

Early-Stage Analysis And Mitigation Tactics For Ransomware Assault Exploits

Chaithanya B N¹, Dr.Brahmanada S H²

Professor, Dept of CSE
GITAM School of Technology
Bangalore, India
cnagaraj@gitam.edu

Professor, Dept of CSE
GITAM School of Technology
Bangalore, India
bsavadat@gitam.edu

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract: Ransomware became an illegal enterprise. Malware that controls or renders data unavailable on the device of a victim. It poses such an immediate danger to the data files of consumers and businesses worldwide. Ransomware encrypts files on an infected device and retains the key to open them until they are paid. Ransomware causes hundreds of millions of dollars of financial harm each year. This disruptive trojan is newly iterated annually. New tools for the attackers are used in recent editions. We give a short introduction to Ransomware and the best techniques for infection prevention, detection, and recovery in this article. This creature's financial loss is estimated to reach 1 billion dollars. Since most Internet users are unaware of Ransomware and don't know how and where to warn and defend themselves, they don't feel they are targeted on such a completely automated platform. You won't be targeted, as you are typical cyberworld users.

Keywords— Cyberworld, Encryption, Malware, Ransomware, Automation.

1. INTRODUCTION

In recent years, internet researchers have been quite attracted to Ransomware, often known as the cryptovirus. Criminals employ this software to obtain personal data. Ransomware is a broad word for Ransomware, which uses the Internet to take ransom from its objectives. Payment or order may take the form of digital money or fees to buy goods from certain shops [1]. This method of digital exploitation can be categorized into two main categories [2], each of which can be further subdivided depending on the families they belong. The two most common types of Ransomware are encrypting, obfuscating, or refusing access to the data and those that block or lock users out of networks. Scareware is the third kind of Ransomware. These hazards are not limited to a single region or operating system, and they could impact a wide variety of products. From Android devices to iPhone and Android systems to Windows computers, anything else is prone to ransomware assaults. The system modus vivendi may differ depending on the objective, and the device's capability may limit the final steps taken, but there are some common patterns that many fraudsters adapt [19]. Ransomware displays with a warning of ransom terms. Each Ransomware goes so far that child pornography on this device is shown while stressing the risk to the victim's life. These awful strategies are used by criminals to make payments appear less complex. [3].

Ransomware can be traced back to Joseph Popp's 1989 piece of malicious software known as AIDS in terms of history. The initial malicious software will replace AUTOEXEC.BAT on compromised computers, allowing 90 reboots before blocking all of the folders and pretending to encrypt the data itself. However, after further investigation, it was discovered that only the filenames were encrypted using simple symmetric cryptography, which was eventually solved and deleted using the software AIDSOUT and CLEARAID.

Today, many digital fraudsters demand cryptocurrencies, most often Bitcoin, as a payment method, but this isn't the only choice. Criminals use a variety of prepaid voucher providers such as MoneyPak, Ukash, and PaySafe. The amount of money demanded as ransom varies for individuals and organizations [4]. Regarding the fact that paying the ransom is not recommended, it is the only way to retrieve the records in some situations.

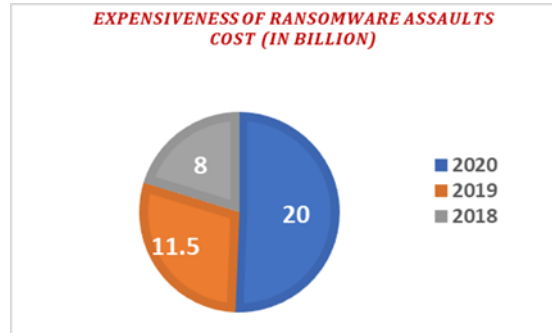
Ransomware fell out of favor in the late 1990s, and it wasn't until 2005 that it began to resurface. The availability of more sophisticated encryption schemes and more system-side processing power brought a new age of

Ransomware, which has kept growing in popularity. It is among the most common ways of attack on computer networks as of 2016, requiring little access to flaws and little analysis upon on target. By the middle of June 2015, one of the most well-known variants, Crypto Wall, was reported to have amassed \$18,000,000. The development of ransomware attacks as they affect businesses and individuals is discussed in this article. And describe the best practices, as well as suggest prevention methods. We go through the various types of ransomware information technology and suggest prevention techniques.

