THE REVIEW OF RANSOMWARE ATTACKS

First A. Author, *Fellow, IEEE*, Second B. Author, and Third C. Author, Jr., *Member, IEEE*

***Abstract*—** **Ransomware is by far the greatest frequent online danger to the electronic architecture. Attackers using ransomware use a number of tactics to acquire access of the data and services of people or companies prior to actually encoding or confiscating those in return for an extortion money. Notwithstanding the widespread use of cyberattacks, ransomware is thought to be among the biggest danger since it puts a significant monetary burden on the company. The hacker uses Bitcoin, an irreversible transaction method, to demand an extortion from individuals while concealing his or her name and whereabouts. This makes it difficult to identify the attacker or attackers' networks. As ransomware assaults are the topic that needs the greatest attention in critical infrastructure, the essay employs the systematic literature review (SLR) technique to give major study on the subject. The document briefly discusses the numerous ransomware variants, vulnerabilities, attack methodology, effects, mitigation strategies, and attack prevention approaches.**

***Index Terms*—Ransomware, Malware, Encrypted attacks, Crypto-currency, Crypto-modules**

# I. INTRODUCTION

C

ritical infrastructures face a serious danger from malware, sometimes known as malicious software [1]. These have been created with the goal of harming the target's computer or communication networks. Malware comes in a wide variety of forms, including viruses, ransomware, spyware, etc [2]. Malware known as ransomware has been shown to employ complex attack methods and many variations. A broad variety of businesses, including health services, public law enforcement, telecommunications, financial institutions, and transportation have been impacted by ransomware. Ransomware uses implanted crypto modules to make user data inaccessible or untraceable. Ransomware either locks down equipment or encrypts files, and then demanding that the organisation pay a ransom to regain rights [3]. Various ransomware display polymorphism and metamorphic tendencies together with code obfuscation, making it difficult to analyze for and identify them with current technologies.

The solutions for finding ransomware may be generally classed as either signature-based or anomaly detection-based. The accepted method for analysing and detecting ransomware is signature-based analysis. To identify the attack, it operates in a signature-covered environment that covers every known ransomware variant. Like fingerprints, the ransomware signatures aid the solution in detecting their existence or threatening activities. Therefore, these approaches are unable to identify vulnerabilities or defects that cause zero-day attacks. For the purpose of identifying malicious behaviour, the anomaly detection-based analysis employs a variety of metrics, including network traffic detection, unusual process calls, and other traffic detection. However, these studies reveal a substantial number of false positives and frequent misclassification of actual traffic.

As it has been shown to be able to recognise both new and disguised malware in addition to already existing malware, machine learning (ML) is growing in favour in the malware identification field [4]. Using machine learning, malware analysis involves two stages of work. The ML algorithms formalise the collection of characteristics gathered from harmful and non-malicious data in the first phase, referred to as the "Training Phase," in order to create a prediction model.

In the testing stage of ML techniques, the prediction modelling created during the training stage is applied to forecast the malware's normal behaviour. Adversarial methods utilising ML are employed in numerous ways to explore this stage impact of classifier tampering by the adversary in training stage. An adversary can influence the result of the training stage [5], [6].

The marketplace is categorised by deployments, purpose, locality, and other factors for both paid and free anti-ransomware products. The new ransomware variations really aren't recognised by the current product, and the effects are only discovered after the operation, despite the fact that there are ongoing upgrades or enhancements to the current anti-ransomware systems. Analysis also demonstrates that no ransomware variations changes after every infection, which enables ransomware writers to remain one move in front of the game since the ransomware's affiliated signatures, domains, and IP addresses become outdated and are no longer recognizable by threat intelligence and signature-based security systems. The following are the main goals of this investigation:

* To comprehend the many aspects of ransomware that affect operating system information security.
* To comprehend how the various ransomware variations affect operating systems' information security.
* To comprehend ransomware discovery, avoidance, and mitigation methods.

The essay is structured as follows: The approaches surveyed are discussed in Section 2. The findings from the systematic literature review are summarised in Section 3.

