"Innovations in Science and Technologies" scientific electronic journal
ISSN: 2181-321
www.innoist.uz
Volume 1
Issue № 3
APRIL, 2024

ADVANCING TOOLS FOR SAFEGUARDING COMPUTER SYSTEMS AGAINST RANSOMWARE THREATS

To'rayev Davron Chinpo'lot o'g'li
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
davronshohofficial@gmail.com

Abstract: This abstract discusses modern methods and tools designed to protect computer systems from ransomware attacks. It emphasizes the need for continuous development of such tools in response to the evolution of threats and attack techniques. Various approaches are discussed, including network defense mechanisms, anomaly detection algorithms, and the utilization of artificial intelligence and machine learning. Current trends in tool development are analyzed, and recommendations for future research and practical applications are proposed.

Key words: ransomware, computer security, cyber threats, defense mechanisms, anomaly detection.

I. INTRODUCTION

In an age where digital transformation accelerates, the threat landscape against computer systems has become increasingly complex and hazardous. Among the myriad of cyber threats, ransomware stands out as a particularly insidious adversary, capable of inflicting significant damage and financial loss to individuals, businesses, and even entire organizations. As ransomware attacks continue to evolve in sophistication and scale, the imperative to develop and advance tools for safeguarding computer systems has never been more pressing.

This paper explores the ongoing efforts and advancements in developing tools specifically tailored to defend against ransomware threats. By delving into the latest methodologies, technologies, and strategies, this research aims to shed light

on the proactive measures undertaken to fortify computer systems against the pernicious effects of ransomware. From network defenses to anomaly detection algorithms, and from leveraging artificial intelligence to harnessing the power of machine learning, a comprehensive examination of diverse approaches underscores the multifaceted nature of combating ransomware.

Furthermore, this introduction outlines the key components of this exploration, providing a roadmap for navigating the intricate terrain of defending against ransomware. By elucidating current trends in tool development and proposing recommendations for future research and practical applications, this paper endeavors to contribute to the ongoing discourse surrounding cybersecurity and resilience in the face of evolving cyber threats.

II. METHODS

Definition of Information Security (InfoSec)

Information security (InfoSec) is a set of measures and technical tools aimed at preventing the dissemination of confidential information about societal objects, which could cause direct or indirect harm to their operations. Such information may include protection of businesses from competitive threats or employee misconduct, confidential production technologies, state secrets, and even personal data. All of this can be exploited for selfish purposes. Information security exists to prevent such occurrences.

The Three Main Principles of Information Security

Information security is based on three key principles that enable a comprehensive approach to its implementation. These principles include system confidentiality, integrity of security measures, and availability.

System Confidentiality

Ensuring information security is directly linked to handling sensitive confidential information and personal data. Care should be taken with all data throughout the analysis chain. Only authorized subjects verified through checks

should be able to view the analyzed information, while it should remain closed to all others.

Integrity of Security Measures

This principle advocates for viewing information security provision as a unified, integral process without exceptions or leniency unless predetermined. Such an approach provides an impartial assessment of the state of affairs and reflects the real picture of what is happening.

Availability

This refers to the ability of approved subjects to access any part of the information and the readiness of security services to process requests.

Threats and Risks of Information Security

A threat is both a potential and actual action aimed at causing material or moral harm to an enterprise or an individual. Naturally, for the most effective establishment of data protection processes, it is necessary to understand the risks and possible threats a company may encounter. There are three main groups of threats commonly identified:

Technological threats (associated with equipment or technology malfunctions within the protected system, as well as the use of specialized technical tools and software). These risks may include:

- Use of pirated software and license circumvention;
- Integration of malicious software (viruses, encryptors, backdoors, blockers, mining programs, etc.);
- DDoS attacks;
- Phishing;
- Physical and software audio and video surveillance tools, etc.

Let's illustrate the implementation of an information security threat due to technological reasons. For instance, the Play ransomware attack on the IT company Xplain in Switzerland, resulting in damage to the local railway network and

numerous government agencies. Hackers gained access to over 1.3 million files, including 65,000 documents of the Swiss Federal Government. Play successfully executed the information security threat through a phishing campaign containing malicious software.Another example dates back to 2010 when the Win32/Stuxnet network worm spread across a large number of private and public computer systems. This virus exploited vulnerabilities in the Microsoft Windows system (a zero-day vulnerability) and intercepted and modified the information flow between Simatic S7 programmable logic controllers and SimaticWinCC SCADA system workstations (Siemens). Win32/Stuxnet could be used for industrial espionage and sabotage (its original purpose). It became the first malicious software in history to cause physical damage to equipment in addition to digital data harm. Infected USB drives became its primary means of distribution.

