Ransomware: stages, detection and evation

Yus Kamalrul Bin Mohamed Yunus
Faculty of Computing
College of Computing & Applied Science
Universiti Malaysia Pahang
Kuantan, Pahang, Malaysia
yus.kamalrul96@gmail.com

Syahrulanuar Bin Ngah
Faculty of Computing
College of Computing & Applied Science
Universiti Malaysia Pahang
Kuantan, Pahang, Malaysia
syahrulanuar@ump.edu.my

***Abstract*—Ransomware attacks has been increasing lately with companies suffer monetarily, wasted business opportunity and wasted time. Big companies are now targeted as they are more profitable for ransomware threat actor. This paper discuses on stages of ransomware attacks starting from reconnaissance to extortion. It also discusses on steps that organization should take to prevent ransomware attack and several detection methods for ransomware. Other than that, it lists anti-analysis and evasion method used by ransomware to evade detections. Lastly, it discusses the latest ransomware attacks.**

Keywords—ransomware, detection, evasion, stages

I. INTRODUCTION

Ransomware as its name implies is a type of software use to extort its victim for ransom. It is categorized as a type of malicious software that is widely known as malware. Ransomware was first discovered in 1994 and was named AIDS[1]. The name was derived from attack method employed where a biologist mailed 20 000 infested floppy disks labelled "AIDS information introductory diskettes" to attendees of World Health Organization AIDS conference. It operates by hiding directories and encrypt files in C:/ directory rendering the operating system unusable. This was the start to an evolving threat to companies and IT professionals. Till date, ransomware has been used to attack various industries including transport, telecommunications, financial and health services[2].

Security researchers and companies regards 2017 as the worst year in ransomware attacks. Most notable attack that year was WannaCry ransomware that spread across the globe infecting 300 000 devices across 180 countries that cost USD$4 billion[1] in lost ranging from home user to time critical infrastructure. Ransomware typically collect ransom through anonymous and hard to trace payment method such as prepaid cash card and cryptocurrency. Since its introduction in 2009 by Satoshi Nakamoto who remain anonymous till date, the idea of using decentralized, peer-to-peer payment method had been eyed by threat actors. Today, bitcoin is the most used payment method utilized by threat actor followed by Monero cryptocurrency that is mined by attacker in Cryptojacking attack. Payment made will enter a public cryptocurrency wallet, upon receiving it, threat actor will either transfer the cryptocurrency to private wallet or physical wallet making the process of tracing the payment impossible.

Ransomware works by utilizing several activation mechanisms. These mechanisms are a trigger to start the attack. The mechanism ranges from user input to remote activation[3]. Ransomware that uses user input will wait for certain action done by user to activate the attack. This can be user clicking certain folders or after user restart their system. Ransomware also can be activated through hidden content that will activate when certain conditions were met such as activation date or user geographical location. Attackers use remote activation by contacting the malware through command-and-control server. This server is hidden in the dark web through TOR network.

TOR network is an open source network that is used to protect user identity and privacy[4]. It was designed by United States Naval Research Laboratory employee to protect intelligence communications online and later the code was released to public under a free license. Communication in TOR network is practically untraceable as it uses onion routing that encrypt communication and randomly bouncing user between relays that is spread around the world. Although it has weaknesses such as consensus blocking, sniper attack and circuit fingerprinting attack, it is still a choice for attacker. Most ransomware uses TOR network to communicate with command-and-control server. Onion routing protects the connection from surveillance while hiding device IP address of said server[4].

Ransomware can be categorized in many ways either by its attack method, type of ransomware or encryption used during the attack. Most discussed category of ransomware are locker ransomware and crypto ransomware. Locker ransomware prevents user from accessing their files by denying user from accessing their desktop. Ransom needs to be paid for user to regain their access. It uses simple method that can be remediated by technical user and the removal of this ransomware does not affect the data in system. Crypto ransomware on the other hand encrypts all data in target machine except for operating system data. To decrypt those data, user need to obtain decryption key from threat actor by paying ransom. Some variant of this ransomware will delete data as time passes to intimidate user to pay the ransom. Some will release the data to public if ransom is not paid after specified time. It works by silently search for important data using file extension as a clue after installation. Upon having those data, it starts encrypting it. It does not require administrator privilege to start the encryption process as it depends on current permission assigned in the victim device. The search for important data can start from local disk and can be extended to other connected drive including network drive[1]. After encryption complete, ransom note will pop on victims' screen showing countdown timer with ransom demand. Some sophisticated ransomwares are location-aware where it targets victims according to their geographical location.

