A state-of-the-art analysis on ransomware

Diogo Gomes
Network Engineering Master's Degree
Universidade do Porto
up201805367@up.pt

Rogério Rocha
Network Engineering Master's Degree
Universidade do Porto
up201805123@up.pt

Telmo Ribeiro
Computer Science Master's Degree
Universidade do Porto
up201805124@up.pt

***Abstract*—There is a crescent in number of ransomware attacks, its complexity and in the ransom values.**

This paper will visit the ransomware's origins through Joseph Popp's AIDS Torjan. It will explain the basic thought behind a generic attack. Mention the most prominent types of ransomware aided by examples of still active malware. We will discuss the EternalBlue exploit and how it still is used by nowadays ransomware. Finally, we present a set of guidelines in order to improve safety against this practice.

***Index Terms*—ransomware, state-of-the-art, AIDS trojan, crypto, locker, eternalblue, mitigation, crypto currency**

I. Introduction

With the world getting more technology bounded, cyber-criminals have the tools and the landscape to exercise practices like blackmail, extortion and theft, traditional crimes that are now a constant in the digital world. These can range from relatively small attacks that target common individuals to large automated attacks aiming government systems and enterprises. Between the attack methods, ransomware stands out, as the amount of attacks per year are rising and, as of 2021, it made headlines when enterprises like Kaseya, Acer and Quanta were targets of this malware.

The first instance of a ransomware is known as AIDS Trojan/PC Cyborg virus [1]. This malware would be introduced into systems through a floppy disk called the "AIDS Information Introductory Diskette", that would be physically mailed to a number of people/institutions. After the break-in phase, this ransomware would hide directories and encrypt file names on the C: drive. Then, it would ask the victim to 'renew the license' and contact the PC Cyborg Corporation for payment, which would involve sending $189 to a post office box in Panama. This ransomware attacked in 1989, and laid the foundation for a market that would just keep rising until today.

In modern times, the steps a ransomware often takes during its operation can be traced back to Joseph Popp's first instance, however, the particular way that each step occurs has changed drastically as the attacks are evolving in complexity every year [2], aided by better encryption methods, networks of proxies and command and control servers (C&C) over TOR and crypto currencies.

Acquiring and deploying such an attack became a much more easy to accomplish task, even for criminals with little to no programming skills. This is driven by the fact that ransomware are primarily sold as part of a toolkit [1]. This toolkit often contain at least two components: a malware that searches for vulnerabilities in the system, such as deprecated protocols and patches, named the Exploit Kit, in order to aid the deployment and spread of the attack, and the ransomware itself. It can have a graphic interface for ease of use and at times even support.

II. Ransomware Attack Model

(i) The attack will often start with social engineering. Common weak points are emails and social media websites [3]. As such, they are used to lure the victim into clicking on an URL or attachment, since many users lack the knowledge to identify such tactics. Although these methods are still the more frequent ones being used, ransomware syndicates will now use different and more complex exploits when approaching enterprises. In this category we have REvil, a ransomware strain that almost deals with enterprises and although it is not a frequent threat, it was the one responsible for the three cases mentioned in the Introduction.

(ii) Upon clicking, either the user will be redirected to an infectious website, also known as landing page, or the attachment will download the malware. Since 2016, there is a trend where the criminal will use Word file's macros, with the objective to download the ransomware [3].

(iii) Either the website or the attachment contains malware with the purpose to identify vulnerabilities in the victim's system, the Exploit Kit with examples being Magnitude, RIG and in the past the infamous Angler. The Exploit Kit will search for deprecated patches and protocols, that were not updated yet, and will use them as the gateway to inject the ransomware in the computer and spread it through the network.

(iv) At this stage, the ransomware is delivered to the system through the compromised protocols.

(v) At some point after the infection, the ransomware will connect to the command and control (C&C) server to retrieve the necessary keys so that it can start the encryption process. A frequent strategy used since the AIDS malware is to wait a fixed amount of time or reboots so it can keep a low profile. This low profile buys time so the ransomware can spread through the network and it helps to confuse the user about the when and how the former got infected [4]. Nowadays, it is usual practice for the ransom note to redirect the user to a webpage on TOR.

(vi) This is the moment when the victim fully understands what happened, since a message will ask for the ransom and often state deadline to the payment where otherwise the files will be deleted. Here social engineering can make itself present again through blackmail or pressure about illegal activities that the hacker supposedly found on the victim's system. The message would state what would happen to the victim if the same was prosecuted and judge guilty as a form of extra pressure.

(vii) The favorite payment methods varied through the years but since Bitcoin's early stages it was adopted as the number one option. It is easy to understand what advantages this currency can bring to the ransomware market, since the way it operates offers a set of protections the cyber criminals crave for. In recent years, crypto currency as a whole have been used in this segment [5].

III. Types of ransomware

The model described serves to explain the general idea behind a ransomware attack. Although there are common practices, which allow for the connection between different malware's implementations under the more global name of ransomware, those implementations vary enough to be grouped into categories.

