Evolution of Ransomware in Cyber Security

Kedar Desai

School of Technology

Pandit Deendayal Energy University

Gandhinagar, India

Kedar.dce20@sot.pdpu.ac.in

Smit Raval

School of Technology

Pandit Deendayal Energy University

Gandhinagar, India

Smit.rce20@sot.pdpu.ac.in

Viral Parmar

School of Technology

Pandit Deendayal Energy University

Gandhinagar, India

Viralparmar93@outlook.com

***Abstract*-**Ransomware is a computer virus that makes a victim's computer inoperable, and criminals are increasingly using it to earn income. Ransomware is a sort of malicious software that prevents a person or organisation from accessing data on a computer. By encrypting these data and demanding a ransom payment in exchange for the decryption key, hackers drive companies into a position where paying the ransom is the simplest and least costly method for regaining access. Over time, the evolution of ransomware assaults has occurred.

I. INTRODUCTION

In this research paper we have discussed how ransomware attacks have evolved over the period of time. We have also discussed what are the different types of ransomware. Basically there are 2. We have discussed the modes of transmission of the ransomware .We have analysed 15 papers and analysed how the ransomware has evolved over the period of time. We have discussed what are the common modes of transmission of the ransomware. We have further analysed how the ransomware is spreading and why it is spreading so fastly. Then we analysed how exactly the ransomware works and what are their primary targets. Then we discussed why it is so hard to find ransomware perpetrators. Then we saw the evolution of ransomware over the period of time with the help of a timeline table. We also discussed the prevention and detection methods. Then we discussed in detail about the prevention practices in the ransomware attacks. Then we discussed how early detection of the ransomware attack can help us and why it is important to prevent yourself from ransomware attacks. And discussed the different types of detection methods to detect the ransomware. Then we have added our own proposed methodology on how we can be prevented from any type of ransomware attacks. After that we have discussed the future work in ransomware.

II. LITERATURE REVIEW

No longer dominated by lone wolves, cybercrime has evolved into a criminal enterprise. Criminals increasingly employ ransomware, a form of malware that encrypts a victim's computer or data and demands payment to regain access. This study contributes to the authors' understanding by examining the transition from early con games to the extortion techniques employed by modern ransomware. They investigate the evolution of ransomware, from the earliest primitive attempts to the most advanced ransomware attack strategies. The damages caused by this crypto war are estimated to cost $1 billion. Given that many Internet users appear unaware of ransomware and take no action to defend themselves, they argue that this low-impact extortion using highly automated methods has proven to be extremely lucrative for criminals. Because they were early adopters (or abusers) of Internet technologies, criminals believe that ransomware will continue to surpass the capabilities of existing defence mechanisms. We learned how ransomware is delivered to the client's server, how it operates, and how data can be recovered.How the attackers distribute ransomware in the client's system and gain access to the computer's data by taking advantage of system flaws, browser, and email security weaknesses. Attackers initially used symmetric encryption keys, but as time went on and encryption technology advanced starting in 2006, attackers began to use asymmetric key encryption methods. With ransomware assaults, attackers also employ social engineering to psychologically manipulate victims into divulging important information or making security blunders. Attackers also employ exploit kits, which are malicious software programs that scan client machines for software flaws and identify them to use such flaws to upload ransomware.[1]

Thanks to several advancements in information technologies, ransomware has significantly increased in prevalence, from the first malware that pretended to be a fix for a problem to the current sophisticated virus that demands massive amounts of money. Criminals are now increasingly adept and proficient at breaking into complex information systems thanks to this progress. Computer networks and systems that have been subjected to ransomware attacks typically also contain additional harmful software infestations. Because ransomware victims are now more informed, vigilant, and skeptical of malware, hackers have had to come up with inventive ways to respond. The evolution of ransomware is examined in this essay from the perspective of what makes a person or a business susceptible to caving into the rising demands of malware. We conclude by making a few forecasts regarding likely future ransomware tendencies. The primary topics covered in the research paper include ransomware targets, the evolution of the ransomware, installation on the victim's computer, the origin of the ransomware, projections for the future, and difficulties associated with ransomware assaults.[2]

Over the last two decades, ransomware has changed from opportunistic operations to meticulously planned assaults as its devastating consequences have intensified. The proliferation of ransomware has persisted, hurting both people and businesses. Others have experienced losses in the hundreds of millions of dollars, while others have been compelled to pay their assailants up to $1 million each assault. Enterprise systems face an inescapable new cyber danger in the form of ransomware. In this paper, we examine how the advent of ransomware and the corresponding paradigm changes in attack strategies have affected technology and finance. We developed an attack model in consideration of the cascading network architectural structures of the typical corporate system. We compared the security state of the ransomware assault process to the state transitions of a finite state machine, in which there are violations of confidentiality, integrity, and availability. We provide a classification system for ransomware virulence based on a suggested categorization technique derived from the File Encryption and Data Removal attack architecture. In categories from CAT1 to CAT5 with increasing severity, potential data retention solutions without paying the ransom are evaluated based on their technical capability and overall effectiveness. Using a WannaCry attack use scenario, we assessed our modelling technique and proposed best practises and mitigation methods based on these models.[3]

Due to its capacity to spread, the ransomware attack that caused problems in 2017 was referred to as a network worm. Because of the encryption, this type of security assault behavior caused academic and corporate viewpoints to re-evaluate how to retrieve the data and how to address this security catastrophe before the ransom spread itself throughout the entire Data Architecture. The research only focuses on the most difficult aspect of crypto-ransomware, which urgently requires protection before asymmetric encryption affects the core of the Big Data Architecture. All of the concepts from the systematic review have been reviewed. \* The majority of ransomware (2017) only demands payment if the entire system is encrypted, however, SeCBD already does automatic recovery when we see changes to major files and decoy files. Researchers discovered that by developing a secure recovery and prevention mechanism, the majority of Crypto-Ransomware assaults may be stopped. Since the makers of ransomware are always innovating, further development of this concept application is encouraged.[4]

