IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# ELEMENTS IMPACTING THE SPREAD OF RANSOMWARE AND PREDICTIONS FOR FUTURE PROBLEMS

**Dr. KAYALVIZHI.R1$^{st}$, Dr. D. JAYAPRABHA2$^{nd}$, Ms. P. LAKSHMI3$^{rd}$**

$^{1}$Assistant Professor$^{1st, 2nd ,3rd}$
Department of Computer Applications$^{1st ,2nd ,3rd}$

ST. THOMAS COLLEGE OF ARTS AND SCIENCE1$^{st ,2nd ,3rd}$, Koyambedu, Chennai

*Abstract:* A difficult threat known as "crypto-ransomware" encrypts user files and demands a ransom to be paid by the victim in order to obtain the decryption key. Cybercriminals can make a significant profit from this kind of malware, as it generates millions of dollars in income annually. Due to the inefficiency of traditional detection-based defenses like antivirus and anti-malware software in thwarting attacks, ransomware is becoming increasingly widespread. Moreover, this particular infection employs advanced encryption algorithms and targets a broader spectrum of file formats. Cybercriminals benefit from this, and no one is safe from becoming their next victim. File encryption ransomware targets both small and large enterprises as well as regular home users. In this research, we look at how ransomware spreads by analyzing the factors that put an individual or an organization at risk of falling victim to its demands. Finally, we make some recommendations based on our projections regarding the future evolution of ransomware.

***Index Terms*** **-** Ransomware, Cybersecurity, Antivirus, Malware, Ransomware prevention, Ransomware detection

## I. INTRODUCTION

Ransomware is a type of malware that resembles extortion and targets computers by encrypting and/or locking user data. Demanding a ransom to unlock compromised devices or release/decrypt user data is the primary goal of these attacks. Ransomware is now a serious threat to electronic assets (data and computers), impacting not just individuals but also governments, hospitals, businesses, and other institutions. For example, in May 2021, a ransomware assault occurred at Colonial Pipeline, one of the biggest companies in the US and the manager of the nation's largest petroleum pipeline on the east coast. This compelled the corporation to spend 4.4 million to restore control of its stolen resources, cease regular business operations, and go offline. Crypto ransomware includes this kind of ransomware. The goal of crypto ransomware is to encrypt your important files, including photos, movies, and documents, but not to interfere with basic computer functions. This raises concerns because users can view their files but not access them. The impacts of crypto ransomware can be severe since a large number of users are unaware of the importance of creating backups in the cloud or on external physical storage devices. A countdown to the ransom demand is sometimes included by cryptocurrency developers. For example, "All your files will be deleted if you don't pay the ransom by the deadline." Many victims so simply pay the ransom to get their files back. Cryptocurrencies, such as Bitcoin, are digital currency designed to function outside of the mainstream financial system. Cryptocurrencies are decentralized money because they record transactions using block chain technology. The buying and selling of digital money, also referred to as cryptocurrency transactions, is mainly managed by a crypto-exchange platform. These transactions are attractive to cybercriminals because they usually involve substantial sums of cryptocurrency and are usually anonymized by the block chain. Like any other system, cryptocurrency trading platforms and procedures are vulnerable to cyberattacks. Bitcoin's creator, Satoshi Nakamoto, proclaimed it to be a cryptocurrency in 2008. The most well-known cryptocurrency is called Bitcoin. Bitcoin was developed in 2009 with open-source software. It is an online financial system devoid of a physical nation, radix, or central banking system. The most widely used decentralized payment system is called Bitcoin, and it fully supports a distributed public ledger. A block chain is created by a few anonymous individuals who manage the maintenance and growth of a distributed public ledger that records Bitcoin transactions. Block chains are composed of implemented blocks. The majority of Bitcoin transactions are completely digital and anonymous. Because of this, a large number of cybercriminals have resorted to Bitcoin as a safe way to conduct illegal activities, such paying ransomware. Payment gateways are the target of a malicious code known as ransomware, which requests a ransom to be paid in exchange.

## I. Ransomware

As we have already discussed, the two main types of ransomware are crypto ransomware and locked ransomware. Both kinds of ransomware usually start off as links to websites or email attachments. Once the victim opens the file or clicks the link they received, the ransomware uses known operating system weaknesses to attack their computer.

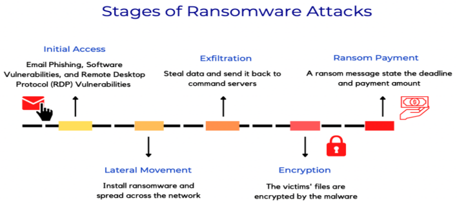
Stages of Ransomware Attacks
Initial Access
Email Phishing, Software Vulnerabilities, and Remote Desktop Protocol (RDP) Vulnerabilities
Exfiltration
Steal data and send it back to command servers
Ransom Payment
A ransom message state the deadline and payment amount
Lateral Movement
Install ransomware and spread across the network
Encryption
The victims' files are encrypted by the malware

Fig 1. Stages of Ransomware attack.

