Targeted Ransomware Attacks

Student Registration Number	Name Of Student
IT21170720	K.D.S.P. Jayawikrama

Individual assignment

IE2022-Introduction to Cyber Security

Table of Contents

Abstract

By clicking on a link that includes a virus, you can download harmful software known as ransomwares onto your devices. This will provide attackers access to the network and workstations of the company, allowing them to eventually read and encrypt crucial information. Once these files have been taken, attackers will demand a ransom.

Many new types of ransomwares are being developed. Threat actors are moving away from random attacks and focusing on specifically targeting their targets with Ransomware to achieve their desired results. Along with Targeted companies, they are striking at the most important or lucrative parts of the network. This is being done with utter disregard for morality.

Targeted ransomware is a subset of malware created to extort money, usually in the form of cryptocurrency, by holding a victim's data hostage. The methods involve preventing users and system administrators from accessing files or even whole digital networks, then presenting them with a "ransom note" that requests payment to recover access. Over 4,000 ransomware attacks take place daily, according to a report released by the US government.

1.Introduction to the topics

The virus family of crypto virology includes ransomwares, which makes the threat to either permanently prevent access to or disclose the victim's personal information unless a ransom is paid. Simple ransomwares can lock the machine without deleting any files, more sophisticated virus uses a method termed cryptoviral extortion. The files of the victim are encrypted, becoming inaccessible, and a ransom demand is made to unlock them. In a properly executed cryptoviral extortion operation, retrieving the files without the decryption key is an intractable task. Additionally, the usage of cryptocurrencies like paysafecard, bitcoin, and other cryptocurrencies to pay the ransoms makes it challenging to identify the criminals.

Typically, a Trojan that looks like a real file is used to carry out ransomware attacks. The user is duped into downloading or opening the Trojan when it shows up as an email attachment. One well-known example, the WannaCry worm, on the other hand, spread automatically between computers without user input. In the present world, there are lot of ransomware attack take place daily.

There are four categories of Ransomware.

1. **Encryption**

   Ransomware that encrypts data and renders it hard to decode without a decryption key is the most prevalent form.

2. **Lockers**

   Your computer is locked, preventing you from working or performing basic activities until the ransom is paid.

3. **Scareware**

   Scareware tries to frighten people into purchasing pointless software. In certain circumstances, pop-ups will overwhelm the screen and demand payment to be removed.

4. **Docxware/Leakware**

   Without payment of the fee, doxware or leakware will threaten to leak customer or business information.

1.1 what is the targeted ransomware attack?

Cybercriminals utilize malware, or harmful software, known as ransomware. A computer or network can become infected with ransomware, which either blocks access to the system or encrypts its contents. In exchange for releasing the data, cybercriminals demand ransom payments from their victims. With new dangers continuously emerging and changing, computer security is a discipline that is rapidly advancing. Malicious actors behind the various strains of malware are compelled to hone their approaches for avoiding detection as computer security providers develop their methods for identifying malware (malicious software), spurring additional development from the computer security industry. Computer security issues can result in complex dynamical behavior due to the interaction between these conflicting agendas. We can shed light on phenomena seen in computer security by analyzing these dynamics and offering insights. The current study uses game theory to examine the dynamics that ransomware has created to shed light on recent advances of technology. [1]

