Science and Technology Publishing (SCI & TECH)
ISSN: 2632-1017
Vol. 8 Issue 12, December - 2024

Threats, Detection, Prevention, And Recovery Techniques For Ransomware

Akpasam Joseph Ekanem[1]
Department of Electrical and Electronic Engineering,
Akwa Ibom State University Mkpat Enin, Akwa Ibom State

Bassey, Samuel Isaiah [2]
Department of Software Engineering,
Federal University of Technology Ikot Abasi
sambassey@futia.edu.ng

***Abstract*— A sort of malicious software known as ransomware prevents access to computers and files while demanding money from the targeted companies in order to restore access to their data and/or devices. Many enterprises throughout the world have suffered financial losses and business delays as a result of ransomware attacks. There is currently no one security solution that can categorize, discover, stop, and mitigate ransomware assaults all at once. This article discusses ransomware threats, detection, prevention, and recovery tactics. There is a brief review of ransomware risks given, as well as practical advice on how to recognize, stop, and recover from ransomware attacks as well as control their spread.**

***Keywords*— WannaCry, ransomware, cybercrime, vulnerability, bitcoin, cryptocurrency, Windows, prevention, security, honeypot, machine learning (ML), intrusion detection (ID)**

1. INTRODUCTION

A malicious program known as ransomware prevents the victim from accessing their computer, platforms, and/or files [1]. According to [2], there are two main categories of ransomware: encryption or crypto and locker ransomware. Advanced encryption algorithms are used in crypto ransomware. System files are intended to be blocked, and a fee is demanded in order to give the victim the key needed to unlock the barred content. CryptoWall, Locky, CryptoLocker, and others are examples [9,10,13,15]. However, Locker ransomware prevents the victim from accessing the desktop, any apps, or any data by locking them out of the operating system. In this instance, the contents are not encrypted, but the attackers still want a ransom to unlock the compromised PC. Examples include Winlocker [2,6,7,14,16] and police-themed ransomware.

You can figure out what kind of ransomware you have by using a few different methods. The first method is to examine the encrypted files' extension. Typically, this will look like. ransom, lock, or encrypt. You most certainly have a ransomware infection if you notice one of these extensions. Examining the ransom note is another method for determining the type of ransomware. Once more, this will indicate the kind of ransomware you are dealing with. Although the ransom note frequently includes information regarding the kind of ransomware that has been used to encrypt your data, it is possible that you don't have this information on hand.

Platforms and devices can be impacted by ransomware. There are ransomwares made to target servers, mobile devices, and personal computers. The most common sort of ransomware, crypto-ransomware, or encrypting ransomware, will be the subject of this study [2].

2.0 THE NATURE OF RANSOMWARE ATTACKS

Ransomware and other sophisticated financial or data theft techniques. There are several ways that malware can spread. In order to propagate harmful content, cybercriminals merely hunt for the simplest technique to infect a device or network [4, 5]. However, the most typical ways for attackers to disseminate ransomware are as follows:

i. . Attacks by Phishers

According to [4], phishing emails are the first step in a cyberattack. By sending emails with

risky attachments (such ZIP files, PDFs, and spreadsheets) or links to malicious websites, hackers utilize phishing and spear phishing techniques to install ransomware on a victim's computer system. These malicious websites aim to deceive you into downloading malware that can infect your entire network [4].

ii. RDP, or Remote Desktop Protocol

A technical standard or protocol called Remote Desktop Protocol (RDP) enables remote access to desktop computers. Remote desktop software can use any of the three protocols: RDP, Independent Computing Architecture (ICA), and Virtual Network Computing (VNC), but RDP is the most used one. RDP was created by Microsoft and is compatible with the majority of Windows and Mac operating systems. However, ransomware typically use Remote Desktop Protocol (RDP) to attack other network nodes. Through the use of the RDP communication protocol, ransomware can propagate laterally by connecting to many computers over a network [8].

