IT20660116.pdf

by

Submission date: 21-Oct-2021 10:05AM (UTC+0530)
Submission ID: 1679805110
File name: IT20660116.pdf (626.02K)
Word count: 5401
Character count: 31121

Sri Lanka Institute of Information Technology

Ransomware Attacks and its Evolution.

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT20660116	Sulaxshayan.N.

Date of submission
2021.10.06

Table of Contents

Abstract

The intention of this report is to provide awareness about ransomware attack and its evolution. This topic must be an understandable topic Because of this global pandemic situation. According to the information, when compare before pandemic and after pandemic started, Ransomware attacks have been risen since 2020(16). Not Because of IT related industries have offered to their employees to do their works from home. This is common in IT industries but after pandemic situation works from home was risen gradually. Lockdown situations also were push others in critical too. People needed thinks to buy but ,Because of lockdown situation all groceries and all other shops were closed until further notice.

So, Medium, and high-level Business environments started selling their product in online. Therefore, peripheral devices and internet usage has risen than usual before pandemic. So, cyber criminals started using this situation to proliferate money by doing cybercrime from medium level business environment to high level business environments and also by this ransomware attack some organizations were affected too. Definitely, Ransomware attacks can be omittable by doing proper practice and mitigation techniques. This report contains information about what is ransomware ; what are the type of Ransomware; Attacker using techniques to infiltrate host machine; History of ransomware attack; Graph description for illustrate depth of ransomware attack; Recommended techniques that are used to mitigate from the attack.

1. Introduction

I. What is Ransomware ?

FIGURE BELOW1)

Ransomware attacks have been inevitable threats for many years from small business environment to highly securable data organizations and also governments. Initially, what the term ransomware means is , typically, It is a malware have been developed from the concepts of cryptovirology that penetrate the system of victim then, it starts encrypting personal data and if sometime even possible to capture entire peripheral or halt access of internal , external communication and services as like hostage until ransom is paid for decryption key.

In sometimes, victim is a ransomware aware one and at the same time program that accomplished attack is elementary, thus that person may be reverse it. However, sometimes threat actors are used to modify highly advanced malware with the support of

them sophisticated programming skill to execute an attack. This attack method called as cryptoviral extortion.

To this attack , all peripheral devices are vulnerable perhaps without a decryption key victim cannot recover files and even unlock the device. for all ransomware attacks motivation is, acquire ransom payment from the victim by all possible ways. Also, they use tactics that really scares the victims and push them to pay ransom. But we cannot sure about after we pay the ransom, we can get decryption key from attacker.

There is lot of ways that an attacker may be run away with our files without giving decryption key. Mostly targets of ransomware attacks are, single business individuals, specific organization which deals with data. When ransomware attackers target an organizations or business individuals, Initially they consider about two main steps. First, they determine ways about how to reach device of victim. After that attacker gained access, program starts to decrypt files and working to deliver ransom message on victim's screen.

According to the past studies, in Early 20's ransomware was not spread extensively because of difficulties in ransom collection. After invention of cryptocurrency ,specially, bitcoin invention in 2010 is inverted everything. Crypto currency contributes a way that cannot untraceable transection methodology which helps to receive ransom from victim without knowing attacker's identity.

Bitcoin pave the way to ransomware attackers to develop ransomware to become a remunerative activity. However, obtain payment by bitcoin not an effortless way from technology illiterate targets. Past ransomware stories are reveling, that the attackers to ensure the payment, they have given technical support to sign up for bitcoin. Nevertheless, those efforts were useless at one time. Cybercriminals once succeed in payment receive , they allocate some amount of money for future development to their research and program of their next ransomware project. In addition, allotment of this fund also means to upgrade cryptosystem, provide services that helps to acquire payment from victims, promoting and operating ransomware as a service in the underworld markets and also Analyze new attack vectors and moreover.