Cybersecurity has always been problematic because it was a computer-related issue. Distribution of ransomware is a criminal action, in addition to other security issues. Although personal computers have only been utilizing it since 2015, networks have been using it since 2005. When compared to locks, both ransomware may be understood: the one prohibits the victim from utilizing their things but permits them to enter the house; the second forbids entry to the victim's home by securing the gate with an unidentified lock. Researchers have separated history into two phases: before and after ransomware since the frequency of ransomware assaults increased when it became a service. Shortly, it will help researchers and society at large save data by displaying ransomware safety suggestions. The review provides a summary of the evolution of ransomware, along with information on its effects on the system, mode of operation, and methods for defending our data against attacks.[5]

Malware is an issue that continues to worsen with time. Malware that spreads like a worm and stops users from accessing their computers until a ransom is paid by locking the system screen or encrypting and locking user data. Opening illegal links and attachments in emails is a typical method of spreading ransomware attacks, thus users should avoid doing so. Using secure cloud email security gateways that prevent the transmission of suspicious emails by isolating them in the cloud, businesses may further enhance their spam prevention. This solution offers an extra degree of protection compared to on-premises email security gateways that confine all emails to your physical mailbox and require them to be downloaded. Once Microsoft's WannaCrypt ransomware protection update becomes available, we may infer that everyone (individuals and organisations) should prioritise updating their Windows PCs. Microsoft has published fixes for operating systems that are not officially supported, illustrating the magnitude of the WannaCry malware danger.[6]

A kind of ransomware exerts control over computers by encrypting or locking their data. The repository stores all I/O activities carried out by ransomware strains, enabling analysis tools to examine file access operations. In this investigation, ransomware activity from over 70 samples captured while encrypting user data is made available as a repository. Other authors may test the specified ransomware detection method using these samples, which were assessed using the available traces. We propose utilising this statistics to compare the performance of various ransomware detection systems. As a consequence, we have classified detection techniques according to whether they can be completely or partly tested against this data. Over 86% of tools may be assessed at least in part based on network activity or ransomware behaviour affecting user data, according to our findings.[7]

Georgia, United States, Kennesaw State University [summary] The danger posed by ransomware to the information assets of people and corporations is growing dramatically. We discuss the history of ransomware, the pros and cons of paying the ransom, and the best techniques to prevent infection and recover if you get infected. Locker ransomware just encrypts the device; saved data is often unharmed. It encrypts the data, making access impossible even if the virus is uninstalled from the device or the storage media is relocated to another location. Since crypto ransomware does not target critical system data, the device may continue to operate even after infection; nonetheless, the device may have to pay the ransom (Savage, Coogan, & Lau, 2015). Between 2014 and 2015, ransomware assaults climbed by 17.7%, while crypto ransomware attacks surged by 44.8%, according to a Kaspersky research. (2016) According to Townsend.[8]

During the 1970s and 1980s, experts and researchers with Internet access conducted beneficial simulated assaults on the whole network. The number of recorded mobile ransomware files increased by more than 86% during the quarter, reaching 218,625 compared to 61,832 in the preceding quarter. Recent reports of actual insects To avoid these sorts of assaults, network security providers faced a formidable obstacle.[9]

Ransomware is a significant danger to the security of information resources. Journal of Regional Development, volume of Journal of Social Transformation Since its start, ransomware has developed and become more destructive, inflicting greater harm to the internet ecosystem (Chhillar, 2017). Ransomware is a sort of virus that spreads like a worm and locks the system screen or encrypts and locks users' data until a ransom is paid (Deo and Farik , 2015). Crypto ransomware is the first kind of ransomware. Because malware deployed by spear phishing enables thieves to gain a range of information about individuals or businesses, criminals see this assault as a major triumph if it is effective.[10]

Elsevier B.V. is the publishing company. Information Systems Security Management, Concordia University of Edmonton, Edmonton, Alberta, Canada, T5B 4C4. This content is publicly available and distributed under Creative Commons licence BY-NC-ND. The primary objective of this report is to give information on the development of ransomware from its inception to March 2016 by analysing samples of various ransomware variants from recognised malware families in Windows and Android environments. The investigation comprised eight Android malware families and seventeen Windows ransomware families. By paying closer attention to the permissions asked by Android applications, at least three ransomware variants per malware family may be prevented. When payment is not received, has began to do much more than reveal vital information to the general public. Using the detection techniques given in Section V, we can validate the provenance of any ransomware samples we employ.[11]

In this post, we discuss a variety of cyber threats to corporate infrastructure. We are primarily interested in ransomware (RW), its variations, and its growth.

There have been a sizable number of cyberattacks as a result of the COVID-19 pandemic and the increase in home offices.

Cybersecurity research from the first quarter of 2020 indicates a rise in the incidence of ransomware (RW). This study also attempts to explore the many attack types, how malware spreads to different systems, and the preventative steps that may be taken to lessen the likelihood that it will infect every machine in a network. Both conventional network antimalware software and several additional packet filtering methods have failed to stop these attacks.

Using current examples of assaults that concentrate on integrated extortion, they have also tried to show how the virus evolves. Private data is taken during ransomware attacks and then encrypted. If victims choose not to pay for a decryption key, attackers will threaten to make stolen data public. The target is still vulnerable as a result of this tactic, even after system backups.[12]

The economics of ransomware have shifted. Occasionally, threat actors employ network or email routes to exfiltrate data from target networks before encrypting or otherwise restricting access to the original material. They then demand payment to have access to the victim's data. When elements of a ransomware epidemic are delegated to external actors, ransomware attacks frequently become more specialised and complex. Since its discovery in 1989, ransomware has progressed a long distance due to greater expertise and other advancements. Although finance remains the primary motivation, ransomware has evolved into a sophisticated menace that may do more harm.