# II. Ransomwares

1. *Characteristics of ransomware*

Malware's behaviour study demonstrates that ransomware behaves uniquely from those other malware. Malicious adverts, hacked websites, spam, social engineering, drive-by downloads, and other methods of attack are some of the several infection vectors employed by ransomware attacks [7]. Whether locally or remotely stored data, or memory, are where the infection occurs. The recently discovered ransomware performs memory infections and fileless file deletions that are undetectable by static or dynamic malware detection. The ransomware's key may be kept locally or obtained through the C&C server. The C&C server's configuration will involve either static or dynamic Domain Name System or an IP address (DNS). If the attacker use symmetric encryption, the key could be kept locally and might not communicate with an outside server. If asymmetric keys are utilised, the local computer may only have access to the public key and must get in touch with the server to obtain the private key. Typically, ransomware merely encrypts a few bytes of data when it infects a system since it doesn't want to draw attention to itself right away. The file extensions are frequently modified during the advanced stages of infection. Finally, the ransomware hides itself by leaving notes describing the steps the victim must do to get their data or resources back. The creation of picture, text, or HTML files is a typical way for keeping notes. System calls may occasionally be made in order to alter the desktop wallpaper or prevent users from logging in.

Presently available antivirus programmes label malware that performs several of the various actions as ransomware, including encrypting data, altering the Master Boot Record (MBR), deleting files, stealing data, and elevating access [8]. The malware examines the system processes and file access patterns. The assault action takes place in accordance with the examined access pattern. When compared to regular system processes, the number of files accessed by ransomware would be significantly high. The file's metadata is accessed by the ransomware through the MBR, and new values are added to prevent access or erase the files. Anti-ransomware software keeps track of file activity in directories or folders using canary files. To avoid being discovered, so many ransomware programmes attempt to remove these canary files. Some ransomware variations also monitor the network activities of compromised computers and grab the access details. By circumventing access restrictions, this malicious software is even able to reach network servers where it can encrypt or erase backups or files.

1. *Variants of ransomware*

Crypto and Locker ransomware are two types of ransomware. The Crypto ransomware encrypts all user data files using a crypto technique and demands a ransom in exchange for disclosing the decryption key. The Locker ransomware limits clients' accessibility to services by using a privilege escalation mechanism through a number of management apps. The Locker ransomware uses persistence tactics to make sure the services are blocked even after a restart.

The PC Cyborg, which initially surfaced in December 1989, is said to be the original ransomware. The files were encrypted using an initialization vector (IV) and a symmetric key. 2004 saw the introduction of the Locker ransomware (such as SMS and False FBI) as well as fake antivirus ransomware like Spysherrif and Performance Optimizer. Later, the cyber world witnessed other ransomware variants that seriously disrupted or caused corporate losses [9]. The ransomware variations that encrypt the files or data saved on the attacked computer include Filecoder, Cryptowall, Cryptolocker, GPCode, and others. The Windows OS's Cryptography Next Generation (CNG) cryptography library is used by the Cryptowall and Cryptolocker to encrypt the data. The files are encrypted using RSA keys that are acquired from the C&C server. Initially focusing on newly installed logical drives, these viruses later developed to encrypt linked drives as well. All non-system files, including network shares, were encrypted in later versions to prevent file retrievals without paying the ransom. The virus searched for network drives and retrieved data to conduct attacks using methods like GetDriveType, GetLogicalDrives, etc. In many instances, a private key will be utilised for decryption after the files have been encrypted during a ransomware assault. Depending on the ransomware family, this private key data, also known as a key blob, is kept as a distinct file, or it may be appended or added to current documents.

The MBR is attacked by the Seftad ransomware, which swaps it with an unauthorised MBR. By doing this, the ransom note is shown and the infected system is unable to load the boot code onto the active partition. By recovering the encryption key that is hard coded into the library, these assaults may be stopped. During assaults, ransomware versions like Urausy, Reveton, Winlock, etc. set up a permanent desktop lock method. By employing the accessibility mode that allows the SwitchDesktop feature and takes inputs from the user end, the virus launches the new desktop. A few variations additionally utilise a different method to lock the desktop and display a lock banner made of a downloaded HTML page with hidden controls that includes a geo-location and a warning message. By executing the hook mechanism, which keeps track of input events, the virus also disables all special keys and keyboard shortcuts throughout the locking process.