2. Evolution of the topic

II. How victims caught by Ransomware?

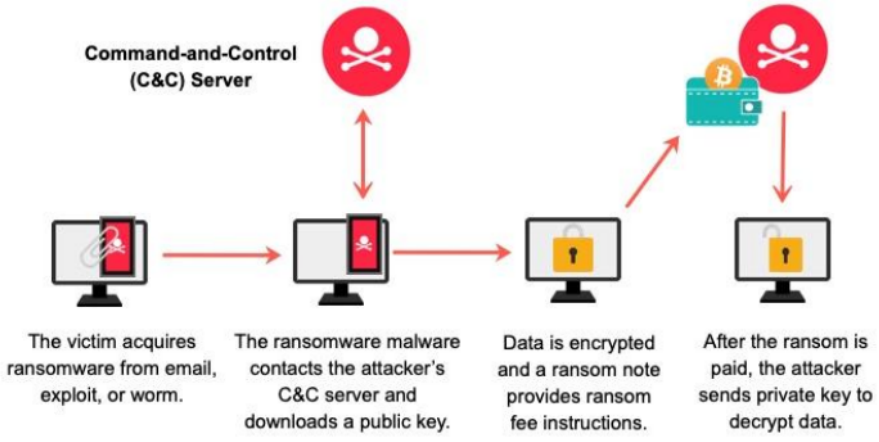

FIGURE BELOW2)

Emergence of the ransomware as service, many impactive ransomware models have been developed by the malware developers. According to the information ,they sell their products to consumers in underworld market either fixed-price or gives as a platform renting with conditions. That is ,when a profit acquires by the attacker from an attack, an amount of or a percentage of ransom should be given to the ransomware developers. These ransomware distributors are working as serviceman for developers, they disperse the infection model as different kind of an attack to different kind of vectors as mentioned in the disperse procedure list. An elementary ransomware attack cycle is showed in figure 1.2. To this success of this model, these following objects should be occurred successfully .

1.Infilirate victim's device

These techniques are used by the attackers to infiltrate targeted host or random peripheral users.

- If a ransomware to encrypts victim file, initially it needs to penetrate the host machine.

  To infiltrate host machine, Ransomware developers apply phishing attack to convey the malware. More commonly attackers send legitimate mails with malicious link or file attachment same as like it comes from law enforcement authorities. An information includes in The email body that really prompt to the victim to click the link. Once click, malicious program starts upload then leaving the victim that an attack took place at all. In file attachment included malware extension type will be .exe and .zip. Recently, Ransomware attackers have evolved their techniques and mechanisms to another level. Now, for pursing the victim's device, attackers try to exploit critical security vulnerabilities and brute-force attacking remote desktop protocol.

- Malware advertisements.

  When visits a website sometimes ads and pop-ups come frequently more than usual.

  All of those ads and pop-ups comes with embedded malicious links. Once, click on , malware started downloading and execute ransomware with other attacks onto victim's device.

- Social medias network

  Ransomware also may be disseminated by social medias. In general, malicious links can be transmitted by among users. When user clicks on link, it redirects to the malicious website with a purpose of downloading and executing ransomware scripts. Thus , social medias may be worked as a capture tool for drive-by download attacks.

- Worm

  Computer worm is a standalone malware it replicates itself in order to spread throw networks. In a network a computer infected by the ransomware worm , there are more
  possibilities here to other computers also infected too.

- Exploit kit

  Exploit kit is a toolset that is designed to perform automated activities. Initially, it searches vulnerability in host machine after that it finds if any vulnerability, attacker is tried to exploit vulnerabilities using exploit kit. Then attacker upload malware payload to the device. Oracle java and adobe system products are being more common targets to the exploit kit.

- Malicious app

  Some verified websites provide free use of some kind of apps which is really use for downloading copyrighted contents from popular websites. When users download these apps also malware payloads execute itself in victim's device.

- Drive by download attack

  Derive by download attack is a malicious program that install user's device without they known. Computer users acquire this threat from authorized web sites. These websites already have security flaws and unsuccessful updates in it , so attacker uses it as a platform to spread malicious code to the back-end device .When a browser loads site like this, malicious code download successfully without user prompt to click on any links. direct drive-by download attack and indirect drive-by download attacks are two types of this attack. Indirect drive-by attack injects malicious code to victim's device in stealthier manner by finding security flaws in user browsers.