Survey by Sophos, a cybersecurity company on mid-size organization across 30 countries conducted in early 2021 shows that 37% of its respondent organization was hit by ransomware last year. 54% of victims' devices managed to be encrypted by the attacker. 96% of those victim got back their data[5]. The survey averages the ransom paid to USD$ 170

404. In average, only 65% of data encrypted can be recovered. This shows that paying ransom does not solve the problem. Total cost bared by the victims including downtime, device cost and ransom was USD$ 1.85 million. Although the number of attacks decreased, the cost is devastating as attacker now focus on larger organization[5].

Fortinet, another cybersecurity company indicates that there is a steady increase in ransomware attack involving data exfiltration and subsequent threat to release data to public if ransom is not paid[6]. Major tactics used by attacker includes phishing email, software vulnerability and exposed services such as remote desktop protocol (RDP). Phishing email with Covid-19 related details was targeted to end user, research firms and healthcare facility as a mean of ransomware propagation[7]. On the other hand, European Union Agency for Cybersecurity (ENISA) recommends organization to use Virtual Private Network and stating that usage of Remote Desktop Protocol is a high risk[8]. According to ENISA, there is more than 800 000 systems with RDP reported being unpatched, among them are IP address range from Microsoft Azure data center.

Although ransomware attacks on mobile phone is increasing year by year, this paper only focuses on ransomware attacks that occur in Windows platform, mainly personal computers. This is because attacks that occur in this platform is getting more targeted and specific rather than previous attacks that is random and scattered. This can be noticed in several recent attacks that occur in North America and Middle East region.

This paper was written to explore what are the stages of a ransomware attack while summarizing how a ransomware is detected in a system and how ransomware evade from being detected. This paper also highlights strategies that is implemented by organizations to prevent and reduce the chances of being attacked by ransomware.

The rest of the paper is structured as follows. Section II lists the stages of ransomware attacks starting from scouting to extortion. Section III lists the prevention strategy and detection method. Detection strategies are steps that can be taken by companies to prevent ransomware attacks while detection methods are some of the methods used by researcher to detect ransomware. Part IV lists anti-analysis and evasion techniques used by ransomware to avoid detection. Finally, part V lists latest attacks of ransomware.

II. STAGES OF RANSOMWARE

There are several common steps taken by threat actor in order to infect a system with ransomware. These steps were discovered by researchers and security companies. These steps were then either be summarized into several short stages or elaborated into a long number of stages. This is due to their current research or observation of ransomware and threat actors. Some threat actors take as simple route, and some took complex steps to deploy their attack.

A. Reconnaissance

This step is only taken if the attack is targeted to specific target. Threat actor will do a reconnaissance of the organization services, device, operating system, software, type of network device, security devices and more. This was done in order to find the best way to attack. Threat actor will then search for any vulnerabilities associated with the information gathered. Some threat actors may already have a zero-day vulnerability that they use in their attack. Therefore, the reconnaissance is only to gather information if the vulnerability is patched or to find a weak spot for them to use to deliver the attack.

B. Distribution

In this stage, after a weak spot was found by the attacker, it is used to deliver the attack. If the attack is not specific to an organization, many distributions method can be deployed by the threat actor. One of the most popular method is through phishing email. A professional looking email with a very convincing email is often used in an attack. Year 2020 shows high phishing email send with Covid-19 theme ranging from the availability for vaccine trial to message from Center for Disease Control on Covid-19 update. Some targeted attack use Covid-19 company policy update as a mean to send illegitimate e-mail to infect user system with ransomware. Other than this, drive-by download is also a popular method[9].

C. Execution

In this stage, several events occur. As a start, the ransomware is successfully installed in the attacked system. If the attacker needs to find further information, other tools will be downloaded to achieve this. The ransomware will go through the local drive to search important documents by searching for specific file extensions. After traversing the local drive, it will spread itself into the network infecting other devices and continue the search process. Upon Completing the search, the important documents will be uploaded to the attacker. The documents will either be uploaded to the command-and-control server or other predetermined server. This process can take days, weeks and sometime months[10].