In 2017, the WannaCry ransomware assault was carried out using the "EternalBlue" exploit created by the U.S. National Security Agency (NSA). Additionally, the hacker installed the malware on an endpoint with the greatest level of rights by using the DoublePulsar code injection technique and privilege escalation. Some ransomwares, like Dharma and Bit-Paymer, employ user access control bypass vulnerabilities that set the path in a particular registry, granting the ransomware the greatest level of authority.

There are ransomware variations that carry out the harmful operations swiftly and have the most damage before being found. The ransomware in these variations efficiently makes use of multithreaded contemporary CPUs.

WriteThrough and FlushFileBuffers are called by several ransomware, including BitPaymer, GandCrab, and WannaCry, in order to make the encrypted files remain on the storage device and be held for ransom. It should be highlighted that Windows 7 computers are the primary target of Wannacry's assaults. The Windows POWERSHELL.EXE vulnerability is exploited by the Sodinokibi and GandCrab ransomwares, which then cause the ransomware to execute automatically over a period of time without alerting the user until the assault is live. The MegaCortex ransomware encrypts documents from a trusted process via the Windows RUNDLL32.EXE programme, and ransomware like Ryuk exploits trusted operating processes like SVCHOST.EXE by injecting malicious code. In order to avoid detection, the BitPaymer ransomware operates through an NTFS Alternate Data Stream (ADS).

1. *Detection, prevention, and mitigation methods for ransomware strikes*

Numerous approaches were put out to investigate and dynamically respond to abnormalities that were found, protecting people and businesses from falling prey to ransomware assaults. Every ransomware programme uses a different cryptographic technique, thus it would be quite helpful to go inside the executables and find these crypto modules. The cryptographic modules are analysed and identified using a variety of ways. The two methodologies for analysis and detection may be roughly categorised as Dynamic analysis and Static analysis.

* Dynamic analysis seeks to pick up the cryptographic algorithms while they are being used. One method of research to comprehend the disruption created is the avalanche impact of input on output. Additional approach in this study is to evaluate the aggregate of contiguous memory accesses from input and output parameters.
* Before to their implementation, crypto-binary functions are found via static analysis. Additionally, it conducts heuristic evaluation, looking for things like loops, entropy, a large proportion of bitwise actions, etc. These methods use data flow graphs to help with signature discovery and crypto constants for analysis.

An archaic technique for stopping ransomware assaults uses decoy files to misdirect the attacker's target files. However, the latest ransomware strains include methods for identifying genuine and fake files using an entropy calculation. The distribution of bytes across the file is shown by the entropy value in the range of 1 to 8, according to Shannon's entropy calculation using the formula shown below. Based on the preceding character in the file, the entropy value predicts the subsequent character. As a result, as compared to compressed or created files, regular files have low entropy values. The frequency of all ASCII (0 to 127) and enhanced ASCII (128 to 255) characters in a file is tallied, and the probability in Shannon's entropy equation is used to determine the file's entropy. Therefore, to adopt this strategy, decoy files that substantially mimic the genuine files must be created.

Ransomware threats cause a substantial amount of system modifications to happen quickly in MFT records of erased documents and a huge amount of MFT records with encrypted information to be inserted into the $DATA variable of records generated with unshared distinct routes. Therefore, the MFT table modifications that occur throughout the generation, encryption, or removal of documents may be carefully watched to spot ransomware. In a similar vein, it would be advantageous to stop ransomware attacks if the solution could keep track of all I/O requests that user-mode programmes make to access file systems and reject the questionable ones before they approach the file system drivers. In certain circumstances, utilising restoration software like Recuva, erased data from ransomware assaults can be recovered. The local or non-resident file has to be transferred depending on the $DATA property. If it is local, just transfer the material to some other place; if not, analyze the RunList in the MFT and move the original data to some other place. Since the documents wiped by ransomware operations are regarded as unallocated chunks, they might be filled with new data, making it impossible to retrieve destroyed contents. The Dharma ransomware changes the size of the file to 0 bytes prior to destruction, providing 0% possibilities for restoration, complicating the retrieval procedure. Hence, a ransomware attack's quick discovery is crucial for restoration.

1. *Solutions to Detect Ransomware Based on Machine Learning*

It is vital to develop systems that can identify both current and new attacks since the developers of ransomware are hosting new assaults by mutating or obscuring the existing ransomware strains. Utilizing ML techniques, there are several machine architectures for dynamic ransomware detection.