Now criminals are focused on exploiting security vulnerabilities with the help of evolving tools set. Once find security vulnerabilities, they deploy ransomware attack.

2.Aquire encryption key

- Once ransomware program infiltrates the host machine, it works with full force to encrypt victim's datafiles. Modern day attackers are used public-key cryptography for encrypt and decrypt victim's file. according to the information which was used to break symmetric key depended on unbounded computation power peripheral devices. Attacker insert his virus into host machine which his public key. Then, this corresponding virus encrypts data on victim's device. In public key cryptosystem that attacker only knows the private-key which corresponding to the public-key. Then, attacker holds this key to exchange it for ransom. But data encryption on public-key approximately slow, so hybrid encryption system was introduced by the attackers. This methodology is being used by attackers to encrypt critical datafiles of victim. In order to encrypt data in hybrid encryption, attacker must be generated a random session key and a random initialization vector(IV).

  For example ,if we denoted attacker's private-key as 'A_p' and virus public-key as 'V_p' then random session key as 'S_k' respectively, where 'W' denotes the attacker and 'V' denotes the writer. To understand about to know how hybrid encryption works. The plain text of victim device will be $\{m=[IV,S_k]\}$, then virus encrypts it with its public key(V_p) to acquire ciphertext $m`=\{IV, S_k\}\ V_p$. Then virus encrypts critical files using initialization vector with random session key and a symmetric encryption key.

So far described think is, how ransomware program encrypts victim's data files. Now we will see how attackers decrypt victim's encrypted files.

- An attacker needs private key in order to decrypt victim's encrypted files and also its private-key stored somewhere in the network. So, attackers create virus programs that is crawled over the network and copies the private key itself. This is resembled illogical, but ransomware programmers are being succeeded in this

attack by insightful in networks and cryptography. According to theory that saying, Entire private key cannot be saved in a node in the network until it gives entire private key user of that nod in the network. But attacker point of view is, concerns all the network as a host then they possibly split and achieve the power of the user. Until it is possible when different users in the network do not access each other's data.

Therefore, attackers use tactic that is, they share private key of the virus among the nodes in the network where nodes should be greater than one. Then, virus finds the secret place of hidden private key. Fact of this over all concept is , Similarly, the virus act as an agent to the virus programmer . It is spread among the network, and it waits for some host machine in the network freed it by themselves. Then, the virus misdeeds and global problem is caused by the host ,. First if anything occurs to host machine, According to the expert's solution, they must examine the network's administrator. Then, virus copies the private key by itself and make it visible to attacker in order to perform user's data encryption. In this case, host machine user is the victim of freed the virus infiltrate into system with attacker involvement.

3. File encryption

- After acquired the encryption key attacker initiates the process of encrypt user's file. Then, attacker search into the victim's device such as where there any confidential text files that victim has or has not. Following wide range of search in victim device, if anything found, attacker only encrypted those files without halting whole operating system. After encryption process end successfully, symmetric key will be destroyed by the attacker for preventing victim from encryption key recovery. So, without attacker acquire back the files is impossible.

4. Display ransom message on screen.

- Once files are encrypted by attacker Then they forward to explain what the thinks were being accomplished by them and what is the think that need to be done by victim in order to recover files. Attackers provide instructions to acquire ransom from victim in safe way. Most of the times that payment method chosen by

attacker is getting ransom in cryptocurrency. Once payment is made by victim there is no guarantee that all victim's encrypted files fully given by attacker.

5.Getting paid

- An amount of payment is depended on, Which level of information is captured, What kind of ransomware technology has used also how much effort and an involvement that has given by the attacker to accomplish an attack. According to the past information, extortion is getting by three level.

- Attacker only Encrypts user data and extorting money , Once ransom receives decrypt victim's file. Attacker does not keep any controls over victim's device after ransom payment receives.