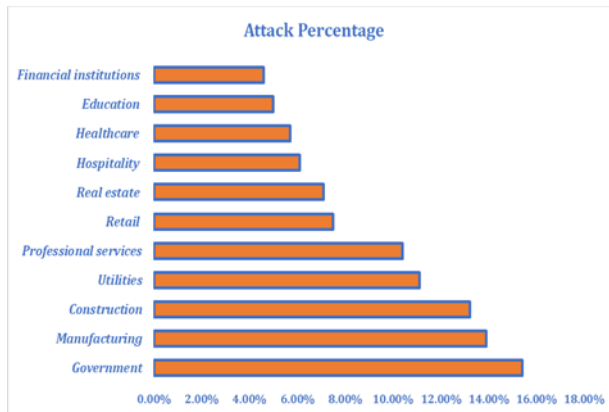
2. RANSOMWARE STATISTICS, TYPES, AND ITS EVOLUTION

2.1 Ransomware Statistics

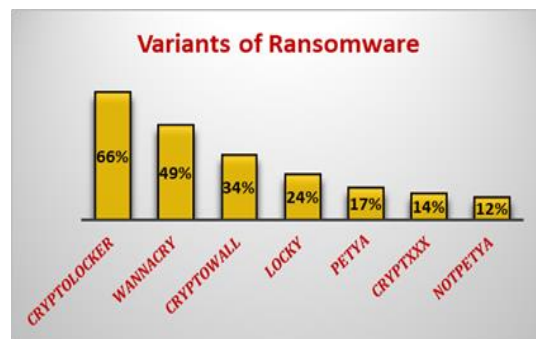
- The Expensiveness of Ransomware Assaults



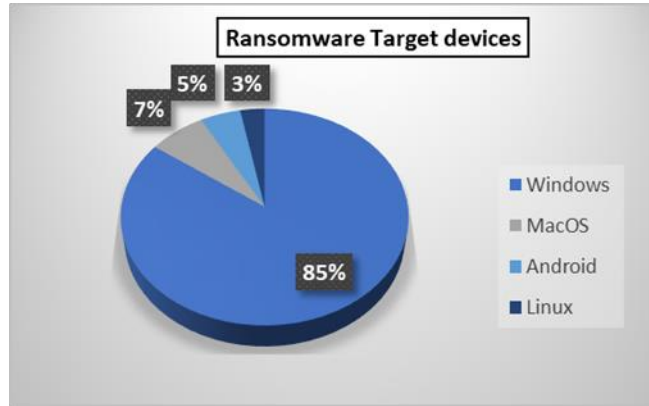
- Ransomware's Key Victims



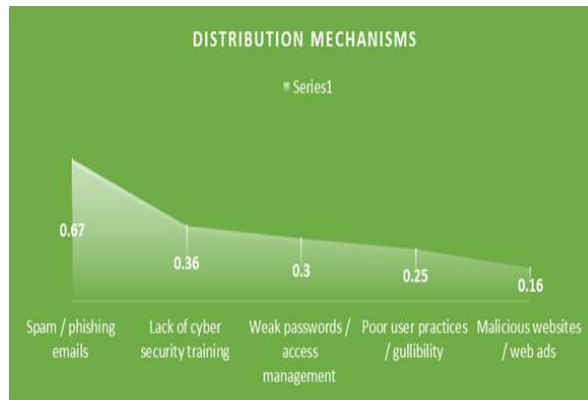
- Widespread ransomware attacks



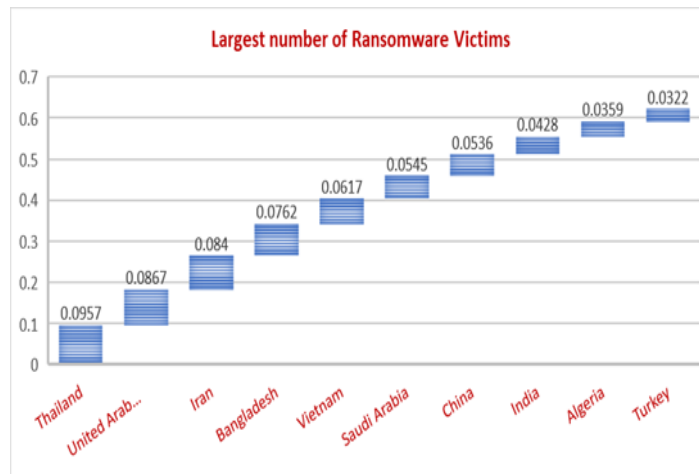
- Typical ransomware target devices



- Typical ransomware distribution mechanisms







- Countries with the most significant number of ransomware victims



2.2 Ransomware Types

There are four major ransomware types shown in table 1, ranging from moderately destructive to extremely dangerous in severity [5].

