RANSOMWARE: TOOL DETECTION VULNERABILITIES AND DEFENSE

Charles Antonin Nivesse[1], Nor Azlina Abd Rahman[2] and Khalida Shajaratuddur Harun[3]
[2]Forensic and Cyber Security Research Centre
[1,3]Asia Pcific University, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
[1] TP065060@mail.apu.edu.my, [2]nor_azlina@apu.edu.my, [3]khalida@staffemail.apu.edu.my

***Abstract*— Ransomware is a type of harmful software that steals personal data. Ransomware infections may be catastrophic to a person or a company, and recovery can be a complex process that may necessitate the assistance of a competent data recovery specialist. In this paper, we will investigate the instruments utilized by authorities to combat ransomware attacks. Several different types of detection tools are employed, and many of them have flaws. Traditional detection systems will find it more difficult to identify malware as it evolves, and updated models of ransomware families behave differently than their predecessors. Following a risk assessment of those tools' possible weaknesses, a business continuity and disaster recovery strategy against ransomware attacks is established. Finally, enhancements to organizational structural and functional security models employing AI-assisted detection methods are offered.**

***Index Terms*—Cyber Attack, Ransomware, Tools Vulnerabilities, Risk Management, Business Continuity Plan, AI-assisted detection tools**

1. Introduction

Ransomware is a type of harmful software that steals personal data. To accomplish this, spyware collects personal information and then demands payment in exchange for a key that permits the information to be decoded. A criminal can also disable all user access to a system until the victim receives a key or a debridement tool in exchange for a sum of money.

Ransomware is frequently disseminated via phishing emails with malicious attachments or drive-by downloads. Drive-by downloading happens when a person accesses an infected website without realizing it, and malware is downloaded and installed without the user's awareness. Ransomware is very effective because its authors generate fear and panic in their victims, causing them to click on a link or pay a ransom, and infecting their systems with additional software [1].

The danger presented by ransomware is quite severe, with new varieties and groups being discovered on the internet and dark web on a regular basis. Given the nature of the cryptographic algorithms utilized by ransomware, recovering from an infection is challenging.

2. The Cyber Attack

To initiate a ransomware assault, only a few actions are required. First, the attackers must get access to the targeted network or device. After getting access, they can use the malware to lock up or encrypt your data and device. Ransomware can infect your computer in several different ways:

2.1 Malicious spam

Some threat actors use spam to gain access to a device or network. They send an email to as many individuals as possible with a malware attachment. A malicious spam email is an unsolicited email that contains malware. Attachments like PDFs might be booby-trapped in the email and it might potentially include harmful website links [2].

2.2 Spear phishing

Spear phishing is a more focused way of launching a ransomware assault. When an assault is directed against specific persons or groups inside a company, this is known as a targeted attack. The word "whaling" refers to such tactics aimed at top-level decision-makers in a company, such as the CEO or senior executives [3].

2.3 Malicious advertising

Malicious advertising is the practice of spreading malware through web advertisements. Because it is done while browsing the web, it does not need much user interaction. Attackers redirect users to criminal servers that keep track of information about the systems. It allows the attacker to select what is most suited to attack the victim [3].

2.4 Mobile ransomware

Mobile ransomware is spread through infecting mobile apps with malicious code. By downloading such programs, you may infect your phone with malware in seconds, then share the infection with your computer the next time you connect to it [2].

There are many distinct types of ransomwares, and they typically differ in terms of how they infect or demand money. As a result, the best way to avoid ransomware seems to prevent it.

3. Tools Against Ransomware

Ransomware infections may be catastrophic to a person or a company, and recovery can be a complex process that may necessitate the assistance of a competent data recovery specialist. Avoiding ransomware attacks is the most effective and crucial strategy to combat them. There are several things that can be done and measures that can be taken to prevent such attacks. The first step is the prevention. There are many best practices to follow, such as keeping the system up to date, avoiding opening email attachments or links, storing multiple backups, not downloading any third-party software, restrict access and even setting up honeypots (fake files or server to lure the attacker).

Despite the importance of these precautions, infection may occur. More automated protection is provided by using various services. There are several detection programs available that can scan your infrastructure for malware, identify malicious activity in the system, and prevent viruses from infecting your PC further. Bitdefender Anti-Ransomware Tool, CryptoDrop or Check Point ZoneAlarm are services are examples of services that add to the security of a system and provide protection.

These services provide multiple services such as anti-phishing, antispam, Network Threat Prevention and Defense (Analysis on network-levels suspicious activities and blocking of exploits, malware, brute force and botnet URLs), Dynamic Analysis (Automated analysis on any suspicious file about their signatures, unique fingerprints, and impact) and Static Analysis (Manual and deeper analysis on malicious files, such as hashes, payload, metadata, or headers information) [4].