When crypto ransomware becomes activated, it automatically encrypts a few important user files. Instead of targeting the victim's whole hard disc, the ransomware in this case only targets a few important files depending on their file extensions. This attack usually uses a 24-bit encryption technique, which is very difficult to decrypt without a key. In addition to emails and websites, ransomware can also propagate through exploit kits.

When an exploit kit is used, the victim is infected through a hacked website; they are not required to open the attachment or click the website link. Subsequently, the hacker requests payment from the target, typically in Bitcoins. The difficulty in tracking down the attacker is the rationale behind the decision to use Bitcoins to pay the ransom. The hacker transmits the unlock key if the victim gives the requested amount. Data loss occurs when hackers fail to provide the decryption key, even after receiving payment. Certain contemporary ransomware attacks capitalize on vulnerabilities in operating systems and self-replicate to propagate throughout the network.

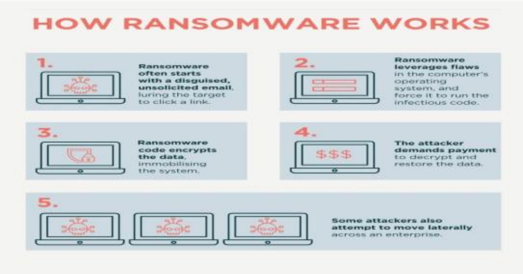
HOW RANSOMWARE WORKS
1.
Ransomware often starts with a disguised, unsolicited email, luring the target to click a link.
2.
Ransomware leverages flaws in the computer's operating system, and force it to run the infectious code.
3.
Ransomware code encrypts the data, immobilising the system.
4.
$$$
The attacker demands payment to decrypt and restore the data.
5.
Some attackers also attempt to move laterally across an enterprise.

Fig 2. Ransomware work.

## 2. Ransomware Targeted Attacks

The data around ransomware is thoroughly examined in this paper from a number of perspectives in order to support, understand, and direct future research endeavors. The numerous ransomware strains that have been around since 2005, the quantity of data that has been impacted, predictions for upcoming infections in the near future, research challenges, and prevention strategies are the main topics of this study. This research further examines the key causes of being targeted by ransomware attacks, which are as follows:

1) User behavior: Research indicates that 70% of employees worldwide are unaware of cybersecurity risks, and the majority of users are not aware of how to use the internet safely. 2) The main source of ransomware targeting is fraudulent email According to CSO Online, emails comprise 92% of the vectors used to deliver dangerous software. 3) A 2018 NETSCOUNT study on the high percentage of easily hackable IoT devices reveals that it just takes five minutes to launch an IoT device attack.4) Connected system backups,5) The usage of malicious websites outside from social media platforms is another growing source. Authors have gone into detail about the various techniques used by researchers to study ransomware as well as the state of the field's research on the virus.

## 3. Malware Analysis

A common method for comprehending the elements and actions of malware, including ransomware, is malware analysis. The purpose of this study is to identify malware attacks and stop them from happening again. Static and dynamic analysis are the two main categories into which malware analysis falls. While dynamic analysis examines a process's behavior and activities while it is in execution, static analysis examines the contents of binary files. "Signature-based malware detection" is a static analysis technique that finds unique patterns in the malicious file to identify it. This is relevant to ransomware and can include looking at the ransomware notes, analyzing the unique byte sequences within the binary file, or determining the function call order. Next, the signature can be contrasted with signatures of known malware samples. The main advantages of signature-based detection are its quick detection times and low false-positive rate, which account for its widespread use. On the other hand, malware that conceals itself using techniques like binary packing for code obfuscation may evade detection. Because dynamic analysis does not rely on studying the binary code itself, it is less susceptible to these evasion techniques than static analysis, which searches for significant patterns or signatures that point to the maliciousness of the examined file. Furthermore, signature-based methods are ineffective against recently developed malware. Some of the processes that ransomware uses to infect a user's machine can be discovered through analysis. For instance, Bajpai and Enbody discovered that.NET ransomware first tries to achieve execution rights before contacting a C&C server to retrieve the encryption key. They accomplished this by doing static and dynamic analysis on decompiled.NET ransomware samples. In order to cause significant network propagation and subsequent damage, Zimba and Mulenga (Zimba and Mulenga, 2018) looked at the static and behavioral properties of the WannaCry ransomware. They found that WannaCry retrieves the network adapter properties to determine whether it's residing in a private or public subnet. Through malware analysis, ransomware's distinct features can be found, which can subsequently be utilized to inform the creation of detection or prevention systems.

and low false-positive rate, which account for its widespread use. On the other hand, malware that conceals itself using techniques like binary packing for code obfuscation may evade detection. Because dynamic analysis does not rely on studying the binary code itself, it is less susceptible to these evasion techniques than static analysis, which searches for significant patterns or signatures that point to the maliciousness of the examined file. Furthermore, signature-based methods are ineffective against recently developed malware.

