A COMPREHENSIVE OVERVIEW OF RANSOMWARE METHODOLOGY

[1]Harshada M. Raghuwanshir, [2]Prof. Ketki R. Ingole
[1] P.G Student, Department of Computer Science & Engineering, Sipna C.O.E.T, Amravati, India[1], Assistant Professor, Department of Computer Science & Engineering, Sipna C.O.E.T, Amravati, India[2]

ABSTRACT

Among the various different types of malware, Ransomware is one such malicious software which affects the target system by locking it through encryption. It is one of the most dangerous attacks which corrupts the data, encrypts it, and also steals the information from the victim computer, rendering the files on the computer useless, unless the encryption key is provided. Depending on the type of ransomware, either individual files or even the entire operating system might get encrypted. Ransomware has been a prominent threat to enterprises, government agencies as well as individuals over the last couple of decades. Any platform can be a likely target of a ransomware attack. In this paper, we have conducted a brief analysis on ransomware, the various families of ransomware, measures that should be taken to prevent ransomware attacks and so on. By means of this paper, we endeavour to create an awareness regarding ransomware attacks and means to accurately detect a ransomware threat.

Keyword: - Ransomware, Malware, Security, Vulnerability, Encryption, Backdoor, Cryptocurrency,

1. INTRODUCTION

In computer network, security problem arises when vulnerability in network is use to harm the user. The vulnerability is actually a source through which any query or a malware enters the system. When vulnerability is in the website, it means there is a bug in the website and so once, when vulnerability is found hackers could easily bypass the authentications to enter into the victim's system. In order to access victim's server attackers, use different types of attacks like spoofing, man in the middle attack, social engineering etc. Using these attacks attackers create a backdoor through which they could easily access the data.

Malware is a abbreviated term for the malicious software. Such software programs are specifically designed to gain access or damage victims computer. A lot of malware is created today for profit through malicious email attachments, infected software apps, infected external storage devices, compromised websites, advertisements or even sometimes they are bundled with other software too. A growing number of attacks have used payload and other approaches that don't rely on any form of user interaction. In this paper we are going to discuss one such type of a hazardous malware that is "Ransomware".

Ransomware is a type of malware that encrypts file on the target computer using strong cryptographic algorithm .The ransomware, after completing the encryption process request ransom from the victim with the information note open on the target computer .The victim cannot open the file without paying the request ransom ,since the private key to open the encrypted file is usually store in the attackers C&C server(Command and control server).So, the actual owner of the file became unable to use his or her files ,and even if he/she has already paid the desire ransom , unfortunately the user are left at the mercy of the attacker since the malware uses asymmetric encryption so that the victim cannot reasonably be expected to recover the (private and undistributed) key needed to decrypt the ransomed files. In this way attackers play an "extortion racket "through Ransomware.

Basically, Ransomware came from two words ransom and ware. Webster's dictionary defined Ransom as "money that is paid in order to free someone who has been captured" and as "a consideration paid or demanded for the release of someone or something from captivity". At the same time, Webster's dictionary likened the word "ware" with "aware and gave example of their use in a sentence "was ware of black looks cast at me".

This knowledge of the two words (ransom and ware) as understood in life and was brought into the cyber technology field.

Ransomware was truly left design in the late '90s and didn't start to come back due to unmistakable quality until 2005. The accessibility of increasingly complex encryption plans, alongside progressively accessible framework side figuring power, helped to introduce this new period of ransomware, which has kept on quickening. Starting at 2016, it is viewed as a standout amongst the most pervasive types of assault against PC frameworks, requiring constrained presentation to vulnerabilities and negligible observation on target.

There are two basic types of Ransomware. The first is locker ransomware. This type prevents the computer's OS and the application from running and even opens the computer to prevent the user from performing normal operations. The second is crypto Ransomware. This ransomware encrypts the file in the computer disk through the function of the computer OS that are running smoothly.