- In some case, attacker encrypts victim's file and reserve some data files for next extortion. After getting paid, Attacker initially brings control back to the victim but remain control on reserved files for another extortion. Sometimes, there are more possibilities that reserved files may be given for cash to third parties in underworld market.

- Last but not least, In sometimes, Attackers never bring victim's data even ransom paid. This is the worst case in ransomware that is no guarantee to recover data even ransom paid.

- According to the information, Bitcoin , Wire transfer, Premium-rate text message , pre-paid voucher service such as PaySafe card ,are being payment option to the attackers.

III. Type of ransomware.

Over the past ten years ransomware attacks were inevitable threat to business organization and meta data organizations. According to the functionalities and intention of the threat actor , Ransomware can be divided by major two categories.

i **Encrypting ransomware.**

ii **Non-encrypting ransomware.**

So far, we have already discussed about what **encrypting ransomware** functionalities and its mechanism that what crypto system that uses in order to encrypt victim's device. In addition, attackers also find ways to extort money from targets without encrypting victim's files or halt access to them device. Attacker extort money from victim Without encrypting victims' files, This attack called **Non-encrypting ransomware** attack.

- **Non-encrypting ransomware** defines, It is type of malware display message over victim's screen and imitates that victim's device has taken over by law enforcement authorities and demand them to pay ransom to release.

- **Exfiltration or Leakware** is also a type of ransomware attack that Threat actor holds victims' sensitive information as a hostage and threaten victim, if ransom payment does not pay then, victim's information will be published in public. This extortion attack different from other ransomware attack where other encrypting attacks encrypts victim's files make it inaccessible to victim but, in this attack, victim can access their information, but disclosure will be a threat.

- **Mobile ransomware**

  Growth of the mobile phone usage, also mobile ransomware has become a profitable attack. In mobile ransomware, Uses blocker mechanism to interrupt or halt access the user from using browser or operating system Then, demand ransom for acquire back access. Downloading APK files from unauthorized websites, Prompt to click emails which comes from unidentified person are major reasons to this attack.

IV. History and Evolution of ransomware

- **AIDS Trojan ransomware.**

This is the first well known ransomware attack in December 1989. This was also called "PC cyborg". Dr. Joseph L.popp was recognized as a creator of this virus who had been Harvard-taught evolutionary biologist at that time. Popp was handled a traditional way to reach his virus to the victims. That is , The infected floppy disk was sent throw an email to victims which labeled as "AIDS Information Introductory Diskette," using impersonate itself as a questionnaire about the AIDS virus and also it was franked a logo of " PC cyborg corporation". Similarly, The method is handled by author is, Make victims trust upon on mail which comes from truly trusted health care organizations. In effort, popp was succeed in his virus spreading methodology. Floppy disc was a source to distribute malware payload for encrypting victims' files. According to the information, that floppy disc was include two files. Two of it , was written in QuickBASIC 3.0. At that time AUTOEXEC.BAT used as a startup file to Windows operating system. Popp notion was hijack AUTOEXEC.BAT in the root directory instead of encrypting the user C file immediately. Also, it was designed to not immediately strike on booting file itself but, When booting started in infected computer, after few numbers of count the malware executed itself. Once execute, Victim's all file names in C: drive encrypts using symmetric key encryption. The malware encrypts victim's files extension instead of encrypting the files for half execution of those files.

Once files encrypted successfully, The malware displays a ransom message that defines as software license had finished, In order to do activities on computer user should renew it. According to the studies, The renewal cost was $189 per year to lease and $378 was lifetime lease. Ransom payment address was displayed on victim's screen(PC cyborg corporation, P.O. BOX 87-17-44, Panama 7, Panama). However, payment received from victims were not expected. In 1990, AIDS trojan virus was nearly come to its end. According to the studies, The cyborg virus inventor

popp was arrested in the Netherlands in January 1990. Strange Activities of popp when baggage checking was happening on the airport , After police was searched his baggage, they found gadget labeled with “PC cyborg Corp”. popp also was working as consulted of WHO in Kenya and also where he had arranged an AIDS awareness programs in every year. So, he protected himself from lawsuit saying like , that money which earned from this attack was to go to AIDS research by Pc cyborg Corp. Later decryption program was introduced by Jim bates, it named AIDSOUT and CLEARAID in January 1990. However, authorities were announced that popp is mentally unfit to locus standi for trial in 1992. (6)