Anthropogenic threats (associated with intentional or accidental dissemination of confidential commercial information):

- Insider leaks;
- Errors in fulfilling job duties;
- Actions of untrustworthy employees.

Ransomware - is a type of malicious software that blocks users' access to computer systems and encrypts files, granting control to cybercriminals over any personal information stored on victims' devices. Subsequently, cybercriminals threaten victims to either leave their files/computer inaccessible or expose their confidential data unless a ransom is paid (in English, the word "ransom" denotes hence the origin of the name for this type of threat).

Ransomware operates as a tool of extortion, and there are numerous ways cybercriminals utilize this type of malware to gain access to victims' devices. One of the most common delivery methods for ransomware to potential victims is through phishing email campaigns—victims receive emails purportedly from

familiar and trustworthy sources, which actually contain malicious attachments that, when executed, infect the computer.

Upon successfully gaining control of the victim's computer, the perpetrators proceed to encrypt some or all of the user's files, such as Word documents, PDFs, images, databases, and more. Ransomware may also spread to other devices connected to the victim's computer network, infecting additional computers or even the entire organization if the victim's computer is on a corporate network.

At the end of the process, the cybercriminal sends the victim a message explaining that their files are now hacked and encrypted, and they can only be decrypted if a ransom is paid. The ransom is typically demanded in the form of an untraceable bitcoin payment, which is to be paid to the perpetrator.

III. RESULTS

Ransomware, a type of malicious software used by cybercriminals, operates by blocking access to a system or encrypting data. Once a computer or network is infected, cybercriminals demand ransom from their victims in exchange for restoring access to the data. To protect against ransomware infections, it is recommended to exercise vigilance and use security software. Victims of ransomware have three options after infection: they can pay the ransom, attempt to remove the malicious program, or reboot the device. The attack vectors used by ransomware Trojans mainly include remote desktop protocol, phishing email messages, and software vulnerabilities. Thus, ransomware attacks can target both individuals and companies.

Detection of Ransomware - Key Differences

There are two main types of ransomware:

Lockscreen ransomware: This type of malware blocks essential computer functions. For example, access to the desktop may be restricted, and the mouse and keyboard partially disabled, allowing interaction only with a window containing the ransom demand for payment. Additionally, the computer may be rendered inoperable. The good news is that lockscreen ransomware typically does not target

important files; its aim is simply to lock your device. Therefore, the complete destruction of your data is unlikely.

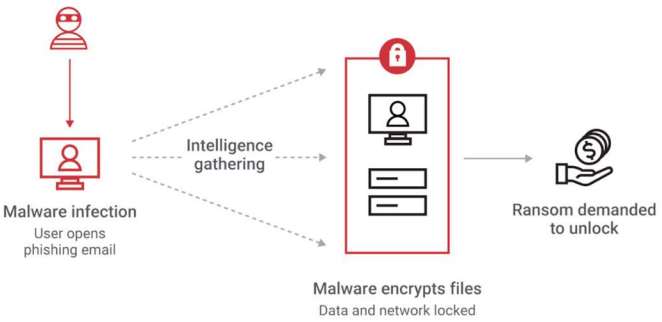

Fig.1. Ransomware structure of processing

Encrypting ransomware: The goal of this type of ransomware is to encrypt important data, such as documents, images, and videos, without interfering with the basic functions of the computer. This often causes panic as users can see their files but cannot access them. Developers of such ransomware often add a countdown to the ransom demand, threatening to delete all files if the ransom is not paid by the specified deadline. Considering the number of users unaware of the necessity of creating backups in cloud storage or on external physical devices, encrypting ransomware attacks can have extremely negative consequences. Therefore, many victims pay the ransom simply to retrieve their files.