There are several ways to detect ransomware and keep it from infecting systems. File-based behavior detection, system-based behavior detection, resource-based behavior detection, and connection-based behavior detection are the four main types of detection methods [5].

- The file-based detection method is the simplest one, as it detects well-known malicious signatures in files.
- By verifying the integrity of files, the system-based behavior technique detects ransomware. It also protects against ransomware by keeping an eye on the system's harmful activity. It is, however, time demanding and results in a high mistake rate.
- The resource-based detection strategy identifies ransomware by examining the rate at which resources are used to encrypt data. It, however, has a high rate of faults and takes a long time to acquire resource use (CPU, I/O).
- By monitoring the connection to the outside, the connection-based behavior detection approach can detect ransomware that requires a connection to the server to get the encryption key.

There are several new approaches for identifying malicious files on the horizon. These solutions make use of cutting-edge strategies including the usage of AI prediction tools to improve prediction rates and defeat evolving and complex assaults. These strategies will be discussed in greater depth later in this work.

If infection is unavoidable and ransomware strikes, several services offer a variety of options. Avast software, ESET or AVG technologies are examples of services that provide decryption tools [6].

4. Tools Vulnerabilities

Even if the tools appear to be effective, they may not provide complete protection for the systems. Each tool contains several flaws that may be used to strengthen future ransomware assaults. Some detection methods, such as file-based detection (heuristic/signature detection), are vulnerable to new ransomware infections that aren't yet well-known, as they base their detection methods around comparison with malicious functionalities database. Malware families are always looking for new ways to disguise their code, prevent detection, and impede replication [5].

The usage of packers and crypters is a frequent evasion strategy utilized by ransomware authors. Packer is a tool that compresses, encrypts, or changes the format of a harmful file. It reduces the likelihood of antimalware detection and aids in the avoidance of security researcher analysis. Packages can make it more difficult for security workers to recognize malware behavior and lengthen the time it takes to analyze it [7]. A crypter is a software program that can encrypt, obfuscate, and alter malware to make it more difficult for security systems to identify. It is used to get around security measures by acting as a benign software until it is installed [7].

Other exploitable weaknesses exist in ransomware detection methods. The fact that most of the approaches have a fluctuating detection rate is the most obvious one. Even the most advanced detection technologies are still unable to detect every attempt. The median rate of detection has been reported in studies including the most well-known anti-ransomware tools. For the most common assault types, detection rates are typically around 80-90 percent. However, when the assault type is complicated with the usage of a packer or crypter, the rate reduces to 10-40%. It will therefore be necessary to utilize specific tools against that form of assault in order to improve the detection rate [7].

Another flaw is that most anti-ransomware software is utilized and concentrates on main systems rather than backups. It frequently leads to a lack of awareness of infection on backup files and systems, and if an attack happens, it may have more severe effects for individuals and organizations [5].

5. Risk Management

Cyber risk management is the method of identifying, evaluating, assessing, and reacting to your organization's cyber security problems. It is subdivided into several sections.

The first step is to identify the threats that might jeopardize your cyber security systems. As previously mentioned, this entails detecting cyber security vulnerabilities in your system as well as how the attackers may exploit them.

The second stage is to assess, rank, and prioritize each risk's severity. It is done by weighing the likelihood of an attack and its consequences against the organization's acceptable risk threshold [8]. The usage of packers and crypters presents an obvious danger to an organization's security, and this sort of risk should be prioritized in a risk assessment system.

The third stage is to determine how you will respond to the risks. The answer differs based on the danger being considered. It can be allowed if the risk is within the risk acceptance criteria of the organization, transferred to another party, handled by introducing extra security controls, or completely eliminated by altering the risk's cause [8]. The usage of packers and crypters is a form of risk that should be addressed by implementing additional security measures and technologies in order to limit the severity of the risk as much as feasible.
The final stage is to always keep an eye on the risks. Because threats change and evolve as frequently as might do your firms' systems, there is a need for constant risk monitoring.

6. Business Continuity & Recovery

The process of developing preventative and recovery measures to cope with possible cyber threats to a company or to assure process continuity in the aftermath of a cyberattack is known as business continuity planning (BCP). It also guarantees operational continuity before and throughout catastrophe recovery. The far more basic element for business continuity is to keep important functions running during a disaster and restore with the least amount of downtime feasible. Natural disasters, fire, epidemics, cyberattacks, as well as other external threats are all things to think about while developing a business continuity plan.

