The Rise of Ransomware: Detection, Prevention, and Response Strategies

Miss. Shweta M Nirmanik
Assistant Professor
Department of Computer Science and Engineering
Rural Engineering College, Hulkoti

Mr. Nitin Gurunath Dasapalli
Student
Department of Computer Science and Engineering
Rural Engineer College, Hulkoti

Abstract

The popularity of ransomware has created a unique ecosystem of cybercriminals. Therefore, the objectives of this paper are to provide a thorough understanding of ransomware's threat and discuss recent detection techniques used. Successful ransomware attack has direct financial implication, which is fueled by several mature enablers, such as encryption technology, cyber currency, and accessibility. Encryption is effective and almost unbreakable. Anonymous cyber currency can avoid traceability. Easily obtainable ransomware code enables easy entry. A combination of these provides an attractive avenue for cybercriminals, producing specialist cybercriminals. In terms of detection techniques, it was found that machine learning (ML) via regression algorithms was the most technique adopted by researchers of ransomware. However, none of the researchers have produced any model to protect against ransomware attacks. This research highlights the need for a solution using ML algorithm for the detection engine.

Key words:

Ransomware, Intrusion Detection (ID), Machine Learning (ML), Honeypot.

1. Introduction

Ransomware has attracted great attention from cyber security experts in recent years because of the fast growth of its attacks and the creation of new variants capable of bypassing antiviruses and anti-malwares [1]. It is a relatively new malware but has generated much interest from cybercriminals because of its successful attack and direct financial interest. Ransomware's objective is to block its victim from accessing their own resources by locking the OS or encrypting targeted files that seem valuable to the victim, such as images, spreadsheets, and presentations.[2]. Basically, there are two types of ransomwares: locky and crypto. Locky ransomware locks the entire system from access by its user, but it is usually easy to resolve. However, crypto ransomware uses encryption technology to lock selected files from user access; this is much more difficult to resolve, and the damage caused may be irreversible. Crypto ransomware is also the more popular type employed by cybercriminals.

2. Ransomware

Ransomware is a type of malware that prevents its victims from accessing their own data until they pay a ransom. This type of malware has direct financial implications, which has promoted an ecosystem of cybercriminals, who employ it as a business model. Ransomware as a service (RaaS) is a service that allows the easy acquisition of ransomware codes at a price. The price could be an outright purchase, or a profit-sharing scheme could be used. This indicates that cooperation exists among criminals. One party is responsible for developing and creating the

ransomware code, while another party is responsible for organizing the dissemination of the infection or an attack campaign, and both parties enjoy the profit from a successful attack. Ultimately, this will promote specialist criminals that authorities will find difficult to tackle.

2.1 Enables of Ransomware Attack

Ransomware attacks have expanded both in frequency andvariant because of the facilitative actions of several enablers. These enablers arose mainly due to technological advancement and lifestyle change.

(i) Encryption Technology

Encryption is used for privacy purposes. In today's heavy dependence on the internet, large amounts of data are transmitted electronically. However, these data can easily be intercepted. Therefore, to ensure that the data is only read by the designated persons, encryption technology wasinvented.

This technology has proven to be a double-edged sword. Ransomware has exploited this technology to encrypt victim's files for extortion purposes. Ransomware mainly uses three types of encryption technology: symmetrical encryption, asymmetrical encryption, and hybrid encryption.

Symmetrical encryption uses one key for both encryption and decryption process. Its advantage is the encryption process can be quickly completed. However, its downside is that it is less secure.

Asymmetrical encryption uses one key for encryption, called public key, and another key for decryption, called private key. The encryption process is slower but more secure.

Hybrid encryption combines both symmetrical encryption and asymmetrical encryption. Initially, the victim data is encrypted using symmetrical encryption, and then the key is encrypted using asymmetrical encryption. This enables a quick encryption process and high security.

(ii) Cyber Currency

Cyber currency is the main payment method for the ransom. This is mainly because such currency allows the recipient to remain anonymous to the authority. Cyber currency such as Bitcoin has received wide acceptance. This is true, especially with the popularity of online stores thataccept cyber currency.

Block chain technology is another form of encryption technology that uses a one-way hash function. This is the key technology employed by the cyber currency payment method to ensure legitimacy of currency.

