International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)

ISSN: 2456-236X

Vol. **04** Issue **02** |**2020**

Ransomware- Prevention & Mitigation

Santripti Bhujel

Master student, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India

ABSTRACT

The paper basically talks about one of the most current affairs that are Ransomware which falls under online extortion of an individual or an organization. The paper indicates the introduction of ransomware and its type, its key characteristics, methodology, the impact caused. The major focus is on how we can implement various preventive measures against the various ransomware attacks. The paper also gives an overview of a brief study on mitigation methods of ransomware.

KEYWORDS: ransomware, prevention, mitigation, public key infrastructure,social engineering.

1. INTRODUCTION

Ransomware is a form of cyber extortion which comes under the family of malware. Malicious software or an online crime involving an attacker threat against the individual or an enterprise designed to obstruct entry to a system up to a certain amount of ransom is rewarded which is asked or demanded by the attacker.

Previously ransomware usually aimed at an individual, but now a day even business is targeted as well. The confidential data of the individual or an organization is being encrypted by the attackers who ask payment for the decryption key.

Ransomware gets into your system in the same way as a virus or any malware gets into your system knowingly or unknowingly through: emails which appear to be an important attachment, certain website, ads which seem to offer valuable stuff for free, fake updates for antivirus and programs, social engineering methods, etc.

2. TWO TYPE OF RANSOMWARE –

a. **Encrypting ransomware-** It utilizes advance encryption rules that obstruct system files and demands the sufferer to pay for the decryption key which can unlock the encrypted data and information.

b. **Locker ransomware-** It blocks the suffereraway from the computingsystem and does not allow him to utilize his desktop and any applications, software or file inside the system. Even though data is not encrypted by the attacker but he still demands payment or ransom from the victim to unlock the system through bitcoins.

This paper deals with the key characteristics, prevention and mitigation of ransomware.

3. LITERATURE SURVEY

There are many researchers and surveys on Ransomware and by using these as a reference the following paper has been created and there are many types of research that have been done to know more about ransomware and moreover, the main aim of this research is to prevent and mitigate against ransomware attacks. Many surveys have been done to record the matter and for future reference. Here are a few referencesthatItook to create this paper.

4. KEY CHARACTERISTICS ON RANSOMWARE

Ransomware possesses unbreakable encryption which does not allow the victim to unblock the files or data of his own.Ransomware has the potential to lock all kinds of data such as docs, audio, videos, picture, etc.It involves various social engineering techniques like phishing, whaling, pretexting, baiting, tailgating, etc. to baffle the person into recompensing the money. Example: shuffling victim’s file names so he won’t be able to predict the pretentious data.After the attack, it will display some kind of image or message that let the person know that his data has been encrypted and a certain amount of money is required to be paid to acquire his data again.Attacker requests the amount in bitcoins as the bitcoins are difficult or impossible to be traced by cybersecurity experts.The payment has a time frame and once the time is excided the ransom will increase and sometimes even data can be lost forever.The attackers often expand their infrastructure by recruiting the infected PCs into a botnet for performing future attacks. It has the capability to spread to another system which is connected in the same network causing further damage.

Ransomware can extract confidential data of the victim like username, pins, mail id, etc. and forward it to repository managed by the hacker.It also has the ability of translation of ransom note into sufferer's native language just to enhance the probability of the money to be rewarded.

5. PREVENTION ON RANSOMWARE

Backup of one's important data and file should be done on a regular basis to prevent data loss in case of any sort of attack or system failure. Storing your confidential data on the cloud as well as in physical stores will be an efficient way.Also, setting the least data access privilege and read-write permission to prevent any kind of modification or erase. The best practice is to check your backed-up data occasionally to ensure the integrity of the data.Ransomware is most of the case are spread though emails so setting an anti-spam setting is one of the many ways to defence through this malware. The setting should be done in such a way so that it will block all the spam mails or block dubious attachment which contains extensions such as .exe, .scr, etc. Think twice before clicking because we receive many dangerous hyperlinks via social networks or instant messengers which are sent by any of our friends or the people we trust. The attackers modify this link and send this to as many people as possible.

