ANALYSIS OF RECENT TECHNIQUES IN RANSOMWARE ATTACKS

BY

DR. NWOSU, JOHN NWACHUKWU

DEPARTMENT OF COMPUTER SCIENCE

FEDERAL POLYTECHNIC OKO

EMAIL: nwachukwunwosu@gmail.com

Phone No: 08035902385

Abstract

This study examined the recent techniques cyber criminals use to carry out ransomware attacks despite efforts by companies to guide against such attacks. Ransomware is a type of malicious software that prevents computer users from accessing computer files, system or network, and demands a ransom payment from the victim before the affected systems can be restored back to operation. The study adopted Qualitative Content Analysis Methodology. It utilized secondary data collection that were obtained from reports of ransomware attacks from well known cyber security companies that include Sopohos, Chainalysis, Cyberint, and Statista. Sophos Ltd. Company is a UK based company, Chainalysis is an American blockchain analysis that uses software to analyze the blockchain public ledger used to track virtual currencies, Cyberint is a cyber security company that is based in UK, and Statista is a German online platform that specializes in data gathering through team survey, analysis and visualization. The findings revealed that ransomware attacks are on the increase and they have great impacts on businesses, government and individuals. The most common type of attack is Ransomware-as-a-Service (RaaS). The attackers form groups which involve expert programmers that create platforms for exploits and non programmers who use the platforms created by the expert programmers to launch attack. The attack format includes the use of crypto-ransomware and lockers. The most common payment method is cryptocurrency and the manufacturing industries receive the highest form of attacks in 2023. Measures to prevent ransomware attacks include installation a good antivirus, update software regularly, use of strong login credentials, avoidance of downloading phishing mails, having backups of files, creation awareness among staff members, and use of Private Network (VPN) services on public Wi-Fi networks.

1.1 Introduction

This study examined the recent techniques cyber criminals use to carry out ransomware attacks despite efforts by companies to guide against such attacks. Ransomware is a type of malicious software that prevents computer users from accessing computer files, system or network and demands a ransom payment from the victim before the affected systems can be restored back to operation. The attack involves the cyber attackers encrypting the files, systems and networks before making request and sending decrypting codes to the victims after the ransom has been paid. With the decrypting codes, the systems can become functional again but that does not however prevent the attackers from making copies of the files they found in the system they attacked and keeping the copies in their custody. Ransomware attackers can cause costly disruptions to operation and loss of critical information and data (FBI, 2024).

Ransomware attacks have been in existence since 1989 when AIDs Trojan (PC Cyborg Virus) was released via floppy disk. Victims needed to send 189 to a P.O. Box in Panama to restore access to their systems, even though it was later discovered that the attack was a simple virus that utilized symmetric cryptography (Barer, 2022). Since 1989, after the success of extorting companies through the PC Cyborg virus attack, cybercriminals have continued to develop programs that are designed to encrypt files and systems, and demand for ransom before the files or systems can be decrypted.

The trajectory of the attacks moved from simple virus attack to more advanced threats with the emergence of bitcoins. Cybercriminals developed crypto locker in 2013 which combined the powers of encryption with bitcoin transactions using 2048-bit RSA key pairs generated from a command-and-control server to deliver attack to the victims making sure that the victim cannot access his files without payment of the ransom. The challenge however was that many victims do not have knowledge of bitcoin operation forcing the threat acts to open call centers where they employ their moles to operate).

Apart from bitcoin encryption attacks, threat actors also use data exfiltration (where they leak the data slowly leaving the most sensitive ones last), spray and pray (which involves attacking many target systems) and Big Game Hunting (BGH) techniques (which targets few victim in which they will have big payoffs). Whenever these threats are observed, companies do develop measures that reduced the ransomware attacks.

1.2 Purpose of study

The purpose of the study was to examine the techniques employed by cyber criminals to carryout ransomware attack in recent times, to find out the nature businesses that were the highest affected and the nature of ransom that were paid.

1.3 Research questions

a. What are the modern techniques cyber criminals used to unleash ransomware attack?

b. Are there new family attack structures or the attackers utilizing the old family attack structure?

c. What are the types of company that are the major victims in the recent ransomware attack?

d. What types of payments are the victims making to get back their data and get their system running?