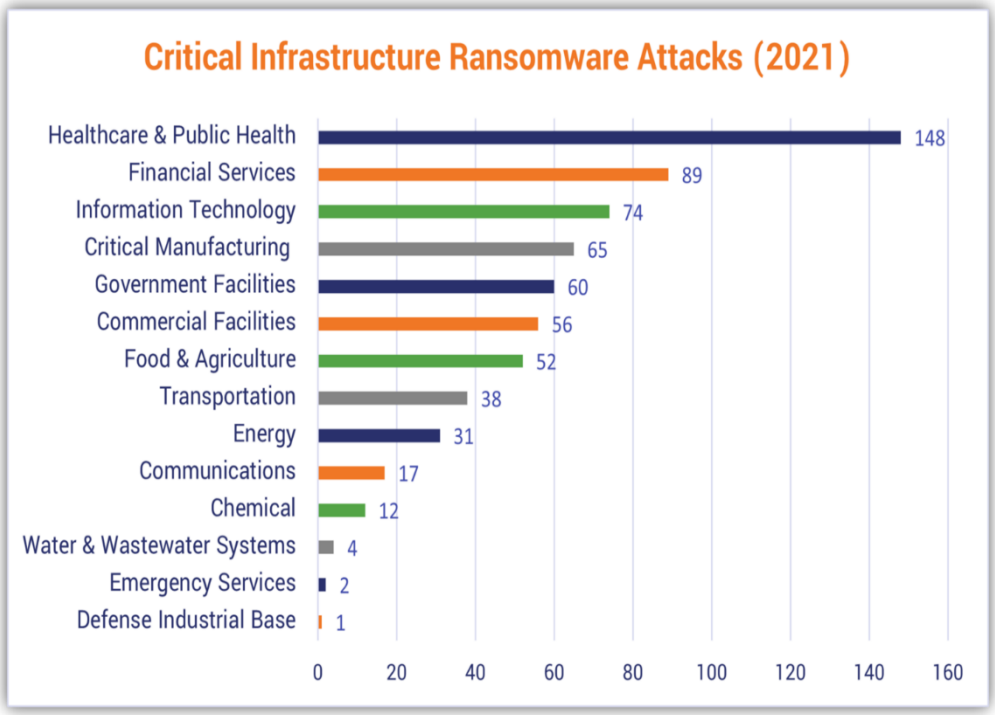
By preventing access to the victim's computer or data until the ransom is paid, ransomware, a type of malicious software, aims to extort money from the victim. Ransomware used to rely on extorting a little sum of money from a lot of victims in order to function. Since it would be pointless to negotiate a modest ransom with numerous victims, the ransom itself would normally be determined at a figure that almost anyone could afford. Targeted ransomware is a new phenomena that has evolved in recent years. Large organizations are the target of malicious actors using targeted ransomware because they may demand far bigger ransoms. The bad actors must pay a lot of money to breach their security because they are also probably to have a higher level of computer security. The bad actors will put more effort into estimating the biggest ransom their victim will agree to pay given the work required to penetrate security. Malicious actors are eager to negotiate the ransom demand to expedite payment because there are higher quantities of money at risk. [2]

1.2 Targeted ransomware attack and cyber security

According to research, the number of ransomware threats discovered increased to almost 1.2 million each month between January and June. Cybersecurity experts at Barracuda Networks have found and examined 106 widely reported ransomware outbreaks over the course of the last 12 months. They discovered that education, municipalities, healthcare, infrastructure, and finance continue to be the top five target industries. Additionally, the number of service providers that have experienced a ransomware attack has increased, according to researchers.

In order to get access to larger organizations, many cybercriminals attack small firms. Therefore, regardless of the size of a firm, it is imperative for security providers to develop products that are simple to use and execute, according to the report.

Ransomware attack is increasing day by day in the future world. Most of modern tools are used to prevent to the ransomware.



1.3 There are many ransomware attacks in the world

1.Locky

In 2016, during a hack, a hacker group used Locky for the first time. They utilized bogus emails with harmful attachments to spread their infection and employed over a hundred and sixty different types of encrypted files. The malware was installed on users' PCs who had fallen for the email scam and worked for the UN organization. Phishing, a social engineering, is that the term for this technique of dissemination. File varieties that are usually utilized by designers, developers, and engineers are the target of the Locky ransomware. [3]

2. WannCry

The attack was the largest the world has ever seen, and it significantly affected the political, hacking, and cybersecurity sectors. Over three hundred enterprises were affected by WannaCry, which spread over a sizable 150 nations. The virus was so big that even when the kill switch was found, it continued to wreak havoc on any systems and data it had previously touched. The total cost is estimated to be over $4 billion, with the UK's NHS alone incurring damages of over £92 million. Although the strike was linked to the Lazarus cluster, which has close ties to North Korea, there is still some uncertainty around the specifics of what transpired.[3]

3.Bad Rabbit

Drive-by attacks were wont to transmit the ransomware attack called dangerous Rabbit in 2017. A client views a web site during a drive-by ransomware assault while not being aware that hackers have hijacked it. All that is necessary in most drive-by attacks is for someone to visit a page that has been hacked in this way, just like tiny Red Riding Hood and her grandmother/wolf. Dangerous Rabbit installed a fake version of Adobe Flash on the user's machine, which then became malware infected. [3]

4.Ryuk

In the summer of 2018, the coding Trojan called Ryuk unfold, lockup the Windows OS's recovery choices. As a result, restoring encrypted information while not associate degree external backup was not possible. Network onerous drives also are encrypted by Ryuk. Devastating effects followed: most targeted North American nation companies were believed to possess pay to ransom amounts. Over $650,000 value of harm has been done. [3]

5.CrptoLocker

Another Trojan that panic-struck the net in 2013 and 2014 was known as CryptoLocker. Phishing emails were not suitable to propagate it. Like several viruses, its infected users' computers and encrypted their files before requesting a ransom to rewrite them. The Federal Bureau of Investigation and an international law enforcement agency, among other groups, eventually destroyed it as part of Operation Tovar. Since the amounts for those that paid the ransom tend to vary according on sources, it's been not possible to work out the economic harm; even so, it had been within several countless bucks. [3]