The malicious messages can not only come from an unknown source but; it can even come from a known source like friends or family. Spoofing emails may impersonate as a notification from any source such as banking institute, law enforcing agency, e-commerce resource, etc. To prevent compromises via exploit kits try keeping your operating system, antivirus, browsers, and software up-to-date.

Try to turn off the internet connection at the early stage of the attack because it may not let the ransomware to establish a connection and thus cannot complete encryption of victim's files andfolder.Turn on the Windows Firewall and configure it properly all the time to stop unnecessary packet inside the private network.

Protection can be further enhanced by setting up additional Firewalls to defence against trespass.Always scan compressed or archived files.Disable Windows PowerShell, enable when needed only. Microsoft Office's security components should be enhanced such that no malicious code is allowed to execute on the host machine.Use a strong and unique password for different accounts such that the password cannot be brute-forced by attackers easily and that may reduce the risk to a certain level.

Disable AutoPlay feature which ensures that the harmful processes should not be automatically launched on the host machine through any external factors.Disabling file sharing option will help ransomware infection to confined to your machine and avoid spreading of infection.Make sure you switch off all the unused wireless connections and switch on only when it is to be used. It will prevent the machine from the exploit. Example- switch off Bluetooth or infrared ports.

6. MITIGATION ON RANSOMWARE

This particular mitigation step confirms a way of securing the assets of an organization by restricting the attacker from accessing the resource. It separates the assets, data, application, and network by compartmentalizing them in such a way if a ransomware attack happens it won't affect the whole system network. Whitelist what can run on the system instead of blocking malicious processes. There are new malware and virus which are emerging lately in high volumes. So, it is very difficult for security suites to keep track of it and even malware signatures are outdated to present cyber threats. The new window AppLocker facilities allow users to create a list of applications and their processes which can be whitelisted if they are authorized and secure to run those applications in the system or network.

The Enhanced Mitigation Experience Toolkit helps with an additional protection layer the malware attackers have to get through to exploit the software. Enhanced Mitigation Experience Toolkit provides features certificate trust. It detects and stops the Public Key Infrastructure (PKI) man-in-the-middle attacks.This tool can be used by individual and deploy it across the enterprise. Maintain secure backup of one's important data and file should be done on a regular basis to prevent data loss in case of any sort of attack or system failure. Storing your confidential data on the cloud as well as in physical stores will be an efficient way. Also, setting the least data access privilege and read-write permission to prevent any kind of modification or erase. The best way is to check your backed-up data occasionally to ensure the integrity of the data. Ransomware attacker usually depends on exploit kits and social engineering to attack the host machine and spread the malicious code. These techniques are very easy to implement because of the high infection rate on the victim's system. The black hat hackers usually send a huge number of spam messages which attract victim to open their attachments. The victim who is vulnerable and falls for the trap and download the unknowingly executing the malware.

The phishing method is usually used for ransomware, using some security detection can help you stay safe. The law of scan states that don't open any suspicious email or links or attachments. Cybercriminals will compromise your account and use it to send other people malicious mail using your account. Hence, even if you know who has sent the mail you should be careful enough to open the attachments that he had sent and think before clicking the links that came along with the mail.Hacker nowadays also use old tactics which infects the shortcuts in Microsoft Office papers. Just make sure that the ActiveX features are disabled because it can result in infection of other application and software also.

The hacker can disguise ransomware executables inside files which looks genuine.They incline to allocatenumerousallowances to the loader that it seems like a harmless data or files. The file named as rose.jpg, accompanied by few gaps and .exe, can be an example of this trick. Finally, when the attacker sends a mail with this attachment the victim thinks that it is an image file and gets infected by it. Hence, configuring the operating system in such a way that it shows the malicious file extension can safeguard in some manner.Ransomware attackers are gradually trusting on these automated programs for delivery. The recent spot called CryptXXX, for example, targets on processers with the support of theill-reputed Angler EK. It initially originates with a web browser or search engine readdress from a slashed website. After that the targetconquests the automated program’s landing page, that permits the malicious code to find vulnerabilities in unpatched programs on the computer. In case a slightambiguity is marked, the automated program sums the ransom onto the organization. The softwarethat is most targeted for such attacks includes Java, Adobe Flash Player, and search engines, so make sure to keep this software up to date.