1.4 Methodology

The study adopted Qualitative Content Analysis Methodology. It utilized secondary data collection that were obtained from reports of ransomware attacks from well known cyber security companies that include Sopohos, Chainalysis, Cyberint, and Statista. Sophos Ltd. Company is a UK based company that operates in North and South America, the Middle East and Africa. Sophos revealed that data for the ransomware report of 2024 came from a Vendor-agnostic survey of 5000 cyber security/IT leaders conducted between January and February 2024 which had respondents in 14 countries across Americas, EMEA and Asia Pacific. Chainalysis is an American blockchain analysis firm headquartered in New York city that uses software to analyze the blockchain public ledger used to track virtual currencies. Cyberint is a cyber security company that is based in UK that offers cyber threat intelligence reports and solutions to cyber security companies. Statista is a German online platform that specializes in data gathering thrugh team survey, analysis and visualization. Data selection focused on ransomware attacks especially those that analyze recent attacks, emerging new techniques and provide technical details about the attacks.

The work is organized in sections. Section 1 is the introduction, section 2 review of related literature, section 3 Findings, which revels the latest techniques threat actors adopted in their attacks, section 4 Discussion on the ways the recent attacks can be prevented, and section 5 Conclusion and Recommendations for further research.

Section 2 Literature review

2.1 Types of Ransomware

Though some people like (Growstile, 2024) suggest that there are five types of ransomware, there are two broad types of ransonmware - crypto-ransomware and lockers or locking ransomware. Crypto-ransomware or encrypting ransomware

Crypto-ransomware

Crypto-ransomware is a type of harmful program that encrypts files stored on a computer or mobile device in order to extort money (F-secure, 2024). These ransomware encrypt the files and data written in a system making the contents inaccessible until a ransom is paid and the decryption key is sent to victim which the victim uses to decrypt the files. Encryption involves accessing files and replacing the original files with the encrypted version. The encryption process involves built-in functions in the operating system. Examples of crypto-ransomware are WannaCry and Cryptolocker.

Lockers

Locker ransomware is a type of ransomware that blocks access to a device or a particular application (such as a browser) and demands a ransom to restore it (Kaspersky, 2024). These types of ransomware completely lock a system or a system’s screen so that files and applications are inaccessible. A lock screen usually display the ransom demand possibly with a countdown clock to increase urgency, urging the victim to act immediately. Examples of lockers are Locky and

Fusob. Others variants of ransomware are scareware, Doxware or Leakware and Ransomewae-as-a-Service (RaaS).

Scareware Ransomware

Scare ransomeware uses scary message to trick a user into making a click (Borges, 2024). In this approach, the threat actors can adopt crypto-ransomware approach, locker ransomware approach, or a hybrid approach that will combine both crypto-ransomware and locker approach. Scareware ransomware is fake software that claims to have detected a virus or other issues on a computer and directs the user to pay ransom for the problem to be resolved. Some types of scareware ransomware encrypts files in the system, some lock the system while others simply flood the screen with pop-ups alerts without actually damaging the files. Examples of scareware ransomware are WannaCry, Cryptolocker, FBI locker, Policelocker, Jigsaw and Makop.

WannaCry and Cryotolocker use encryption and cryptographic techniques to lock files and demand payment for the decryption key. FBI locker and Police locker use a locker approach to lock the systems or screen displaying fake warning or message. Jigsaw or Makop combine both approach, encrypting files and locking the device or screen. They may use encryption to lock the files and then display a locker-style warning or message demanding payment to unlock both the files and the file.

Doxware or Leakware

Doxware is ransomware which extorts victims by threatening to release sensitive information if a ransom is not paid (SecureMac, 2024). Like scareware ransomware, doxware ransomware can adopt crypto-ransomware approach, locker approach, or a hybrid of the methods. Doxware ransoware involves attackers threatening to distribute and publish sensitive personal or company information online, asking people to pay ransom to prevent the data from falling into wrong hands or entering into the public domain. An example is Chimera.

Ransomware-as-a-Service (RaaS)

RaaS is a business model between ransomware operators and affliliates in which affiliates pay to launch ransomware attacks developed by operators (CrowsStrike, 2024). RaaS operators can adopt both crypto-ransomware and locker ransomware approach.

RaaS operators often provide their affiliates with a range of tools and techniques to carry out attacks. Such tools and techniques include encryption algorithms to lock files, or locking capabilities to lock a system or system's screen. A RaaS kit may include 24/7 support, bundled offers, user reviews, forums and other featurers identical to those offered by legitimate SaaS providers (CrowdStrike, 2024). Examples of RaaS ransomware are REvil, Grancrab and maze.

2.2 Layers of attack

There are five major layers for ransomware attacks. These are (a) defense penetration, (b) malware deployment, (c) launch of attack, (d) demand for ransom, and (e) unlocking the system.