- **Crypto locker**

  Crypto locker is an encrypting ransomware. It was appeared with new encryption algorithm in 2013. This model was totally evolute rather than other old ransomwares. It was designed to search victim’s encrypted files within available platforms. Such as hard drive, shared network drives, USB drives, external hard drives . Once reached the device ransomware works with 2048bit RSA key pairs generated from the attacker command and control server in order to encrypt victim’s file(12). Initially, infected computers halt access from victim , to recover files; victims instructed to pay ransom by bitcoin or prepaid voucher within 3 days since infection. According to the information, ransom payment was approximately $300 per key.

- **TeslaCrypt**

  TeslaCrypt ransomware introduced in February 2015. Initially, Computer gamers was the target of this attack. It was designed infect gaming files such as game saves, database files , Recorded replays, documents etc. Once penetrated the victim’s device this virus started delete available backup and restore points for prevent victim from file recovery(14). End of the accomplished encryption, Attacker was demanded $500 from victim in order to acquire decryption key. According to the information, (15) ransom payment was doubled unless to pay or delay.

- **Petya Ransomware attack.**

  Petya ransomware attack was appeared in March 2016. This ransomware technique is different when compared with others. The notion of this virus creator is, instead of encrypting all victim's files directly, encrypts Master Boot Record(which contains the information about how logical participations are coordinated , how containing file systems are organized; also, it contains loader program of installed operating system (17) used by NTFS file system. To sum up, attacker injects malicious code(Petya) that shows ransomware message when victim boot ; It halt the system boot until ransom paid (18)(13). According to the information, ransom payment was $300.

- **WannaCry ransomware.**

  It was discovered on 12th May 2017. Attackers were used phishing attack to intrude the user's device. Initially, it was spread throw internet by the exploitation of EternalBlue.

  EternalBlue is a Microsoft server SMB vulnerability exploit which was developed by the U.S National Security Agency , That was exposed by the Shadow Brokers hackers' group(13). According to the information, over 150 countries there were ten of thousand infections recorded and In addition, this malware was designed to run in 27 different languages(19). For recover files , Attackers were demand $300 threw the Bitcoin crypto currency. However, According to the information, The wide spread of this ransomware at that time halt many operations. That are , One of the multinational telecommunication companies in Spain was affected and some more; British National Health Service had halted its services, One of the third largest telecom operators in Russian called "MeganFon" was affected by this attack. Lately, on 13th May 2017 security patches were issued by Microsoft for operating system Windows XP, Windows 8, and Windows Server 2003(19).

- **SamSam Ransomware .**

  In 2016 this ransomware was arrived with new technique to extort money from critical infrastructure organizations, large enterprises also induvial peripheral users. Mainly This malware found in United States and other some countries. The

vulnerability exploitation in Windows Server was led to intrude victim's network. According to the information, Attacker used the JexBoss Exploit Kit to find vulnerability in the webserver. Attackers were accessed Remote Accessed Protocol by Brute force log in credentials or stolen login credentials. Once attacker infiltrate the network, it was easy to acquire administrator level access (Privilege escalation attack) Therefore malware program executed successfully without the user permission. Most likely, victims were instructed to pay ransom by Bitcoin threw Ransomware note which was left by attackers. Once payment received, attackers sent links to the victims to download decryption key or decrypting tools to decrypt their network. (20)