iii. RMMs and MSPs

Managed IT service providers (MSPs) can remotely and proactively monitor client endpoints, networks, and PCs. Thanks to the remote monitoring and management (RMM) process. Hackers regularly target managed service providers (MSPs) in supply chain assaults by taking advantage of the MSP's remote monitoring and management (RMM) software. The pressure on the MSP to pay the ransom increases as a result of this attack, which enables hackers to spread ransomware to all of the MSP's clients [8].

iv. Evil-looking Ads

Malvertising, or malicious advertising, is a common way to distribute ransomware. In order to connect an exploit kit to genuine internet advertising space, hackers must purchase it. When you click the advertisement, the exploit kit searches your computer for information, including information about your operating system, software, browser, and more. It will try to install malware on your computer if a vulnerability is found [6,7].

v. System Propagation

Network propagation (NP), in cybersecurity, is the process by which malware is introduced into a target network or system via email attachment or an infected USB stick. Ransomware outbreaks can then propagate laterally to other network devices and possibly crippling large enterprises. It's significant to notice that later ransomware variations have network dissemination capabilities, in contrast to the first few varieties. This is as a result of their limitations to exclusively attacking infected objects. However, ransomware variations are getting more complicated and are now able to spread to additional network-connected devices through self-propagating methods [8].

vi. Licensed Illegally

Some software has been downloaded illegally or that has been bundled with adware can contain ransomware. Websites hosting illegally downloaded software may also be more susceptible to malware or drive-by downloads. The possibility of contracting ransomware may rise when using illegal software. Additionally, users of unlicensed software might not get security updates since they don't get software updates, which raises the possibility of hackers exploiting a zero-day vulnerability [6,7,8].

vii. USB Drivers & Portable Computers

Due to their frequent use for work and capacity for significant amounts of sensitive data storage, laptops are particularly susceptible to ransomware assaults. Because they are portable and can be inserted into numerous computers, USB drives are also frequently used to distribute ransomware. Once the USB drive is plugged in, the virus on it will instantly run and infect the machine. As a result, all linked devices may get encrypted and ransomware may propagate throughout the network [6,7,8].

viii. Unpatched/Zero-Day Vulnerabilities

Hackers pay for access to zero-day vulnerabilities, which are unpatched security flaws, so they can use them to target enterprises. Zero-day flaws make it possible for hackers to set up ransomware undetected, greatly facilitating their work. By regularly managing your patches, you can increase your safety quotient by ensuring that you're using the most recent malware defenses and security updates [6,7,8].

ix. Open WiFi

Regrettably, ransomware frequently uses open WiFi to conceal itself. You need stringent measures to safeguard your data and network from the risks of free WiFi if you have remote workers who frequently access your network in public. Take into account outright banning public WiFi use, but If working in public places is unavoidable, consider using a secure 4G/5G connection, or VPN services [6,7,8].

x. Pay-For-Install Attacks

Through an infected memory stick, cybercriminals have persuaded people in important positions to install ransomware directly on a computer network. This technique gets around practically all security measures you've put in place. consider prohibiting the usage of USB devices in your organization to avoid this type of attack [6,7,8].

xi. Network Inspection

Attackers will leverage the discovery of one vulnerability to discover others that they may exploit, such as:

- ARP scanning: Converting logical (IP) addresses from physical addresses;
- Vertical scans: Checking several ports on a single IP;
- Horizontal scans: Checking multiple IP addresses for a specific port;
- Box scanning, including both horizontal and vertical scans;
- Port scanning: Looking for gaps or weak spots in a network [8].

xii. Drive-by-Downloads

Drive-by downloads are the most unsettling because they take place without your knowledge. There are various methods for this to happen:

- visiting a web page designed to host harmful software;
- Visiting a trustworthy website that has malware put into known vulnerabilities;
- Regardless, the malicious content executes ransomware and checks your device for weaknesses [6,7,8].

xiii. Text messages

With regard to ransomware that targets mobile devices, attackers may employ SMS messaging [8];

xiv. Affiliate Programs

By assisting in the further spread of ransomware, affiliate programs in ransomware-as-a-service allow other online criminals to profit from the scam [8].