6.GoldenEye

The reincarnation of Petya as GoldenEye in 2017 resulted in a global ransomware outbreak. The "deadly brother" of WannaCry, GoldenEye, with success smitten over two,000 targets. various banks also as vital Russian oil companies were victims. The urban center nuclear energy plant employees were even had to admit manual radiation level checks when being fast out of their Windows OS by Goldeneyes. [3]

7.SamSam

The SamSam ransomware was discovered in late 2015 and inflated within the years that followed. The organizations that are to pay to possess their information came back, as well as hospitals and schools, are those that its developers fastidiously choose as their targets. The ransom demands are over the market norm, and that they recently reached $6 million in illegal profits. The SamSam ransomware either employs brute-force techniques against weak passwords or security flaws to realize access to the victims' network. Once inside the network, the hacker employs a spread of techniques to extend their access levels untill they reach the domain admin account. [3]

8.Petya

The ransomware assault called Petya happened in 2016 and reappeared as GoldenEye in 2017. This malicious ransomware encrypted the whole victim's hard drive, not just a few selected files. In order to prohibit access, the computer file Table (MFT) was encrypted. Organizational unit of time departments were affected by a fake application that had a Dropbox link that was compromised by Petya ransomware. Petya 2.0 is that the name of a special variation, and each are equally harmful to the victim's device. [3]

1.4 How to Prevent Ransomware Attacks

There are many techniques to protect against ransomware infestation. Technology is frequently changing, therefore it's important to adhere to fundamental cybersecurity rules and be vigilant.

1) **Keep All System and Software Updated**
   Always use the foremost recent version of your OS, applications programmed, antivirus program, and the other computer code you employ. You need to make sure that everything is patched and current since malware, viruses, and ransomware are always changing with new versions that could sneak past your antiquated protection procedures.
   The attack was aimed against machines running outdated versions of Microsoft Windows. A recent patch that may have prevented the spread of malware was released, but many of us and companies were unwilling to upgrade and fell for the scam as a result. Global security experts advised companies to update their systems as soon as possible after this incident. [4]

2) **Install antivirus software & Firewalls**
   Comprehensive antivirus and anti-malware products are the most often used type of ransomware protection. They can look for, discover, and respond to cyber dangers. You will also need to set up your firewall because antivirus software only works at the internal level and can only detect an attack once it has already entered the system.

A firewall is typically the first line of protection against any incoming external threats. It is capable of fending off attacks that are both hardware- and software-based. A firewall is essential for any business or private network because it can filter and stop suspicious data packets from getting into the system. [4]

3) **Network segmentation**

Ransomware should quickly penetrate a network; thus, it is crucial to block its spread as much as possible in the event of an attack. The company could isolate the ransomware and prevent it from infecting further devices by using network segmentation, which involves slicing the larger network into several smaller ones.

Every scheme must have its own security precautions, firewalls, and different access to prevent ransomware from reaching the target knowledge. In addition to preventing the attack from reaching the largest network, metameric access will provide the security team more time to locate, contain, and eliminate the problem. [4]

4) **Maintain Backups**

The MS-ISAC advises that the foremost economical approach to get over a ransomware occurrence is to keep a copy very important knowledge. But there are certain things you can count on. So that hackers cannot access them, our backup data must be well secured and undamaged off-line or out-of-band. Because many cloud services save previous versions of your data, allowing you to restore an unencrypted version if necessary, using them might help you prevent a ransomware incident. Make careful to assess backup performance on a regular basis. In the case of an attack, ensure sure your backups are clean before rolling back.

5) **Develop plans and Policies**

Plan for incident response so that our IT security team will be prepared in the event of ransomware. The communications protocols and roles that will be used during an assault should be laid out in the strategy. A list of contacts, including any partners or vendors who would need to be contacted, ought to be included. Are there any "strange email" policies at WEW? If not, think about establishing a corporate policy. This will assist in educating staff members on what to do if they get an email that raises questions. Simply sending the email to the IT security staff might be sufficient. [4]