**4.Ransomware challenges and prevention techniques**

Law enforcement and cybersecurity vendors are especially conscious of the threat that ransomware poses. The publicizing of new attack techniques and the periodic education of the public about them forces criminals to adapt their strategies. Criminals are constantly searching for novel approaches to hide their attack strategies and their elusive payment methods. People and institutions need to be more cautious in such situations. Table 1 discusses some notable challenges that may arise during prevention from Ransomware attacks and their possible solutions

| Challenges | Prevention techniques |
|---|---|
| An IoT device that has previously been compromised could not always respond to a simple reset, requiring the user to pay a ransom. | To overcome this challenge, researchers should develop some techniques for the early detection of ransomware. The seller of IoT devices should also supply a list of data file extensions that are safe to use on an IoT network. |
| The diversity of IoT networks may make it difficult to implement a single security policy. | For full protection against ransomware attacks, IoT devices should be able to mitigate ransomware over the whole application execution lifetime. |
| Criminals employ malicious emails and URLs to advertise; sometimes, these advertising attract new users, who then click on the link. | To overcome this issue, employers could provide their employees with training on trustworthy websites. Additionally, IoT security needs to be mentioned to prompt the user |
| One of the problems with ransomware is the way it spreads over networks. | Organizations should restrict user rights to protect data security. To avoid causing disruptions to the network, malicious nodes must be promptly discovered. As soon as an infection is discovered, the compromised system needs to be shut down. |
| Abuse of one's privileges | Restricted rights |

Table 1. Ransomware challenges and prevention techniques.

Being watchful is essential in addition to the previously discussed preventive measures since, as the adage goes, "precautions are better than cures." To protect themselves from having to pay the ransom, both individuals and organizations must implement best practices. A variety of best practices have been suggested by the FBI, including limiting access, performing frequent backups, turning off Java and macro scripts, enforcing laws limiting software usage, and training staff members on ransomware awareness. See his coverage on ransomware in Android devices, smart homes, criminal networks, and e-health apps for more reading on ransomware in various sectors.

## 5.Conclusions

The paper offers a comprehensive examination of the detrimental effects of ransomware. For researchers, information security professionals, and average users, ransomware is undoubtedly growing in importance with the advent of cybersecurity technology and the growth of the Internet of Things. Given that ransomware has changed since its early phases of proliferation, the essay offers some predictions on potential problems in the future. Future studies will concentrate on comprehending the various ways that ransomware influences user behavior in homes and enterprises in order to develop more resilient security measures to repel it.

## 6.Future works

Ransomware is the primary problem with recent technological advancements. However, this development needs a safe and secure path to continue growing. Future development is challenged by the increase in ransomware assaults, which is an open study topic. In the future, we'll continue to search for more efficient solutions to reduce ransomware.

## References

1. Tomer B. Newest CTB-locker campaign bypasses legacy security products. 2015. [cited 2015 Jan 28].
2. Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS 2016); 2016 Jun 22–24; Denver, p. 97–111
3. An ISTR Special Report: Ransomware and Businesses 2016". Symantec corporation. 2016. [accessed 2016 Nov 3]
4. Furnell SM, Katsabas JD. The challenges of understanding and using security: a survey of end-users. Comput Secur. 2006;25(1):27–35.
5. Yali S. Anatomy of CryptoWall 3.0 – a look inside ransomware's tactics. 2015. [accessed 2016 Nov 3].
6. Choi KS, Scott TM, LeClair DP. Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. Int J Forensic Sci Pathol (IJFP). 2016;4(7):253–258.
7. Sittig FS, Singh H. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Appl Clin Inform. 2016;7(1):624–632. DOI:10.4338/ACI-2016-04-SOA-0064.
8. Hillick M. Scareware traversing the world via a web app exploit. Bethesda (MD): SANS Institute InfoSec Reading Room; 2010.
9. Brulez N. Ransomware: Fake Federal German Police (BKA) notice. 2011. [cited 2011 Mar 24]. Available
10. Savage K, Coogan P, Lau H. Security response – the evolution of ransomware. Mountain View (CA): Symantec Corporation; 2015.