xv. Social Engineering

Attacks using crypto-ransomware use a deft combination of technology and social engineering (also known as psychological manipulation) to deceive innocent victim into getting ransomware [9, 10]. As cybercriminals learn from their mistakes and improve their malicious code to be stronger, more intrusive, and more suited to dodge cybersecurity solutions, these attacks get more sophisticated day by day [10]. Because of this, each new ransomware version differs somewhat from its predecessor. Malware authors include new evasion techniques and cram their "product" with tools for piercing software holes, exploit kits, and more.

3.0 TECHNIQUES FOR DETECTING RANSOMWARE

The many detection methods used to find and recognize ransomware are covered in this section. The standard methods are covered below [3]:

i. Computer Learning

In order to build a model, machine learning (ML) includes studying the patterns in the data. When fed with fresh data, this model may then forecast the result [7]. Finding the ideal method to match the nature of the data and the desired result is the challenge with ML, though. With sufficient training data, ML has the advantage of being able to anticipate the result with accuracy. Training data should be balanced in terms of the distribution of expected results. ML is less likely to be obscured because it involves learning the pattern in the data.

ii. Hostility

Setting up a honeypot allows the malware to target fake data. The ransomware can be found after these files are accessed [21].

iii. Statistics

To better understand the key elements of ransomware, statistical analysis might be applied. But using this method as a detecting mechanism is difficult. Understanding ransomware's workings better is the goal of ransomware

analysis. On the basis of this knowledge, defense measures can be developed to stop further infections. Static analysis and dynamic analysis are two different forms of analysis that can be done. The executable file's source code serves as the foundation for static analysis. Following the alleged ransomware's execution, the dynamic analysis is conducted [3].

iv. Analysis in Static

By comparing an executable chunk of code's features to previously identified harmful code, static analysis can be completed fast. Analyzing the harmful code is simple and rapid. The ransomware can be avoided without having any chance of being executed if this detection is successful. However, when the code is encrypted, the analysis is equally ineffective. Additionally, multi-phase attacks are not effectively countered by static analysis [3].

v. Dynamic Analysis

Behavioral-based analysis is another name for dynamic analysis. A sandbox is typically used as the controlled and supervised environment in which malicious code is executed. Every action is recorded for analysis.

4.0 TECHNIQUES FOR PREVENTING RANSOMWARE

Poor cyber hygiene has been a major contributor to the success of ransomware attacks. Few and universal preventative methods are available to the general public to safeguard their devices from the devastating Ransomware. A few cutting-edge strategies for ransomware avoidance have been offered by researchers, however they are only applicable in certain settings and to certain types of ransomware, therefore they cannot be considered universal solutions. In this section, general methods for consumers to utilize to safeguard their devices from ransomware are provided.

i. On the PC locally

a) Don't keep all of your vital information on a personal computer (PC). Data backups should be kept both locally and, in the cloud, such as Dropbox, Google Drive, etc.
b) Check to see if the Dropbox, Google Drive, OneDrive, etc. Computer programs are not activated by default. Open them solely to sync data, then shut them after you're done.
c) The software and operating system should be current, including all security updates.
d) Instead of using an administrator account for regular use, utilize a guest account with restricted access. [20].
e) Word, Excel, PowerPoint, and other Microsoft Office applications' macros ought to be disabled.

ii. 4.2 On the web page.

a) 6. Browsers should no longer contain the Adobe Flash, Adobe Reader, Java, or Silverlight plugins. Instead, the browser should be configured to request authorization before activating these plugins [17,18,19].
b) 7. For improved security, change the privacy and security options of your browser.
c) 8. Browsers should be cleared of any outdated plugins and add-ons, and only the ones that are routinely used should be kept and updated to the most recent version.
d) 9. To protect yourself from the risk of possibly harmful adverts, use an ad blocker.

iii. Online conduct

a) 11. Emails from unknown senders or spam should not be opened.
b) 12. Refrain from opening attachments in spam or dubious communications.
c) 13. Do not click on links in spam or shady emails.

iv. Security software against ransomware

a) Install a trustworthy, high-priced antivirus program with a real-time scanner and an automated update mechanism.

b) Install a traffic-filtering program that offers proactive ransomware defense.

v. Training on cyber security

To prevent falling prey to a ransomware attack, workers and other system users must receive training on identifying and preventing potential dangers. They should understand the risks of opening email attachments from unfamiliar senders, for instance, and never stick in a USB drive from an unreliable source.