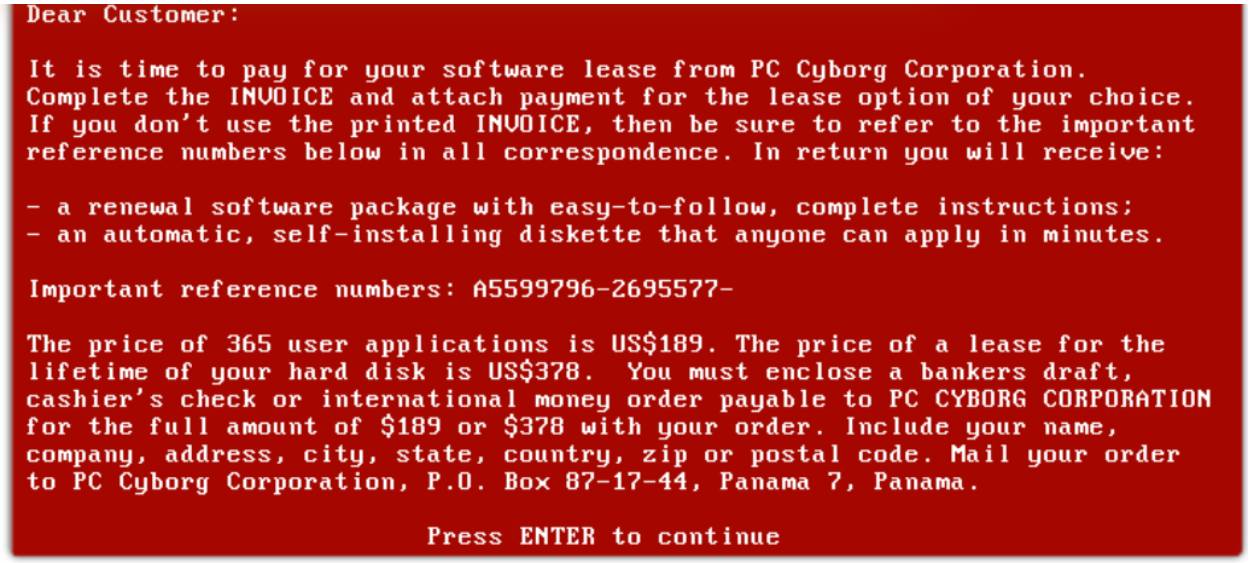
We can get important action to prevent actions additionally above detail. It can be implemented Individually.

1) Check the regular backups and make the backups regularly.
2) Avoid clicking on unsure links to prevent malware from being delivered and spreading to devices
3) Prevent malware from running on devices
4) Prepare for an incident

2.Evolution of Targeted Ransomware Attacks

2.1 The Early Year Ransomware

Usual terminology for the initial ransomware attack is "AIDS trojan." The term "AIDS" originated during the World Health Organization (WHO) AIDS summit in 1989, where researcher Joseph Popp gave away 20,000 tainted floppy disks to delegates. Once the user had started up 90 times, the user's file names would be encrypted, and the message below would appear, asking victims to send US$189 to a PO box in Panama. The removal of the ransomware was quite easy using online decryptor tools. This ransom note comes from the "AIDS trojan" virus. [5]



No significant improvements in the field of ransomware were made after this original occurrence until 2005, when it resurfaced and employed secure asymmetric encryption. The "GPcode" and "Archiveus" trojans were among the first ransomwares that gained widespread attention. At first, GPcode employed symmetric encryption to target Windows operating systems. It later used the more secure RSA-1024 encryption algorithm in 2010 to encrypt files with specific file extensions. . [5]

Early ransomware variations contained relatively basic code, which made them easier to identify and study for antivirus vendors, despite the efficiency of these encryption techniques. The password for Archives was compromised in May 2006 when it was found in the virus' source code. Hackers tended to prioritize hacking, phishing, and other attack routes since file recovery was commonly possible without a password, much as how GPcode changed to RSA. [5]

2.2 Ransomware embraces cryptography

The "Vundo" malware, which encrypted computers and offered decryptors for sale, first surfaced in 2009. Vundo downloaded itself when victims opened on malicious email attachments or exploited flaws in Java-written browser plugins. After being installed, Vundo targeted or blocked anti-virus software like Windows Defender and Malwarebytes. 2010 saw the quick appearance of the "WinLock" malware. The malware was employed by ten hackers in Moscow to lock their Pornographic content is shown on the victims' PCs until they pay them about $10 in rubles. Even though the scam initially netted US$16 million, the gang was captured in August of that year. The program was modified in 2011 to impersonate the Windows Product Activation system. The virus eventually extorted data from users and appeared to need a reinstall of the software as a result of fraudulent use. The "Reveton" ransomware scareware originally debuted in 2012 and delivered messages to its victims accusing them of watching illegal pornography while posing as US law authorities. It periodically turned on the camera on the user's device to give the impression that they had been videotaped. Additionally, to avoid legal action, it requested payment from the victim. There was a Mac version of this malware, however it lacked cryptography. There were 150 identical iframes that had to be closed one by one, giving the appearance that the browser was frozen. [5]

