat and a very difficult problem to fix.

The only thing that had helped Encryption experts crack down on ransomware at this point was the problem of how hackers were forced to collect their money through traceable means. However, with the development of crypto-currencies and the ransomware program CryptoLocker which demanded bitcoin payments a widespread epidemic had begun. First appearing in 2013 from then on ransomware criminals were now able to make hundreds of millions of dollars off victims.

Still today new variations of ransomware are still in development and on the rise in popularity and potential for cybercrime organizations. CryptoWall applies the ransomware as a Java Script, using email attachments as its method of infection. FuSob is a type of malware which affects mobile devices, meaning that no device is safe from ransomware [3]. IoT devices, database tables, and any system that can hold data is at risk [6]. With no set number of ransomware variants or set methodology behind them, the development of intrusion prevention systems for ransomware is an enormous task.

Even as defense mechanism are put in place such as Bitdefender's Anti-Ransomware Tool, highly advanced ransomware such as NotPetya is being developed. A dangerous malware which no longer requires a victim to download, or even launch it. NotPetya can spread by exploiting current backdoors and exploits already developed by other countries. NotPetya has used the M.E.Doc backdoor developed in Ukraine and used by almost every major business in Ukraine. It has also exploited EternalBlue and EternalRomance two exploits developed by the NSA that focus on cheating the SMB protocol [8]. What makes NotPetya so dangerous is that it encrypts everything, nothing is left when NotPetya malware enters the system. Worst of all the ransom displayed on the screen is meaningless, in almost all cases the damage is too severe to ever repair and when companies pay the ransom nothing is done about decrypting their files.

Although it may sound like ransomware is unbeatable, there are prevention methods out there and steps that users and companies can take to ensure they are protected from ransomware attacks.

III. METHODOLOGY

There are many examples of reverse engineering that has been done on ransomware. Over 100 different types of ransomware have known decryption keys and methods of how they enter, encrypt, and decrypt files. From this many IPS have been developed such as Bitdefender's Anti-Ransomware Tool and Cryptostalker. Along with this, Eternal Blues has developed a free scanner designed to look for the same vulnerabilities that ransomware looks for on your system with ways how to fix these holes in defense.

Anyone can be targeted by ransomware. The vulnerability of a system to a ransomware attack is determined upon how attractive the data is to the hackers perusing it, how critical the information is so that the victim responds quickly to the ransom demand, how vulnerable the security of the system is, and how well the employees at the company are trained. [6]. A major tactic of ransomware is to inflict fear and panic to the victim, the hacker wants the user to not have time to think about what they should do and instead pay the demand or face losing information or even leaking secret personal information about clients. However, not only commercial organizations are targeted, Academic organizations such as colleges and universities, Government agencies such as the police force which are time-sensitive, Healthcare, and other utilities storing sensitive patient data, and even mobile devices [6].

There is a seemingly endless amount of ways ransomware developers have come up with to get their malware onto a system. As it stands, the only part of ransomware infection that the hacker must ensure is getting the malware on the victim's computer. To do this many type of ransomware have been developed all with different methods of penetration. As with the cause of NotPetya developers have even begun to create self-sufficient ransomware capable of infecting like a worm malware. CryptoLocker.F and TorrentLocker are Trojan horse ransomware, their main objective is to create backdoors and remain hidden, pretending to be a useful until the files that will be used for encryption and the ransomware attack can be successfully sent to the victim's machine [2]. CryptoWall uses Java Script embedded in email attachments or fake website, when a user clicks on the link in the email, they are innately downloading the ransomware directly to their machine without any knowledge. WannaCry is the latest and most dangerous ransomware and targets MS-Windows and the exploits that already exist in Windows 10.

When any of these organizations are attacked the first thing any ransomware program will do is a deep dive of the system. During this dive of the system the ransomware is looking for any sensitive data. This data is then sent back to the C2 command and control server where they can sell it online to the highest bidder. The selling of this data can cost organization even more in legal damages. Organizations are paying thousands of dollars to ransomware attacks each year and in 2017, the US was the most affected country by ransomware, the country alone accounted for 29% of all ransomware infections [2].

