Journal of Data Applications
Issue: 1, 2023
E-ISSN: 2980-3357

İSTANBUL UNIVERSITY PRESS

RESEARCH ARTICLE

An Improved Protection Approach for Protecting from Ransomware Attacks

Ferhat GUVÇİ[1,2], Ahmet ŞENOL[3]

ABSTRACT

Ransomware is a type of malicious software that has become a significant threat to the security and availability of computer systems and data. Ransomware has found a special place in the world of malware and is the subject of many scientific studies, as it is a malicious software designed to benefit the user directly by using sensitive data of individuals or institutions. This research provides an in-depth study of ransomware, including its history and evolution. The primary objective of this research is to analyze the impact of ransomware attacks on organizations and individuals and to evaluate the effectiveness of existing countermeasures and mitigation strategies.

To achieve this objective, a comprehensive review of the literature and security provider sources on ransomware was conducted and data analyzed from real-world ransomware incidents. The findings indicated that ransomware attacks are becoming more sophisticated and complex, targeting a wide range of industries and geographical regions, which poses a significant financial and reputational risk to victims.

Moreover, this research showed that traditional security measures such as antivirus software, firewalls, and backups may not be sufficient to prevent or recover from ransomware attacks. Instead, artificial intelligence applications and a multi-layered defense approach that combined technical, administrative, and legal measures is necessary to reduce the likelihood and impact of ransomware incidents.

Overall, this article provides a valuable contribution to the understanding of ransomware threats and the development of effective countermeasures, and contributes to the literature especially on defense methods by explaining how to apply defense methods against ransomware attacks in light of field experience.

Keywords: Encryption, Machine Learning, Malware, Ransomware

DOI: 10.26650/JODA.1312412

[1]Uskudar University, Cyber Security Masters Degree Program, Istanbul, Turkiye
[2]İHS Kurumsal Teknoloji A.Ş., 34718, Istanbul, Turkiye
[3]Uskudar University, Faculty of Engineering and Natural Sciences, Department of Computer Engineering, Istanbul, Turkiye

ORCID: F.G. 0009-0005-4329-8550;
A.Ş. 0000-0001-9891-4596

Corresponding author:
Ferhat GUVÇİ,
Uskudar University, Cyber Security Masters Degree Program, Istanbul, Turkiye
E-mail: ferhat.guvci@st.uskudar.edu.tr

Submitted: 09.06.2023
Revision Requested: 09.06.2023
Last Revision Received: 07.07.2023
Accepted: 09.07.2023

Citation: Guvci, F., & Senol, A. (2023). An improved protection approach for protecting from ransomware attacks. *Journal of Data Applications, 1*, 69-82. https://doi.org/10.26650/JODA.1312412

Introduction

Ransomware is malicious software that locks your computer or blocks access to your data using private key encryption until a ransom is paid. It can spread through malicious links or attachments in emails, downloads from malicious websites, or drive-by downloads. Once installed, ransomware encrypts files on the computer and demands payment in exchange for a decryption key. If the ransom is not paid, the files remain encrypted and inaccessible. Ransomware attacks can be highly costly as they can lead to significant data loss and disruption in business operations (Richardson & North, 2017).

The secure storage and protection of information against constantly changing and evolving cyber-attack vectors are becoming increasingly important. Cyber-attacks are on the rise worldwide, causing significant financial damage to both individuals and organizations, amounting to millions of dollars. Among malicious software, ransomware holds a significant position in terms of financial harm. Ransomware, a customized and specialized form of malware, is designed to threaten the integrity and accessibility of data by encrypting and stealing it, aiming to profit through extortion.

This study focused on examining ransomware and its impact, explaining the working principles of ransomware, exploring how artificial intelligence and machine learning algorithms could be utilized for protection against ransomware, and providing information on methods to safeguard against such malicious software.

Literature Review

Numerous studies have been conducted in the world on the status of ransomware activities and methods of protection. Maurya et al. (2017), examined the historical development of ransomware and the general characteristics of popular types of ransomware. They studied the attack principles of different types of ransomware and conducted research on infection types and revealed how systems were affected by ransomware attacks. Richardson and North (2017), presented a brief history of ransomware, the arguments for and against paying the ransom by detailed research on the payment methods and the best practices to prevent an infection, how to specifically deal with an infected machine, and recover from an infection should one happen. Askarifar et al. (2018) did in-depth research on WannaCry, one of the most popular ransomware applications, and discussed how cybercriminals bypass computer defensive systems, and how WannaCry, as well as other types of ransomware, affected computer systems overall.