(iii) Ransomware Accessibility

Ransomware codes can be easily obtained with the existence of RaaS. In addition, free development kits, such as Torlocker, TOX and Hidden Tear, are available for unskilled individuals. This greatly reduces the entry barrierof ransomware.

2.2 Ransomware Lifecycle

There are seven steps in the lifecycle of ransomware, as shown in Fig. 1. The lifecycle shows the formation of a cybercriminal ecosystem, in which there is a close cooperation between 'creator' and 'campaigner'. The creator is the programmer that develops and produces the ransomware code, while the campaigner is theorganizer of the attacking campaign. This kind of cooperation allows both parties to improve and sharpen their knowledge and skills in their areas of focus with eachcycle. Ultimately, this produces specialist criminals.

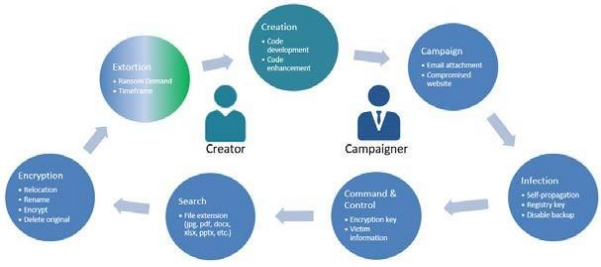

Fig. 1 Ransomware lifecycle.

(i) Creation

Creating ransomware with programming codes is the main task of the creator. The creation stage also involves enhancing codes to increase the potency of the ransomware at the end of each cycle. Lessons learned from a cycle can be used for improvement in the next cycle.

(ii) Campaign

Distributing or disseminating the ransomware to the victim's system is the main task of the campaigner. Basically, there are two types of target victims: individual and institutional victims.

For individual victims, the dissemination objective is usually to reach as many victims as possible. Dissemination to individual victims may be simpler, because not many victims are computer-savvy.

However, for institutional victims, the ransomware needsto be specifically targeted and highly sophisticated. This is because, usually, some form of security defense is already in place.

Some common infection vectors are email attachments, email links, compromised websites and social media. The campaign success depends on how effective the human psychology of fear and insatiability is exploited.

(iii) Infection

When the payload has reached the victim's system, the ransomware setup behavior may begin. However, more sophisticated ransomware may employ certain precautionary steps, which are detailed in Section 4.

(iv) Command and Control

Once the setup is complete, the ransomware may contact Command and Control center for several reasons, the most common being to obtain the encryption key for the encryption process. Another possible reason is to download more files for more advanced infections.

(v) Search

After obtaining the encryption key, the ransomware canstart searching for seeming valuable files such as text, documents, spreadsheets, presentations, images, and databases.

(vi) Encryption

Once all valuable file types have been identified, the ransomware starts the encryption process. Ransomware normally uses three types of encryption technology: symmetrical encryption, asymmetrical encryption, and hybrid encryption. These are discussed in detail in theprevious section.

Depending on the step(s) involved, the encryption process can be divided into three classes: class A, class B and classC, which are discussed in the next section.

(vii) Extortion

After the above steps have been completed, the final step in the cycle is to display the ransom demand. The demand note will inform the victim of the infection and specify the mode of payment. In addition, the note may also contain the ransom payment deadline, after which the ransomware will start deleting the valuable files.

2.3 Types of Ransomware Attacks

There are mainly two types of ransomware attacks: locky ransomware, which locks the system from being logged in, and crypto ransomware, which encrypts specific file types, making them inaccessible to the victim.

(i) Locky

Locky ransomware locks the system from being logged in by its victim. However, the system can be usually restored by rebooting or running in safe mode. Therefore, this type of ransomware is less detrimental and can be resolved quite easily.

(ii) Crypto

Crypto ransomware encrypts specific file types that are considered valuable to the victim such as documents, spreadsheets, pictures, and databases. It can employ symmetrical, asymmetrical or hybrid encryption. Depending on the step involved, the encryption process can be classified into three: Class A, the file is encrypted but not renamed or relocated; class B, the file is encrypted and renamed, but not relocated; and class C, the file is encrypted, renamed, and relocated, increasing the difficulty of tracking, and restoring the file.