V. Reported Ransomware attack around the World.

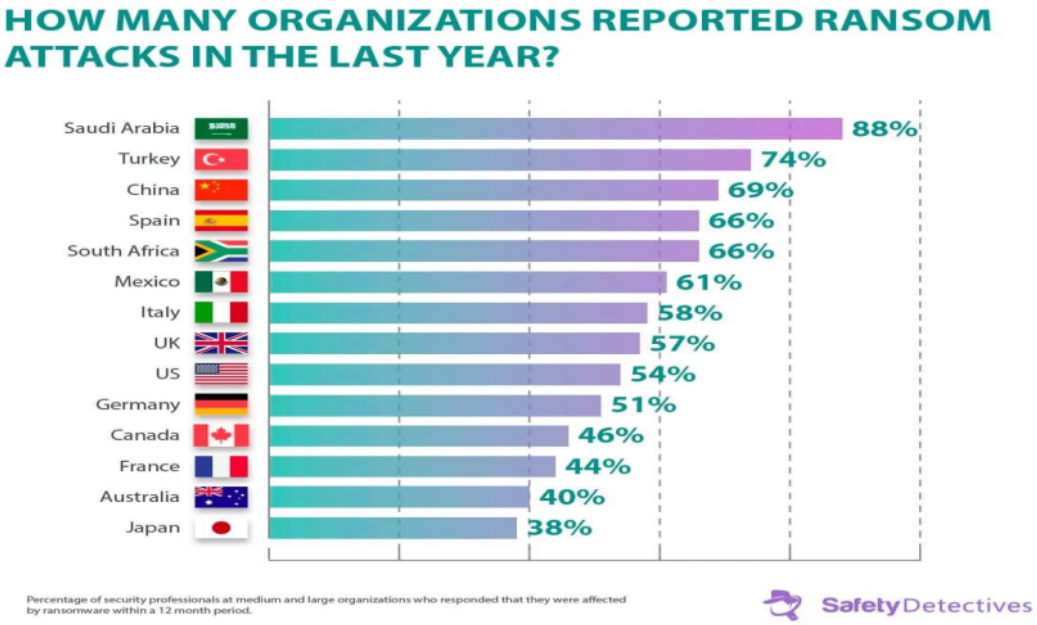

FIGURE BELOW11)

This graph gives information about the percentage of security professionals who reported that they medium to large level organizations were damaged by ransomware in 2019. The x axis depicts percentage of security professionals who reported about an attack , and y axis illustrate that percentage of reports were came from which countries. Most of the response were came from Saudi Arabia, that is 88 percentage. 38 percentage of response were recorded in Japan and, it was lowest percentage of that year. Spain and South Africa remain same percentage of response were recorded on that year ends. Turkey and China are arrived in responded percentage; second and third respectively.

Overall, Ten countries data is illustrated about that above 50 percentage of their medium and large organizations has affected at the end of that year. Also, security professionals in four countries were response below 50 percentage that are Canada, France, Australia, and Japan. In addition, Organizations in France are affected by more than 4 percentage when compared organizations in Australia . At the end of the year, Affected organizations in UK is led by 3 percentage when compared with US. When compared Japan and Saudi Arabia once, There were 50 percentage lead

between both countries. Besides, There were 34 percentage lead between Australia and turkey ; when 40 percentage organizations were affected by ends of that year in Australia. When compared China and France; there were 25 percentage lead affected organizations on China than France. When compared Canada and China; there were 20 percentage lead between both countries and less affected organizations were recorded in Canada. Similarly, reported organizations in US and Mexico response 54 percentage and 61 percentage respectively. Here , 7 percentage of organizations affected more in Mexico when compared to the US.

In addition, Organizations in Italy and UK were affected nearly same but, it was decreased by a percentage in UK. Finally, Assumption of all these statistics is illustrated about organizations in which countries had reported more than 50 percentage should be evaluated about their organizations Threat, Risk, and mitigation techniques; To sum up, Always to be prepared in Incidence response planning too.

3. Future developments in the area

VI. Mitigation Techniques.

The evolution of the ransomware and those intended mechanisms, there are different kind of mitigation techniques are being introduced by the network and cyber security experts. To avoid being infected victims of ransomware attack, following the provided practice of expert and, Analyze them references, should be inevitable for maintaining organizational strength, keep strengthen the people's reputation, improving computational strategies and well-organized response when ransomware attack occurred.