Two varieties of ransomware exist: locker and crypto. Infected computers with locker ransomware are locked, preventing users from accessing their data. The data on a target machine is encrypted by crypto-ransomware.

In both cases, ransomware operators demand payment to unlock or decrypt data.

Some threat actors may mix ransomware and lockers in hybrid attacks. A third, less common kind of ransomware either does not supply the decryption key or is unable to do so owing to technical restrictions.

These assaults, known as wiper ransomware, are either damaging by purpose or the outcome of ransomware-related technological difficulties. Since 2013, crypto-ransomware has dominated the ransomware landscape.

It has been established that healthcare-related environments are far more susceptible to ransomware's disruptive effects than other industries.[13]

Extortion against people is currently taking place on a scale that has never before happened in human history. Recently, as personal internet and computer usage has surged, fraudsters have developed to take advantage of this burgeoning market by preying on unwary consumers with a variety of malware. Most of these threats are meant to deprive the victims of money, either directly or indirectly. Ransomware is currently one of the most difficult malware subcategories.

Ransomware is basically of two types. Crypto ransomware, which encrypts files and personal data, is the most prevalent kind at now. The locker ransomware, on the other hand, locks the computer and prevents people from accessing it.

In this study, we'll examine the operation of various ransomware variants from both a technological and psychological standpoint. We will also examine the development of these threats, the circumstances that have led to ransomware becoming the significant issue that it is today, and the likely locations for the next outbreak of ransomware.[14]

This study addresses the use of ML and DL approaches in investigations to identify ransomware attacks. The external nature of ransomware, the difficulty of eliminating a ransomware epidemic, and the need of preventing malware from accessing a system were the primary motivations for this investigation. As machine learning plays a larger role in the battle against ransomware, we looked for methods' shortcomings and ways to strengthen them.

Ransomware poses a particularly serious threat since new families and variants are consistently being discovered on the internet and dark web. Because of the nature of the encryption techniques they employ, ransomware outbreaks are challenging to recover from.

This increase in ransomware is also associated with the growth of artificial intelligence. Given that machine learning and deep learning can detect ransomware, there is a tremendous deal of interest in studying these approaches.

In this survey, we examine well-known research articles that all demonstrate the effectiveness of ML and DL in identifying ransomware viruses. These papers are picked based upon how frequently they were referenced in other studies. We conducted experiments to find out how the evolution of malware affects the research projects that were mentioned.

We also looked at the different routes that ransomware is taking and how we predict it will change over the next several years, including its growth into the Internet of Things (IoT), which is becoming more and more interwoven into homes and infrastructure.[15]

III. RANSOMWARE FROM SCRATCH

A.*About Ransomware*

An advanced kind of virus, ransomware, may lock away private files or information on a computer until a ransom is paid. In order to extort money from their targets, hackers often restrict access to data using a binary encryption key.

For companies, hospitals, schools, and other organisations that regularly rely on this information, ransomware attacks may be devastating. In the majority of instances, refusing to pay the ransom may result in the irreversible loss or exposure of critical data.

B.*Common modes of transmission of ransomware attacks*

* Email phishing
* Visiting vulnerable sites (drive-through downloading)
* Downloading corrupted file documents or malware-infested documents
* Risks to the system and its connections
* Tackling the remote desktop protocol (RDP)

*C. Types of ransomware*

Small enterprises and large corporations alike might fall victim to ransomware attacks. Malware of this kind has the potential to encrypt anything from a single file (such a document or image) to an entire database, potentially exposing highly sensitive information. There is a wide variety of ransomware, but most of it can be categorised into two broad categories. Lockers and cryptominers are at the heart of this malicious software.

*1. Crypto Ransomware:* By encrypting crucial computer data, crypto ransomware makes them inaccessible. Cybercriminals that utilise crypto-ransomware assaults gain income by holding victims' data as ransom and demanding ransom payments to unlock it.

### *2. Locker Ransomware:* Locker ransomware, unlike crypto-ransomware, does not encrypt data. It goes a step further by offering to lock the victim out of their device. Cybercriminals will demand a ransom to unlock the victim's device during these attacks.

### Both sorts of assaults might force patients to try a return to normality. It is vital to prepare your systems for recovery in order to prevent them from becoming targets of cyberattacks.

*D. Reason of ransomware spreading*

For a variety of reasons, ransomware attacks and their variations are rapidly evolving to circumvent defensive measures.

* Malware development tools are readily available and may rapidly generate new malware samples.
* Cross-platform ransomware is created using well-known, dependable generic interpreters (for e.g. Ransom32 uses Node.js loaded with JavaScript).
* utilising unique techniques, such as ciphering the whole disc as opposed to specific files

Modern thieves do not even need technical sophistication. Online markets for ransomware have emerged to provide malware strains to would-be criminals and generate extra cash for the software's producers, who often want a portion of the ransom payment.

*E. Working of Ransomware*

Ransomware needs access to a victim's computer in order to encrypt its data and demand payment.

Even though the specifics of each ransomware variant's distribution are distinct, they always follow the same three phases.

vectors of infection and distribution: Similar to other infestations, ransomware has several entrance ways into a system. However, ransomware developers pick a limited number of distinct attack paths.

There are also phishing emails. A malicious email may include an attachment that contains a downloader or a link to a website that offers a malicious download. When a recipient falls for phishing, ransomware is downloaded and run on their computer.

The Remote Desktop Protocol and other services are often abused by ransomware as attack vectors (RDP). An attacker may utilise RDP to remotely access and authenticate to a corporate network-connected computer after getting or guessing an employee's login credentials. This access enables the direct download and execution of malware on the controlled machine.

While WannaCry used the EternalBlue vulnerability in a passive manner, others may attempt to launch an aggressive assault on computers. The infection vectors used by modern ransomware are often several.