The kind of privations the user is submitted to, is what defines the category of the malware.

The following ransomware were active threats as of 2021, except for WannaCry [6].

Crypto ransomware will encrypt certain file extensions, which may vary from ransomware to ransomware, considered sensitive and/or vital to the user, when the task is completed it will notify the former through the ransom note. In this category falls malware such as GANDCRAB, Cerber and WannaCry. GANDCRAB was the most active ransomware as of 2021 and works as a crypto ransomware's textbook example. Cerber, which was debuted in March 2016 is still a major threat and very active. This malware is known for not encrypting files in machines of ex-soviet's countries and doubling the ransom if the former was not paid before the deadline. WannaCry, as of 2017 already had affected more than 150 countries and 250000 computers through the EternalBlue exploit.

On the other hand, locker ransomware often leaves most of the files unencrypted, encrypting only the ones needed to keep the user without access to the machine. This objective is commonly accomplished by reducing/changing the User Interface or through removing the functionality of some I/O devices. Malware such as the Locky, Reveton and Petya are members of this category. Locky was first deployed in 2016 and is known for being able to behave as a crypto ransomware if that's the desire. Reveton first appearance was in 2011 and used to lock the computer mentioning being a police's service and prompting the user to pay a fine, threatening that otherwise, the user would be persecuted in court. Petya, on the other hand, modifies the Master Boot Record and encrypts the locations of various file and then blocking the system.

IV. EternalBlue

Although WannaCry is no longer the threat it was, the EternalBlue exploit still lives on in modern times. It targets Windows's machines that did not apply the MS17-010 patch, and as so, it preys on a Microsoft's compromised implementation of the Server Message Block, allowing the malware to spread over LAN [7]. The first version of the Server Message Block mishandles specially crafted packets from remote attackers, allowing them to remotely execute code on the target computer. The NotPetya strain still uses this exploit as a mean to spread through networks, since there are still a plethora of devices not patched, as there are Exploit Kits looking out for them.

V. Mitigation

The encryption methods used nowadays, such as RSA and AES, are effective tools, meaning that the task of decrypting a file without the key is an intractable problem, as such, current tools as the provided by McAfee and AVG often rely on the criminal's mistake [1]. Armed with that knowledge, when the system is already partially or fully encrypted, there is no solution apart from formatting the machine and uploading the files from a safe stored backup, when that is the case.

As of 2021, it was known the most common ways to get infected with this type of malware were through email's URLs and attachments, websites (apart from the ones being mentioned), social media and USB sticks, in that order [3]. Infected emails alone are the reason for more than 50% of all infections and 11% of phishing email's recipients click on the attachment, as of 2017 [4]. The avoidance of emails and USB sticks coming from unknown and/or unexpected sources and the continual user's attention when on unfamiliar websites, are guidelines we can safety assume, will reduce the amount of cases.

When looking to the data provided, it is with ease we confirm the typical user is not well versed on the Internet's risks. As such, programs that aim to teach common risks and good practices are strongly suggested as their continual development and implementation.

VI. Related Work

Different studies on ransomware attacks, their evolution, impact and mitigation have already been documented. In this section we will summarize and discuss different papers that we analyzed so we could write this state-of-the-art on ransomware.

A. Internet of things and ransomware: Evolution, mitigation and prevention

The main focus of this paper is to provide awareness to researchers and practitioners about the severity of ransomware attacks by showing what it is, how it works, and what can be done if we are a victim. This is made possible by providing a detailed picture of ransomware attacks in the context of Internet of Things.

Internet of Things (IoT), refers to the interconnected network of devices, actuators, software, etc. that store and exchange information. The IoT is a rapidly growing phenomenon, mainly due to the need of this exchange and storage of information. But this growth of IoT brings along different challenges, being on of them ransomware. Ransomware exploits the exchange of information to get to the victims and affects the stored information.

B. Evolution of Ransomware

From early-day scams, to the extortion implemented by current ransomware, this paper aims to not only inform about this attacks and their evolution through time, but also give some perspective on how the lost data can be recovered, and the financial impact behind a ransomware attack.

The Internet is a highly connected network, serving millions of users and thereby creating a target-rich environment. So, in essence, a collection of communication protocols that support the propagation and delivery of software, which also includes ransomware. Many tools and encryption libraries exist, that lowers the skills entry level required to carry out an encryption attack. Electronic currencies (such as Bitcoin) enabled criminals to monetise their activities through an anonymous payment method. Nowadays we store important business and personal details electronically

Three data recovery methods are suggested: paying the ransom, using decrypting tools and services and the backup strategy. General advice is don't pay the ransom. However, when all else fails some victims see a 200$ or 300$ as the most straight forward option to retrieve irreplaceable data, even though the victims have no guarantee of recovering all data.