- **Backup the organization's data**
  Backup is the main important aspect of ransomware mitigation technique. Back up must be happened at daily routine and Previously did back up files should be checked before the backup routine. If user does not maintain these activities often, Preventing files from ransomware is being worthless. In addition, When Threat actor infiltrates the computer initially, he/she search into PC to check available backup. If anything, available first that threat actor destroys it. So according to the expert technique , one system having multiple backups is important and also experts encourage to have backup in physical storage too. Because victims no need pay ransom they can wipe the system then,
  They can restore information directly from physical storage.

- **Maintaining incident response plan.**
  When a ransomware attack occurs, Attacker never gives much time to responding back to that attack. According to the studies, attacker minimum gives three or four days to response unless victim's confidential information's will be sold in under world market. Therefore, constructing and maintaining an incidence response plan is significant to the organizations.
  In sometimes, some organizations having incidence response plan but reviewing it only when an attack take place. Objectives of good incident plan teaches each one in organization; how to response efficiently when a cyber-attack happens.

- **Organizations should have critical system in form of "Gold images" .** at the event of reconstruct system. Sometimes in some hardware component does not install or cannot accessible some kind of images, when it happens user needs run those in different needed software environments will be a good practice.

- Regularly checking the system or device for intend of **finding vulnerabilities** to mitigate the risk from attacker's exploitation .

- **Update application to newer version and update operating system.** When updating to newer version, security flaws in oldest software or application has been removed or patched. So, software infecting percentage will be mitigated.

- **Maintaining strong password** Some malwares like WySIWyE, SamSam does brute force attack to acquire remote desktop protocol logins. Therefore, maintaining properly installed network firewall and provide strong passwords which will mitigate from being caught by ransomware attack .

- **Remove or block protocols** unwanted protocol and oldest versions which have not been used in communication.

- **Aware among peripheral users about phishing attack.**

  Most of the time attackers send malware with email attachment to spread them ransomware. The notion of the attacker is capturing the feeling of victim in the body part of the mail for that, attacker pretend like whatever(Legitimate law enforcement authority or someone that victim has known).Therefore, before clicking the attachment make sure that mail comes from whom it states. After confirm everything, Make sure that antivirus software up to date and scan that attachment manually. Finally, after all safety measures , it does not seem apprehensive then click on the attachment. Sometimes for the effect use of application, it may be enabled automatic download attachments or files by default. So, we make sure that is also disabled.

4. Conclusion

The evolution of modern technologies in computing and expansion of internet usage also increased computing related cyber-crimes too. There are more talented persons who are genius in computing do good thinks around the world but also , There are some kinds of persons in our society who are profinite money from doing cybercrimes with them broad understating on computer science. However, One of the well-known cyber-crimes is Ransomware attack .Ransomware attacks have been developing since past from now. According to the studies, Attacker handles strategies and technique also different form each attacks they have applied.

From bitcoin and cryptocurrency related invention; ransomware attacks and extort money from victim has gradually increased. According to the information, Also Ransomware as a service has been introduced by the ransomware developers. Attackers find possible ways to penetrate victim's device. In sum, New scripts that have been evolved from past ransomware scripts and they design malicious script threw finding existing vulnerabilities on victims 's device. According to the studies, Past ransomware attacks are illustrated that how much ransomware evolved in cryptography ; they were illustrated that how much they had been mastered in crypto system by successfully acquired ransom.

According to the studies, They were some named ransomware attack that remain another side of internet crimes still. Different encrypting algorithms had been used by those ransomwares. Later they were some cryptographers found anti-malware in order to decrypt files and some people who were accused of that crime; they were some found by law enforcement authorities and gone sentenced for their crime. In some case, they kept them anonymity last long. However, Ransomware attack cannot be removed totally from internet but, it is avoidable by using proper practices and mitigation techniques.

5. References

1) Hoşcan, M., (2019) Free ransomware protection and decryption tools. [ONLINE]. Available at: https://www.kaspersky.co.in/blog/anti-ransomware-all-in-one/16914/ [Accessed 18 September 2021].