If ransomware successfully encrypts all of your data, it will eventually ask you to pay up. This may be done in a number of ways, depending on the specific strain of ransomware, but often involves either a ransom note being shown as the new backdrop of the screen or a text file being added to each locked directory. These messages often ask for a certain amount of bitcoin in exchange for the victim's data. After receiving payment, the ransomware's creator will provide the private key or a copy of the symmetric encryption key. Using this information, the user may potentially reverse the encryption and recover access to their data by entering it into a decryptor tool that the cybercriminal will also provide.

These three fundamental processes are shared by all ransomware variants, however each may utilise a unique implementation or incorporate extra steps. Before encrypting data, ransomware versions such as Maze search for vulnerable PCs to infect. The WannaCry ransomware then seeks to infect and encrypt vulnerable PCs.

*F. Reason to find ransomware perpetrators*

Criminals may more easily hide their identities and their proceeds when they do business using anonymous cryptocurrencies like bitcoin. Cybercriminal groups are increasingly resorting to ransomware tactics as a means of making a quick buck. The availability of open-source code and drag-and-drop platforms for ransomware creation has increased the pace at which new ransomware variants are created and made it simpler for those with no programming experience to produce malware. Ransomware and other forms of modern infection are often designed to evade signature-based protection based on file hash.

*G. Evolution of Ransomware*

TABLE I

| The emergence of Ransomware | 1989 | The first ransomware attack is often referred to as the "AIDS trojan." The name commemorates the 1989 World Health Organization (WHO) AIDS summit. |
| --- | --- | --- |
| The early years | 2005-2009 | The most noteworthy of these early ransomwares were the "Archiveus" trojan and "GPcode" The Archiveus virus, the first ransomware to utilise RSA, encrypted all files in the "My Documents" folder when GPcode infected Windows operating systems. |
| Ransomware embraces cryptography | 2009-2013 | The "Vundo" malware, which encrypted computers and offered decryptors, debuted in 2009.  The WinLock Trojan surfaced in 2010. The programme was used by ten hackers in Moscow to lock victims' computers and show pornography until the victims paid them around $10 in rubles.  Reveton ransomware, which surfaced in 2012, was a sort of scareware that presented messages to its victims stating that US law enforcement had identified the user watching unlawful pornography. |
| Ransomware becomes dominant | 2013-2016 | "CryptoLocker" appeared in 2013. CryptoLocker was a pioneer in a number of ways: it was the first ransomware to be propagated through botnet, in this case the "Gameover Zeus" botnet, and it also employed more conventional methods, such as phishing. CryptoLocker utilised 2048-bit RSA public and private key encryptions, making it very tough to crack.  FileCoder, the first real ransomware for Mac, was also identified in 2014, but it was later determined that it began as early as 2012.  The "Oleg Pliss" assault also occurred in 2014, in which a threat actor used stolen Apple account credentials to get into accounts and then exploited those accounts to remotely lock iPhones via the "find my iPhone" function.  In 2016, "KeRanger" was the first successful cryptographic ransomware assault on a Mac. Associated with Transmission version 2.90. |
| The emergence of RaaS | 2016-2018 | By 2016, ransomware variations had become more prevalent. The first ransomware as a service (RaaS) versions have appeared; these are partnerships in which a single party creates the ransomware code.  The year 2016 also witnessed the introduction of the well-known malware "Petya." Initially, the ransomware was less effective than CryptoWall, but on June 17, 2017, a new strain surfaced that Kaspersky called "notPetya" to distinguish it from the original. Using the "EternalBlue" Windows flaw revealed by the NSA, it swiftly spread from Ukraine to the entire globe. |
| Ransomware  and malware merge | 2018-2019 | January 2018 marked a turning point for ransomware with the appearance of "GandCrab." GandCrab became the most prevalent RaaS and the most active ransomware strain in 2018 and 2019.  Team Snatch, a group of threat actors that debuted in 2018, was a partner of GandCrab and pioneered the new method of releasing victim data to extort money. |
| The risk of leak sites | 2019-2020 | In an effort to coerce Allied Universal and prospective victims into paying the ransom, the "Maze" ransomware organisation released 700 MB of stolen data from the company in November 2019.  The "Sodinokibi" ransomware family has also been a major player in this arena. |

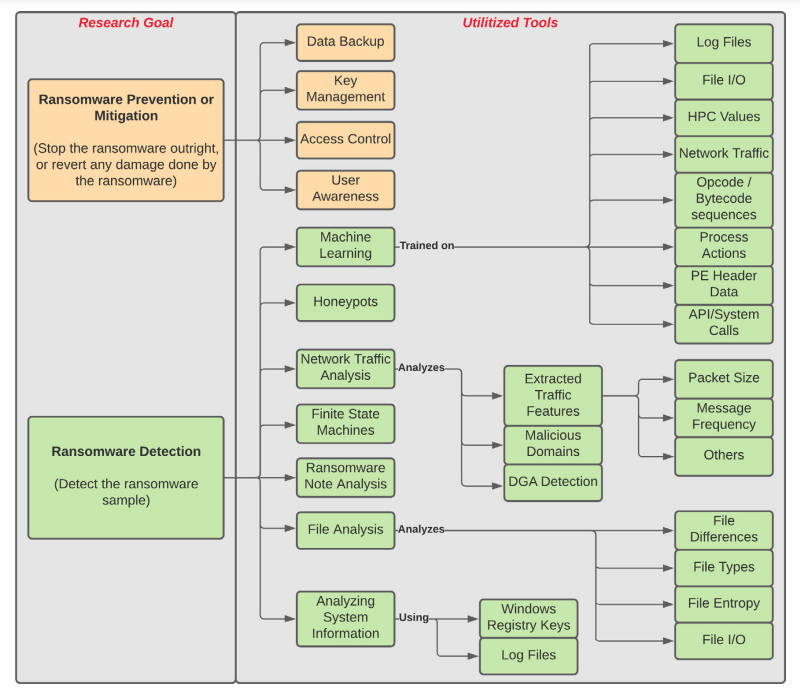


Fig. 1. An overview over the utilized tools observed in literature for both ransomware prevention/mitigation and detection[16]

*H. Ransomware prevention and detection approaches*

The objective of preventive measures is to prevent, mitigate, or erase the effects of ransomware. Implementing severe access limits, securing data and/or passwords, boosting user awareness, and educating users are common preventive measures. Raising user awareness of ransomware attacks and educating users on how to avoid them contributes to the prevention of attacks. Researchers deploy several detection strategies to identify ongoing ransomware attacks. The ransomware-detected programmes may be terminated and disabled. Below is a classification of several detection methods.