5.0 RANSOMWARE RECOVERY METHODS VERSION

5.1 Procedures for Data Recovery:

Step 1: Avoid paying the ransom because there is no assurance that the developers of the ransomware would release your data.

Step 2: Locate any backups that are still accessible, and think about storing your data backups in safe, off-site places.

Step 3: If there are no backups, you must attempt to use ransomware decryptors to unlock the data that has been encrypted by ransomware. The actions are shown in Figure 1.

Figure 1. How to lessen the impact of ransomware attacks

5.2 Free Methods for Decrypting Files That Have Been Encrypted

A few suggestions can help you resume normal operations when ransomware has been found.

First, keep in mind that not all tools are capable of fixing what each variant does. Additionally, because the tools are made for a particular kind of ransomware, it is best to determine which ransomware variant was responsible for the infection. Once found, the appropriate tool can decrypt your files.

Second, be sure to delete the original file or the ransomware itself before sanitizing and decrypting your system and files. Otherwise, after you complete the recovery process, the data will still be encrypted.

A wide range of ransomware, such as WannaCry, Petya, NotPetya, TeslaCrypt, DarkSide, REvil, Alcatraz Locker, Apocalypse, BadBlock, Bart, BTCWare, EncrypTile, and Globe, may be unlocked by the majority of decryptors. Unfortunately, in order to make their software more difficult to decode, ransomware producers frequently distribute the newest updates and patches. The majority of decryptors don't offer assurances because they need to update and change theirs due to this arms race.

For some of the most prevalent forms, there are currently a lot of free ransomware decryption solutions available. However, as additional ransomware decryption tools are being developed right now, the list below is not complete and probably never will be. Therefore, the victim should also use supported research. It might be challenging to safely decrypt data, therefore the victim should make every effort to be comprehensive.

i. Project to End Ransomware

The main objective of the software is to defend users against ransomware assaults. It is capable of identifying and removing the many various kinds of files that may be encrypted because it has over

100 encryption keys that act as protection measures.

To eliminate ransomware, experts from cybersecurity firms and law enforcement agencies have teamed up. In reality, this initiative has developed into a useful tool for anyone hit by ransomware [22].

Important characteristics:

- It contains decryption keys for more than 100 ransomware variants identified only in the past year.
- There are comprehensive instructions for restoring files that have been ransomware-encrypted.
- It educates users on ransomware infections and the various defenses.
- The website is updated regularly with new ransomware decryption keys on a regular basis.
- Has a separate area for reporting illegal activities, such as ransomware.
- More than 25 languages are supported by the service [22].

ii. Trend Micro File Decryptor for Ransomware

It's a fairly recent piece of software made to stop malware from entering your computer. The ransomware decryption program can also run on compromised devices and help you successfully unlock a file that the virus has encrypted.

Additionally, Trend Micro Ransom File Decryptor is a lightweight, simple-to-use application. Despite all of this, Trend Micro has previously assisted in the victory over ransomware. Its decrypting tools will keep you secure and have no negative effects on the operation of your device [23].

Important characteristics:

- A single program contains all of the decryption tools.
- It comes with decryption keys for over 25 different varieties of ransomware.
- Information on the Trend Micro website can be used to identify the type of ransomware.
- As new threats surface, the program will be updated to include new ransomware signatures.
- Trend Micro has a special help line for ransomware victims [23].

iii. Emsisoft's tool for decrypting ransomware

It is regarded as one of the top Windows-installable apps for decrypting ransomware. This kind of essential tool has always been successful in unlocking files that have been encrypted by well-known ransomware like Apocalypse, Xorist, Stampado, and BadBlock [24].