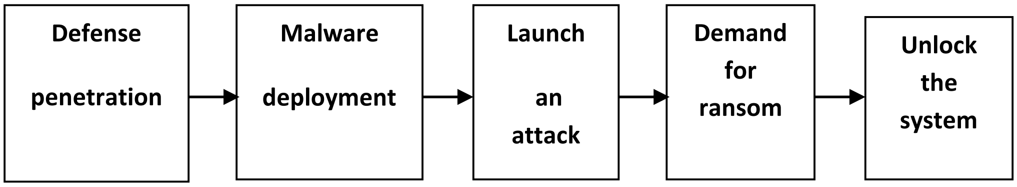

Fig. 1. Layers of ransomware attack

Defense penetration

This involves the techniques employed by attackers to penetrate the defense guards of a system. These could be done by through phishing, Remote Desktop Protocol, or through any means that will permit an attacker to exploit holes in operating system or other system software.

A malicious email may contain a link to a website hosting a malicious download or an attachment that has downloaded functionality built-in. If the email recipient falls for the phish, then the ransomware is downloaded and executed on the computer (Checkpoint, 2024). Gendre (2024) identified methods attackers use for ransomware email attacks to include inline phishing links, attachment links and fake attachments.

Another popular infection vector is Remote Desktop Protocol (RDP). RDP is a legitimately and widely used technology for remotely accessing and managing Windows systems. Many organizations use it for remote work, provision of technical support and managing servers. Attackers can launch attack by exploiting weak or default credentials, theft of credentials, or exploiting vulnerability in RDP implementation to gain unauthorized access to a system (Bullwall, 2024). Once they the attacker penetrates the system, he will deploy the malware. Sophos, UK-based security vendor analysed 150 of its incident response cases from 2023 and found RDP abuse featured in 90% of them to give threat actors remote access to Windows environment (Muncaster, 2024).

Malware deployment

Once the criminal have breached the target device, the malware is deployed. And once it it deployed, it will automatically install itself in the victim's device.

Attack

The attack process involves utilizing any of the two methods of ransomware attacks – crypto-ransomware which encrypts the files, or locking the device. If it is malware that uses encryption method, since encryption functionality is built into operating system, the process involves accessing files, encrypting them with an attacker-controlled key and replacing the originals with the encrypted versions. Some variants of encryption malware will take steps to delete backup and shadow copies of files to make recovery without the decryption key more difficult. Ransomware variants such as Maza performs file scanning, registry information and data theft befoe encryption, while WannaCry scans for other vulnerable devices to infect and encrypt (Check Point, 2024).

If it is a locker ransomware, it can simulate device locking, by opening a browser window in full-screen mode, hiding the cursor or disabling hotkeys. The attackers can equally change the password or PIN, or modify critical system elements such as the master boot record. Common known lockers are WinLock, Reveton and Lockerpin (Kerpersky, 2024).

Demand for ransom

Once the malware succeeds in encrypting the files or locking the user out of the system, the stage is now set for the criminals to make demands for ransom. Different ransomware use different approach to make demand for ransom but the most common is to have a display background changed to a ransom note or text file placed in the encrypted directory containing the ransom note or directly placed on the screen if it is a locker ransomware. The note demand a set amount of cryptocurrency in exchange for access to the victim’s files (Check Point, 2024).

Unlocking the system

Once the ransom is negotiated and paid, the ransomware operator will either a copy of the private key used or a copy of the symmetric encryption key itself for the decryption (if the system is encrypted), or they will unlock the system from their end if they used a locker method.

2.3 Notable ransomware attacks

The first ransomware attack was the AIDs program named from the 1989 World Health organization (WHO) AIDs Conference in which biologist Joseph Popp handed out 20,000 infected floppy disks to the event participants. After a user had booted up ninety times, the name of the user’s file would be encrypted and a message would appear, asking the user to send US$189 to a Post Office Box in Panama (Flashpoint, 2024). The P Cyborg hid directions and encrypted the names of all the files on the C drive preventing access to the files.The ransomware was relatively easy to remove using online decryption tools.

After the attack, the next notable ransomware attack was in 2005 - the Archieviews Trojan and GPcode. GPCode attacked Windows operating systems first using symmetric encryption and later in 2010 using more seeve RSA 1024 to encrypt document with specific file extension (Drake

2022). Antivirus was effective in handling the attack until bitcoin was introduced cybercriminals embraced cryptography.

3.0 Findings

The nature of recent attacks can be viewed from three perspectives - types of industries that have been attacked, modus of payment, and types of attack method.