(ii) Scareware

This ransomware-type tricks users into downloading or buying malicious or sometimes useless software by displaying startling messages, often done using pop-up ads. Users who take the bait inadvertently install ransomware on their devices. This type of ransomware does not necessarily pose a real threat to its victim.

(iii) Leakware

also known as Doxware, is a new and potent form of ransomware that threatens to make users' data public unless the ransom is paid. The damage caused is irreversible as anyone can access the data once it is open to the public.

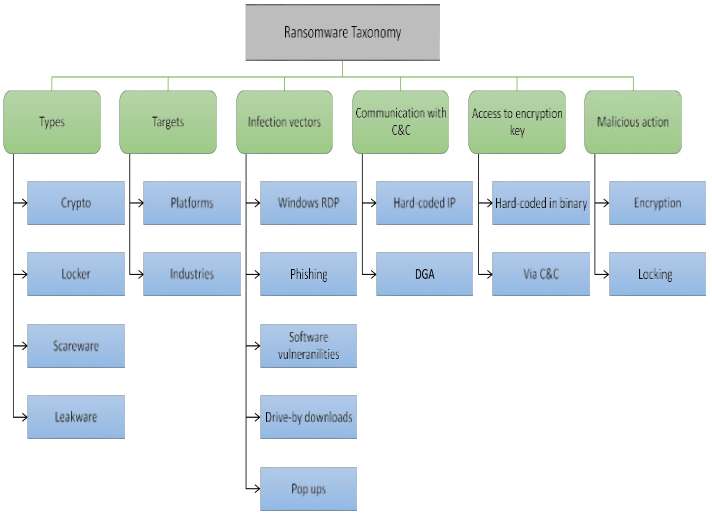

Fig. 2 Taxonomy of Ransomware.

3. Ransomware Setup Behavior

After the ransomware has been successfully uploaded into the victim's system, the setup step, as shown in Fig. 2, is crucial in ensuring a complete and successful infection. Ransomware may employ one or more of the precautionary actions below.

Fig. 3 Ransomware setup behavior.

3.1 Payload Persistence

This action is to ensure that the attack can be persistent even after the system is rebooted. Common techniques used are placing an executable file in the startup directory, adding a new registry key and setting a scheduled task.

3.2 Restrict System Restore

This action is to prevent the victim from restoring the system to the pre-infection state. Common

techniques usedare to delete scheduled backup, backup system and backupfiles.

3.3 Stealth Mode

This action is to prevent the attack from being visible to the victim. Common techniques used are to execute from %AppData% directory as well as using the same name as the common system executable.

3.4 Environment Mapping

This action is to ensure that the infection is actually in the victim's system and not in a sandbox. A sandbox is the common setup for dynamic analysis of malwares. Common techniques used are to check the security setting and policies, geographical location, user language, file system architecture and network drives.

3.5 Communication Masking

This action is to ensure successful communication with Command and Control center. A domain name can be randomly generated using an algorithm; this will complicate the tracking performed by the authority.

3.6 Privilege Elevation

This action is to enable the attacker perform actions as an administrator. Many system-related actions can only be performed by the administrator; therefore, elevating to administrator level will ensure all actions can be performed without restriction.

4. Types of Ransomware Analysis

The objective of ransomware analysis is to better understand how ransomware functions. Based on this understanding, defensive steps can be formulated to prevent future infections. Two types of analysis can be performed: static analysis and dynamic analysis, as shown in Fig. 3. Static analysis is based on the source code of the executable file. For dynamic analysis, the ransomware is executed in a controlled environment, and all its actionsare recorded for analysis.

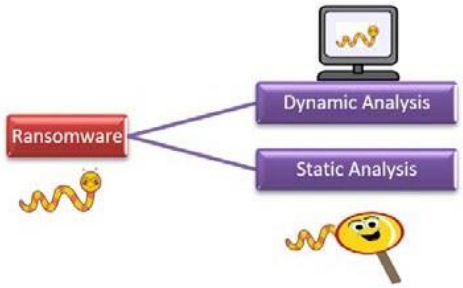

Fig. 3 Ransomware analysis.