When a robust encryption algorithm is implemented in ransomware, data retrieval is intractable unless victims have a backup system. This said, these ransomware creators are not infallible and poor decryption key management has led to investigations that have found these keys, which were then used to develop decrypting tools to reverse the ransomware. Some examples are the McAfee and AVG decrypting tools. Having a backup strategy is still the best way to recover data.

C. Comprehensive Survey on Petya Ransomware Attack

One of the major ransomware attacks in recent past is the Peyta ransomware attack. In this paper, we are introduced to ransomware, how does it compare with other types of malware, differences between types of ransomware, but we also get some awareness about Peyta, how it works and what exploits it uses.

Petya ransomware was first witnessed in March 2016 and again attacked with the new variant in June 2017. The first infections began in Europe, mainly in Ukraine. Other than this another 64 countries also got affected including Brazil, Germany, Russia, India and United States.

The working of this ransomware is by modifying the Window's system's Master Boot Record (MBR), which cause the crashing of the system. This ransomware is distributed via phishing e-mails and for the further distribution of the ransomware within the network the malware uses: MS17-10 vulnerability, which allows remote code execution by the attacker. Petya also uses remote access to Windows Management Instrumentation (WMI). To make the attack analysis harder system logs are cleared. It writes its code to Hard Drive MBR and initiates system reload, adds reload commands to Windows planner. And when the system reloads it shows as it is repairing the sector of the hard disk but in the backend it's actually encrypting the Master Boot Table, which will later deny access to files. If you try to stop the encryption process by turning off the system, then also it will resume its encryption process when again started from where it was shut down as it also saves the log along with encryption.

D. On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems

This paper goes through the motivations and concepts of a crypto ransomware, the role of the crypto currencies, how are the ransomware attack campaigns done with examples and then the economic significance of this ransomware attacks and the mitigation strategies.

The major motivation towards attacking businesses and organizations as opposed to targeting single users is the high expected turnover. Recovery efforts tend to cost way much more than the demanded ransom for big enterprises as was the case of the city of Atlanta which spent over $2.6 million on emergency efforts in the aftermath of a ransomware attack. Even after paying the ransom organizations not only have a guarantee that the data will be retrieved, but also have to handle high downtimes which cost loss of revenue and reduced productivity, having huge economic impact.

Like most cybercrime activities, the ultimate goal of any ransomware campaign is to receive money. Before crypto currencies, the attackers generally required victims to pay the ransom via money transfer agencies or deposit the money directly into a specified bank account.This transactions had high transparent traceability owing to the identity associated with the participants. Because of this, cybercriminals had been looking for an anonymized way of getting the money, and that's where crypto currencies come in. Crypto currencies are almost impossible to precisely pinpoint who participates in the transactions. The crypto currency system is a decentralized ecosystem which operates independently of a third-party intermediary like a central bank. Thus, the digital money can be secretly converted into fiat money through a third party which is very difficult to trace. These features attract cyber criminals and are thought to fuel the ransomware business model.

VII. Conclusion

In light of the recent boom in technology, ransomware has developed to be one of the greatest cyber security threats. Not only is it very hard to detect before hand but nearly impossible to dissipate once it has taken control over a system. The Internet has created such an ecosystem that allows criminals to execute these types of attacks anonymously, thanks to crypto currencies, and with high monetary returns if the attack is successful, and to add up to all of this, the so called 'tool kits' have helped to entice criminals with little to no knowledge in scripting to also execute these attacks. Couple that with the shocking truth that most of the Internet users aren't aware that such threat exists and you've got a recipe for mass spread of the malware.

References

[1] P. O'Kane, S. Sezer and D. Carlin, ”Evolution of ransomware”, IET Networks, vol. 7, no. 5, 2018.

[2] SOPHOS, ”The state of ransomware 2022”, available at https://www.sophos.com/en-us/content/state-of-ransomware, 2022

[3] M. Humayun, N. Z. Jhanjhi, A. Alsayat and V. Ponnusamy, ”Internet of things and ransomware: evolution mitigation and prevention”, Egypt. Informat. J..

[4] McAfee Labs, ”Understanding ransomware and strategies to defeat it”. available at https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-understanding-ransomware-strategies-defeat.pdf, 2017

[5] Zimba A., Chishimba M. ”On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems.”, Eur. J. Secur. Res. 2019

[6] VIRUSTOTAL, ”Ransomware in a global context”, available at https://www.virustotal.com/go/ransomware-in-a-global-context-2021, 2021.

[7] ”Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN”. ESET North America. Archived from the original on May 16, 2017. Retrieved on October 21, 2022.

[8] J. S. Aidan, H. K. Verma and L. K. Awasthi, ”Comprehensive survey on petya ransomware attack”, Proc. Int. Conf. Next Gener. Comput. Inf. Syst. (ICNGCIS), Dec. 2017.

[9] Irwin A., Turner A., ”Illicit Bitcoin transactions: challenges in getting to the who, what, when and where”, J. Money Laundering Control, 2018