*Prevention practices for ransomware attacks:-*

*1. Maintain a Recent Copy of Your Files:-* One of the easiest methods of risk reduction is backing up your data to an external hard drive or cloud server. A ransomware victim may delete everything on their computer and start over using a backup copy of their files. In a perfect world, a company would routinely back up its most crucial information.

The 3-2-1 rule is a popular strategy. In addition to one offline copy, you should keep three unique copies of your data on two separate kinds of storage. You may add a further step to the procedure by saving an additional copy on an immutable and unerasable cloud storage server (cannot be deleted).

*2.Upgrade your hardware and software regularly:* When possible, upgrade your OS, browser, antivirus, and any other software you use often to the newest available version. Because new variants of malware, viruses, and ransomware are always being developed, it is essential that you keep your systems patched and up to date.

*3.Put in place certain firewalls and anti-virus programmes.:* Most people protect their computers against ransomware by using antivirus and anti-malware programmes. A cyber danger may be detected, identified, and countered by them. Antivirus software is essential, but it can only protect your computer from threats after they've already entered your network, so you should also set up a firewall.

When protecting from the outside world, a firewall is often the first line of defence. It may prevent problems with both software and hardware. Firewalls are essential for the security of any private or public network, since they can detect and prevent the entry of malicious data packets.

*4.Segmenting the Network:* Given the speed with which ransomware may infiltrate a network, it's crucial to limit its ability to spread as much as possible during an attack by dividing the network into separate sections. By dividing the network into subnetworks, the company can stop malware from spreading to additional computers.

For ransomware to be successfully thwarted, every layer of the infrastructure must be equipped with its own set of safeguards, including firewalls and access controls. By isolating the compromised area from the rest of the network, the security team will have more time to investigate the situation and eliminate the threat.

*5.Email Protection:-*The vast majority of malware nowadays is spread via email phishing attacks. In 2020, phishing was the most common form of ransomware dissemination, as reported by 54% of managed service providers. (MSP). Another FBI analysis predicts that by 2020, phishing will be the most common kind of cybercrime, costing businesses and individuals a combined total of over $4.2 billion in losses.

An infected email may spread ransomware in numerous ways:

* Opening questionable attachments in emails
* Visiting malicious sites after clicking on a link
* Manipulation of society (tricking users into exposing sensitive information)

You may take further precautions by adopting the following approaches or technologies, in addition to antivirus software:

* Do not click on links in unsolicited emails. Never download or open anything from an unknown or illegal source.
* Keep your email client up-to-date; otherwise, criminals will exploit security holes caused by antiquated software and hardware.
* The Sender Policy Framework (SPF) is a protocol for authenticating senders and receiving mail servers.
* DomainKeys Identified Mail (DKIM) - Offers a digital signature and encryption key to verify that the sent email was not tampered with in transit.
* Domain-based Message Authentication, Reporting, and Conformance (DMARC) - Offers enhanced email authentication by adhering to SPF and DKIM specifications.

*6. Application whitelisting:* Whitelisting is a method used to control which programmes may be installed and run on a computer system. Access to any non-whitelisted unauthorized application or website will be limited or refused in the event that an employee or user inadvertently installs harmful software or visits a compromised website. It is also possible to "blacklist" or restrict certain programmes and websites by using whitelisting software like Windows AppLocker.

*7. End terminal Security:-*The protection of endpoints should be a major consideration for rapidly growing businesses. More and more computers, smartphones, and servers will need to be protected as companies expand and their user bases expand. Each new external connection increases the risk that sensitive data or possibly the whole network itself may be compromised.

All users of the network, whether they are remote workers or employees of a large corporation, should have endpoint protection platforms (EPP) or endpoint detection and response (EDR) installed. Thanks to these advancements, system administrators may check on and adjust the safety of any remote equipment. When it comes to dealing with and preventing modern network risks, EDR is a step up from EPP.

The following preventative measures are often included in EPPs and EDRs:

### *I. The Need for Early Detection:-*

### Dealing with a cyber attack requires continual awareness for early identification. The faster an occurrence is discovered and controlled, the less probable it is that an attacker would acquire sensitive data or do other damage to the organisation.

### Because ransomware may inflict irreversible damage, early detection is far more crucial than for the majority of other forms of attacks. Even if the victim pays the ransom, insecurely backed-up data encrypted by ransomware may be irretrievably lost. To limit the effects of ransomware, it is essential to detect and remove the infection before encryption starts.

### The importance of early detection of ransomware has grown as the threat has progressed. Today's ransomware variants often take sensitive information from a business before encrypting it. Firms may prevent a potentially expensive and embarrassing data breach if ransomware is detected before data is stolen.

### *J. Detection Techniques of Ransomware:-*

### There are a number of telltale signs that indicate a ransomware outbreak has set underway. The following are examples of popular methods for identifying ransomware:

*1.Detection using signature:-* When it comes to identifying malicious software on a computer, signature-based detection is the most straightforward option. The malware's C&C server domains and IP addresses, along with file hashes and other identifiers. Safety against malicious software and computer viruses.

* Data ciphering
* Prevention of the loss of data
* Detecting the intrusion
* Protecting the Web browser
* Mobile & PC security
* Examination of networks for security teams
* On-time detection and notifications for security

samples are all included in malware signatures.