4.1 Static Analysis

Static analysis can be conducted quickly by examining the features of an executable piece of code and matching it to a previously observed malicious code.

(i) Pros

The malicious code is easily and quickly analyzed. Successful detection here also means that the ransomware can be avoided without it having any chance to be executed.

(ii) Cons

It is susceptible to code obfuscation. Simple addition of normal operation codes can result in mismatch with previously identified malicious codes.

In addition, the analysis is also not effective when the codeis encrypted. There is currently no efficient way to decryptan encryption using brute force. It is simply time- consuming.

Static analysis is also not effective towards multi-phase attacks. The initial code could merely be a simple process to open a backdoor for additional codes to be downloaded and thus may not have a similar malicious action.

4.2 Dynamic Analysis

Dynamic analysis is also called behavioral-based analysis.Malicious code is executed in a controlled and monitored environment, usually a sandbox. All actions are captured for analysis.

(i) Pros

This type of analysis is less prone to obfuscation, and encrypted code can be analyzed. Malicious action must be part of the process in order to achieve its objective. Encrypted code must be decrypted before the malware can perform its action.

(ii) Cons

Setup for this type of analysis is both costly and time- consuming. To accurately capture the ransomware behavior, it is important that the environment setup closely imitates an actual environment.
As discussed previously, one of the setup behaviors of ransomware is environment mapping. If the analysis is performed using a virtual machine, which can cut cost and resources, the ransomware may discover this and prevent itself from exhibiting all its behaviors.

5. Ransomware Detection Techniques

This section discusses the various detection techniques used to discover and identify ransomware. The papers reviewed are summarized in Table 1, while the general techniques are discussed below.

5.1 Machine Learning

Machine learning (ML) involves learning the patterns in data to create a model. This model can then predict the outcome when fed with new data [7]. However, the difficulty in using ML is in finding the correct algorithm to match with the type of data and the needed outcome.

(i) Pros

The advantage of ML is that it can accurately predict the outcome with adequate training data. Training data should be varied with balanced distribution of outcomes to be predicted. Because ML involves learning the pattern in the data, it is less prone to obfuscation.

(ii) Cons

Finding the correct algorithm is often not straightforward and may require some runs of trial and error. Moreover, biasness and overfitting may occur if adequate caution is not taken.

5.2 Honeypot

Honeypot involves setting up decoy files for the ransomware to attack. Once these files are accessed, the ransomware can be identified.

(i) Pros

The traps or honeypot files can be set up, and then they simply wait to be attacked. Therefore, the technique does not require much maintenance or processing power from the system.

(ii) Cons

There is no guarantee that the honeypot files will be attacked by a ransomware. Therefore, it is important to know the characteristics of files that the ransomware will attack.

5.3 Windows based

Fig.4 Timeline of ransomware families (Windows-based).

Fig.5 Overview of ransomware attack "kill chain".

- **Reconnaissance**: This initial stage focuses on identifying (enumerating) a list of potential hosts to target for ransomware transmission. Hackers or RaaS affiliates can use a range of methods here, including port scanning, mailing lists, Internet/social media crawling, or directly purchasing lists from darknet marketplaces, etc.
- **Distribution/Delivery**: The next step focuses on delivering ransomware binaries to the identified hosts. Again, a wide range of techniques are used here, e.g., spam/phishing emails, website exploits (drive-by attacks), even manual transfers using removable drives. As expected, there is almost always an (inadvertent) human element involved in downloading malware onto a device.
- **Installation/Infection**: This stage entails ransomware setup on infected hosts. Most advanced strains also try to hide their entry/presence by doing various things, e.g., limiting pre-attack "paranoia" activities, uncovering/disabling back- ups, blocking host defense/firewalls, etc. Spreading (propagating) ransomware designs also perform internal reconnaissance to identify other hosts to infect, i.e., worm-like operation.
- **Communication**: This stage usually runs prior to encryption and involves communicating with the C&C server. The details here can vary based on the type of encryption being used. For example, symmetric encryption designs generate a local key which is either sent to the external C&C server or stored locally (but encrypted with the attacker's public key). Hence victims must contact the C&C server to obtain the decryption keys. However, symmetric encryption is vulnerable to interception by anti-virus programs as it stores decryption keys on local hosts (at least for some time). Hence other standalone designs use asymmetric public key encryption along with the attacker's public keys. However, such encryption is generally slower and more vulnerable to detection by host anti-virus programs.
- **Encryption**: This is the main step where ransomware runs encryption algorithms to lock user data and/or machine access. The original data is usually wiped (along with any detected backups) and a message of some sort is displayed. However, excessive calls to encryption routines can take time and consume a lot of processor cycles. In turn, these signatures can be detected by host defenses. Hence some ransomware strains try to maximize their impact by only encrypted a small portion of a file (but still enough to render it useless to users).
- **Extortion/Payment**: This final stage involves the actual handling of ransom payments and any terminal action sequences. Again, many ransomware designs request payments in cryptocurrencies or through the darkweb. Depending on the intentions of the malactors, some ransomware designs may not even release encryption keys after payment.