Hacker my use the properties of Windows PowerShell to install his malicious code into the system. Usage of Windows PowerShell helps the infected code escape antivirus recognition; hence, restricting it can result in stoppage tactics sometimes.As we know that most of the ransomware is distributed through ads so a browser extension that has the capability to block unnecessary popup ads can ensure safety as well. Hence, by using a popup blocker we can bring down the risk of getting affected by ransomware by clicking links which appear to look harmless and if once clicked can run the ransomware program in the background that encrypt user’s files and folders.Setting an unrepeated or tough to guess passwords is another way to make the task of attacker hard. In case if hackers succeed in guessing your credentials than taking over the system is an easy task for him. So, the password should be such that an attacker couldn't brute force it and the best practice is to change your password on a regular basis.

Some of the ransomware exhibit self-replicating features like womb and virus and causing harm to other unaffected systems also. There are many removable devices which can hold ransomware malicious code and result in infecting one system and eventually other system connected to it. Being a user if you are accessing the services remotely, make sure to adopt two-factor authentications and stay logged out when not using those services.This method will not totally clear the ransomware but it will keep the contamination isolated to a single machine in the network and does not allow it to spread from one affected system to other unaffected system connected in a network.

Using software restriction policies is one of the simple yet effective ways to avoid the crypto attack. Most ofthe most ransomware attack will function from a particular system path. Hence, by adding a new path rules helps in avoiding malicious .exe from executing if in case they are placed inside the files and folders.If in case, you suffered from an attack of ransomware you may face a situation wherein the attacker will ask the victim for ransom to decrypt his file and if he does not pay the amount in time the ransom value will increase. The time given to the victim is about 6-7 days within which the attacker gets complete access to the files. Luckily, there is a more effective way to stop this. Configuring system BIOS clock to an earlier date will give more time to the victim and slow down the countdown time and gives the victim an extra bonus time to find and fix that problem.

There are many variants of ransomware which could be decrypted by researchers who gave free decryption solutions for the victims who were affected by ransomware. Therefore, if you encountered any kind of ransomware or Trojan than make sure that you check up the name on the Internet and search for help immediately. You may find some help regarding the decryption of the encrypted files over the internet.

Always have a response in advance**.** When an organization is attacked by ransomware, it is necessary for the affected parties to perform preventions and mitigations factors before the time given by the attacker and before the ransom amount increases. Hence, IT professionals or IT Administrator should monitor and look after the confidential data assess it, take the backup of those critical data and calculate the effect on the organization if those data is compromised.

7. CONCLUSION

The above paper indicates a brief detail on Ransomware. Ransomware is one of the most known malware in present-day which not only have the capability to encrypt user's confidential files and data but also ask money for decrypting those files. Hence, we users should be aware of this type of malware because it can affect anyone at any point in time. So, to avoid such scenes we should know a few prevention and mitigation steps for our own data protection and to avoid unnecessary payment. We should also have an idea of what to do in a situation if we get affected by ransomware.

8. ACKNOWLEDGEMENT

I would like to express my deep and sincere gratitude to my research guide, Mr. Subarna Panda, Assistant Professor, Department of MCA, Jain Deemed-to-be University, for his valuable and constructive suggestions throughout this research work. His willingness to give his time so generously has been very much appreciated.

9. REFERENCE

[1]https://www.tripwire.com

[2]https://nakedsecurity.sophos.com/2016/03/24/8-tips-for-preventing-ransomware

[3]https://blog.barkly.com/ransomware-statistics-2016

[4]www.symantec.com/.../ISTR2016_Ransomware_and_Businesses.pdf

[5]http://resources.infosecinstitute.com/ransomware-mitigation-and-prevention/#gref

[6]http://blogs.systweak.com

[7]www.symantec.com