2) Gantenbein, K., (2020) How Ransomware Works and How to Prevent It. [ONLINE]. Available at: https://www.extrahop.com/company/blog/2020/ransomware-explanation-and-prevention/ [Accessed 22 September 2021].

3) Worst Ransomware Attacks in History to Date. 2019. Daniel Tobok. [ONLINE] Available at: https://cytelligence.com/resource/worst-ransomware-attacks-in-history-to-date/. [Accessed 23 September 2021].

4) Baker, K. (2021). HISTORY OF RANSOMWARE. [online] www.crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/ [Accessed 23 Sep. 2021].

5) A. Young and M. Yung, "Cryptovirology: extortion-based security threats and countermeasures," in Proceedings 1996 IEEE Symposium on Security and Privacy, 2002.

6) Sdxcentral.com. [Online]. Available: https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/. [Accessed: 01-Oct-2021].

7) Ponemon.org. [Online]. Available: https://www.ponemon.org/local/upload/file/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf. [Accessed: 02-Oct-2021].

8) "Cyberattacks are inevitable. Is your company prepared?," Harvard business review, 09-Mar-2021.

9) "Protecting Against Ransomware," Cisa.gov. [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST19-001. [Accessed: 03-Oct-2021].

10) "2021 cyber security statistics: The ultimate list of stats, data & trends," *Purplesec.us*, 08-Nov-2020. [Online]. Available: https://purplesec.us/resources/cyber-security-statistics/. [Accessed: 04-Oct-2021].

11) Guest Writer, “Ransomware isn’t going away any time soon - facts, trends & statistics,” *Disruptive.asia*, 25-Jun-2020. [Online]. Available: https://disruptive.asia/ransomware-isnt-going-away-any-time-soon-facts-trends-statistics/. [Accessed: 04-Oct-2021].

12) “CryptoLocker Ransomware Infections,” Cisa.gov. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/TA13-309A. [Accessed: 05-Oct-2021].

13) Wikipedia contributors, “Ransomware,” Wikipedia, The Free Encyclopedia, 29-Sep-2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Ransomware&oldid=1047163373. [Accessed: 05-Oct-2021].

14) Cisa.gov. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf. [Accessed: 05-Oct-2021].

15) Kaspersky, “TeslaCrypt Ransomware Attacks,” Kaspersky.com, 13-Jan-2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/teslacrypt. [Accessed: 05-Oct-2021].

16) C. C. in February et al., “20 Ransomware Statistics You’re Powerless to Resist Reading - security boulevard,” Securityboulevard.com, 28-Feb-2020. [Online]. Available: https://securityboulevard.com/2020/02/20-ransomware-statistics-youre-powerless-to-resist-reading/. [Accessed: 05-Oct-2021].

17) Wikipedia contributors, “Master boot record,” Wikipedia, The Free Encyclopedia, 06-Sep-2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Master_boot_record&oldid=1042707845. [Accessed: 05-Oct-2021].

18) L. Constantin, “Petya ransomware is now double the trouble,” Networkworld.com, 13-May-2016. [Online]. Available: https://www.networkworld.com/article/3069990/petya-ransomware-is-now-double-the-trouble.html. [Accessed: 05-Oct-2021].

19) Indicators Associated With WannaCry Ransomware,” Cisa.gov. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/TA17-132A. [Accessed: 05-Oct-2021].

20) “SamSam Ransomware,” Cisa.gov. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/AA18-337A. [Accessed: 05-Oct-2021].

IT20660116.pdf

ORIGINALITY REPORT

4%	3%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	global.oup.com Internet Source	1%
2	Submitted to Sri Lanka Institute of Information Technology Student Paper	1%
3	www.isaca.org Internet Source	<1%
4	ftp.cerias.purdue.edu Internet Source	<1%
5	medium.com Internet Source	<1%
6	www.riskbasedsecurity.com Internet Source	<1%
7	www.business2community.com Internet Source	<1%
8	en.wikipedia.org Internet Source	<1%
9	www.tandfonline.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	< 5 words
Exclude bibliography	On		