When a file enters or is run on a system, signature-based detection systems keep a signature library and compare the signatures to determine whether the file is malicious.

Even still, signature-based detection is becoming less and less effective. Signature-based detection has never been effective against new malware since no signatures exist for it. As ransomware groups release new malware versions (with unique file hashes, command and control infrastructure, etc.) with every attack campaign, signature-based detection is rendered useless.

*2.Detection by behaviour:-*Behavioral detection is an additional method for detecting ransomware on a computer. It is possible to construct algorithms for behavior-based detection that search for dangerously aberrant or odd behaviours or actions.

To identify ransomware, behavior-based malware detection makes use of the fact that it behaves in a highly unusual way. For instance, for ransomware to encrypt data, the virus must first access a large number of files on the host system, read their contents, and then replace them with encrypted duplicates. It's possible that anti-ransomware technology may aid in spotting ransomware if it monitored file activity and alerted on odd behaviour, such as the use of encryption methods.

*3.Detection by abnormal traffic:-* Endpoint file activity monitoring is an example of behavior-based threat detection. On the other hand, ransomware may be uncovered in the network by keeping an eye out for strange traffic patterns that might be the result of a ransomware or other malware attack.

In order to remain undetected on the system until it was ready to begin encrypting data, ransomware performed a series of network operations. In order to increase the attacker's bargaining power and increase the likelihood that the victim would pay the ransom, modern ransomware exfiltrates and steals sensitive data before encrypting it.

A massive data breach requires the ability to move massive amounts of data from inside the network to external systems controlled by the attacker. Even if ransomware is successful in hiding these data transfers, they may still cause abnormal network activity that may be traced back to the current malware outbreak.

### 4.*Detect and Secure Against Ransomware with Harmony Endpoint:-*By the time a ransom message appears on a compromised computer, the harm has been done. This occurs only after all data has been encrypted and removed from the machine by the ransomware.

### The best way to reduce the damage caused by ransomware is to stop the virus from taking hold in the first place. According to the 2021 MITRE Engenuity ATT&CK Evaluations, Check Point Harmony Endpoint is the best solution for detecting threats.

### For more information on ransomware and other cyberthreats your company may face, check out the 2021 Cyber Attack Trends research. You may check out how well Harmony Endpoint can detect ransomware with a free trial.

*5.Recovery methods from ransomware attack:-*

*a. Freeze infected systems:* Disconnect infected devices from the network and any wireless access points immediately to prevent further compromise (Wi-Fi, Bluetooth). The virus may not propagate even if other users are affected, thanks to network isolation.

*b.*Identify the source:Knowing the origin of the infection will aid in pinpointing the ransomware's entry point. This information may allow the organisation to strengthen its security procedures and training.

*c. Report the incident to authorities:* Reporting the attack to the proper authorities is necessary since ransomware is against the law and merits further investigation. In addition, law enforcement agencies could have access to cutting-edge data recovery tools and methods not available to other businesses. In rare cases, data that has been stolen or compromised may be recovered, and the perpetrators can be brought to justice.

IV. FUTURE WORK

*A. DeepFake Ransomware;*

To impersonate a genuine person, an attacker uses DeepFakes, which are digital representations that have been altered (Güera and Delp, 2018). Attackers might develop ransomware that produces DeepFake content of a victim committing an intimate or incriminating behavior that the victim never committed. The ransom will be demanded from the victim to stop that content from being posted online. Due to the speed at which data is generated and the abundance of social media channels available for content distribution, it would be difficult to resist such ransomware attacks.

*B.Vulnerabilities in remote work:*

Due to the recent outbreak of COVID-19, many institutions have been forced to introduce or adopt remote working options - Own Device (BYOD) Policy (Palanisamy et al., 2020). The recent outbreak of COVID-19 has forced some companies to start implementing work-from-home policies. This allowed the attackers to exploit many vulnerabilities and launch various ransomware attacks. According to one of Skybox Security’s reviews, ransomware attacks have increased by 72% year-on-year. Investigating how to mitigate such attacks when working remotely is one of the future research directions.

*C. Countermeasures Based on the Blockchain*

Due to its distributed nature, linked hash function, timestamp function, and consensus process, blockchain data cannot be tampered with (Hakak et al., 2020a) ( Hakak et al, 2020b; Hakak et al, 2020). An operational manifestation of the RaaS paradigm is the Cerber ransomware assault. The popularity of ransomware as a service has been growing for a while now. As time goes on and more people start using the internet, it's only natural that these kinds of attacks will become more common. Efforts to prevent such attacks in the future seem to be a fruitful field of research.

*D. Making Esthetic Ransomware Objects*

The Aesthetic ransomware project has published its source code on GitHub. You can find it at https://github.com/kregg34/AESthetic. Once the decryption tool is ready, I will provide the code to you. We will provide the AES aesthetic code once the decryption tool is finished. Researchers at SkyBox Security found that the number of ransomware attacks increased by 72% in the last year.

Antivirus systems were likely able to detect the other known samples owing to their signatures. Programs designed to identify viruses would have certainly been able to recognise additional, similar samples based on the signatures they carried. Our virus, AESthetic, is undetectable since it lacks a matching signature. It's possible that this points to a problem with the products' reliance on static analysis at the expense of dynamic analysis. Because antivirus software is a mystery, further research is needed to back up this claim.

V. PROPOSED METHODOLOGY

Below shown are the techniques to detect and prevent malicious codes:-

*1. Honeypot:* Network administrators employ honeypots, which are essentially fake computers that act as decoys, to identify instances of intrusion. In other words, it's a form of detection predicated on the use of deceit.

2. *Heldroid:* Heldroid correctly identified all ransomware samples, and it didn't get confused by rare but similar but harmless applications.

3. *Cryptolocker*: For example, if a task is being performed that seems to be modifying a common ransomware indicator set, Cryptolocker will terminate it. Through its use, a reliable detection system may be created, drastically lowering the amount of data lost by victims.