TABLE 1: RANSOMWARE TYPES

	<p>False computer tools, pretending to have noticed bugs on your computer and seeking money to repair them. Wrong computer tools, acting to have seen bugs on your computer and seeking money to improve them. Such forms will fill your device with warnings that pop up, while others will lock your device. The interruptions will proceed if you don't do anything, but your files are usually secure.</p>
	<p>Locks entry to the directories through encrypting them and gradually deletes them slowly. Hackers know that your files are valuable to you and that you are willing to pay immediately instead of wasting time losing sensitive information.</p>
	<p>Ransomware locks you off your device and flashes an alert. The service sometimes claims in cases that the FBI has locked the system, the police, or some other official, and also that illegal activity has been detected on your computer, and you'll have to pay the penalty.</p>
	<p>This kind of Ransomware is intended to unlock files or photos hacked illegally if the victim never paid a ransom. Because of the forced release, users may find it difficult to resist having to pay the ransom.</p>

2.3 Evolution of Ransomware

In today's world, Ransomware like Ragnar Locker, Ryuk, Egregor, Conti, and other vicious, well-funded organizations can threaten everyone, including COVID-19 vaccine producers, merchants, banks, city governments, and colleges, to make a profit. Although Ransomware wasn't the most common form of malware impacting end-users, the risk of harm is essential, and the danger is rising by the day. Ransomware is already rapidly developing for nearly two decades, and it shows no sign of stopping down shortly. Encrypting Ransomware is a sophisticated and sophisticated cyber challenge that employs all available techniques to make a large sum of money for malicious hackers [6].

If you're wondering how it all began, here's a rundown of Ransomware's background. It might be impossible to believe, but the first Ransomware appeared in 1989 (32 years ago). It was known as the AIDS Trojan, and its method of operation seems primitive today. It was distributed through floppy disks, and ransom was paid by sending \$189 to a Panama postal service. In May 2017, the Wannacry Ransomware became a widespread outbreak [20]. Ransomware has arisen to fuel the profit-making machine as go-to Ransomware as malicious hackers switch from cyber hacking to corporate cyber-crime. Bitcoin's introduction and advancement in cryptographic algorithms rendered the context ready for the invention of Ransomware too. As per a new study from PurpleSec [7], the frequency of ransomware attacks has risen 350-fold since 2018. The total ransom demand has been increased by over 100 percent for the year, downtime has been increased by 200 percent, and the average price per attack is rising. Table 2 illustrates how many forms of Ransomware attacks researchers found in the last 30 years [18].

TABLE 2: EVOLUTION OF RANSOMWARE

<i>Year</i>	<i>Ransomware attacks</i>
1989	<ul style="list-style-type: none"> • <i>AIDS Trojan</i>
2005	<ul style="list-style-type: none"> • <i>Archievus</i>
2012	<ul style="list-style-type: none"> • <i>Reveton</i>
2014	<ul style="list-style-type: none"> • <i>Cryptowall</i>

	<ul style="list-style-type: none"> • <i>Torrentlocker</i> • <i>Cryptolocker</i>
2015	<ul style="list-style-type: none"> • <i>Chimera</i> • <i>Lowlevel04</i> • <i>Cryakl</i> • <i>Scatter</i> • <i>CTB-Locker</i> • <i>Teslacrypt</i>
2016	<ul style="list-style-type: none"> • <i>CrySis</i> • <i>Jigsaw</i> • <i>Petya</i> • <i>Locky</i> • <i>SamSam</i>
2017	<ul style="list-style-type: none"> • <i>BadRabbit</i> • <i>Goldeneye</i> • <i>Ryunk</i> • <i>Bitpaymer</i> • <i>NotPetya</i> • <i>Wannacry</i>
2018	<ul style="list-style-type: none"> • <i>Katyusha</i> • <i>Snatch</i> • <i>GrandCrab</i>
2019	<ul style="list-style-type: none"> • <i>Purelocker</i> • <i>Zeppelin</i> • <i>LockerGoga</i> • <i>REvil</i> • <i>DoppelPaymer</i> • <i>RobinHood</i> • <i>Maze</i>
2020	<ul style="list-style-type: none"> • <i>Sodinokibi</i> • <i>Nempty</i> • <i>Nefilim</i> • <i>Netwalker</i> • <i>CLOP</i> • <i>Tycoon</i> • <i>Sekhmet</i> • <i>Egregor</i>
2021	<ul style="list-style-type: none"> • <i>Xorist Ransomware</i> • <i>Namaste Ransomware</i> • <i>POLA STOP Ransomware</i>

3 PHASES OF RANSOMWARE ATTACKS

Ransomware has found it an intriguing trend in its capacity to distribute across multiple devices and thus enforce larger payments to adversaries [8][22]. To effectively address such cyber threats, the attack measures must be understood. Each of the intrusion vectors delivers the malware payload to the victim's device at the outset of the ransomware attack. After taking Control of the computer, an active ransomware attack prevents users from accessing or information stored on the device. Crypting and locking are mostly preventative acts. The next move is to leave a ransom note to remind the user of the hostage detention of her/his resources. After getting the lending, ransomware

initiatives in the cyber world should promise to set free recovery (e.g., by decrypting computer resources or releasing non-data services). As the assault progresses, Fig 1. explains each of the levels.