Since many supervised learning approaches are used in ransomware detection systems employing ML, a training phase is necessary. These suggestions are based on several sets of statistics that were taken from the ransomware operations. There are, however, not many suggestions that also make use of unsupervised algorithms. This is accomplished by using techniques like Decision-Tree, Naive Bayes, K-Means Clustering, Support Vector Machines (SVM), etc.

70,000 features were retrieved from the API calls made by rogue programmes or services by Chen et al. [10]. The findings from the Naive Bayes, Simple Logistic algorithm, SVM, and Random Forest are utilised to minimise the dimensionality using the applied correlation approach.

Special registers on contemporary chips keep track of numerous hardware processes. One of these CPU actions at the hardware level is high encryption, and this insight serves as the standard for ransomware identification. When there were no ransomware attempts, the sampling number of these specific register entries was employed in an autoencoder, an artificial neural network employed in an unsupervised learning technique. Only abnormality recognition from the learnt behaviour is employed for ransomware identification in the computer because no ransomware information was included in its development.

There are several approaches that did not feed the ML model with all of the retrieved information. These methods were created using a hybrid strategy that combines ML as well as other ad hoc methods. The ransomware's analysis of the file system revealed that the fake documents are its primary objective. For the investigation and analysis, a classifier built on the k-Nearest Neighbors, Decision Tree, and Random Forest algorithms was utilised.

# III. Conclusion

Techniques and strategies need to be improved since ransomware in this day and age is changing so swiftly. To identify and stop these assaults, there are several commercial and scholarly suggestions that are implemented on local hosts, servers, cloud, etc. Numerous theories contend that ransomware must be discovered immediately by examining records of RAM dumps, storage sector operations, network communications, etc. The essay therefore illustrates the problems and difficulties of existing methods for using these strategies in the real world owing to a variety of constraints based on the research that is now accessible. For improved ransomware identification and avoidance, the current methods, which are intuitive, emphasise the usage of AI/ML approaches. It has been determined that ML is the most efficient method for analysing enormous logs from several resources and enhancing classification performance. The choice of the characteristics is the primary criterion for applying ML algorithms to these logs. According to the results of the comprehensive literature research, the efficiency of anti-ransomware systems would be increased by the rapid and simple categorization of logs from multiple resources utilising ML technology and accurately recognised characteristics.

# **References**

|  |  |
| --- | --- |
| [1] | K. Rieck, T. Holz, C. Willems, P. Düssel and P. Laskov, "Learning and classification of malware behavior," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2008. |
| [2] | P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti and M. Rajarajan, "Android security: a survey of issues, malware penetration, and defenses," *IEEE communications surveys \& tutorials,* vol. 17, no. 2, pp. 998-1022, 2014. |
| [3] | S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security,* vol. 24, no. 1, pp. 31-43, 2005. |
| [4] | K. Rieck, P. Trinius, C. Willems and T. Holz, "Automatic analysis of malware behavior using machine learning," *Journal of computer security,* vol. 19, no. 4, pp. 639--668, 2011. |
| [5] | B. Chen, Z. Ren, C. Yu, I. Hussain and J. Liu, "Adversarial Examples for CNN-Based Malware Detectors," *IEEE Access,* vol. 7, pp. 54360 - 54371, 2019 . |
| [6] | K. Grosse, N. Papernot, P. Manoharan, M. Backes and P. McDaniel, "Adversarial Examples for Malware Detection," *European Symposium on Research in Computer Security,* p. 62–79, 2017. |
| [7] | T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi and Loris, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features," *Journal of Computer Virology and Hacking Techniques,* vol. 15, no. 4, pp. 277-305, 2019. |
| [8] | I. Nadir and T. Bakhshi, "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques," *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET),* pp. 1-7, 2018. |
| [9] | J. A. H. Silva, L. I. B. López, Á. L. V. Caraguay and M. Hernández-Álvarez, "A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters," *Remote Sensing,* vol. 11, no. 10, 2019. |
| [10] | Z.-G. Chen, H.-S. Kang, S.-N. Yin and S.-R. Kim, "Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph," *International Conference on Research in Adaptive and Convergent Systems,* p. 196–201, 2017 . |