During the encryption phase the ransomware attacks the system encrypting the user's files such as .doc .pdf .jpg .xlsx etc [1]. Any encryption method can be used but the strongest ransomware variants have been using AES-256 for their private key as in the case of WannaCry and NotPetya while using RSA for their public key. In many cases these keys are downloaded from a C2 beacon which connects the victim's computer to the hackers allowing them the ability to setup cryptocurrency payments, and the ability to give the ransomware its encryption key [4]. However, newer more dangerous versions of ransomware such as WannaCry and NotPetya are locally generating the private key onto the system itself requiring not C2 beacon. Latest variants of ransomware zeroize the target files to prevent any recovery from tools such as Photorec or Recuva which help recover lost files via meta-data and directory structures [4].

IV. CRYPTOCURRENCY

Crypto ransomware attacks come in three basic variants, asymmetric, symmetric cryptosystem based, or a hybrid of both [4]. In the first iterations of crypto ransomware many attacks used symmetric encryption with the use of one key and an encryption algorithm embedded in the malware. Today's variants no longer have the need for custom encryption algorithms and instead exploit the operating systems Crypto API functions [4]. These are available to authenticated users meaning all the hacker must do is make sure the ransomware ends up on an authenticated user for that machine. By doing so the ransomware gains all read-write-execute permissions on the system allowing the ransomware to prevent backup recovery making the attack that much more dangerous. WannaCry is a hybrid-based algorithm which locally creates its private key using AES-256 and once the encryption of all targeted files is complete will encrypt its private key with the public key making the public key the only method of decryption.

In order to create a cryptocurrency unit proof-of-work must be shown to obtain the digital currency. The way to accomplish this proof-of-wok is to compute cryptographic algorithms. These algorithms take a lot of CPU power and in almost all cases require a GPU or some other form of processing unit to complete the proof-of-work in a considerate amount of time. This is where crypto ransomware comes in; by exploiting vulnerable hosts online, hackers can add victim's machines to a crypto mining pool of devices a botnet of crypto miners. They can complete the proof-of-work much faster by enlisting hundreds if not thousands of machines to this botnet. On top of this with several hundred machines in their botnet hackers are then able to unleash DDOS attacks. The attacker does not need to worry about overheating their own system as in many cases when attempting to complete these algorithms CPUs and GPUs are overheated and overloaded.

Many devices are subject to crypto ransomware including IoT devices with onboard computing, mobile devices with access to the internet, and any other device that the hacker can exploit. A new rising trend with crypto mining has come to exploiting web browsers in conventional PC's and browser capable devices [4]. Using spearfishing devices are led to a compromised website and are immediately used to start mining cryptocurrencies. Since no malware code is running on the host machine many IoT and mobile devices are incapable of detecting any problems. This has also extended to cloud services as of 2018 [4].

V. FRAUD

In many cases as companies are dealing with criminals or cyber organizations even when ransoms are paid many companies are permanently locked out information or it is corrupted away. If a system is lost and can not be restored by backup a company must preform a cost-benefit-analysis, deciding if the price of the data is worth more than the cost of the ransom. According to research from Trend Micro, although 66 percent of companies say that they would not pay a ransom at any point, in fact 65 percent of all companies do when they are attacked [5]. Ransomware attackers try to put victims in a state of panic, however, they know that if they do not keep the price of the ransom low enough, that their victims will not pay it. Therefore, attacks will usually range between $700 to $1,500 for small to medium size companies. This way hackers can ensure that they make quick money without the company having much time to think about the cost analysis or develop a plain to combat the ransomware. The idea of sending the company into a panic stems from the idea of scareware; attackers will make malware that seems as though it has taken control of the victim's machine, while in fact, it has not encrypted their data at all. The hacker is hoping they can cause enough panic and disturbance that no actions will be taken or investigated that have a chance of combating or figuring out that they are in fact a fraud. Many companies have begun incorporating a small reserve of Bitcoin in their security plans specifically to pay ransoms. Gary Sockrider, principal security technologist at Arbor Networks, estimates around 65 to 70 percent of the time victims receive their data back [5].