While traditional threat-based databased defense methods were often used for this purpose in the past, today we see that these methods are supported by artificial intelligence and machine learning Fernando et al. (2020) conducted a survey about how machine learning and deep

learning algorithms contributed to detection of ransomware attacks. They investigated the contributions of research into the detection of ransomware malware using machine learning and deep learning algorithms and attempted to identify weaknesses in machine learning approaches and how they could be strengthened.

Kapoor et al. (2021) presented Detection Avoidance Mitigation (DAM). They devised a framework including tools, strategies, techniques to avoid, detect and mitigate Ransomware since there was no such consolidated framework. Gwozdenko (2023) did a comprehensive study on how artificial intelligence could be used against ransomware and made important recommendations for future AI-shaped protection systems. In addition, the study took a visionary approach to predict future ransomware attacks with the help of machine learning algorithms and how to take necessary precautions before an attack occurs.

History of Ransomware

The history of ransomware dates back to 1989 when the first known ransomware, called the AIDS Trojan, was created by Joseph Popp. The initial ransomware was distributed on floppy disks to participants at the World Health Organization's International AIDS Conference. It used simple symmetric cryptography to encrypt file names, and tools to decrypt and the encryption key were released shortly afterward. In May 2005, the first modern ransomware, known as the GPCoder Trojan, spread through spam email attachments. In 2013, CryptoLocker emerged as notorious ransomware and spread in an unprecedented manner. It gained momentum by disguising itself as an email from well-known courier companies like UPS and FedEx. The original CryptoLocker version could encrypt 67 different file types. With subsequent versions, the software made it difficult to trace the attacker by accepting payments in Bitcoin. It demanded two Bitcoins from its victims, later increasing to ten Bitcoins. By December 2013, over 250,000 machines had been infected by this malicious software (Teodoro et al., 2021). By the end of 2015, the total ransom payments made by CryptoLocker victims reached around $27 million, according to estimates from the FBI. CryptoLocker used asymmetric cryptography for encrypting the files it targeted, directly attacked and encrypted the 'My Documents' folders by design. In January 2016, a ransomware named KeRanger emerged, which was the first ransomware attacks targeting Apple systems. KeRanger was primarily distributed through a compromised version of the Transmission BitTorrent client, a popular macOS application used for downloading files through the BitTorrent protocol. Attackers managed to infiltrate the official website of Transmission and replace the legitimate software installer with a malicious version containing the KeRanger ransomware. KeRanger needed three days to be activated and successfully encrypted more than 300 file types (Maurya et al., 2017). In April 2016, a ransomware named Petya emerged, which encrypted the entire hard disk and denied access without paying the ransom. Petya worked by overwriting the Master

Boot Record (MBR), rendering the operating system unable to recreate unencrypted files and leaving victims with the option to either pay the ransom or replace the disk. In 2017, the Bad Rabbit and WannaCry attacks gained global attention and affected numerous international companies. WannaCry exploited a vulnerability in the Windows operating system called EternalBlue, which was allegedly developed by the U.S. National Security Agency (NSA) and later leaked by a hacker group called The Shadow Brokers. The ransomware propagated through the network by scanning for vulnerable systems and exploiting the EternalBlue vulnerability to gain unauthorized access. The WannaCry ransomware attack impacted more than 150 countries and resulted in damages reaching up to $1 billion within a week, with at least 100,000 organizations worldwide being affected (Askarifar et al., 2018).

In the years 2020 and 2021, another prominent ransomware attack software was NetWalker, also known as Mailto. NetWalker used asymmetric cryptography for the encryption process. This malicious software made a name for itself by incorporating the COVID-19 pandemic into its attacks, reaching a large audience through phishing emails related to the coronavirus. One example which targeted K-Electric, Pakistan's largest private power utility company, demanded $3.85M initially, $7.7M after a week. NetWalker collected around 2,795 Bitcoin (roughly $30M as of mid-September 2020 Bitcoin value), purportedly making it one of the most profitable active variants of ransomware (Health Sector Cybersecurity Coordination Center, 2020).