Fig 1: Phases of Ransomware attacks

- 1) *Infection*
 - The victim receives a spam email with an attachment (Zip file containing MS word document with VBA macro) or a link.
 - This email has various subjects such as unpaid invoices, package tracking, and so on.
- 2) *Installation*
 - Dropper decrypts and runs a launcher. It will create a new process.
 - The launcher uses process hollowing techniques to inject its malicious code into explore.exe or svchost.exe.
 - The registry is modified for reboot persistence.
 - Volume shadow copies are deleted.
- 3) *Communication*
 - Ransomware uses a hardcoded URL inside the executable file. In case of failure, it utilizes DGA.
 - It communicates with Command & Control server through POST requests over HTTPS and relies on SSL to encrypt its traffic. Command & Control sends the ransom note
 - Harvested email addresses, SMTP credentials, and contact lists are sent to the Command & Control.
- 4) *Execution*
 - It searches for files on all mounted drives and network resources
 - To encrypt the files, a 256-bit AES key is created.
 - Files with specific extensions are encrypted
 - The AES encryption is done with an RSA-2048 public key before being sent to and placed on the command-and-control server.
 - AES key is destroyed on the victim's machine.
- 5) *Extortion*
 - The ransom note is shown on the screen
 - The payment should be in Bitcoin
 - The payment page is reachable via a Tor network.
- 6) *Release*
 - After verifying payment details, decryption software is sent that contains the private key.
 - A "Decrypt Single File "is offered for unrestricted service.

3.1 Forms of Ransomware Encryption

To prevent access to the information, it retains for payment; Ransomware employs a kind of encryption. Encryption scrambles data using an encryption scheme and a unique encryption key to secure it. Encryption, when used correctly, prevents data from unauthorized entry (i.e., the unique decryption key). The decryption key is kept hidden until the ransom is paid, and Ransomware is programmed to keep it secret. We'll go through the most common encryption models used by modern Ransomware in this section, as well as the benefits and drawbacks of each is shown in table 3[9]

TABLE 3: RANSOMWARE ENCRYPTION

Symmetric Encryption	<ul style="list-style-type: none"> • Due to a fundamental mathematical procedure, the encryption process is quick. For encrypting massive amounts of data, this is an excellent option. • The identical key could also be used for decrypting the data for encryption. If the target can locate the key for encryption, he would use the same key for decryption on his computer drive.
Asymmetric Encryption	<ul style="list-style-type: none"> • Two separate public and private keys to encrypt and decode data are encrypted by public keys while the data is decrypted with the private key. Ideal option for tiny messages encryption. • Due to sophisticated math operations with significant quantities of data, they are slower.
Hybrid Approach	<ul style="list-style-type: none"> • Because of quicker coding, large amounts of data are coded. • Once it has been impacted, no communications are needed for the key exchange procedure with the command-and-control server. • Implement several mechanisms to secure the key from victims and from outside

4 ANALYSIS OF RANSOMWARE ATTACK EXPLOITS IN THE EARLY STAGES

First and foremost, vulnerability to this form of attack is dependent on user understanding and caution. Most ransomware examples show that ransomware attackers or even some other software gain user confusion by posing legitimate invoices, advertisements, or even intriguing articles for reading. As a result, people need to be aware that not all connections they get in email or social media can be trusted. They can avoid installing device or smartphone applications via unknown sources. The indicators are shown in below figure 4

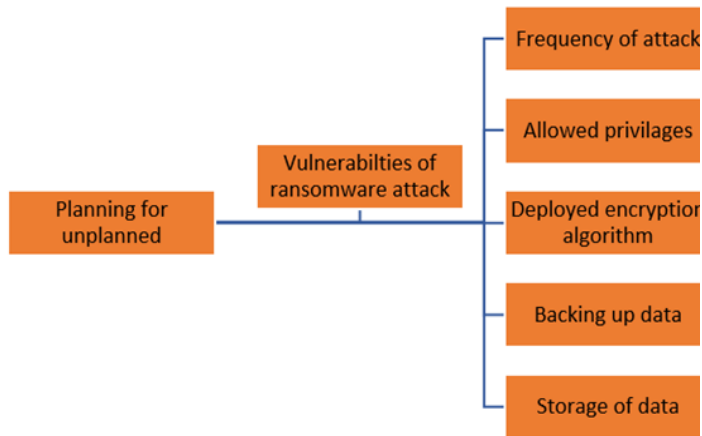


Fig 4: Vulnerabilities of a ransomware attack

4.1 Assault Frequency

Studies show that malware may be hacked for research or if it has already been compromised. The criteria for this assessment are below:

1) *Form of Operating System:*

If a device has previously been a victim of ransomware assaults, further in experiments or current situations, it is most undoubtedly sensitive and at grave risk from such assaults. Because of the large number of potential targets and the ease with which users can install third-party malware from various sources, Windows systems have become the most common focus of ransomware attacks. Since Android and Windows share these attributes, Android users worldwide are often targeted [10]. Ransomware can infect sensors, refrigerators, televisions, and other intelligent home gadgets. Home thermostats, for example, are vulnerable to such attacks in experiments conducted by researchers and white-hat attackers employing command injection [11,12].