6. Evolution of Ransomware

Fig.6 Evolution of Ransomware.

This section delves deeper into some of the significant ransomware variants that emerged

throughout each decade since its emergence, providing a comprehensive understanding ofthe progression of this threat. Figure-6 depicts the progression of ransomware, beginning with its inception in 1989, through the era of rapid internet expansion, and culminating in the present-day utilization of Ransomware-as-a-Service modelsand double extortion tactics by attackers. This illustration provides a comprehensive overview of the evolution of this threat.

Ransomware first emerged late in 1989 when a professor, called Dr. Popp, distributed 20,000 virus-infected floppy disks to people at the international AIDS conference. Once it was loaded onto a system, the virus began hiding directories, locking files, and required a payment of $189 for the restoration of access to the affected data Ironically,Dr. Popp was neither a computer scientist nor a programmer but a biologist. He was eventually arrested and charged with10 counts of blackmail and causing damage through the distribution of what is now referred to as the ‘‘AIDS Trojan’’. Eventually, it was determined that he was incapable of standing trial due to psychological reasons. Ransomware tooka long hiatus of 15 years since its emergence in 1989. The next time it appeared was with the advent of digitaland crypto currencies allowing for a more elegant form of payment. The re-emergence of ransomware was also driven by the widespread adoption of the internet and email as daily tools for communication and business. At the early stage of the internet era, two of the most significant ransomware attacks were GPCode and Archives. These attacks were different from today’s ransomware, as the attackers requested a low ransom because they preferred targeting a high volume of victims, rather than targeting a smaller number of high- value victims. GPCode, which surfaced in 2004, used two infection vectors to attack victims, namely phishing emails and malicious website links. By 2006, Archives marked a shift in the evolution of ransomware as it was the first strain to use Rivest-Shamir-Adleman (RSA) encryption. This evolution of encryption technology showed how cyber criminals had been adapting to the changing landscape of cyber security. The year 2007 saw the emergence of the first locker ransomware variants that locked victims’ machines and prevented them from using their computers’ basic functions. Winlock led this era of ransomware. It operates by taking control of the victim’s screen and displaying explicit images, forcing the victim to pay a ransom via paid SMS to regain access to their computer. This type of malware represented a unique and particularly aggressive form of ransomware that caused widespread concern among computer users and security experts alike.

A couple of years later, analysts learned of 2013’s most malicious malware threat called Crypto Locker. By December of 2013, this potent form of ransomware had impacted roughly 250,000 Windows-based computers. It was also during this time that security researchers learned that cyber- criminals were not only targeting professionals but also home-based internet users. The primary source of infection during this year seemed to be phishing emails that contain malicious attachments. In mid-2012, a password-stealing malware named Reveton ransomware, also referred to as Win23/Reveton, the FBI Virus, or the Police Trojan, made its appearance. This later evolved into ransomware that exploited hundreds of thousands of dollars from its victims every month. It achieved this by posing as law enforcement agencies to deceive victims and coerce them into paying a ‘‘fine’’ or facing the consequences of being arrested. 2014 marked a significant milestone in the evolution of ransomware when Simple Locker made its debut, becoming thefirst strain to target Android devices and encrypt images, documents, and videos stored on SD cards. This new strain expanded the potential targets to include a wider rangeof victims and opened the door to a whole new set of attacks.Probably the most notorious