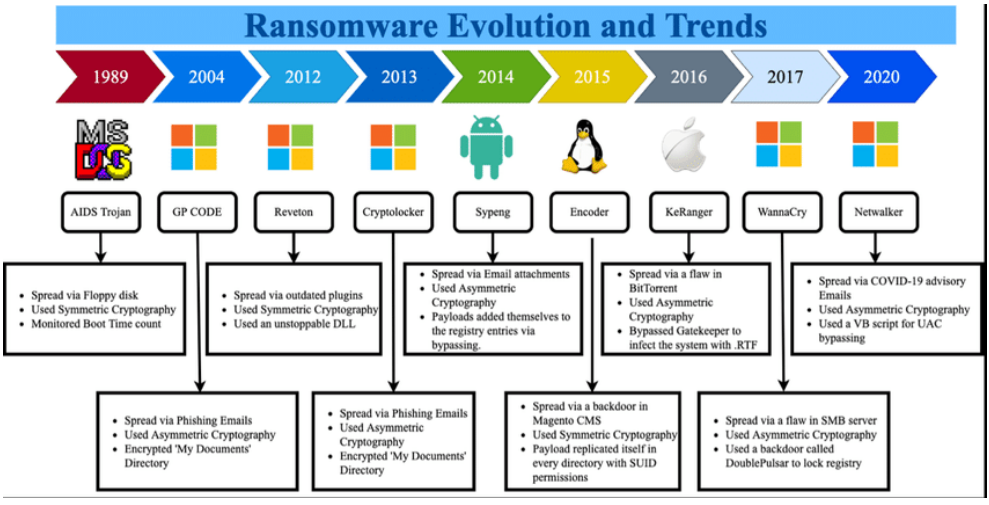

Figure 1. *Ransomware Evolution and Trends (Kapoor et al., 2021).*

How Ransomware Attacks Happen

The attack process is very similar across ransomware types. Attackers gain unauthorized access to a system or network through various methods, such as phishing emails, exploiting vulnerabilities, social engineering, or compromising weakly protected credentials. Any malicious website enters the victim's machine via email attachment or any malicious link and uses it as a base. When it starts running on the victim's machine, it establishes a connection to the Command and Control server. It sends the victim's machine information, reconnaissance information of other machines in the vicinity to the attack center and receives a randomly generated symmetric key from there. After obtaining the encryption key, it searches for specific files and folders to be encrypted (Monika et al., 2016). In some cases, it searches all disk drives, network shares, and removable drives to encrypt its data, without looking for the file path for encryption (Monika et al., 2016). Meanwhile, the malware deletes backup folders, all restore points and shadow copies. When the encryption process is completed, a message about what happened to the victim is displayed or the victim is directed by showing the directory where this message is located (Monika et al., 2016).

Stages of a Ransomware Attack

It is possible to classify the attack stages for ransomware attacks as follows (Dwyer, 2021).

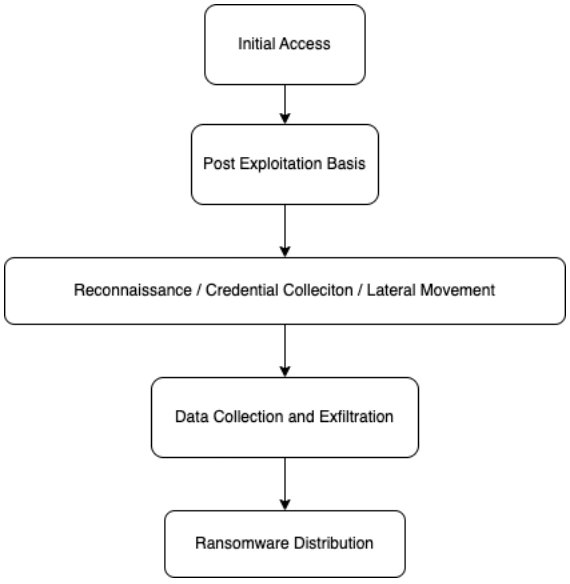

Figure 2. *Ransomware attack stages.*

Initial Access

The initial access stage of a ransomware attack is the phase where attackers gain their first unauthorized entry into a targeted system or network. It is the crucial point where the attackers exploit vulnerabilities, employ social engineering techniques, or use other means to establish their access to the targeted system.