2) *Legitimate operating system:*

When a computer is supplied with a legitimate or authenticated operating system (OS), the most recent security features are configured and modified. As a consequence, a genuine operating system is more robust than a pseudo-operating system.

3) *The operating system is updated:*

An operating system that has been upgraded with the most recent security features is more resistant than one that has not been patched.

4) *Linked to a network*

If Ransomware infects any system or computer by downloading malicious software or opening malicious emails, being online is like allowing malware to infiltrate the machine or device over the first time.

5) *Apps or websites that were deployed*

Following the analysis of recent data breaches, it was discovered that Ransomware is typically spread by downloading fraudulent or malicious applications. As a result, the software application installed and the sites accessed play a role in determining the sensitivity of Ransomware.

4.2 Access that has been granted

Ransomware, just like every other software, is limited by the operating system's legal rights or privileges, such as Windows, Android, Linux, and so on. The malware attempts to increase its rights in various ways after being installed, posing a legitimate upgrade and requesting administrative access [13]. When these rights are granted, generally by the victims themselves, the virus spreads, and the Ransomware does what it's supposed to do, whether it's encrypting passwords, modifying the PIN or password, or locking the computer. The measures for this assessment are as follows:

1) *A user's or an app's permissions and rights.*

The collection of permissible permissions limits a user's or application's activities, such as if they are permitted to read-only, read and write, or perform all actions for that individual.

2) *'Jailbroken' system*

Few iOS or Android users may utilize the 'jailbreak' process to remove all rights, including all their phones. Some applications can be uninstalled and the file controlled by you. This conduct poses a severe hazard from cyber-attacks for the machine and user data.

4.3 The algorithm used for encryption

Some kinds of crypto-ransomware cannot encode users' data using cryptographic algorithms and only use local cryptographic techniques of the victim. Windows OS devices with Windows security calling assault CryptoLocker and CryptoWall (e.g., Windows CryptoAPI). Other variants of crypto-ransomware are connected to the command/control server (C&C) for the secret key used to encrypt victim data.[14]. The following indicators accompany this metric:

1) *Admin rights are needed to access encryption features, which are supervised.*

This indicator indicates whether users with administrator rights can access encryption feature calls and how a system tracks these calls to find any unusual use or behavior.

2) *API series calls for encrypt, uninstall, and modify extensions are being monitored.*

This flag shows when a system searches for questionable behavior. Calls for encryption, deletion, and duplicating of data processing process.

4.4 Data backup

Because certain forms of ransomware target data, when encrypted by the individual or the company and kept as a control, the current backup of these data will remove this leverage.

The problem is that massive or large quantities of evidence should be backed up, for example, in large companies or medical reports. One approach may be the storage, through the up-to-date infrastructure and the limiting or managed access to that information, of such an enormous volume of data or documents on a cloud server. The following metrics are given for this measure:

1) *The information is backed up as of the last date.*

Keeping the most recent version of the information backed up removes the perpetrators' power. It means that you can restore the information before needing to pay the ransom money to retrieve it.

2) *Is the backup stored off-site?*

Since specific Ransomware can spread through systems to access information backups and other devices, creating an off-site copy, such as on Disks or in a reliable storage server, is a better option.

4.5 Data storage

Ransomware typically targets photos, Office files, PDF files, and other files that are considered valuable or confidential to users. As a result, because ransomwares wander compromised devices looking for potentially sensitive data or files to encrypt, it's likely that storing data out of full view, as it normally is, it will make it more difficult for ransomwares to locate private or sensitive files to encode or get them as motivation. As a result, saving files in encoded format or maintaining file extensions in encoded format may be a way to protect sensitive data from Ransomware. As a result, the following measures are assigned to this metric:

- The information is encoded.
- Encoding of extensions.

4.6 Preparing for the unexpected

Ransomware is emerging as the new major danger, posing a significant risk to individual people and businesses of all sizes, especially in light of the rapid growth of IoT across the globe. And, as in the case of electricity production, transport power systems, and manufacturing methods, almost any aspect of our lives is regulated by a machine or a sensor of some kind.