Ransomware uses different attack vectors like spam and phishing emails using social engineering techniques. A Ransomware is generally activated by opening the email containing the malicious macro and loading to the computer executable file of the script running with the activation of macro which is in the file. In addition, the methods of opening the addons sent by spam emails, fake software that comes from trusted source, obtaining administrator authority and providing permanent access are all among the attack vectors. These dangers are not constrained to a specific geography or working framework, but can also make a move on any number of gadgets. Everything from your Android gadgets, iOS frameworks, or Windows frameworks all are in danger of this kind of abuse. However, Ransomware in other cases can do specific damage to the computer data files. Although it can hit any file on the computer, ransomware often target specific files types having file name extensions like.txt, .doc, .rft, . ppt, .cbm, . cpp, . asm, .db, .db1, .db1, .dbx, .cgi, .dsw, .gzip, .zip,, jpeg, .key, mdb, .pgp, .pdf.

To perform such type of abuses attackers, make use of C&C server because it is very important for the attackers to ensure confidentiality and keep the location of the C&C server undetectable. They create their own payload and bypasses the two step verification authentications. However, new generation ransomware attacks are made via encrypted HTTPs protocol or the TOR network. Additionally, C&C server use the Dynamic DNS service, which allows a different IP address assignment by the ISP to the domain after a certain TTL value.

2. TYPES OF RANSOMWARE

There are different types of Ransomware. Though the purpose of the Ransomware is the same the mode of a request for demanding the ransom varies and hence the types. In this part of our study, we will be discussing the features of seven most commonly known ransomwares in the previous five years i.e Cryptolocker, Crypto-Wall, Cerber , Locky ,WannaCry, Petya and Bad Rabbit.

2.1 Cryptolocker

Cryptolocker as Troj/Ransome-ACP,is a malicious program as ransomware. Some ransomware freezes your computer but cryptolocker is different, it makes us to work on our computer as well as software but our personal files, such as documents, spreadsheets, and images are encrypted. The criminal retains the only copy of the decryption key on their server-which is not saved on our computer, so we cannot unlock our files without their assistance. Cryptolocker is particularly interested in that it functions by encrypting victim's computer files with a combination of RSA-2048 and AES-256 encryption. Once encrypted, victim is provided a window of specific time in which they can pay the attackers to receive the key needed to decrypt their files. Unfortunately, once the malware has successfully encrypted a victims file there is no way to decrypt them without the private key.

2.2 WannaCry

WannaCry is such a malware that began to spread on May 12,2017, by means of exploit vector named Eternal Blue which was developed by exploiting the gap in the Microsoft's Server Message Block (SMB)protocol. According to Microsoft's analysis and report,it exploits the SMB vulnerabilities in unpatched version of OS:XP,Vista,Win7,8,8.1 by using Eternal Blue exploit kit and Double Pulsar Backdoor. Once the WannaCry is executed on the system it starts further processing of exploiting vulnerabilities on the system due to its worm like capabilities that block the access to the entire system as well as files and even replicate itself to entire network of a computer via SMB. It has spread about 150 countries affecting 300,000 computers which has been the largest ransomware attack in the history.

2.3 Locky

Locky is such a malware that was firstly seen in February 2016, it is a very complicated type of a ransomware and works as a malicious software. It arrives by mails and attachment in a word document with a macro.

Upon opening the document, the macros infect the computer by activating itself and performs a particular background process and start executable file of locky. And once it updates itself it becomes a very dangerous ransomware as it is undetectable to antivirus too. Locky encrypts not only the files on the computer but also the VSC's (Volume shadow copy services) to prevent user's file from restoring. Locky also encrypts external hard drives, database files, all network resources, and Bitcoin wallet to force the victim to pay the ransom. And so due its strong policies within the first few days only locky had infected about 100,000 computers

2.1 Petya

Originally Petya was detected in March 2016 by bundling itself with other ransomware known as Mischa which was the combination of two ransomware in the box.It is also known as GoldenEye.Later on this ransomware again revealed its appearance in the mid of 2017,but this time all alone and got many new name as ExPetr,NotPetya.etc Petya goldeneye variant is distributed through theme based spam campaign consisting of malicious pdf regarding the job resume with subject and file name including a German word 'Bewerbung' . Once click on it, it start downloading the fake pdf file and before opeing that file it elevates a window asking for a user permission and once user click on "YES"option it provide all the admin access to that pdf and thereby petya is installed in the system and gains all the write to modify the MBR(Modifying Boot Record).

Otherwise if "NO" option is click then Mischa

Is install on the system and in such case, user has no other option rather than to be a victim of either Petya or Mischa. This virus spread through EthernalBlue or EthernalRomance by exploiting on the loophole. Actually, during execution of the Petya the Mimikatz or Window acess token thief tool performs its actual task of stealing all the credentials and whatever victim types (ex spearphishing, keylogger) and send all stolen information to its master control.