4. *Sandbox:* Separating processes for safety is what a "sandbox" is designed to do. Sandboxes often confine guest programmes to a controlled environment, limiting their access to system resources like RAM and hard disc space.

*A. The proposed techniques for the prevention from the ransomware attacks is as follows*

The three most efficient parts of the suggested method's implementation are configuration, monitoring, and processing (Figure 1). The suggested method relies on a monitoring list table, which is generated by the setup module. It's the initial piece of configuring software. The Monitoring module keeps track of how much each process is using the system's CPU, RAM, and disc I/O in real time by employing statistical methods. The processing module then makes a choice on how to deal with the ransomware process, which might involve making an exception for it or isolating it completely.

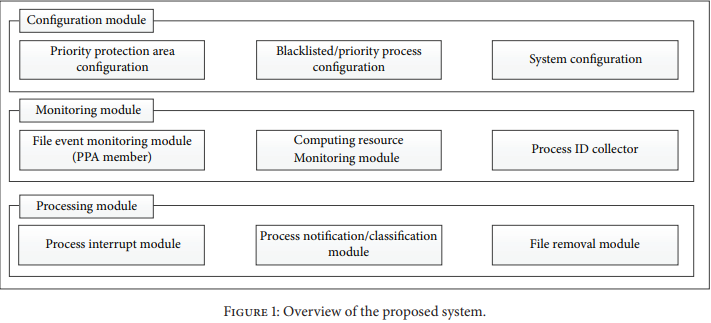


Fig.2. overview of the proposed system

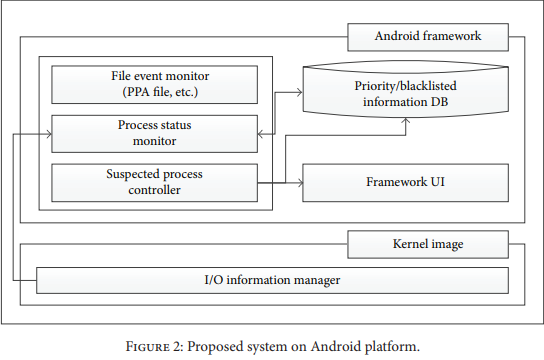
As shown in Figure 2, the proposed method employs the Android platform's framework and kernel to implement the configuration module, the monitoring module, and the processing module. The framework also provides the database that the configuration module needs, as well as the user interface component that is integrated to the Android Settings. The kernel generates an image that has a component for creating I/O data for process monitoring.

Fig.3. proposed system on android software

Below algorithm shows the operation flow of the basic technique proposed in this paper. Details are described later in different topics.

| | **begin** | | | --- | --- | | **Input**: process id *P* | | | ProcessInfo ProcessDatabase(*P*); | | | **if** *ProcessInfo* is blacklist **then** | | | KillProcess(*P*); | | | ProcessRemovalProcedure(*P*); | | | return; | | | **else if** *ProcessInfo* is not priority protection member **then** | | | enqueueMonitoringProcessID(*P*); | | | **end** | | | **end** | |   *1.Configuration Module:***-**When the suggested method detects ransomware, the configuration module will be applied as the primary set-up. As described here, the Android platform's pre-installed processes and applications have their default settings saved as database entries. The primary function of the configuration module is to provide the location of the files that need to be secured against ransomware. One subset of these critical documents is known as the "priority protection area" (hereinafter PPA). If the suggested method is put into practise properly, it will gather PPA data, add it to the watch list table in the monitoring module, and provide real-time protection for the related files. The second step is to keep track of how the user dealt with the potentially malicious procedure that was uncovered by the monitoring component. The system will remember the procedure even if the user later decides it was ransomware. It can detect the process and, if necessary, kill it without any input from the user. Even if a process is subsequently discovered to be malicious, the system will not remove the data associated with it or kill the process if the user first deemed it to be safe.  *2.Monitoring Module;-*By keeping an eye on the PPA and the process, the monitoring module can spot ransomware. The functions of the monitoring component determine its structure, which typically consists of two subcomponents (file monitoring and process monitoring).  *a. File Monitoring Module:.* In order to identify ransomware assaults, it keeps a close eye on all file I/O operations, such as reading, writing, copying, and erasing, for a specific PPA specified in the configuration module. In this paper, the workflow of the file-monitoring module developed for this research is depicted.  *b. Process Monitoring Module.:* It monitors parameters such as processor share by process, memory consumption, I/O count, and storage I/O count in order to spot ransomware. Process monitoring module workflow is detailed in this paper.  After determining the offending process, it restricts access to the configuration module's database for any malicious or exceptional processes. The monitoring component will promptly terminate and delete any harmful processes it identifies. If the user confirms that a normally unusual procedure is safe to run, it will be allowed to do so on a regular basis.  *2.Processing Module;-*The processing module immediately stops the monitoring module's ransomware-suspicious procedure and polls the user population to determine the best next steps. After a decision has been made on how to proceed, the relevant process data will be added to the database and used by the configuration module.  ID is where the tuple's sequence number is stored. The name of the software's package is PackageName. The riskiness of an action can be indicated by its RiskType. In the event that more explanation is needed, comment is generated.  The processing module further alerts users to the risk of ransomware by analysing Android permissions.  *a. System Permission.* : The malware can use the computer's tools. It removes the ability to make changes as an administrator and locks off regular users. The user's private information might be at danger if the app is allowed to access it without their knowledge or consent. Admin approval is required.  *b. SMS Permission:* A normal software that requires SMS permission provides customers with a convenient service, but ransomware steals these messages and exploits them for malicious reasons.  *c.Contract Permission.:* The device is where permission to access contacts is saved. Fraudulent uses of this permission include phishing and smishing.  d*.Permission to automatically detect linked networks and run encrypted software. :* Ransomware locks people out of their devices by locking them out of their own devices. It can potentially steal sensitive information from the gadget.  The processing module gives users the option to keep or remove the required software after stopping a possibly infected process. If the user agrees he wants to uninstall the software, it will be destroyed immediately the next time it appears without prompting the user again if the user has already determined that the programme is ransomware. If he determines that the process is routine, it will be carried out without risk, and the suggested plan of action will not be implemented. The offered approach would also alert the user if any part of the procedure is insecure. |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