malware infection of all time was the infamous WannaCry of 2017, a crypto-ransomwareworm that attacks Windows PCs. This is still actively used by cyber attackers today. Maze ransomware first surfaced inMay 2019 and has been highly active since December 2019. The malware not only encrypts data but also exfiltrates the targeted data, threatening to release it publicly unless the victims pay a ransom. This type of attack can have severe consequences for businesses, as it uses double extortionwith regular ransomware actions. This makes it a particularly concerning threat for organizations. Furthermore, the information on this type of malware is constantly evolving and new attack methods are being developed by the cyber- criminals behind it.

One of the worst threats that 2020 saw was in the form of Egregor ransomware. Egregor ransomware is a highly sophisticated form of malware that has gained notoriety for its brutal double-extortion tactics. Despite its destructive capabilities, little is known about this ransomware as it employs various anti-analysis techniques such as payload encryption and code obfuscation to evade detection and analysis. Egregor isbelieved to have links to the now-defunct Maze ransomware. Conti ransomware is particularly destructive due to its rapiddata encryption speed and ability to spread to other systems. The Conti group often uses phishing attacks to install Trick-Bot and Bazar Loader Trojans, granting them remote access to infected machines. After encrypting the data, Conti follows a two-step extortion process. Darkside, which initiallyappeared in mid-2020, was responsible for the attack on the Colonial Pipeline, termed the most devastating cyber-attackof 2021. The group is known to only attack organizations that can pay a huge amount of ransom, rather than targeting governments, non-profit organizations, and hospitals. In 2022, the highest number of cyber-attacks was from among the newer variants that also employed double extortion tac- tics. Lockbit ransomware was able to quickly make its mark in the Raas space due to its ability to upgrade its attack techniques frequently.

7. Prevention of Ransomware Attacks

Fig.7 Ransomware Attack

- **Employee Training:** The initial step is to educate employees on cyberattack risks and teach them cybersecurity practices like strong passwords, avoiding suspicious links/attachments. Phishing and social engineering are common techniques, so training employees to identify and counter such attempts is crucial.
- **Regular Backups:** Backing up files and applications regularly is another essential practice to prevent data loss in case of an attack. Offline data backups should also be secured and not permanently connected to the networks they are backing up.
- **Network Segmentation:** This method can help prevent the spread of malware from an infected system to other computer systems. Production and general-purpose networks should be segmented so that if an infected computer infects one of the smaller networks, the ransomware can be isolated before it spreads throughout the entire organization.
- **Review Port Settings:** Reviewing port settings is also crucial to prevent ransomware attacks, as open **RDP ports** and **Server Message Blocked**

port 445 are often targeted. Limiting user access privileges and defining user permissions thoroughly can also help prevent ransomware attacks by restricting access to applications, desktops, and files. Adding security layers in line with the Zero Trust model is recommended to ensure control over user access and actions, as even authorized employees cannot always be trusted.

8. Response Strategies

Fig.8 Victim of Ransomware Attack

- **Isolate the infected device:** Disconnect the infected device from the network to prevent the malware from spreading to other devices.
- **Determine the type of ransomware:** Identify the type of ransomware that has infected your device, as this can help determine if there is a known decryption tool available.
- **Contact Law Enforcement:** Report the attack to law enforcement, as this can aid in investigations and potentially lead to the apprehension of the attackers.
- **Do Not Pay the Ransom:** It is not recommended to pay the ransom, as there is no guarantee that the attackers will decrypt your data. Paying the ransom also encourages the attackers to continue their criminal activities.
- **Restore Data from Backups:** If you have backups of your data, restore the files from the backup. It's essential to make sure the backups are not also infected with the ransomware before restoring the data.
- **Consider Professional Help:** In some cases, it may be necessary to seek professional help from a cybersecurity firm to decrypt the data or assist in the recovery process.
- **Improve Security:** After the attack, it is important to review your security measures to prevent future attacks. Ensure that your software and operating systems are up-to-date and that your employees are trained in cybersecurity best practices.