Important characteristics:

- More than sixty decryption tools are available from Emsisoft to fight a variety of ransomware variants.
- Determining the type of ransomware present requires analysis of the encrypted file.
- It offers detailed steps for restoring your data and decrypting ransomware-encrypted files.
- New features are often added to already existing decryption tools [24].

iv. Recover against McAfee Ransomware

Another great decryption program you may use to restore your encrypted files is McAfee Ransomware Recover. With the aid of McAfee Ransomware Recover, files, programs, databases, and other types of files that have been encrypted by ransomware can be restored.

Additionally, the tool that stores extra decrypting keys receives regular updates so you can always have access to them [25].

Important characteristics:

- McAfee is a kind of workhorse in the world of computer security. For instance, in response to the ongoing rise of fresh ransomware assaults, they are actively building decryption tools.

- Mr2, sometimes referred to as McAfee Ransomware Recover, is an extremely advanced decryption program.
- Among other things, it can unlock a user's files, applications, databases, and applets.
- Their decryption architecture is open source and may be changed and enhanced by anyone working in the security industry.
- It offers in-depth knowledge on ransomware [25].

v. Decrypting AVG Ransomware Program

For ransomware that encrypts files using various algorithms, AVG Ransomware Decryption Tools can be a smart choice. However, it is limited to decrypting data that have been encrypted using Apocalypse, Bart, Crypt888, Legion, or TeslaCrypt [26].

Important characteristics:

- The user interface of the antivirus program is simple and streamlined, and it has all the time-saving automatic features.
- It safeguards users against harmful links and dangers that can be downloaded.
- You may use AVG Antivirus on your mobile device to remotely scan a computer [26].

vi. Tool for 360 Ransomware Decryption

Using a tool created by the 360 Ransomware Decryption Tool team, you may remove ransomware from your computer without having to pay the demanded ransom. This was developed to aid in the removal of Petya, but it can also be used to locate the decryption key for other ransomware strains [27].

Important characteristics:

- Several separate decryption keys are bundled with a single piece of software.
- It provides decryption services for numerous new, sophisticated ransomware.
- They have a number of helpful ransomware materials on their website.
- It is an easy-to-use ransomware removal application.

vii. Free Ransomware Decryption Tool: Quick Heal

When you give Quickheal permission to scan your computer, it can quickly and effectively remove the infection while safeguarding your documents.

Before the operating system starts, Quickheal's software scans for contaminated files and deletes them. On a flash drive, the software is to be installed before being booted. Quickheal will instantly remove ransomware if it is found [28].

Important characteristics:

- A single program that comes with several decryption keys.
- It offers decryption for some of the more peculiar ransomware that is currently available.
- Their website offers useful ransomware knowledge.

This ransomware cleanup tool is straightforward [28].

viii. 8. Protective encryption with Heimdal

By identifying and thwarting attacks at the DNS, HTTP, and HTTPs layers, Heimdal Threat Prevention safeguards your endpoints and network against ransomware and data exfiltration. Ransomware authors won't stand a chance when used with the Heimdal Ransomware Encryption Protection [29].

6.0 CONCLUSION

Being watchful and proactive is one of the most effective strategies to stop the threat of ransomware from wreaking havoc and encrypting your sensitive data.

In order to stop this kind of cyber assault, it is actually advised that the fundamental and easy procedures described in this article be taken.

Every company's cybersecurity plan should include safeguarding offline copies of critical data and providing businesses with cyber-insurance. IT staff can wipe the system clean and restore the most recent backup even if fraudsters get access to PCs and infect them with ransomware. Although this won't end the double extortion ransomware problem, it can at least get the system(s) back to normal operation.