VI. WANNACRY

With all that has been said about the different types and dangers of ransomware; lets now dive into WannaCry, an absolute devastating set of ransomware attacks which affected over 150 countries [1]. In the infection stages of WannaCry the attacker specifies the encryption algorithm and generates a public key which will be imbedded in the ransomware's payload. This key can also be withheld and instead stored within the attacker's botnet. WannaCry could be delivered to the victim's machine in many ways, through network exploits, URL redirects, DNS tunneling, or even a Trojan already on the machine. The major point is to make sure WannaCry is on an authenticated users account on the victim's machine, the ransomware will want full access to read-write-execution permissions. During the encryption stage WannaCry will attack specified documents mention before, first it must generate a private key locally on the machine, it will use this key to encrypt all the files deemed important by the attacker. Once the files are encrypted the ransomware will use the pay loaded public key to encrypt the generated private key making the only way for decryption through the public key. It will finally delete all shadow files not allowing the user to restore or backup the files Next C2 communication is established once the file encryption has been successful. The victim is given a notice of the encryption of their files and what they must pay. C2 communication works through a Tor network and allows the transaction of cryptocurrency in the case of WannaCry either Bitcoin or Monero to be completely untraceable [1].

VII. NOTPETYA AND MAERSK

Although the WannaCry attacks cost the entire world millions of dollars in ransom debts one ransomware that seems the most devastating is NotPetya. Almost entirely like WannaCry, NotPetya is also a crypto ransomware that creates its own private key using AES-256, encrypts all the data on the victim's machine, and displays a ransom, however, there are differences that make NotPetya a much scarier ransomware. To begin, NotPetya can spread completely independent of the hackers. Meaning the attackers not longer need to worry about how the ransomware gets on to the machine, instead the ransomware is able to exploit government exploits. NotPetya had spread throughout 50,000 Maersk computers using these same exploits. Once NotPetya had access to these computers it begins stealing important data and encrypting all files on the machine. Without being detected NotPetya had been able to steal and encrypt thousands of personal data files and important data from Maersk. The next major difference between NotPetya and WannaCry is that NotPetya encrypts the files for good. It is no longer a ransomware that encrypts for money, the monetary amount displayed on the screen effects nothing. Even if the ransom is paid not decryption key is provided and the files are corrupted beyond repair. The incident costed Maersk about $300 million dollars as they had to pay to reinstall all infected computers and other legal damages [1]. NotPetya was not a long-lived ransomware but the impact it had was devastating.

VIII. HOW TO STAY PROTECTED

Although ransomware can have devastating affects on a company there are ways to defeat it. Preventative measures such as staying up to date on patching, making sure every system is fully patched is a great way to prevent any malware from infecting a user's machine [7]. Education of staff is essential, knowing what a phishing email is, knowing not to click on links that may be corrupted, and never letting a website install another vender's software for them is knowledge that must be taught. A whitelisting program which only allows authorized programs to run is a safety mechanism that gets overlooked constantly. Make sure to never put a USB or CD from an untrusted person into your machine. Having policies and recovery plans for how to backup, restore, and respond to ransomware attacks is also an important step.

The ways to protect devices from ransomware, mentioned in this paper, are promising and applicable to various cyber security, data mining and machine learning fields. [9-20]

IX. CONCLUSION

Throughout this paper ransomware has been discussed as something that many companies fear; However, by using the protection methods demonstrated in this paper and having an awareness and knowledge of ransomware any business can combat ransomware threats. Presented are the general steps to a ransomware attack and the methodologies behind all attacks. Now knowing what these steps are and what the mindset of an attacker who uses ransomware is; the best protection is to stay informed about current ransomware threats and how to stay protected from any new ransomware variants.

With the rising use of cryptocurrencies incorporate this into the company's disaster recovery plan. As ransomware begins to target increased number of devices take care to protect all company devices including any device connected to a company email.

In the future this study could be expanded by including the possible solution to ransomware; including code taken from ransomware with a dissection more into the algorithms that are used when carrying out an attack. Ransomware is not something to be fear, it is simply another malware to be protected from.

REFERENCES

[1] A. Zimba and M. Mwenge, "A Dive into the Deep: Demystifying Wannacry Crypto Ransomware Netwrok Attacks via Digital Forensics.," International Journal on Information Technologies & Security, vol. 10, no. 2, pp. 57-68, 2018.