2.3 Ransomware become Dominant

"CryptoLocker" first appeared in the second part of 2013. In addition to using more conventional techniques like phishing, in countless more aspects, CryptoLocker was a pioneer. The "Gameover Zeus" botnet was used to spread the ransomware, making it the first to do so. Another noteworthy feature of CryptoLocker was the use of 2048-bit RSA public and private key encryptions, making it extremely challenging to decrypt. It was not until 2014 when CryptoLocker's related botnet, "Gameover Zeus," was destroyed. [5]

Also discovered in 2014 was "FileCoder," the first authentic ransomware for Mac, however it was later determined that its origins date back to 2012. Despite encrypting data and demanding money, the virus was never completely developed since it only ever encrypted its own files. On the Mac infrastructure that year, other non-cryptographic assaults were more successful. A threat actor remotely locked iPhones using the "find my iPhone" feature in 2014 as part of the "Oleg Pliss" attack, which also took place in that year. The threat actor logged in to accounts using stolen Apple account credentials. Then they requested a ransom to unlock the phone.2014 witnessed the first cryptography assault on mobile devices, with "Spyeng" targeting Android, much as Oleg Pliss attacked iPhones. Additionally, Spyeng sent messages with download links for the ransomware to each contact on the victim's contact list. [5]

"KeRanger" was the name of the 2016 cryptographic ransomware assault that was successful on Mac. The ransomware, It was linked to Transmission version 2.90 kept a victim's machine hostage until 1 bitcoin (worth $400 US at the time) was given to threat actors. In February 2017, the Mac

ransomware "Patcher," also known as "filezip," first appeared. It further attacked victims through torrenting, this time by impersonating a cracker for well-known software applications like Office 2016 or Adobe Premiere CC 2017. Notably, regardless of whether the ransom was paid or not, Patcher could not be decrypted owing to design defects. [5]

The popularity of CryptoLocker contributed to a sharp rise of ransomware variants. Although it has been in circulation since at least November 2013, CryptoWall replaced CryptoLocker and only gained popularity in 2014. By March 2014, CryptoWall had emerged as the main ransomware threat, spread mostly through spam and phishing emails. By the end of 2018, damage caused by the particularly persistent CryptoWall is estimated to have totaled US$325 million. [5]

2.4 The Emergence of Ransomware as a service

By 2016, there were more variations of ransomware. The first ransomware-as-a-service (RaaS) versions appeared as joint ventures between organizations that build the ransomware code and work with hackers to identify system flaws. Some of the most well-known ones included "Stampado," which sold for only $39, "Ransom32,", "shark" which was hosted on a public WordPress website and disseminated via an 80/20 split in favor of distributors, "Ransom32," which was the first ransomware to be created in JavaScript, and others. [5]

During 2016, the well-known "Petya" malware also made its debut. Initially less successful than CryptoWall, the ransomware began to show signs of improvement on June 17, 2017, when a new variant surfaced and was given the moniker "notPetya" by Kaspersky to set it apart from the original. Through the NSA-found Windows vulnerability known as "EternalBlue," it started in Ukraine and swiftly spread around the globe. The White House claims that NotPetya caused damage of $10 billion. The governments of the USA, UK, and Australia have blamed Russia for the virus. [5]

2.5 Ransomware and malware merge

Ransomware underwent a paradigm shift in January 2018 with the introduction of "GandCrab." Even while GandCrab by itself was not very noteworthy, it was combined with the information-stealing program "Vidar" to generate the GandCrab ransomware. As a result, the ransomware both stole and locked a victim's data. As of 2018 and 2019, GandCrab was the most widely used Ras a Service and active ransomware strain. [5]

As a partner of GandCrab, "Team Snatch" was a group of threat actors that first surfaced in 2018. They introduced the novel practice of releasing victim data to demand money. Team Snatch began distributing victim data in April 2019. Snatch was established by threat actor "Truniger," who worked on Exploit. On April 28, 2019, Truniger published a statement on Exploit stating that one

of their victims, Citycomp, had declined to pay a ransom and that as a result, their data will be made available to the public. However, the GandCrab ransomware is no longer in use as a result of the creators' announcement that they will retire on June 1, 2019, and the FBI's July 2019 release of the malware's decryption keys. [5]

2.6 The rise of leak sites

In November 2019, the "Maze" ransomware organization leaked 700 MB of documents that had been stolen from Allied Universal in an effort to force the firm and other potential victims into paying the ransom. Therefore, ransomware groups started developing leaky sites to increase pressure on their victims. Ransomware creators put a victim at risk of further financial loss by leaking stolen information if, for instance, delicate financial details, consumer personally identifiable information (PII), or business secrets are disclosed.[5]