9. Conclusion

Ransomware represents a persistent and evolving threat, demanding a multifaceted approach to cybersecurity. This guide serves as a comprehensive resource for organizations aiming to fortify their defenses against ransomware. By understanding the threat landscape, addressing vulnerabilities, and implementing robust prevention and recovery strategies, organizations can significantly enhance their resilience in the face of this growing menace.

References

[1] "Ransomware defense validated design guide," *Cisco Systems*, 2016.
[2] "Ransomware facts, trends statistics for 2022," *Safety Detectives*, 2022.
[3] A. Kapoor, "Ransomware detection, avoidance, and mitigation scheme: A review and future directions," *Sustainability*, vol. 14, no. 1, Dec. 2021.
[4] "Senate bill to mandate cyberattack, ransomware payment re- porting," *Bloomberg Government*, September 28, 2021.
[5] E. Berrueta, D. Morato, E. Magan˜a, and M. Izal, "A survey on detection techniques for cryptographic ransomware," *IEEE Access*, vol. 7, pp. 144 925–144 944, October 2019.
[6] R. Moussaileb, N. Cuppens, J.-L. Lanet, and Bouder, "A survey on windows-based ransomware taxonomy and detection

mechanisms," *ACM Computing Surveys*, vol. 54, no. 6, July 2022.

[7] A. Almashhadani, M. Kaiiali, S. Sezer, and P. O'Kane, "A multi- classifier network-based crypto ransomware detection system: A case study of locky ransomware," *IEEE Access*, vol. 7, no. 1, pp. 47 053–47 067, 2019.

[8] D. Mulders, "Network based ransomware detection on the samba protocol," *MS Thesis, Dept. of Mathematics, TU Eindhoven*, 2017.

[9] D. Morato, E. Berrueta, E. Magan˜a, and M. Izal, "Ransomware early detection by the analysis of file sharing traffic." *Journal of Network and Computer Applications*, vol. 124, no. 1, pp. 14–32, 2018.

[10] G. Cusack, O. Michel, and E. Keller, "Machine learning-based detection of ransomware using sdn," in *SDN-NFV 2018*, Tempe, AZ, March 2018.

[11] B. Lokuketagoda, M. Weerakoon, U. Kuruppu, A. Senarathne, and K. Abeywardena, "R-killer: An email based ransomware protection tool," in *ICCSE 2018*, Singapore, July 2018.

[12] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, and S. Hashemi, "Drthis: Deep ransomware threat hunting and intelligence system at the fog layer," *Future Generation Computer Systems*, pp. 94–104, Jan. 2019.

[13] K. Ade and R. Imam, "Detection and analysis cerber ransomware based on network forensics behavior," *International Journal of Network Security*, vol. 20, no. 5, 2018.

[14] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware Payments in the Bitcoin Ecosystem," 2018.

[15] D. Nieuwenhuizen, "A behavioral-based approach toransomware detection," 2017.

[16] D. Distler, "Malware Analysis : An Introduction." SANS Institute, USA.

[17] S. Kok, A. Abdullah, M. Supramaniam, T. R. Pillai, and I. A.T. Hashem, "A Comparison of Various Machine Learning Algorithms in a Distributed Denial of Service Intrusion," Int. J. Eng. Res. Technol., vol. 12, no. 1, pp. 1–7, 2019.

[18] J. A. Gómez-Hernández, L. Álvarez-González, and P. García-Teodoro, "R-Locker: Thwarting ransomware action through a honeyfile based approach," Compute. Secur., vol. 73, pp. 389–398, 2018.

[19] C. D. D. Biomedico and C. Alberto, "SoLA: Social Leopard Algorithm for Intrusion Detection Honeypot to detect ransomware attacks," IEEE Trans. Cogn. Development Syst., no. Submitted, pp. 16–23, 2018.

[20] N. Hampton, Z. Baig, and S. Zeadally, "Ransomware behavioral analysis on windows platforms," J. Inf. Secure. Appl., vol. 40, pp. 44–51, 2018.

[21] H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, and A. K. Sangaiah, "Classification of ransomware families with machine learning based on N-gram of opcodes," Future. Gener. Compute. Syst., vol. 90, pp. 211–221, 2019.

[22] Monika, P. Zavarsky, and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," Procedia Compute. Sci., vol. 94, pp. 465–472, 2016.