The most common initial access vectors for ransomware attacks are email attachments, flash drives, malicious advertising (malvertising), social media, and SMS (Kapoor et al., 2021). The vast majority of phishing attacks that result in a ransomware event are carried out using known trojans and derivatives such as Bazar, TrickBot, QakBot or Valak, and the next stage is passed after the first access to the system through these pests (Dwyer, 2021).

Post Exploitation

Affected by the initial access vector, a remote access agent (RAT) or malware may be used in the next stage after which interactive access will be gained with an offensive security tool such as Cobalt Strike or Metasploit. It's important to note that the post-exploitation phase can vary depending on the specific attack and the objectives of the attackers. The activities mentioned above are common in many ransomware attacks, but the exact methods and techniques employed can differ.

Reconnaissance / Credential Collection / Lateral Movement

In the third phase of the attack, the attackers focus on understanding the local system and domain they are currently accessing and obtaining credentials to enable lateral movement. Local system discovery is usually done with built-in tools such as net, whoami, and tasklist.

Ransomware attacks use open-source utilities like AdFind to facilitate domain discovery. Such programs basically work as a command line Active Directory query tool, which were created by blending the features of ldapsearch, search.vbs, ldp, or dsquery tools.

The attackers enter the commands they want to run in a file in the script (batch) format they have created to collect information and save the outputs of these commands in different text files and use them to expand their knowledge about the environment. They usually forward this information to command and control servers. Some general discovery commands are shown below.

Table 1. *Adfind commands and outputs.*

Command	Action
adfind.exe -f "(objectcategory=person)" > ad_users.txt	Finds all person objects and saves in ad_users.txt
adfind.exe -f "objectcategory-computer" > ad_computers.txt	Finds all person computers and saves in ad_computer.txt
adfind.exe -sc trustdmp > trustdmp.txt	Finds all person computers and saves in trustdmp.txt
adfind.exe -subnets -f (objectCategory-subnet)> subnets.txt	Finds all subnets and saves in subnets.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt	Downloads all trust objects and saves in trustdmp.txt
adfind.exe -sc domainlist > domainlist.txt	Lists all domain naming contexts and saves in domainlist.txt
adfind.exe -sc dcmodes > dcmodes.txt	Lists the modes of all Domain Controllers and saves in dcmodes.txt
adfind.exe -sc adinfo > adinfo.txt	Shows Active Directory information and saves in adinfo.txt
adfind.exe -sc dclist > dclist.txt	Lists the names of the Domain Controllers and saves in dclist.txt
adfind.exe -sc computers_pwdnotreqd > computers_pwdnotreqd.txt	Lists the users who are not forced to use passwords and saves pwnotreq.txt

Although credentials can be collected by many access trojans, Mimikatz, ZeroLogon, and PrintNightmare are generally popular and used to obtain credentials that are then used for the rest of the attack (Dwyer, 2021).

In ransomware attacks, after Network and Active Directory reconnaissance movements, lateral movement is usually carried out via a server message block (SMB-Server Message Block) or remote procedure call (Remote Procedure Call) protocols. Additional systems may continue to collect credentials as necessary to obtain domain admin privileges (DFIR Reports, 2020).

Data Collection and Exfiltration

The focus at this stage of the attack is primarily to identify valuable data and extract it. Even if the institutions/organizations or individuals exposed to the attack are performing backup operations before the attack, the attack has achieved its purpose by threatening disclosure of data that should be kept confidential.

At this stage, it often moves laterally to additional systems to determine data what to leak, via SMB, RPC, and remote desktop protocol (RDP). They use the method of accessing and extracting data to collect before leaking it, which they can access via a RDP connection, but

data collection is mostly done over the SMB protocol (Dwyer, 2021). Tools that are often used in good faith by IT teams such as WinSCP and RClone to avoid attracting attention are the most common tools used to leak data.

Ransomware Distribution

When the above-mentioned stages of the attack are completed and this stage is reached, the ransomware is distributed to as many machines as possible to make the incident irreversible, with the aim of putting pressure on the victim to pay the ransom they want. During the ransomware distribution stage, attackers want to infect as many systems as possible to maximize the impact and increase the likelihood of victims paying the ransom.