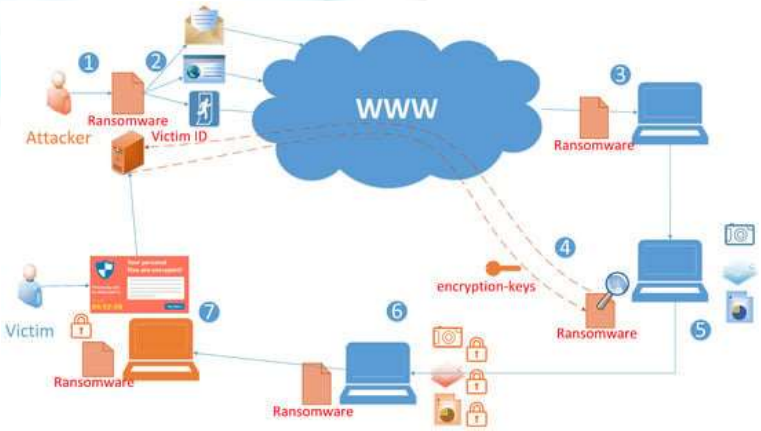

Fig.2. Steps of ransomware life cycle.

First, the developer creates a new version of ransomware. They may take advantage of various ransomware development kits, such as Torlocker, TOX, or Hidden Tear. Solutions like Ransomware-as-a-Service (RaaS) have also facilitated the easy deployment and dissemination of new ransomware variants via cloud platforms. This reality has empowered individuals without advanced skills to contribute to the design and development of new ransomware iterations.

Once the virus is prepared, the attacker spreads the ransomware in search of victims. The most common infection vectors include phishing or spam emails, exploit kits (malvertising), downloader and trojan botnets, social engineering tactics, and traffic distribution systems (TDS), among others. The infection vector may contain the ransomware code itself or malicious links to connect to a server and download the threat. Upon arrival, the ransomware scans the environment and collects user information. It identifies the host and generates a unique device ID. Subsequently, the ransomware attempts to connect to the Command and Control (C&C) server to obtain an encryption key. In the next step, a malicious search process is executed, typically targeting common file extensions such as docx, jpg, pptx, xlsx, and others.

Once the ransomware obtains the encryption code and locates the victim's files, it proceeds to encrypt them. The original files are deleted, and the encrypted files are usually renamed. Finally, the infected device executes a malicious process and displays the attacker's ransom demand. This message includes payment instructions, such as the deadline for payment or the preferred payment method (e.g., bitcoin transaction).

IV. DISCUSSION

Ransomware Analysis

In the contemporary landscape, the research community is actively engaged in developing innovative methods and strategies to mitigate ransomware attacks, encompassing the entire analysis process to ensure information security across three main branches: prevention, detection, and prediction. The fundamental idea

underlying these concepts is to diagnose the state of the device and anticipate potential attacks. Subsequently, based on gathered information, appropriate countermeasures or actions are determined. To achieve this goal, intelligent methods have been introduced in current research, such as Bayesian Networks (BN), decision trees, Support Vector Machine (SVM), among others. Each of these branches focuses on specific activities, as outlined below:

Prevention: This area pertains to actions taken to prevent or minimize the likelihood of a ransomware attack. These actions may include maintaining an updated operating system, installing or utilizing specialized applications, among others. It also involves creating file backups to mitigate the risk of extortion. The primary objective of this phase is to address system vulnerabilities or security loopholes exploited in the past.

Detection: This phase aims to employ various mechanisms to detect ransomware attacks either during or after they occur. The core concept of detection is to assess the end devices and identify suspicious events or conditions. By doing so, it becomes possible to thwart a potential attack in its early stages, thereby minimizing its impact on the system. Detection may encompass both proactive and reactive responses.

Prediction: This area is focused on preemptively thwarting attacks before they occur. This is achieved by gathering different parameters or connections from end devices, analyzing this information, and correlating it to predict potential attacks. Intelligent techniques play a crucial role in prediction, enabling users to implement countermeasures to halt or prevent an attack.

In this context, the following section presents current research categorized by prevention mechanisms and detection/prediction approaches. It is important to note that prediction and detection are often used interchangeably, with some authors referring to the detection phase as "early prediction". This section also provides descriptions of these proposals and their characteristics.

Detection and Prediction:

To effectively assess the actual state of the end device and deploy countermeasures in response to a suspicious event, it is imperative to understand the underlying conditions and how to address them. In this regard, the analysis process commences with data gathering or feature extraction. During the detection phase, this information is correlated and analyzed, enabling predictions based on a set of metrics. Subsequently, if a significant event is detected or predicted, a proactive or reactive response can be implemented. Numerous proposals utilize different approaches and intelligent techniques to aid in the detection and prediction process.