Worldwide, organizations, such as health facilities, lost millions of dollars owing to ransomware attacks. Attentats led to loss of productivity, information security, denial - of - service, mismanagement of healthcare and additional expenditures and recovery. [15].

Some institutions are more attractive to perpetrators than others; for example, due to the sensitivity and quality of their records, medical facilities are the most suitable victims for assailants. As a result, some clinics or health care providers nearly sometimes have no interest in paying the ransom after the attack occurs in regaining access to their clients' records, as well as some ransom money is in the vast amounts of money [16].

Ransomware has previously targeted industrial networks, resulting in massive financial losses, not just from needing to pay the payment but also from wasting precious time and having to slow down manufacturing [17].

The recovery from this challenge should also be part of any company's contingency plan as a final defense. Maintaining an upgraded restore or documents, raising awareness and employees about the problem, the device's ability to restore and rebound from the assault (when feasible), they plan to isolate the affected components and regain function or power, or the potential to partially replace that infected part are all measures in a contingency plan for an organization to include. As a result, the following measures are assigned to this measure:

- Is the problem known to the staff or users?
- Whether or not the infrastructure is backed up and whether or not periodic restore points are held
- Is it possible to recover control of the system by rebooting the device and its access points?
-

5 PREVENTION STRATEGIES

Preventing any device compromise with Ransomware before your organization can be done by following these steps.[24]

- **Your resources inventory:** To secure yourself from a ransomware attack, you first must understand what hardware components and applications resources are connected to. Extensive exploration will assist, but assets installed from other departments may not be discovered. Considering this flaw, the passive finding can create a detailed inventory and update the linked hardware and apps list.
- **Customize the spam protection the correct way:** Most Ransomware versions are believed to propagate through emails containing harmful links. Documents or other commonly used file forms within the company could be included in each of these attachments. However, some people can come in an unusually seen format. You will then customize to block these attachments for your webmail server.
- **Forbid against accessing attachments that appear alarming:** It only refers to messages received by unfamiliar individuals. It's all about the senders you feel are acquainted with. Phishing emails are masqueraded as updates from an access provider, an e-business resource, an intelligence agency, or a financial organization.
- **Resist handing away confidential details:** Threat users would receive your details from elsewhere if attackers intend to anonymously give you a malicious email containing Ransomware. Probably, via a data leak that has been released on the deep web, they could get the relevant data. However, they can only use OSINT techniques by ripping critical details from social media links or public profiles. Besides that, unless it is essential, it is crucial to do not over-share digitally and to stop handing away identifiable forms of identification
- **Consider twice before going to click:** Hazardous hyperlinks received from social networks or instantaneous messages. Online criminals also hack somebody's identity and then deliver harmful links to their whole list of contacts. Which illustrates how someone you confide in, such as a friend, co-worker, or relative, might be

the source of a bad link. Irrespective of where it arises from, do not open on a suspicious link. If you are uncertain if the person aims to give you the link, use an alternative form of communication to access them and confirm.

- Training the users: Those mentioned above best practices underline the need to educate your customers about some of the more popular phishing attacks. To achieve this, you should indulge in developing the safety culture by educating the whole staff on security awareness. This software could explicitly test employee awareness of phishing techniques using phishing simulations
- Using the File Extensions function: View File Extensions is a built-in feature of Windows that lets's determine which file formats were accessed to keep potentially dangerous files secure. This is beneficial as fraudsters try to use a misleading tactic where one file appears like it has two or three extensions.
- Patch and upgrade your software: In the failure of a patch, threat users can leverage a flaw with an attack kit in their operating system, server, antivirus, or other applications. These threats include code manipulation for known vulnerabilities that cause Ransomware and other harmful payloads to fall away. As a result, you must ensure that security experts can prioritize remedies and mitigating efforts appropriately to protect the whole of all the associated software resources.
- Disable the Site automatically if you find a strange operation on your device: At the outset of the attack, this strategy is highly effective. Several ransomware perpetrators must establish a connection with their C2C servers to complete their authentication procedure. The Ransomware would remain idle on an infected computer without getting internet access. Such a scenario helps you to delete the malicious software from an infected device without decrypting any files.
- Download from only websites that you confide in: Trust plays a crucial role in stopping ransomware infection. You must also aim to approve updates from locations that you trust, just as you should attempt to avoid untrusted procedures from operating on your device. It covers websites using "HTTPS" on your mobile device and AppStore markets
- To Authorized Lists, add applications: Requests that might initiate a threat to your environment mustn't be installed in terms of the trust. As a way of accepting programs your systems should run in compliance with your company's security policy, you can add applications to the approved list.
- Maintain Windows Firewall activated and installed correctly every time: The Windows defender will shield your systems from unwanted entry, like an attacker trying to compromise your computers.
- Use the access control concept: Firewalls allow you to track traffic to avoid malicious actors accessing the network. As such, the less privilege theory should be applied by analyzing the control levels and the written privilege instances you dole out. It prevents malicious actors from traveling across your system using a manipulated account.
- Adapt the protection tools to search stored or compressed files: Most ransomware attackers claim they can break past the email filters by shielding their packets from compressed or cached file attachments. As such, you have software that can search these kinds of data for malware.
- Use efficient spam filters and user authentication: Besides the ability to search compressed or cached data, you require powerful spam filters that keep users from receiving phishing emails.
- Unenable the host for Windows Script: Any malware actors use VBS (VBScript) on a targeted host to execute Ransomware. To prevent malware using this file form, you can deactivate Windows Script Host.
- Improve your Microsoft Office applications' protection: Unfortunately, people tend to spread their malicious payloads using armed Microsoft archives. Macros and ActiveX in specific widely found in these scripts. To avoid malicious code from running on Windows PC, you can deactivate macros and ActiveX.