VI. CONCLUSION

Our research explores the many changes that ransomware has experienced throughout time. We have seen that hackers develop ransomware because they want a steady stream of direct cash from victims all around the world. Start off with less efficient direct methods of making money. Hackers have gotten more brazen in their use of malicious software like PC performance utilities since they discovered how to trick users into downloading and installing them. Deceptive software evolved into false antivirus schemes, which paved the way for today's widespread ransomware threats like locker and crypto ransomware. According to the results of this investigation, crypto ransomware now constitutes 64% of all binary-based malware found by the end of 2015. The volume of new crypto ransomware surged by 250 percent between 2013 and 2014. Dangers to children, animals, and the planet. There is a high cost associated with ransomware, with the average ransom demand for an individual user reaching an astounding $300. Over the past year, hackers have asked for a total of US$21 to US$700 in ransom. Varying ransom demands may be necessary depending on the victim's location and the specific strain of ransomware. After a certain amount of time, some thieves have even pledged to return stolen data at no cost. We also explore the many factors that have contributed to the rise of ransomware, its dissemination strategies, and the sophistication with which cybercriminals utilise psychological tactics to extract payments. We assessed the scale of the ransomware threat, which impacts most countries in the G20. The fact that ransomware can be adapted to certain regions indicates how pervasive the issue is throughout the world. We also looked at whether or not cybercriminals may use ransomware to attack unanticipated industries as a result of technological advances like the Internet of Things and the booming wearables industry. Our research shows that it doesn't take much effort to adapt Android ransomware to infect Android Wear smartwatches, which might provide criminals with a new source of income. More than anything else, this research highlights how important it is for everyone to pay attention to security. Every one of us can make a difference in the fight against ransomware. Designers of new technologies or products may no longer ignore edge cases in favour of typical, benign use cases. Cybercriminals will find flaws that allow them to manipulate physical things or restrict user access. Engineers and designers have a dilemma when they have to think about how to make their products safer to use in potentially harmful situations. Several simple security steps, such as staying away from questionable websites and attachments and keeping software up-to-date, can help protect data against ransomware. Knowing the potential impact of ransomware allows you to better prepare for such attacks.

REFERENCES

1. O'Kane, P., Sezer, S. and Carlin, D. (2018), Evolution of ransomware. IET Netw., 7: 321-327.
2. Ezhil Kalaimannan, Sharon K. John, Theresa DuBose & Anthony Pinto (2017) Influences on ransomware’s evolution and predictions for the future challenges, Journal of Cyber Security Technology, 1:1, 23-31, DOI: [10.1080/23742917.2016.1252191](https://doi.org/10.1080/23742917.2016.1252191)
3. Zimba, Aaron & Chishimba, Mumbi. (2019). Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures. International Journal of Computer Network and Information Security. 11. 26-39. 10.5815/ijcnis.2019.01.03.
4. Henry Chong,SeCBD: The Application Idea from Study Evaluation of Ransomware Attack Method in Big Data Architecture,Procedia Computer Science,Volume 116,2017,Page 358-364,ISSN 1877-0509
5. Maurya, A.K. & Kumar, Neeraj & Agrawal, Alka & Khan, Prof. Raees. (2018). Ransomware Evolution, Target and Safety Measures. International Journal of Computer Sciences and Engineering. 6. 80-85. 10.26438/ijcse/v6i1.8085.
6. Shah, Nadeem, and Mohammed Farik. "Ransomware-Threats Vulnerabilities and Recommendations." International Journal of Scientific & Technology Research 6.06 (2017): 307-309.
7. E. Berrueta, D. Morato, E. Magaña and M. Izal, "Open Repository for the Evaluation of Ransomware Detection Tools," in IEEE Access, vol. 8, pp. 65658-65669, 2020, doi: 10.1109/ACCESS.2020.2984187.
8. Richardson, Ronny and North, Max M., "Ransomware: Evolution, Mitigation and Prevention" (2017). Faculty Publications. 4276.
9. Shakir, Hasan & Jaber, Aws. (2018). A Short Review for Ransomware: Pros and Cons. 401-411. 10.1007/978-3-319-69835-9\_38.
10. Aini Khalida Muslim, Dzunnur Zaily Mohd Dzulkifli, Mohammed Hayder Nadhim, and Roy Haizal Abdellah, “A Study of Ransomware Attacks: Evolution and Prevention”, jstard, vol. 1, no. 1, pp. 18–25, Jul. 2019.
11. Monika, Pavol Zavarsky, Dale Lindskog, Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization, Procedia Computer Science, Volume 94, 2016, Pages 465-472, ISSN 1877-0509
12. Rohan Mahesh,Ms. Bhargavi Dalal,Khushi Jain,Dr.Nilakshi Jain,Nidhi Adatiya,Ransomware and its Evolution with the Covid-19 Pandemic.IRJET,Volume:8,Issue:6|June2021.
13. EVOLUTION OF RANSOMWARE Kellyn A. Wagner Ramsdell and Kristin E. Esbeck The MITRE Corporation © 2021 MITRE # 21-2257
14. The evolution of ransomware Kevin Savage, Peter Coogan, Hon Lau Version 1.0 – August 6, 2015
15. Fernando, D.W.; Komninos, N.; Chen, T. A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques. IoT 2020, 1, 551-604. https://doi.org/10.3390/iot1020030
16. Craig Beaman, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, Muhammad Khurram Khan, Ransomware: Recent advances, analysis, challenges and future research directions,Computers &Security,Volume111,2021,102490,ISSN0167-4048,https://doi.org/10.1016/j.cose.201.102490.