2.5 Cerber

Cerber ransomware was originated in Russia in July 2016. It is kind of bundled attack that employ Betabot Trojen that steal credentials, Banking data and other sensitive information as much as possible. Cerber initiates the attack with vbscript injected macro enabled office document as spam mesage . This injected vbscript called out Power shell for downloading the malicious file of cerber and killing the active antivirus processes (bypassing). When macro is enabled unknowingly, on opening the document the injected vbscript runs the Powershell to propogate itself throughout the network and place the downloaded payload in %AppData% directory or folder. Before executing further task, it check for the installed language pack to be Russian and other defined by Liska,if detected to be there then it stops the execution of ransomware and removes the system

silently .Once it has installed itself successfully Cerber disable safe boot and remove the Volume Shadow Copy's to eliminate the chances of recovery and empowering the probability of targeting more and more vulnerabilities on servers. In this way cerber performs their methodology.

2.6 BadRabbit

The year 2017 witness numerous ransomware attack, the third largest attack of such kind that is preplanned well-coordinated and target attack that originates with petya in July was Bad rabbit that showed its devastating effect later, on 24 oct 2017 which victimize large corporate networks and multinational firms .The Bad Rabbit Ransomware spread through "drive by attack " where insecure websites are compromised "While the target is visiting a legitimate website, a malware dropper is being downloaded from this threat". Bad Rabbit binds itself with package of Adobe Flash Update infected computers worldwide by showing itself as an Adobe Flash Player update patch. Bad Rabbit has spread over internal and external networks via SMB services as in WannaCry and Petya, by using information obtain from infected computer and user name and password information define in itself. It gives ". encrypted" extension to the end of the encrypted file.

2.7 Crypto-Wall

The CryptoWall Ransomware is a ransomware Trojan ,having different version like Cryptowall2.0 , Cryptowall3.0, Cryptowall4.0, Cryptowall5.1 that carries the same strategy as other encryption ransomware infections such as Cryptorbit Ransomware or CryptoLocker Ransomware does., It was first appeared in November 2013,and still is one of the most widely used Ransomware In just six months, it had infected more than 6000000 machines and encrypted about 5.25 billion files. One of the more recognizable variations, CryptoWall (right now old), was assessed to have gathered $18,000,000 by the center of June 2015. The CryptoWall Ransomware is designed to infect all versions of Windows, including Windows XP, Windows Vista, Windows 7 and Windows 8. As soon as the CryptoWall Ransomware infects a computer it uses the RSA2048 encryption to encrypt crucial files. Effectively, the CryptoWall Ransomware prevents computer users from accessing their data, which will be encrypted and out of reach. The CryptoWall Ransomware claims to pay $500 USD to recover the encrypted data. This payment is demanded using TOR and Bitcoins in order to maintain the recipients' anonymity. Malware researchers strongly advise against paying the CryptoWall Ransomware ransom. This only encourages ill-minded persons to continue carrying these types of attacks.

3. METHODOLOGY OF RANSOMWARE

Ransomware attacks take place in five phases. Basically, the lifecycle of ransomware consists of six different phases that are referred to as a kill chain. However, the general trend of kill chain enforces to summarize these stages can be categorized to reach its destination. These phases are

1. Deployment
2. Installation
3. Command and connect server
4. Destruction
5. Extortion

3.1 Deployment

This phase is the Initial phase where attacker search for the vulnerabilities to spread the threads into the victim systems that are associated with the spread of ransomware. This phase is also known as the knocking phase. This phase involves tracing of various ways through which ransomware tries to enter into the victim system. In order to achieve its purpose ransomware installs all those components that are used to infect, encrypt or lock the victim's machines. Some of those methods include drive by download, phishing emails, social engineering and

different attack vectors. In this way ransomware tries to obtain anyhow the authorized permission to create space for itself into the target system. Some commonly used entry point can be described as

3.1.1 Spam attack

Victims are aware of junk folder in mails wherein emails come from the untrusted sources or fake ids which gets collected into the spam folder .This spam folder consist of spam messages .The spam messages consist of threads to download on the victim system and when it get downloaded then attacker remote the victim system by using that payload , nowadays those payloads are also available for the android platform too .In today's condition most of the ransomware uses spoofed electronic mails as their primary distribution method that are send via botnets to reach victims system.