- To prevent pop-ups, enables a browser add-on: Pop-ups offer a simple access point to ransomware assaults by malicious actors. Thus, you can search for browser add-ons to avoid pop-ups in your paths.
- Using efficient passwords: If a weak password exists, malicious hackers can brute into a device or an account. They might then use the link to indirect attacks to execute Ransomware or travel laterally across the network. As a result, you can create strong, different passwords for all of your accounts and use them consistently.
- AutoPlay disables: AutoPlay is a Windows feature that enables users to run portable files, such as USB disks, flash sticks, and CDs, instantaneously. Malicious hackers may use such gadgets on their computers to hide Ransomware. It would be best if you deactivate this function on all work areas in response.
- Do not use unknown media: It's indeed one thing that malicious attackers hack the supply chain of an enterprise and dispatch trojan-powered media. One other choice is to insert an unseen device into your machine voluntarily. You cannot realize what might be hidden on an unusable USB drive or a CD. Therefore, if you did not buy them from a trustworthy company, you should stop using this media.
- Ensure that you prevent sharing files: In your system, you wouldn't want hackers to infect several devices. Therefore, file sharing must be disabled. If the ransomware assault felt, crypto-malware would not spread to other properties on your computer.
- Remote services disable: Hacktivists will use the Remote Desktop Protocol to extend the security risks and gather a foothold on the system. You must deactivate remote services to mitigate this risk. It removes a remote access point.
- Usage policies with software restriction: Software Restriction Policies are, according to Microsoft's records, confidence policies that allow businesses to handle application processes on their machines. For example, it offers the ability to specify where applications are and are not authorized to run. It will help deter ransomware infection since attackers typically execute their malicious processes through program Data, AppData, Temp, and Windows.
- Prevent unauthorized IP addresses reported to Tor: Tor (The Onion Router) access points have been one of the key ways to connect with your C&C server for ransomware attacks. As such, you can obstruct potential malware IP addresses, which can further deter vital malicious processes.
- Allow use of information from threats: Ransomware actors continue to evolve emerging technology, start new assaults and produce new crypto-malware strains. You must have a system to keep track of whatever is happening in the threat world regarding this fact and what threats could impact other companies in the same area or sector. By ensuring you provide access to reliable security intelligence feeds, you could do this.
- Segmentize the infrastructure: Attackers can use a persistent channel to propagate across the overall infrastructure. By segmenting the network, you can avoid this. You may want to put the industrial assets and Internet of things devices in their sections, in general.
- Check for malicious activities on the network: You have to keep a check on vulnerability activity that may suggest a malware assault or security breach in any manner you plan to arrange your network. It's why you ought to use devices to detect malicious behaviors on the network.

6 CONCLUSIONS

Every year the intensity and threat of Ransomware increase. We have found that ransomware costs governments millions of dollars each year after a thorough study of over 30 Ransomware types. It uses complex ways of encryption. It is applicable in numerous different phases, incorporating different methodologies. More and more cybercriminals rely on it as a method of income. In Germany, the first fatality of Ransomware was caused by the loss of hospital archives in 2020. Every company or person with Internet access is an attainable goal for Ransomware. It's tricked by a website or an email from considerable companies to a small lad who merely wants free skins for Minecraft. The first

is to obtain a good grasp of fraud and phishing. In short, two main strategies of avoiding this exist. The critical files of the system are typically offline backed up.