3.1 Types of industries attacked

A report by Statista revealed that the manufacturing industries are top on the list of companies attacked by ransomware in 2023 with 25.7% of the attacks. This is followed by Financial institutions (18%), professional bodies, wholesale, healthcare, government, transportation, education, media and telecom (1.2%) (Statista, 2024).

A report by Sophos limited validates the report from Statista that the manufactirung industries had the most ransomware attacks in 2023. Although, Sophos report shows that the manufacturing companies witnessed 65% of ransomware attacks in 2023, an increase from the previous two years (56% in 2023, and 55% in 2022), with a 41% increase in the attacks since 2020 (Sophos, 2024).

3.2 Modus of payment

A report by Sepicyber revealed that cryptocurrency, most especially Bitcoin, is the most modus of payment to the ransomware actors. Cryptocurrency is favoured as the best mode of payment because of a number of reasons: a. it is easily accessible to the victim which makes the transfer of the ransom a smooth process; b. The payment can instantly be verified by the public Blockchain;

and c. Bitcoin provides the hacker with anonymity since the ransomware payment can easily be laundered (Sepio, 2024). Chainalysis 2024 report revealed that $1billion were paid to cryptocurrency to ransomware actors in 2023 (Chainlysis, 2024).

3.3 Types of attack method

3.3.1 Exploitation of software vulnerability

This refers to the exploitation of weaknesses or flaws in software that result from unpatched or outdated software, libraries or frameworks. These are more prevalent in operating systems such as Windows 7. A report by Sophos revealed that exploited software vulnerabilities were the most commonly identified root cause of an attack, impacting 32% of the organization. The report was corroborated by Cisco Talos research report which showed that software vulnerability exploitation is the preferred tactic for ransomware actors to gain initial access to a victim's environment (Waldan, 2024). Attackers use exploit kits such as flash exploits, Java exploits, Internet Explorer exploits, etc. to launch an attack.

3.3.2 Exploitation of network vulnerabilities

This involves weak passwords, open ports, or misconfigured network devices. A weak password is any password that doesn't follow password best practices (Trevino, 2024). Ransomware attackers use weak passwords through various methods which include brute-force attacks (automated tools that try multiple password combinations), dictionary attacks (trying common passwords and variations) and password spraying (using single passwords across many usernames).

Open ports are network ports that are not blocked by a firewall or other security measures. Commonly targeted open ports are Remote Desktop Protocol (RDP) port 3389, Server Message Block (SMB) port 445, File Transfer Protocol (FTP), port 21, Secure Shell (SS) port 22, and Hypertext Transfer Protocol (HTTP) port 80 or HTTPs port 443. Actors perform port scanning using specialized tools and launch attack if there is vulnerability opening. The easiest and most common way is brute force using local usr account such as “admin” or “administrator” (Chaudhari, 2024).

3.3 Stolen credentials

These include phishing (tricking individuals into giving out their credentials through the use of deceptive mails), or credential stuffing (using previously breached username and password pairs). Stolen credentials are a prime commodity in dark web (Juan, 2024).

3.4 Ransomeware-as-a-Service (RaaS)

A report from Sophos shows that RaaS is on the increase. RaaS is the major factor in the increae in ransomware attacks. Threat actors can seek easily exploitable vulnerabilities or opt to pay for ransomware services. RaaS gang remains active in 2023. Lockbit attacked Taiwan semiconductor manaufacturing company (TSMC) and demanded for a ransom payment of $70million. They also attacked an IT products and Services company CDW and made a demand of $80million. In 2024, the group claimed responsibility for attacks on Saint Anthony Hospital and Lurie Children’s Hospital in Chicago (pallardy, 2024).

4.0 Discussion

From the findings, ransomware attackers greatly utilize software vulnerability exploitation in their attacks. They exploit software vulnerabilities because there are many internet-connected devices which require many applications, and demand for inter-platform connectivity makes software more complex thereby opening doors for vulnerabilities. Also, some software designers use outdated system architecture which are susceptible to attack (Irwin, 2024).

Attackers also exploit network vulnerabilities because it allows attack to spread quickly and laterally across networks. Network vulnerabilities can evade traditional security measures.

Attackers utilize credential stuffing because there are many techniques they can use to get credentials of users of systems in a network. At times they buy stolen credentials from the dark web.