Researchers decode some strains of ransomware as new varieties appear, but others receive new forms, and it may appear to be a cat and mouse game in which being proactive is essential. Data recovery is never guaranteed even after paying the ransom because it can still be put up for sale on the Dark Web.

As a result, prevention is still the best strategy.

REFERENCES

[1] E. P. Torres P. and S. G. Yoo, “Detection and neutralizing encrypting Ransomeware attacks by Using machine-learning techniques: A literature review,’ Int. J. Appl. Eng. Res., Vol. 12, no 18, pp. 7902-7911, 2017.

[2] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, “Ransomware threat success factors, taxonomy, and countermeasures: A survey

and research directions," Comput. Secur., vol. 74, pp. 144–166, 2018

[3] SH Kok, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam,"Ransomware, Threats and Detection Techniques: A Review", IJCSNS International Journal of Computer Science and Network Security, Vol. 19 No2, pp 136-146, February 2019

[4] James, L. (2014). Phishing Exposed. Rockland, MA: Elsevier Science, pp.2,3. \

[5] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[6] Hatton, L. (2011). E-mail forensics. [New Malden]: Bluespear Pub.

[7] Aldwairi, M., Hasan, M. and Balbahaith, Z. (2017). Detection of Drive-by Download Attacks Using Machine Learning Approach. International Journal of Information Security and Privacy, 11(4).

[8] How Does Ransomware Spread? Here's What You Need to Know available at https://www.heimdalsecurity.com accessed July, 2023

[9] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[10] Rubens, P. (2017). Types of Ransomware. [online] Esecurityplanet.com. Available at: https://www.esecurityplanet.com/malware/types-of-ransomware.html, accessed July, 2023

[11] Www.03.ibm.com. (2016). Ransomware Study: Parents will Pay for Digital Memories. [online] Available at: https://www-03.ibm.com/press/us/en/pressrelease/51230.wss#release, accessed July, 2023

[12] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[13] U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, "An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[14] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[15] F-secure.com. (2019). Crypto-ransomware. [online] Available at: https://www.f-secure.com/en/web/labs_global/crypto-ransomware, accessed July, 2023

[16] Kaspersky.co.uk. (2019). Different types of ransomware? [online] Available at: https://www.kaspersky.co.uk/resource-center/threats/ransomware-examples, accessed July, 2023

[17] Essential Eight Explained. Available at: https://www.cyber.gov.au/publications/essential-eight-explained, accessed July, 2023

[18] iOS Hardening Configuration Guide. Available at: https://www.cyber.gov.au/publications/os-hardening-configuration-guide, accessed July, 2023

[19] Microsoft Office Macro Security. Available at: https://www.cyber.gov.au/publications/microsoft-office-macro-security, accessed July, 2023

[20] Restricting Administrative Privileges. Available at: https://www.cyber.gov.au/publications/restricting-administrative-privileges, accessed July, 2023

[21]. Chris Moore, "Detecting Ransomware with Honeypot techniques,"pp.77,2016

[22]. No more Ransomeware available at: https://www.nomoreransom.org/en/index.html accessed July, 2023

[23] Trend Micro Ransomware File Decryptor available at: https://success.trendmicro.com/ accessed July, 2023
[24] Emsisoft: Free Ransomware Decryption Tools available at: https://www.emsisoft.com/en/ransomware-decryption/, accessed July, 2023
[25] McAfee Ransomware Recover (Mr2) available at: https://www.mcafee.com accesses July, 2023
[26] AVG Ransomware Decryption Tool available at: https://www.avg.com/en-us/ransomware-decryption-tools#pc accessed July, 2023
[27] 360 Ransomware Decryption Tool available at: https://blog.360totalsecurity.com/en/ransomware-decryption-tool-petya-wannacry-released/ accessed July, 2023
[28] Quick Heal – Free Ransomware Decryption Tool available at: https://www.quickheal.com/free-ransomware-decryption-tool/ accessed July, 2023
[29] Ransomware Encryption Protection available at: https://heimdalsecurity.com/enterprise-security/products/ransomware-encryption-protection accessed July, 2023