For this purpose, they target Domain Controllers centrally where they can distribute ransomware quickly, and to load the ransomware, attackers usually use SMB from a share and payload with PsExec, WMIC, RunDll32 or tools like CrackMapExec. It is then distributed by creating scheduled tasks, a service that is provided by the Windows operating system (Dwyer, 2021).

Ransomware Detection and Prevention with Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) plays a crucial role in preventing ransomware attacks through early detection and blocking mechanisms. By leveraging machine learning algorithms, potential threats can be identified and prevented from infiltrating a system. This is particularly beneficial in the case of zero-day vulnerabilities, which are unknown to software vendors and lack patches. AI can swiftly detect these vulnerabilities, enabling security professionals to proactively safeguard against attacks. Furthermore, AI enhances the accuracy and speed of threat detection. Traditional security systems rely on predefined rules and signatures, often overlooking new or unfamiliar threats and necessitating time-consuming processes.

In contrast, AI can analyze vast amounts of data, discern patterns, and identify behaviors that indicate a potential ransomware attack. Consequently, AI outperforms conventional security systems, expediting threat detection and fortifying ransomware prevention efforts. Virtual assistants powered by AI are also instrumental in ransomware prevention. These assistants diligently monitor user behavior, scrutinizing anomalies that may signify an impending ransomware attack. For instance, sudden access to numerous files or attempts to download suspicious software trigger alerts to the security team, who then intervene promptly. Virtual assistants offer real-time guidance and recommendations to users, empowering them with knowledge on how to evade ransomware attacks and fortify their organizations. AI greatly enhances incident response during ransomware attacks. Assessing the extent of damage and

identifying encrypted files can pose challenges for security professionals (Gvozdenko, 2023). AI aids in this process by analyzing the affected system, swiftly pinpointing impacted files. This expedites the determination of the attack's scope, allowing the security team to take appropriate action promptly. Consequently, the time and resources required for responding to a ransomware attack are significantly reduced, minimizing disruption and mitigating damages caused by an attack.

As ransomware behaviors can be detected in different ways a sudden increase in the amount of encrypted data being transferred across a corporate network can be a strong indication of a potential ransomware infection. Encrypted files tend to have more random byte sequences compared to unencrypted files, leading to differences in statistical measures of randomness and information density. Therefore, performing statistical tests can be useful in determining whether a file has been encrypted or not. Following tests can be conducted to identify the encrypted files.

- Chi-square Test
- Entropy
- Arithmetic Mean
- Monte Carlo Value for Pi
- Serial Correlation Coefficient

These tests will most likely provide lots of false positive results. To minimize the occurrence of incorrect positive results in individual statistical tests, a classification machine learning (ML) model was created by security product providers. This ML model is designed to determine whether a file is encrypted or not. It considers various features, including statistical tests and other file characteristics, based on a vast dataset comprising millions of real and synthetic files of diverse types. LightGBM, a machine learning algorithm similar to decision trees, is employed by the model to autonomously discern the disparities between encrypted and unencrypted files.

Methods of Defense Against Ransomware Attacks

Most ransomware attacks have commonalities, and defenses based on these commonalities are vital in repelling attacks. The recommendations conveyed below include countermeasures against ransomware attacks, given what we know about the ransomware attack flow.

Ransomware attack prevention methods are listed as follows,

• Keeping all software and operating systems up to date by applying the latest security patches.

• Using strong passwords and two-factor authentication

• Regularly back up data and store it in an offline location.

• Using reliable antimalware/antivirus software and updating antivirus databases to always have the most current version.

• Disabling macros in Microsoft Office documents.

• Educating employees on cybersecurity best practices.

• Restricting access to sensitive data and systems.

• Monitoring of network traffic to detect suspicious activity

• Filtering of executable applications in email attachments (Mohurle & Patil, 2017).

Limitation of Privileged Access

The number of administrative accounts such as Domain Admin, Enterprise Admin, Schema Admin should be limited to a minimum and unnecessary members of the Domain Admins group, which include Domain Admin accounts, which are frequently used accounts in the execution of business processes, should be removed. Likewise, groups such as Enterprise Admin and Schema Admin, which are critical groups, should be constantly monitored, and actions such as adding, removing, or changing account passwords in these groups should be reported to the security teams as alarms and should be checked immediately.