A few ransomwares at this stage can also propagate the network to find backup files and destroy them to maximize the effect of the attack. Victim later will not be able to recover their system and is at the mercy of the attacker.

D. Encryption

The encryption of systems affected by the ransomware will start. It will connect to command-and-control server to create encryption key pair. Some ransomware can achieve the process in an offline device. It will also hijack system resources and lock the system[9].

E. Extorsion

Upon completing the encryption process, the ransomware shows ransom note on the victims' screen with payment instruction. It also contains time period before the deadline of ransom payment ends. Some ransomware gradually delete file in victim system to pressure them. If the victim refuses to pay, either of these several scenarios will occur. The ransom amount will increase, victim's data leaked to public or complete data destruction.

III. PREVENTION STRATEGY AND DETECTION METHOD

Prevention strategy are steps that can be taken to thwart ransomware attack or at least delay the attack. Ransomware commonly infect systems with unpatched vulnerabilities and organization that have poor cybersecurity awareness.

Implementing a good backup strategy is important to the survivability of affected systems[11]. Having a regular backup can save time and resources during a ransomware attack as much energy can be redirected to prevent data leakage by

attacker while continuing organization operation. As seen before, there are malware that can find and destroy backup data, therefore, having a cloud backup and a cold storage backup is important. Device that stores those backup files should not be directly connected to main networks. It is better is the system is airgap.

Eliminating remote access is one of the recommended actions as this protocol do contain vulnerability that is a threat to organizations. Administration interfaces should not be connected to primary network environment[7]. They should have a dedicated plane in order to prevent organization from collapsing during an attack. If administration interfaces were encrypted by ransomware, the organization will have a massive loss of time and the cost to recovering them is high. If the use of remote access is a must, limit its usage and limit administrator access while regularly patching the system.

Network segmentation is one of the important steps during network planning as it can save the whole company during an attack[12]. Segmented network prevents attack from spreading from one area of the organization to the other. Separation between Information Technology (IT) network and operations network can save the company from shutting down its operation during an attack. As the IT network is separated and unaffected by the attack, they can focus on minimizing the number of affected devices.

Cybersecurity training should be conducted regularly[11] with user understanding of the material is the focus rather than having a training where user is not concentrating. Hands on training in identifying a phishing email can help user to understand the differences between a legitimate email and a phishing email. The training can also show a live example by security professional on how the attack looks and what its affect are so that user is aware of the consequences of those attacks.

While organization focuses on prevention strategy, researcher is focusing on detection method. There are several well-known detection methods such as behavior based, signature based, and machine learning based.

Behavior based observe in real time changes of user files and data[13]. UNVEIL is a method that generate an artificial environment mimicking a typical user environment while detecting lockers. It monitors activities system-wide and not focuses on a certain section. It set callback on each I/O request and monitor the buffer data entropy as well as file access pattern for a activity that looks suspicious. The pattern includes read, write and delete.

Signature based create a signature or fingerprint for each threat to help it detects the presence of those threats in the system. It is the standard way in detecting malware. When a detection program run in a system, it creates a signature of every file it scans. In order to detect the presence of ransomware, the program compare the signature of ransomware with the signature of the file it is currently scanning, If the signature matched, it detects a ransomware, if not, it will continue to scan other files. The drawback to this method is it only can detect ransomware that has been detected before, if there is a new ransomware or zero day, it is unable to detect those threat.

Machine learning based uses a training model to detect presence of ransomware[2]. This process involves 2 steps namely training phase and testing phase. Training phase is where the model is trained from feature set. Upon completion of the training phase, testing phase commence. It uses the model generated in training phase to detect threat in the system. There are several drawbacks to this method. First is attacker can manipulate the output of training phase and this is called as classifier manipulation. Other than this, biases and overfitting may occur during model creating and training phase.

IV. Anti-analysis and evasion

Ransomwares utilize multiple evasion technique to avoid detection during an attack. This to ensure that their attack is successful, and the attack can be deployed in other device and be utilized longer without the need to change its code or write a new ransomware. Till date, many ransomwares evolve and changes its code to prevent detection and to utilize new vulnerability.