A victim who has backed up their data may be less willing to pay extortionists for a decryption key alone if they have done so. this added leverage can be highly effective. The new method eventually implies that data backups no longer help to reduce the risk of ransomware attacks. The visibility of ransomware has significantly grown thanks to this new approach, and it also seems to have gained in favor. The NetWalker group alone generated more than $25 million in 2020. [5]

2.7 Ransomware Today

More than thirty years have passed since ransomware first became widely used. Technology that enabled it to transform from a tool used by a single hacker or group into one that is managed by a community, such virus integration and encryption techniques, as well as technology that surrounds it, like Bitcoin and the anonymous Tor network, had an impact on its appeal. Threat actors are increasingly using ransomware as the entry barrier grows lower, however it has not entirely replaced other forms of malware. Now that ransomware as a service application are readily available on illegal and underground online forums, threat actors may swiftly and cheaply work with ransomware creators. In the past, a ransomware assault would only provide a little profit and take years of development, cryptography, and penetration testing expertise. These Ransomware as a Service platforms are also highly sophisticated, including technical assistance, user dashboards, and instructions. The prize is finally becoming bigger. With the development of tools like Cobalt Strike and Metasploit that automate advanced penetration testing and offer increasingly sophisticated access to corporate networks through illegal marketplaces like Genesis Market, Access to organizations is expanding, and the market for ransomware is rising and become more profitable. By threatening legal action against the target organization, the combination of ransomware with data exfiltration allows for even greater ransoms. These all play a part in the rising power and destructive potential of ransomware. [5]

3. Future developments in the area

Attacks using ransomware have sharply increased after the COVID-19 pandemic. Numerous institutions have come under attack, including those in the political, financial, and medical fields. The surprising rise in attacks may have various explanations, but it appears that working remotely from home may be one of them. Cybercriminals are always experimenting with new ways to spread ransomware, such as phishing scams and other social engineering attacks. As a result, we examined recent advancements in ransomware prevention and detection in this paper and offered prospective directions for future research. Additionally, we researched a number of well-known ransomware samples and created our own experimental ransomware that may perhaps avoid being detected by eight well-known antivirus solutions. [6]

No time soon, ransomware will be outdated. With 304.7 million alleged ransomware attack attempts in the first half of 2021, the threat from ransomware increased dramatically. We recently received the 9th edition of the ENISA Threat Landscape (ETL) study, which offers us a fresh perspective on ransomware now and some important predictors of its future performance. NISA has placed ransomware as the top threat for the 2020–2021 reporting year, an enormous leap from the threat chart's previous position of thirteen. [7]

The most popular technique employed by nation-state thieves is ransomware, which is frequently distributed through extremely skilled spear phishing operations. Research experts at ENISA (European Union Agency for Cybersecurity) believe that nation-state threat actors will continue to pose a ransomware assault danger for some time to come. Researchers warn that rather than repeating past mistakes, state-backed threat actors have tightened their operations, increased their own security, and made a point of not leaving any high-fidelity evidence during their intrusions that may identify them. Analysts warn: "State-backed actors will undoubtedly continue undertaking revenue-generating cyber assaults with varied levels of national accountability." These threat actors are not immune to the siren song of profit either. [7]

The main worry in the field of modern technology is ransomware. However, for this growth to continue its boom, a safe and secure channel is needed. An ongoing research question and a barrier to continued development is the rise in ransomware attacks. Future research will look at more effective ransomware mitigation techniques.

In the future world, Ransomware affect for the development of the cyber security field. Regardless of size or sector, there are a rising number of trends and risks that organizations should be aware of.

3.1 Access control

Through the restriction of file system access, access control inhibits ransomware encryption. Studied how to utilize built-in security safeguards to stop ransomware from running with elevated rights on the host machine in 2017. When a user has high-level rights, ransomware can access files using the user's credentials. He recommended using role-based access control, restricting data access as high up the directory structure as is practical, and performing regular audits of permissions and roles to achieve least privilege and the separation of duties. It either disables access to the system or encrypts its data when ransomware affects a computer or network. To have the data released, cybercriminals demand ransom payments from their victims. [8]

2020 suggested a whitelist of authorized applications for each file type in an access control list. Only applications on a whitelist are permitted access to files. As a result, rogue programs are implicitly prevented from reading and encrypting data. A whitelist may effectively block new malware that hasn't been found, but a blacklist can't stop ransomware for which it lacks a code signature.