3.1.2 Exploiting loopholes

Loopholes means weakness of any website. It is also called as vulnerability. There are many ways to get the vulnerabilities from any website, any system or any device. Whenever a website is scanned some open ports and closed ports are shown wherein attackers perform their attack which is called as a loophole where the exploitation attack can be done easily. These loopholes can be outdated or partially updated OS that are used for redirecting the user to exploit the kit page, ad an iframe is injected. Once an appropriate vulnerability is identified it is utilized to make a space for ransomware in the system by dropping its infectious executable(installer)into the computer for initiating the infection. There are different tools that are available on darknet from where we can hire any criminal services. rnability scanner, nmap, zinmap etc which are open source.

3.1.3 Drive-by-downloaded attack

Drive by download is a concept where the attacker forces the victim to download the latest versions of software like Adobe Flash, Web Browser, Oracle JRE etc through repeatedly popup windows that comes from previously hacked website. Attacker gives victim the lust in order to achieve their target also it gives a beneficial message in order to force victim download their software.

3.2 Installation

During the initial phase or the distribution phase the attacker manages the downloaded package file on the host system to install ransomware itself on the victim's system or the devices by taking the trusted administration privilege, and in this manner the infection process begins. The package file containing the small piece of malicious code escape itself from detection and communicates with C&C server. On the other side ransomware downloads itself from C&C server and gets install on the victims system .It sets the key on the Windows vault and checks and sets the client benefits by making changes to User Access Control(UAC) with the goal that malicious payload acquired can run easily at whatever point the framework boots or reboots .Moreover it tries to kill the any active security such as (firewall ,anti-virus)solution to establish an untraceable link like FUD(fully undetectable payload)with its master in next phase and gathers all required information to design the encryption key without any interruption by any anti-malware tool. It shows itself in the task manager as the trusted package is running. In addition, ransomware spread itself throughout the network by utilizing WMIC (Windows Management Instrumentation Command line) tools that easily spread from the newly infected device to other linked devices by extending the WMI utilities for providing not interacting as well as interacting mode of retrieving information about the status of the system.

Once the infected code is installed successfully, then it tries to connect the listener port. It connects the listener i.e attacker in such the way it contains the gateway IP of the listener and the port number using C&C server. C&C server work as the handshaking i.e it contacts with the extortionist. And it behaves like the attacker get the

master control and the victim system is fully under control to the attacker. In order to access the attacker server, generate the list of domains and checks the embedded link within the payload. The initiation of this communication begins from the victim where the install ransomware scans the system and gives only those information that is required enough for the attacker .Since the modern ransomware uses a combination of AES (Advanced Encryption Standards) and RSA cryptographic algorithms, the AES key is produced within the system to encrypt files and RSA key pair is generated on the own simple web python server that work as the temp server that used by only the Attacker.

In this way the malicious code encrypts the file and send the credential data of the victim to the attacker using the tor network, that hide their identities.

3.3 Command and Connect Server

The attacker operates the ransomware and its family through C&C server. C&C server helps the attacker to get the victims credentials. Following is the working of this basic system

- It consists of command and control server
- The C&C server communicate with a botnet (sending a number of packets to the server) via IRC (internet relay chat) command
- The command and connect server then carry out scheduled activity (deniel of service attacks, data theft, identity theft, etc)

The command and connect server have different types of working structures it may be online server or offline server or any switch or an access point through which intruder works on back side and create their own server and access victim's data through point to point connection. Command and control malware activity routinely take hidden form such as –

1. Tor traffic network: - The tor browser uses a specialise network of world-wide servers to deliver a botnet services that uses incognito tab in the browsers which is very hard to trace it original source of attacker.
2. Social Media: - The social media can be used to issue botnet command and this traffic is very difficult to distinguish itself from genuine traffic. Ex- Facebook pages, etc
3. Multilevel command and control server for example if server A is block through some issue by the botnet then the entire traffic is diverted toward the remaining server but in case there is a single sever the botnet attack stop the web-services and searches the vulnerability and exploit on it get the data.