For instance, Gangwar et al. [13] proposed a mechanism for ransomware detection by analyzing patterns such as file paths, network activity, dropped files, ransom footprints, among others. Various metrics were collected through exploit kits, and subsequently, application payloads were analyzed, encompassing both goodware and malware samples. Decision tree algorithms such as J48 Decision Tree, Random Forest, and Naive Bayes were employed to classify these patterns. Additionally, a dynamic analysis approach was proposed to detect ransomware within user data by observing file system activities. This approach involves recording a registry of file access rates, monitoring user activity on their device using Process Monitor software, and considering parameters such as registries, process activity, network traffic, and entropy in the analysis process. FileAccesses within the file system were logged, and screenshots of execution were captured.

V. CONCLUSION

In conclusion, the threat of ransomware continues to evolve, posing significant challenges to information security. However, advancements in research and technology offer promising avenues for mitigating these risks. Through the concerted efforts of the research community, innovative methods and strategies have been developed across the prevention, detection, and prediction fronts.

In the realm of prevention, actions aimed at closing system vulnerabilities and enhancing security measures play a critical role in reducing the likelihood of

ransomware attacks. These measures include maintaining updated operating systems, deploying specialized applications, and implementing robust backup protocols to safeguard against data extortion.

Detection mechanisms serve as a vital line of defense against ransomware threats, enabling the timely identification of suspicious events or activities. By leveraging intelligent techniques and proactive monitoring, organizations can swiftly respond to potential threats and minimize their impact on the system.

VI.REFENENCES

1. Cleary, G.; Cox, O.; Lau, H.; Nahorney, B.; Gorman, B.; O'Brien, D.; Wallace, S.; Wood, P.; Wueest, C. ISTR 2018. *Internet Secur. Threat Rep.-Symantec* **2018**, *23*, 80–89.

2. Azmoodeh, A.; Dehghantanha, A.; Conti, M.; Choo, K.K.R. Detecting Crypto-ransomware in IoT Networks based on Energy Consumption Footprint. *J. Ambient Intell. Hum. Comput.* **2017**, *9*, 1141–1152.

3. Eset, E. *ESET Security 2018*; Technical Report; ESET: Bratislava, Slovakia, 2018.

4. O'Brien, D. Ransomware 2017, An ISTR Special Report. Symantec. Available online: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf (accessed on 5 April 2019).

5. Kumar, M.S.; Ben-Othman, J.; Srinivasagan, K. An Investigation on Wannacry Ransomware and its Detection. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 1–6.

6. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E.C. Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection. *arXiv* **2016**, arXiv:1609.03020.

7. Monika; Zavarsky, P.; Lindskog, D. Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Caracterization. *Procedia Comput. Sci.* **2016**, *94*, 465–472.

8. Bajpai, P.; Sood, A.K.; Enbody, R. A Key-management-based Taxonomy for Ransomware. In Proceedings of the 2018 APWG Symposium on Electronic Crime Research (eCrime), San Diego, CA, USA, 15–17 May 2018; pp. 1–12.

9. Kelley, D. *Cybesecurity in the Cognitive Era: Priming your Digital Immune System*; Technical Report; IBM: Somers, NY, USA, 2016.

10. Endsley, M.R. Design and Evaluation for Situation Awareness Enhancement. *Proc. Hum. Factors Soc. Annu. Meet.* **1988**, *32*, 97–101.

11. Conti, M.; Gangwal, A.; Ruj, S. On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective. *Comput. Secur.* **2018**.

12. Hernandez-Castro, J.; Cartwright, E.; Stepanova, A. Economic Analysis of Ransomware. *arXiv* **2017**, arXiv:1703.06660.

13. Gangwar, K.; Mohanty, S.; Mohapatra, A. Analysis and Detection of Ransomware Through Its Delivery Methods. In Proceedings of the International Conference on Recent Developments in Science, Engineering and Technology, Gurgaon, India, 13–14 October 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 353–362.

14. Moore, C. Detecting Ransomware with Honeypot Techniques. In Proceedings of the 2016 Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan, 2–4 August 2016; pp. 77–81.