In 2018, the Antibiotics solution included a challenge-response system, a policy enforcement driver, and a policy specification interface. To stop data from being deleted or modified, this application uses both biometric identification (like a fingerprint) and human reaction (like a CAPTCHA). Through the periodic presentation of identity challenges, Antibiotics enforces access restriction. Based on a rule set by an administrator and input from efforts to edit or remove files, this software grants access permissions to executable objects. Because it was only tested on Windows OS, this software has certain restrictions. Aside from that, even if current ransomware could not get around Antibiotics, it is feasible that ransomware in the future may develop a defense against it. [8]

A framework was suggested in 2021 that allows access control decisions to be postponed when necessary, allowing time to examine the effects of an access request on the file system and, if necessary, undo modifications. According to the authors, a malware-resistant file system might be implemented using their technology, and ransomware assaults may potentially be avoided. Through a prototype test that included key ransomware scenarios, they showed how useful their framework is. Their system can be successfully used in practice, according to the testing findings against a sizable ransomware dataset. [8]

With the understanding that ransomware relies on the fake random number generators that contemporary operating systems make accessible to programs in order to produce keys, researchers in 2018 devised an access control method. Pseudorandom number generator functions are regarded as vital resources, and they suggested an approach to reduce ransomware threats that limits access to their APIs and prevents unauthorized programs from calling them. Testing their approach against 524 real-world live ransomware strains, including versions of WannaCry, Locky, CryptoLocker, CryptoWall, and NotPetya, they were able to halt 94% of them. [8]

3.2 Data Backup

Making frequent backups of the data stored on a computer or network can considerably lessen the consequences of ransomware. The only data that has been damaged is the data that has been added since the last backup. Since there is a cost associated with backing up significant amounts of data, decisions must be made on how frequently and how long backups should be kept.

Developed in 2017, the FlashGuard solution is completely independent of software. Instead, it makes use of the fact that Solid State Drives (SSD) utilize a garbage collector to erase data after a time rather than immediately overwriting it. The authors modified the SSD firmware to delay data removal by the garbage collector, allowing for the recovery of lost data. FlashGuard successfully recovered encrypted data when tested with ransomware samples without having an adverse effect on SSD performance or life.[8]

In 2018, a literature review on functional backup architecture paradigms, ransomware attack processes, and backup protection capabilities was completed. They also provided a new tool for doing backup system evaluations during information security risk assessments, along with suggestions on how to improve information security risk assessments to better manage ransomware threats. This technology improves an organization's ability to fend off and recover from a ransomware assault by allowing auditors to examine backup systems more efficiently. [8]

A self-contained SSD backup and recovery solution called Amoeba was recently (2018) presented as a ransomware defense. In addition to a fine-grained backup control system that minimizes the amount of space needed for original data backup, Amoeba incorporates a hardware accelerator that instantly identifies ransomware attacks on pages. The authors implemented Amoeba in the Microsoft SSD emulator extension, and to assess their system, they used accurate block-level traces that were acquired while running the genuine ransomware. As a result of their tests, they discovered that Amoeba surpassed the most recent SSD, FlashGuard, in terms of performance and space economy, and had a tiny overhead. [8]

A transparent buffer for all storage I/O is maintained by the Redemption system, was suggested in 2017. It requires just minor operating system update. Redemption keeps an eye out for any indications of ransomware-like activity in the I/O request patterns of individual processes of apps. I/O request patterns that point to suspected ransomware activity can be used to halt the offending processes and restore the data. When their method was evaluated, it was discovered that Redemption could ensure no data loss when facing the most recent ransomware families without affecting user experience or raising the user's alertness level. They also showed that Redemption had acceptable overhead, with real-world workloads averaging 2.6%.[8]

3.3 Key Management

The act of identifying the encryption key that was used to encrypt data and utilizing it to unlock it without paying the ransom is referred to as "key management." This procedure could be made quite straightforward by some ransomware strains, including those that hard code the key directly into their executable file. This can be more challenging for hybrid models because the key is only accessible in plaintext while the data are being actively encrypted.

There are eight main types of.NET ransomware, and it was discovered that certain ransomware versions employ subpar key generating methods that make use of standard libraries. By maintaining a backup of an attacker's symmetric encryption key, ransomware defenses can take use of this information. Later, you can retrieve any encrypted data using this key. For instance, In 2018, it was discovered that many ransomware programs create the encryption key using the CNG library (Cryptography API: Next Generation), a cryptographic library for Windows computers. They created a defense mechanism that hooks these operations in order for the system to save the encryption key whenever ransomware calls them. a prototype ransomware software was created to evaluate their system. They also put into practice their preventative strategy, which entails trying to intercept the ransomware program's encryption process in order to get the encryption key. When the example ransomware creates the encryption key, the prevention application shows it after hooking and extracting the encryption key. Their ransomware protection solution was always able to retrieve the encryption key in tests where the ransomware program tried to encrypt ten times, one hundred times, one thousand times, ten thousand times, and one hundred thousand times. This method has the drawback of assuming that ransomware utilizes a certain library to obtain the encryption key; if this assumption is incorrect, the solution is rendered useless. [8]