5.0 Preventive measures for ransomware attacks

a. Install a good antivirus

Most antivirus are anti-malware, they scan all parts of the system for virus, worms and other malicious software and prevent them from attacking the system.

b. Update software regularly

Most attacks are launched through error in program codes. When these errors are identified, they are rectified and send to users as updates. So with constant updated versions, software vulnerabilities would be avoided.

c. Strengthening of credentials

It is important to implement multi-factor authentication which requires more than one method of identification. Strong passwords are very important and users should avoid using one password on multiple accounts.

c. Avoid download of phishing mails

Most exploits are performed using phishing mails so users should avoid downloading mails that are suspicious.

d. Maintain backups

Backups are the first line of recovery from an attack. So it is important to make and keep copies of files in external disks or the cloud to fall back in case of an attack.

e. Create awareness among staff members

Let the staff members be conscious of security and keep vigilante of possible attack vectors. This will make them not to click and file that is suspicious.

f. Use Virtual Private Network (VPN) services on public Wi-Fi networks

When using a public Wi-Fi network on a system, the system I more vulnerable to attacks, therefore, use a secure VPN service which creates a secure anonymous connection between you and the Internet so that your activities and location details are hidden.

6.0 Conclusion

Ransomware attacks are on the increase in 2024 and they have great impacts on businesses, government and individuals. Businesses lose their customers, their image, and they pay heavily to restore their activities. The most common type of attack is Ransomware-as-a-Service (RaaS). The attackers form groups which involve expert programmers that create platforms for exploits and non programmers who use the platforms created by the expert programmers to launch attack.

The attack format includes the use of crypto-ransomware and lockers. The most common payment method is cryptocurrency and the manufacturing industries receive the highest form of attacks in 2023. It should be noted that at times, the ransomware attacker may not be able to unlock the system after collecting ransom if he uses auto random key generation.

7.0 Recommendations

a. Businesses should adhere strictly to the procedures for protecting their systems against ransomware attacks.

b. More research should explore Artificial Intelligence (AI) and Machine Learning (ML) use for threat detection and response.

c. Businesses should collaborate in establishing Analysis Centres where they will sgare information on threats and mitigation processes.

8.0 References

Baker, k. (2022). History of ransomware. Retrieved from http:// www.crowdstike.com on 30th July 2024.

Borges, E. (2024). 7 popular ransomware. Retrieved from http://www.recordfuture.com on 11th July 2024.

Bullwall (2024). How has RDP become a ransomware gateway and what to do about it. Retrieved from http://www.bullwall.com on 10th August 2024.

Chainanalysis(2024). Rasomeware on the increase. Retrieved from http://www.chinalysis.com on 13th September 2024.

Chaudhari, V. (2024). How ransomware launch ransomware using RDP attacks and how to stop them. Retrieved from http://www. Linkedin.com on 8th August 2024.

Drake, V. (2022). The history and evolution of ransomware attacks. Retrieved from http://.www.flashpoint.com. on 12th July 2024.

FBI, (2024). How can we help you? Retrieved from http://www.fbi.gov/how-we-can-help-you on 15th August 2024.

Flashpoint (2024). The History and Evolution of ransonware attack. Retrieved from https://www.flashpoint.com on 12th July 2024.

F-Secure(2024). Crypto-ransomware. Retrieved from http://www.f-secure.com on 11th July 2024.

Gendre, A. (2024). Four ways hackers use to launch ransomware attacks. Retrieved from http://www.Vadesecure.com on 12th July 2024.

Irwin, L. (2024). 6 reasons why software is becoming more vulnerable to cyber attacks. Retrieved from http://www.itgovernance.eu/blog on 12/9/2024.

Juan, H. (2024). Dark web: lifecycle of stolen credentials explored. Retrieved from http://www preyproject.com on 7th July 2024.

Kaspersky (2024). Locker ransomware. Retrieved from http://www.kaspersky.com on 12th September 2024.

Muncaster, P. (2024). RDP abuse present in 90% of ransomware breaches. Retrieved from http://www.Infosecurity-magazine.com. on 10th June 2024.

Pallardy, C. (2024). 2023 ransomware hits $1.1billion record. Retrieved from http://www.informationweek.com on 13th July 2024.

Satista (2024). Report on ransomeware attacks. Retrieved from http://www.satista.com on 11th September 2024.

SecureMac(2024). What is Doxware? Retrieved from http://www.securemac.com/blog on 13th August 2024.

Sepio (2024). Ranso,ware payment. Retrieved from http://www.sepiocyber.com/blog on 5th September 2024.

Sophos (2024). Reansmware attacks 2023. Retrieved from http://.www.sophos.com on 12th August 2024.

Trevino, A. (2024). How weak passwords lead to ransonmware attacks. Retrieved from http://www. Keepersecurity.com on 17th July 2024

Waldam, A. (2024). Ransomware gangs increasingly exploiting vulnerabilities. Retrieved from http://www.techtarget.com on 3rd September 2024.