REFERENCES

1. Luo and Q. Liao, "Awareness Education as the Key to Ransomware Prevention", *Information Systems Security*, vol. 16, no. 4, pp. 195-202, 2007. Available: 10.1080/10658980701576412 [Accessed 10 December 2020].
2. Kharrazi, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirida, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," *Cutting the Gordian Knot: Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 3-24, 2015. Available: 10.1007/978-3-319-20550-2_1 [Accessed 1 November 2020].
3. H. Chittooparambil, B. Shanmugam, S. Azam, K. Kannoorpatti, M. Jonkman, and G. Samy, "A Review of Ransomware Families and Detection Methods," *Advances in Intelligent Systems and Computing*, pp. 588-597, 2018. Available: 10.1007/978-3-319-99007-1_55 [Accessed 27 November 2020].
4. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in *Magnetism*, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
5. P. O'Kane, S. Sezer and D. Carlin, "Evolution of ransomware," *IET Networks*, vol. 7, no. 5, pp. 321-327, 2018. Available: 10.1049/iet-net.2017.0207 [Accessed 10 November 2020].
6. Gostev, R. Unuchek, M. Garnaeva, D. Makrushin and A. Ivanov, "IT THREAT EVOLUTION IN Q1 2016", Kaspersky Lab, 2016.
7. S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Ransomware, Threat and Detection Techniques: A Review," *IJCSNS International Journal of Computer Science and Network Security*, vol. 19, no. 2, pp. 136-146, 2019. [Accessed 25 November 2020].
8. <https://www.exabeam.com/information-security/defending-against-ransomware-prevention-protection-removal/>
9. Srinivasan CR. Hobby hackers to billion-dollar industry: the evolution of Ransomware. *Computer Fraud & Security*. 2017 Nov 30;2017(11):7-9. 2017.
10. <https://purplesec.us/resources/cyber-security-statistics/ransomware/>
11. 2018 Data Breach Investigations Report, Verizon, 2018, https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf, (Accessed June 2018).
12. Young and Moti Yung, "Cryptovirology: extortion-based security threats and countermeasures," in *Proceedings 1996 IEEE Symposium on Security and Privacy*, 1996, pp. 129-140.
13. K. Savage, P. Coogan and H. Lau, "The Evolution of Ransomware," Symantec, 2015.
14. R. Brewer and L., "Ransomware Attacks: Detection Prevention and Cure," *Network Security*, pp. 5-9, September 2016.
15. Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, Syed Zainuddin Mohd Shaïd, "Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions," *Computers & Security* (2018), <https://doi.org/10.1016/j.cose.2018.01.001>, 21 2018.
16. Magazine, "#DefCon: Thermostat Control Hacked to Host Ransomware," *InfoSecurity Magazine*, 7 August 2016. [Online]. Available: <https://www.infosecurity-magazine.com/news/defcon-thermostat-control-hacked/>. [Accessed 20 March 2019].
17. M. P. Zavarsky and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms-Evolution and Characterization," *Elsevier B.V-Science Direct*, pp. 465-472, 2016.
18. [14] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirida, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," in *DIMVA*, 2015.
19. Mahmood Alsaadi, Malik Qasaimeh, Sara Tedmori, Khaled Almakadmeh, "HIPAA Security and Privacy Rules Auditing in Extreme Programming Environments," *International Journal of Information Systems in the Service Sector*, vol. 9, no. 1, pp. 1-21, 1 April 2019.
20. Paul, III, D. P., Spence, N., Bhardwa, N., Coustasse, A., "Healthcare Facilities: Another Target for Ransomware Attacks," in *54th Annual MBAA Conference*, Chicago, IL, 2018.
21. D. Formby, S. Durbha and R. Beyah, "Out of Control: Ransomware for Industrial Control Systems," in *RSA Conference*, San Francisco, 2017.
22. Chaithanya B N, Dr. Brahmananda S H, "Variants of Ransomware Assaults and Prevention Strategies" *International Journal of Grid and Distributed Computing*, Vol. 13, No. 1, (2020), pp. 1628-1639.

19. K. Cabaj and W. Mazurczyk, "Using software-defined networking for ransomware mitigation: The case of CryptoWall," *IEEE Netw.*, vol. 30, no. 6, pp. 14–20, Nov. 2016. [Online]. Available: <https://doi.org/10.1109/mnet.2016.1600110nm>.
20. D. Goodin, "A new ransomware outbreak similar to WCry is shutting down computers worldwide," 2017. [Online]. Available: <https://arstechnica.com/security/2017/06/a-new-ransomware-outbreak-similar-to-wcry-is-shutting-down-computers-worldwide/>
21. Kolodenker, E.; Koch, W.; Stringhini, G.; Egele, M. PayBreak: Defense against Cryptographic Ransomware. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi, UAE, 2–6 April 2017; pp. 599–611.
22. A. Young and M. Yung, "Cryptovirology: Extortion-based security threats and countermeasures," in *Proc. IEEE Symp. Secure. Privacy*, Oakland, CA, USA, May 1996, pp. 129–140. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1947337.1947357>