One of the well-known technique and a technique that is still widely used is code obfuscation[14]. Obfuscation can appear in 2 form which is polymorphic and metamorphic obfuscation. Polymorphic obfuscation may create several decryptor engine. I make changes to the default encryption settings as well as changing the decryption code. The virus code does not change rather the encryption alters only its appearance. Metamorphic uses permutation engine to mutate its code body. Rather than hiding behind an encryption, it alters itself. It adds unnecessary code sequence to its source code or changing the code sequence. The altered version is the recompiled and executable is created. It looks different from the original version.

Modern advance ransomware can detect if they are in a virtual machine or in an analysis environment. It will then conduct several actions to hide itself from detection. Some may suspend its process and hide by going into hibernation mode. Some will abort any code downloaded from command-and-control server or any remote device to make the network appears normal. Some will cut its connection from command-and-control server to achieve this.

Some ransomware will use steganography in order to evade detection. It will bind itself to system process or user files. During contact with command-and-control server, the malware can also be instructed to download and view images from other location. Upon downloading those images, it will extract command from those pictures and perform the commands.

Advance ransomware encrypt its network traffic making other programs unable to scan those packets. While this method works, advance intrusion detection system uses a strict rule when allowing connection to went through its scanning process.

V. Latest attacks

Ransomware attacks is becoming more and more prevalent in these years starting from fast propagating attack such as WannaCry to ransomware treated as a business in Ransomware as a Service (RaaS) by several threat actors. The most discussed of RaaS group is DarkSide due to its attack of United State pipeline company, colonial.

A. DarkSide

Ransomware as a Service has been in the talk of researcher and security professional alike for some time now. Recently, this was being discussed in society due to an attack perpetrated

by DarkSide who attacks a pipeline company, Colonial. This threat actor surfaced in year 2020 and became a topic now due to several claims made by the group.

This ransomware surfaces in august 2020 and already claimed hundreds of victims. They primarily target large organization with monetary gain in mind. It uses SALSA20 and RSA-1024 encryption to encrypt user systems while demanding ransom ranging from USD$ 200 000 to USD$ 2 million for the decryption of file[15]. This categorizes the ransomware as a cryptolocker as it locks the user from accessing their files and it encrypts user's data. They claimed to have the fastest encryption and decryption methods in the market. They use double extortion method as they encrypt data and ask for ransom, they also exfiltrate targets data and threatened to release those data. Their targets were English speaking countries while avoiding former soviet countries such as Russia, Ukraine and Armenia. They achieve this by checking system and user default language.

While carrying those attacks, they also offer services to other threat actors. They offer their platform in tandem with Software as a Service model. They have a business-like professional dashboard for their clients. It also contains a payment gateway that uses bitcoin as payment method for their client to pay fees as agreed between them.

They put forward several code of conduct for themselves and their client. Some of them are by no means any attack should be made on hospitals, schools and governments[16].

This attack sparks panic to several states in United States of America as the company is one of the largest pipeline operators in the country. It carries 100 million gallon of fuel daily. The attack affects the business side of the company rather than the pipeline system itself, but the company took certain systems offline to contain the attack. Consumer starts hoarding fuel causing fuel shortage that cause further panic in the area affected. Other than that, 100 GB of data were taken hostage by the attacker causing the company to pay ransom of 75 bitcoin which worth 5 million dollar at the time. This attack demonstrates that a ransomware attack can affect a company financials, reputation and can cause problems for people who is directly dependent to the company.

B. Agrius

Agrius was observed by SentinelLabs operating in Israel starting in 2020[17]. It was deployed as a destructive wiper that wipes user data while masquerading as a ransomware. They extort user by claiming they stole and encrypt user data. One of their wiper was then evolved into a full-fledged ransomware.

This group utilizes Virtual Private Network (VPN) to access web facing applications. They either deploy webshell or access target by using their targets vulnerable VPN solution. They then use those shells to tunnel RDP traffic. On devices that is attractive to them, they deploy a custom malware that is a backdoor to exfiltrate data and deploy additional malware.