Ordinary users should not have Local Admin rights, if there are any, they should be removed. For service accounts, Local Admin rights should be kept to a minimum. Since the backbone of ransomware attacks is the process of distributing the malware through the Domain Controller, changes in the Domain Admins and Enterprise Admins groups mentioned above should be monitored continuously and carefully. Since attackers usually prefer working outside of normal working hours, these and similar changes should be immediately reported to system administrators by the Security Operation Center, and every action to be taken by authorized users outside of working hours should be considered suspicious and followed up.End-user devices should be protected from unknown and untrusted executable files by controlling the use of removable devices and by using Application Control security solutions within the organization.

Protection of Privileged Accounts

Privileged accounts have elevated permissions and access to critical systems and data, making them prime targets for attackers. Privileged accounts should be added to the Protected Users Security Group to reduce the risk of internal credential disclosure.

The use of PAM - Privileged Access Management (Privileged Access Management) solutions within the organization is necessary for monitoring privileged accounts and performing access controls. With the use of these applications, stealing privileged accounts and taking unexpected actions within the knowledge of the system administrator can be prevented.

Management of Active Directory Structure

Unnecessary domain trusts between domains should be audited and, if unnecessary, this trust relationship should be removed. The purpose of the trust relationship is to ensure that users authorized by a domain on more than one domain can be used. If this structure is necessary and has to be used, it should be constantly monitored, and possible disasters can be prevented by creating alarms through security applications.

A group policy must be configured to allow the Domain Admin to log on only to domain controllers and to prohibit access to other domain-joined Windows systems. All systems within the organization should be configured to reject authentication attempts via legacy protocols. These authentication methods are insecure as both the username and password information are transmitted over the network and in some cases stored on the machine, so this critical information can be easily accessed by attackers.

Lateral Movement Restriction

Network segmentation policies should be strictly enforced. Access to high-risk resources should only be through specially designated management networks or pre-made jump servers should be used to access these resources.

The Network Configuration of the Institution must be carefully designed, the risk of using applications that allow file sharing and remote management with other machines on the network such as SMB (Server Message Block), RPC (Remote Procedure Call) and RDP (Remote Desktop Protocol) can be avoided through network segmentation. The more subnets are defined, and the communications of the subnets are connected to rules designed according to needs, the more restricted the horizontal movements of the attackers.

Defense Against Phishing Threats

An e-mail software security solution should be used that can detect phishing attack e-mails by checking reputation and content before it reaches the end user which plays a critical role in preventing the infiltration of ransomware into systems. Infiltration of data belonging to employees within the organization should be checked by using CTI tools, domain names that are similar to the corporate domain name should be constantly checked to prevent a possible fraudulent action against the company that could result in a ransomware attack.

Only technical measures fall short of ransomware attacks. It is very important to plan and run Awareness Training within an organization against Phishing attacks to ensure that end users are prepared for this type of attack. Using Phishing simulations with real-life scenarios, the attention and awareness levels of the end users can be increased, and measures taken against possible attacks.

Security Awareness Trainings

Ransomware attacks exploit human vulnerabilities by enticing them to click on malicious links or opening infected email attachments. By raising awareness and providing education on common attack techniques, security awareness training helps employees recognize potential threats and make informed decisions to protect themselves and their organization. Security awareness training helps employees understand the nature and scope of ransomware attacks. They learn about different attack vectors, such as phishing emails, social engineering techniques, and unsafe browsing habits. This knowledge empowers employees to be prepared, identify potential risks, and take appropriate precautions. Training sessions provide employees with practical guidelines and best practices for maintaining good cybersecurity hygiene. This includes tips on creating strong passwords, regular software updates, safe browsing habits, data backup strategies, and incident reporting procedures. These practices can significantly reduce the likelihood of a successful ransomware attack.

Patch Management

The application of security patches shared by manufacturers of the applications used on all devices without wasting time prevents possible security vulnerabilities and reduces the risk. By following the results of vulnerability scans carried out within the organization, using resources with vulnerability management standards such as the National Vulnerability Database (NVD), updates shared by cyber intelligence services, and the attack area is narrowed when updated versions of applications are used within an organization.