[2] L. Thirupathi and R. P.V.Nageswara, "Understanding the Influence of Ransomware: An Investigation on Its Development, Mitigation and Avoidance Techniques.," Grenze International Journal of Engineering & Technology (GIJET), vol. 4, no. 3, pp. 123-126, 2018.

[3] D. J. Oberly, "Best Practices for Effectively Defending Against Ransomware Cyber Attacks," Intellectual Property & Technology Law Journal, vol. 31, no. 7, pp. 17-20, 2019.

[4] A. Zimba, "Recent Advances in Cryptovirology: State-of-the-Art Crypto Mining and Crypto Ransomware Attacks.," KSII Transactions on Internet & Information Systems, vol. 13, no. 6, pp. 3258-3279, 2019.

[5] J. Fruhlinger, "Ransomware explained: How it works and how to remove it," CSO, 19 Dec 2018. [Online]. Available: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

[6] J. A. Martin, "Who is a target for ransomware attacks," CSO, 14 JUL 2017. [Online].

Available: https://www.csoonline.com/article/3208111/who-is-a-target-for-ransomware-attacks.html.

[7] R. A. Grimes, "How to prevent ransomware infection and recover if you're hit," CSO, 24 JAN 2017. [Online]. Available: https://www.csoonline.com/article/3160766/the-evolution-of-and-solution-to-ransomware.html.

[8] J. Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now," CSO, 17 OCT 2017. [Online]. Available: https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.

[9] M. Chowdhury and K. Nygard, "Machine Learning within a Con Resistant Trust Model", The 33rd International Conference on Computers and their Applications (CATA 2018), March 19-21, 2018.

[10] M. Chowdhury, K. Nygard, K. Kambhampaty and M. Alruwaythi, "Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm", The 4th Annual Conference on Computational Science & Computational Intelligence, December 2017.

[11] M. Chowdhury and K. Nygard, "An Empirical Study on Con Resistant Trust Algorithm for Cyberspace", the 2017 World Congress in Computer Science Computer Engineering & Applied Computing, July 17-20, 2017.

[12] M. Chowdhury and K. Nygard, "Deception in Cyberspace: An Empirical Study on a Con Man Attack", The 16th Annual IEEE International Conference on Electro Information Technology, May 14-17, 2017.

[13] M. Chowdhury, “Deception in Cyberspace: Con-Man Attack in Cloud Services,” Ph.D. dissertation, Dept. of Computer Science, North Dakota State Univ., Fargo, ND, 2018. Accessed on: March. 25, 2020. [online]. Available: https://library.ndsu.edu/ir/handle/10365/28761

[14] R. Gomes, M. Ahsan and A. Denton, "Random Forest Classifier in SDN Framework for User-Based Indoor Localization", the 2018 IEEE International Conference on Electro/Information Technology.

[15] M. Ahsan, R. Gomes and A. Denton, "SMOTE Implementation on Phishing Data to Enhance Cybersecurity", the 2018 IEEE International Conference on Electro/Information Technology.

[16] R. Gomes, A. Denton and D. Franzen, "Comparing classification accuracy of NDVI with DEM derived attributes using multi-scalar approach in Geographic Information Systems," 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 2019, pp. 249-254,

[17] M. Ahsan, R. Gomes and A. Denton, "Application of a Convolutional Neural Network using transfer learning for tuberculosis detection," 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 2019, pp. 427-433.

[18] M Ahsan, K Nygard, "Convolutional Neural Networks with LSTM for Intrusion Detection," Proceedings of 35th International Conference on Computers and Their Applications, vol 69, pages 69--79.

[19] M. Chowdhury, J. Tang and K. Nygard, "An Artificial Immune System Heuristic in a Smart Grid", the 28th International Conference on Computers and Their Applications, 2013.

[20] M. Chowdhury, “An Artificial Immune System Heuristic in a Smart Electrical Grid,” M.S. Thesis, Dept. of Computer Science, North Dakota State Univ., Fargo, ND, 2014. Accessed on: March. 25, 2020. [online]. Available: https://library.ndsu.edu/ir/handle/10365/27236.