The business recovery strategy includes numerous measures in the event of a ransomware attack. The risk assessment and business impact analysis are the initial steps in the recovery strategy. The second step is to generate various strategies for each of the risks outlined before. Multiple strategies might be explored when using tools to complicate the attack and overcome prediction and analysis technologies. The employment of new prediction algorithms and tools to scan and sort out dangerous files appears to be the most obvious one. After assessing the risks and developing strategies to counter it, the solutions should be executed and evaluated to ensure they meet the requirements. Finally, routine maintenance ensures that no new risks need to be assessed [8].
If the organization's IT infrastructure is compromised, a disaster recovery process must be followed to regain access and functioning. A disaster recovery plan is an important aspect of a company's Business Continuity Planning since it includes both reactive and preventative parts. It is a formal document prepared by a company that gives precise instructions on how to respond to unexpected events. The plan includes tactics for limiting the effects of a disaster so that a company may continue to function. It is more concentrated than a business continuity plan, and it may not include all alternatives for company processes, assets, human capital, or company associates. The methods, rules, and processes that prepare an organization's critical IT infrastructure to efficiently recover disasters and preserve business continuity are referred to as disaster recovery. It must have instructions that anybody may execute. The most crucial thing to do when a ransomware assault happens is to immediately block the attack's access to avoid further infection.

7. Security Improvements Using AI-Assisted Identification

Criminal activity detection software is becoming increasingly overtaken. New methods of detection and analysis are beginning to emerge.

Based on measured entropy, several approaches employ machine learning to categorize clean files and ransomware-infected files. K-Nearest Neighbors (KNN), decision tree, kernel trick, linear model, and deep learning are some of the machine learning models that are employed. The National Institute of Standards and Technology (NIST) issued NIST 800-90b, which included methodologies and instruments for measuring uniformity. It is based on Poisson distribution, hamming distance, and spontaneous emission methods for determining entropy [5].

To develop more effective prediction capacities, other AI approaches employ context awareness to determine the most relevant attack pathways, vectors, and subsequent events. It extracts information characteristics (connection requests, software upgrades, etc.) using context ontology and Machine Learning techniques to forecast ransomware attacks. This approach focuses and relies on early detection and prediction of ransomware attacks on systems. This strategy not only improves the detection rate of ransomware assaults, but it also cuts down on the time it takes to do so [9].

There are a lot of other methods emerging, such as EldeRan, RansomWall, RansHunt, Support Vector Machines (SVM), Software-Defined Network (SDN), NetConverse, Resilient Machine Learning, API Sequence-Based Detection, Two Stage Ransomware Detection, Deep Neural Networks, Long Short-Term Memory (LSTM), Shallow and Deep Networks or Digital DNA Sequencing. They're all based on AI prediction techniques like machine learning and deep learning. These methods may be used to create prediction models that can learn how ransomware behaves and utilize that information to find variations and families that haven't been seen before [10].
These new approaches should be included into an organization's operational security model. It would effectively lower the vulnerability of the system to the majority of ransomware assaults. Other enhancements to organizational security and awareness might be made and implemented. Changes in

operational security models would imply changes in technical security operations' structure.

Ransomware assaults are also developing, thanks to the rise of AI-assisted detection tools. The monitoring and risk assessment procedures used by the organization should have an influence on the defensive strategies used to keep track of those developing dangers.

8. Conclusion

Although signature-based and system-based detection were formerly effective, they have since become outdated. As the number of vulnerabilities grew, so did the number of weaknesses in the methodologies, ransomware assaults have evolved over time, and new strategies to combat them are required. The job of previous detection techniques got taken over by AI-assisted detection methods, which aligned with the organization's business continuity strategy. It is certain that machine and deep learning models can be used to identify ransomware based on the findings. However, their capacity to withstand the test of time and adapt in tandem with ransomware's rapid improvement is unclear. AI-assisted detection systems will need to be maintained and evolved in such a way that they can withstand the test of time and not be outpaced by new ransomware attack variants.

References

[1] Akhtar Kamal, M. D. (2021). A User-friendly Model for Ransomware Analysis Using Sandboxing. Tech Science Press.

[2] All about ransomware attacks. (2021). Retrieved from malwarebytes: https://www.malwarebytes.com/ransomware

[3] Reed, J. (2019, April 30). Methods and Tools for Ransomware Detection. Retrieved from Nakivo: https://www.nakivo.com/blog/methods-tools-ransomware-detection/

[4] Akashdeep Bhardwaj, V. A. (2016). Ransomware Digital Extortion: A Rising New Age Threat. Indian Journal of Science and Technology.

[5] Kyungroul Lee, S.-Y. L. (2017). Machine Learning based File Entropy Analysis for Ransomware Detection in Backup Systems. IEEE.

[6] Nadeem Shah, M. F. (2017). Ransomware - Threats, Vulnerabilities And Recommendations. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH.

[7] SECHEL, S. (2019). A Comparative Assessment of Obfuscated Ransomware Detection Methods. Informatica Economică, 45-61.

[8] Amazon. (2021). Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF).

[9] Vytarani Mathane, P. L. (2021). Predictive Analysis of Ransomware Attacks using Context-aware AI in IoT Systems. International Journal of Advanced Computer Science and Applications.

[10] Damien Warren Fernando, N. K. (2020). A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques. IoT 2020, 551-604.