Using Antimalware Software

Direct defense against ransomware that will reach the target system is done by antimalware-antivirus software. Today, there is defense software that can perform advanced behavior analysis and a high level of protection can be provided against ransomware. Even if it cannot completely prevent a ransomware attack, it can ensure that the danger is noticed earlier through generated alarms (Furnell & Emm, 2017). In this way, security teams can focus on alarms and take actions to detect and reduce the damage by neutralizing the pest before later stages of the attack can occur.

Conclusion

Ransomware has become a method of cyber-attack that threatens almost every institution and individual, and it has evolved into a form that can cause serious harm to individuals and institutions today, where information is digitized and stored in digital media. Ransomware is a threat that can cause political crises at a high level by exceeding individuals and institutions through the theft of sensitive information, not only as attacks for non-material purposes. In today's cyber world, where new methods and attack techniques are added every day, defense mechanisms and individual cyber awareness needs to develop in the same way and with the same momentum.

Cyber-attacks, including ransomware attacks, have become a part of daily life in our age. Every individual needs to increase their cyber literacy, always be careful against Phishing attacks, where the first access is the most intense in malicious attacks and implement basic security controls. Apart from the measures taken individually, inspecting institutions to which an individual entrusts their data as data controllers and subjecting them to sanctions is a very important factor in making relevant investments. In this context, institutions at all levels should provide cyber security awareness in the education of each employee, increasing the time and budgets that are allocated to develop their cyber security infrastructures, inspections and exercises carried out before attacks occur, and preparing for a possible ransomware attack and disaster recovery in case of a successful attack. The readiness and viability of attach scenarios should be monitored continuously in a disciplined manner, and it is expected that the content and forms of the sanctions will be deterrent that will enable the institutions to take the necessary measures.

Acknowledgment: This work was supported in part by İHS Kurumsal Teknoloji A.Ş.

Ethics Committee Approval: Authors declared that this study does not require ethics committee approval.

Peer Review: Externally peer-reviewed.

Author Contributions: Conception/Design of Study- F.G.; Data Acquisition- F.G.; Data Analysis/Interpretation- F.G., A.Ş.; Drafting Manuscript- F.G.; Critical Revision of Manuscript- A.Ş.; Final Approval and Accountability- A.Ş., F.G.; Material and Technical Support- A.Ş., F.G.; Supervision- A.Ş.

Conflict of Interest: The authors have no conflict of interest to declare.

Grant Support: The authors declared that this study has received no financial support.

References

Askarifar, S., Rahman, N. A. A., & Osman, H. (2018). A review of latest wannacry ransomware: Actions and preventions. *J. Eng. Sci. Technol*, *13*, 24-33.

DFIR Report, Reports. (2020, August 31). *NetWalker Ransomware in 1 Hour*. https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/

Dwyer, J. (2021, November 30). *Understanding the Adversary: How Ransomware Attacks Happen.* https://securityintelligence.com/posts/how-ransomware-attacks-happen/

Fernando, D. W., Komninos, N., & Chen, T. (2020). A study on the evolution of ransomware detection using machine learning and deep learning techniques. *IoT*, *1*(2), 551-604.

Furnell, S., & Emm, D. (2017). The ABC of ransomware protection. *Computer Fraud & Security*, *2017*(10), 5-11.

Gómez-Hernández, J. A., Sánchez-Fernández, R., & García-Teodoro, P. (2022). Inhibiting crypto-ransomware on windows platforms through a honeyfile-based approach with R-Locker. *IET Information Security*, *16*(1), 64-74.

Gvozdenko, A. (2023, April). *How AI will Revolutionize Ransomware Prevention.* https://www.cynergy.app/cyber-research/how-ai-will-revolutionize-ransomware-prevention/4765/#:~:text=AI%2C%20on%20the%20other%20hand,overall%20effectiveness%20of%20ransomware%20prevention

Health Sector Cybersecurity Coordination Center (2020, September) U.S. Department of Health and Human Services,

https://www.hhs.gov/sites/default/files/netwalker.pdf

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. *Sustainability*, *14*(1), 8.

Maurya A.K, Kumar N., Agrawal A., Khan R.A(2017). Ransomware: Evolution, Target and Safety Measures. International Journal of Computer Sciences and Engineering, Volume-6,Issue-1.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 1938-1940.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, *94*, 465-472.