3.3.1 Concept of C&C server

Once the malicious code is installed it will begin to reach out the C&C server for instructions. These instructions consist of total information about the file which is going to be encrypted. Some ransomware also reports system information such as Domain name, subdomain name, IP address, mac address, OS, and the language they are using for their hosting and other .C&C channel can be unencrypted http, encrypted https and anonymous. Tor increases the complexity to reach exact location of attacker. Also, in this phase key exchange occurs wherein private keys are held by the C&C server.

3. 4 Destruction

This phase starts when the attacker gets the administrative access of the victim, and the payload injected files or infected files start encrypting by the malicious code which include all forms for example – JPGs, GIFs, PNGs, CAD etc. When the Destruction phase start the infected file, it gives the flash pop up of command prompt and shows the instruction of auto repairing the system but in background it is actually encrypting the files.

3.5 Extortion

Pop-up messages are shown on the victim after the files have been encrypted. This pop-up message includes the information regarding ransom, and background process that include the working of an algorithm that are used for the encryption. Also, it contains the description about how they have been infected.

Education and Awareness (Preventions):

1. As a matter of First importance, makes certain to back up your most vital record all the time – Ideally, backup activity should be diversified, so that the failure of any single point won't lead to irreversible loss of data. In order to prevent your important files, store one copy of it in the cloud. In the cloud for example: - Dropbox, Google cloud, Mega. And if you want to store the copy of data offline so we can also make used of portable HDD.
2. Customize the setting to protect from attacker to stop spams- Most ransomware variants are spread through eye-catching emails that contain contagious attachments its great idea to configure the webmail server to block the spam attachment with extensions like .exe,.vbs or .src ,.bat .
3. Avoid opening the connection that look suspicious- This is not only applicable for the messages sent by the unfamiliar people but also to the sender whom you believe could thread. Phishing email may show a false notification from a delivery services, and e-commerce resource, a low enforcement agency, or a banking institution.
4. Reconsider before clicking- Dangerous hyperlink can be receive by the social network or instant messengers and the sender are likely to be the people to trust. For this attack to be deployed cyber criminals compromise their account and submit bad link to as many people as possible.
5. The show document of augmentation highlight can prevent ransomware plagues, too- This is native windows functionality that allows you to easily tell what type of files are being open, so that you can keep clear of potentially harmful files. The fraudsters may also utilize a confusing technique where one file can be assigning a couple of extension.
6. Fix and keep your working framework, antivirus program, Adobe streak player, Java and other programming software up-to-date This habit can prevent compromise via exploit kits.
7. Consider disabling windows power shell, which is the task automation framework - Keep it enable only if absolute.
8. Deactivate autopay- This way harmful process won't be automatically launch from external media.
9. switch of unused wireless connects such as Bluetooth, WIFI- There are cases when Bluetooth get exploited then it gets control by other compromised machine
10. Make sure that your file sharing is disable. - This way ransomware infection if caused to your machine then it will stay isolated to the machine itself .
11. Used strong password that cannot be brute-forced by remote criminal. - Set the unique passwords for different accounts to reduce the potential risk
12. Install a browser addon to block pop-ups as they can also pose an entry point for ransom trojan attacks

4. CONCLUSION

In today's digital era, where every critical piece of information is being stored in the form of data, it is absolutely vital that we are aware of the threats that we may face. It is better to be prepared rather than regretting the lack of information after the damage is done. In this paper, we have discussed briefly on one such common threat of nowadays called as Ransomware. We have provided the different types of ransomware, the working of ransomware and also provided a list of measures which must be implemented to immunize ourselves from this threat. These measures must be practised thoroughly to keep our data safe from attackers. Hence, we addressed one of the most dangerous common malware attacks and ways on how these attacks can be prevented and dealt with.

REFERENCES

1. A.K. MauryaNeeraj KumarNeeraj KumarAlka AgrawalAlka AgrawalProf. Raees Ahmad KhanProf. Raees Ahmad Khan, "Ransomware Evolution, Target and Safety Measures", International Journal Of Computer Sciences And Engineering 6(1):80-85 January 2018
2. Arina Alexei, "Network Security Threats To Higher Education Institutions", Central and Eastern European e|Dem and e|Gov Days 2021At: Budapest, Hungary, July 2021
3. Ali, A.. Ransomware: A research and a personal case study of dealing with this nasty malware. Issues in Informing Science and Information Technology Education, 14, 87-99, 2017
4. T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review" , International Journal of Information Management Data Insights, 2021