Some varieties of ransomware encrypt data using symmetric session keys. This key, which encrypts the user's data, is kept on the victim's computer. In 2017, a signature-based key backup technique called Paybreak was developed. The session keys used by PayBreak, including the attacker's symmetric key, are kept in a vault using a key escrow mechanism. During the test, PayBreak was able to retrieve every file that had been encrypted using recognized encryption signatures. [8]

3.4 User awareness

In her study on combating ransomware attacks within businesses and organizations, Chung Chung (2019) made the case that managers and supervisors should assist staff members in taking safeguards against ransomware frauds. This is particularly crucial since, as was previously indicated, ransomware attacks are increasingly focusing on institutions like banking or healthcare businesses. For workers to follow, the author provided five preventative suggestions:

1. Make sure that every computer and mobile device in use has antivirus or anti-malware software installed.

2. For both personal and professional accounts, use secure passwords.

3. routinely backup data to an external hard disk.

4. Avoid clicking on dubious email attachments

5. Use mirror shielding technology, like NeuShield, as an extra layer of data security.

This article concentrated on how people may avoid falling for phishing attempts, which are a frequent initial step for ransomware. 2018 also addressed how consumers and staff within businesses can prevent ransomware assaults. Following a poll of various security experts, the author came up with a number of recommendations. The first suggestion was to divide up the company's workforce into groups depending on things like their expertise with phishing and the significance of their individual roles. The second piece of advice was to offer customized training for each group after segmentation. Real-world examples should be utilized to illustrate the seriousness and harm that phishing may do, together with authentic case studies and examples from the company itself, in this training. [8]

techniques for spotting malware Researchers have released a variety of detecting techniques to recognize current ransomware attacks. Ransomware programs may be stopped and removed once they are identified.

4.conclusion

A ransomware attack is a harmful form of malware that locks a user's computer by encrypting the data using different encryption methods and then demands payment in exchange for the decryption key or the decryption key to unlock the device. Security teams need to be more aware of the danger that this type of malware poses as ransomware grows and expands its reach to various corporate and healthcare sectors. By taking the proper steps at the appropriate time to avoid, detect, and recover from the ransomware assault without actual system damage, the potential effect of a ransomware attack may be considerably minimized.

Many kinds of financial losses exist, affecting both businesses and people. The possible loss of productivity for organizations and individuals, a rise in IT expenditures as a consequence of lost systems and devices, the need to upgrade networks, as well as the purchase of new services and programs, are some examples of the monetary losses mentioned above. By implementing the proper incident response processes and security technology, businesses can prevent ransomware. Several security tools are available to track network activity and look into server data, including security event managers. Another tool that might help maintain the computer system updated is patch management. One of the other tools is antivirus software with ransomware protection capabilities, like Bitdefender. Additionally, there are technologies that can deter ransomware attacks and alert you to any unusual behavior.

This report shows what is the ransomware, what is nature of the ransomware, how much millions of ransomwares take can cost. additionally, what are most popular ransomware attacks, how to prevent ransomware attacks, how is the future development area of the ransomware.

5.References

[1] Y. Gandhi, "What is Targeted Ransomware?," 16 Nov 2021. [Online]. Available: https://www.analyticssteps.com/blogs/what-targeted-ransomware.

[2] J. F. H. A. A. Pierce Ryan, "Dynamics of Targeted Ransomware Negotiation," IEEE, 21 March 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9738625.

[3] F. Melnyczuk, "Famous Ransomware Attacks," 24 December 2021. [Online]. Available: https://antivirus.com/2021/12/24/famous-ransomware-attacks/.

[4] "7 Steps to Help Prevent & Limit the Impact of Ransomware," Center for Internet Security, [Online]. Available: https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware.

[5] V. Drake, "The History and Evolution of Ransomware Attacks," 29 July ,2022. [Online]. Available: https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/.

[6] S. Rauch, "The Rise of Ransomware in the Era of Covid-19," siple learn, 28 Oct 2021. [Online]. Available: https://www.simplilearn.com/rise-of-ransomware-in-the-era-of-covid-article.

[7] M. MEISSNER, 14 APR 2022 . [Online]. Available: https://blog.pcisecuritystandards.org/the-threat-of-ransomware-attacks-2022.

[8] A. B. D. A. H. K. K. Craig Beaman, "Ransomware: Recent advances, analysis, challenges and future research directions," National Center of Biotecnolgy Information, 24 Sep 2021 . [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8463105/.

[9] F. Melnyczuk, "Famous Ransomware Attacks," 24 December 2021. [Online]. Available: https://antivirus.com/2021/12/24/famous-ransomware-attacks/.