As the attack is believed to be backed by a nation state and is attacking another nation state, the impact of this attack such as number of affected devices, monetary loss and data loss was not disclosed as of the time this paper is written.

VI. CONCLUSIONS

This paper provides general stages of a ransomware attack. Although ransomware attack stages vary from one researcher to another, the main viewpoint is still near to each other. Th attacker will start with reconnaissance, then spread itself in the network and search for important files and after acquiring it, the system is locked and encrypted. On the other hand, ransomware can be detected by using several methods namely behavior based, signature based and machine learning based methods with machine learning methods is being explored ever more by researchers. While that is in progress, attacker equip their ransomware with evasion technique such as code obfuscation and anti-analysis methods while introducing new methods in iterations of their ransomware attacks. This paper provides details on current ransomware attack and details of the attack to show that although methods of detection has been evolving, attacker continually find a new way to evade those methods. It is important that researcher either an academician or industry researcher to continually perform analysis on malware and research new ways to detect those evasion methods and develop methods to defeat it.

In future works for this field, several methods can be implemented to either improve existing research or as a base of a new research. Implementation of semi-supervised feature selection technique can be utilized for ransomware detection[18]. Other than that, extending forensic-by-design by using classification technique such as fuzzy classification may improve the existing result[19].

REFERENCES

[1] N. A. Hassan, "Ransomware Overview," in *Ransomware Revealed*, Berkeley, CA: Apress, 2019, pp. 3–28.

[2] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 2, p. 100013, Nov. 2021.

[3] M. Ryan, *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*, vol. 85. Cham: Springer International Publishing, 2021.

[4] X. Lin, "Ransomware Analysis," in *Introductory Computer Forensics*, Cham: Springer International Publishing, 2018, pp. 455–504.

[5] "The State Of Ransomware 2021," Apr. 2021.

[6] "Global Threat Landscape Report A Semiannual Report by FortiGuard Labs 2H 2020," Feb. 2021.

[7] R. Richardson, M. M. North, and D. Garofalo, "Ransomware: The Landscape Is Shifting-A Concise Report-Background and Framework." Accessed: Jun. 04, 2021. [Online]. Available: https://www.csoonline.com/article/3518864/more-targeted-.

[8] "Ransomware ENISA Threat Landscape," 2020.

[9] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Computers and Security*, vol. 74. Elsevier Ltd, pp. 144–166, May 01, 2018.

[10] "The State of Ransomware: 2020's Catch-22 - SecurityNews." https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22 (accessed Jun. 04, 2021).

[11] Z. Manjezi and R. A. Botha, "Preventing and Mitigating Ransomware," in *Communications in Computer and Information Science*, vol. 973, Springer Verlag, 2019, pp. 149–162.

[12] "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks | CISA." https://us-cert.cisa.gov/ncas/alerts/aa21-131a (accessed Jun. 04, 2021).

[13] C. V. Bijitha, R. Sukumaran, and H. V. Nath, "A survey on ransomware detection techniques," in *Communications in Computer and Information Science*, Dec. 2020, vol. 1186 CCIS, pp. 55–68.

[14] M. N. Olaimat, M. Aizaini Maarof, and B. A. S. Al-Rimy, “Ransomware Anti-Analysis and Evasion Techniques: A Survey and Research Directions,” Jan. 2021.

[15] “Ransomware Profile: DarkSide | Emsisoft | Security Blog.” https://blog.emsisoft.com/en/38577/ransomware-profile-darkside/ (accessed Jun. 07, 2021).

[16] “Darkside Ransomware does not attack hospitals, schools and governments - Acronis.” https://www.acronis.com/en-au/articles/darkside-ransomware/ (accessed Jun. 04, 2021).

[17] “From Wiper To Ransomware The Evolution Of Agrius.” https://assets.sentinelone.com/sentinellabs/evol-agrius (accessed Jun. 04, 2021).

[18] F. Noorbehbahani and M. Saberi, “Ransomware Detection with Semi-Supervised Learning,” in *2020 10h International Conference on Computer and Knowledge Engineering, ICCKE 2020*, Oct. 2020, pp. 24–29.

[19] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, and R. Khayami, “Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence,” *IEEE Trans. Emerg. Top. Comput.*, vol. 8, no. 2, pp. 341–351, Apr. 2020.