Introduction to Ransomware

Deepika G. Vaghela
Assistant Professor - Computer Science & Engineering Department ,
ITM Universe , Vadodara.

Abstract

Ransomware is a typre of malicious software which is designed to block the computer system until sum of money is paid by victim . Ransomware aimed at individuals , it is only matter of time. During given time victim has to pay money which is mentioned by Ransomware software. This paper indicates the introduction of ransomware , How it works and what are the Prons and cons of ransomware.

Keywords — *Ransomware, encryption, decryption, Private key, Cryptography, Crimeware*

I. INTRODUCTION – Ransomware

Ransomware[1] is a type of malicious software designed to block access to a computer system until a sum of money is paid.

Although ransomware is usually aimed at individuals, it's only a matter of time before business is targeted as well.

The process is similar to how a virus or malware gets into a computer: Email messages claiming to contain important attachments, drive by download — from websites or even ads that seem to offer valuable/illegal stuff for free, fake antivirus/anti-malware downloads, fake updates for popular programs, social engineering methods, friends on social networks enticing you to click on certain links, through botnets, etc.

A. There are two types of ransomware

1) Encrypting ransomware , which incorporates advanced encryption algorithms. It's designed to block system files and demand payment to provide to provide the victim with the key that can decrypt the blocked content. Examples include CryptoLocker[2], Locky, CrytpoWall[3] and more.

2) Locker ransomware, which locks the victim out of the operating system, making it impossible to access the desktop and any apps or files. The files are not encrypted in this case, but the attackers still ask for a ransom to unlock the infected computer. Example include the police-themed ransomware or Winlocker.

II. Key Characteristic

A. Ransomware has some key characteristics apart from malware.

1. **Unbreakable encryption**[5]**,** you can't decrypt the files on your own.
2. **It encrypts all kind of files** , like documents , audio, video, pictures etc.
3. It can shuffle your file names, so you can't predict the affected data. This is one of the social engineering tricks used to confuse victims into paying the ransom.
4. It will display **an image or a message** that lets you know your data has been encrypted and that you have to pay a specific sum of money to get it back
5. It **requests payment in Bitcoins**, because this crypto-currency cannot be tracked by cyber security researchers or law enforcements agencies
6. **The ransom payment has a time-limit**, deadline of time limit typically means that the ransom will increase, but the data will be destroyed and lost forever.
7. It **often recruits the infected PCs into botnets**, so cyber criminals can expand their infrastructure and increase future attacks
8. It **can spread to other PCs connected in a local network**, creating further damage
9. It **has data excretion capabilities**, which means that ransomware can extract data from the affected computer (usernames, passwords, email addresses, etc.) and send it to a server controlled by cyber criminals

10. It **sometimes includes geographical targeting**, meaning the ransom note is translated into the victim's language, to increase the chances for the ransom to be paid.

III. Methodology

Phase 1:
Exploitations and Infection : When attack has successfully done , the malicious ransomware file needs to execute on a computer. Through some techniques like phishing attack and exploit kit exploitation has been done. In the case of the CryptoLocker malware, the Angler Exploit Kit[ ] is a preferred method to gain execution.
Phase 2:
Delivery and Execution : During this phase , the actual ransomware executables are delivered to the victim's system. Through which it can attack to the victim's system.

Phase 3:
Backup Spoliation : The ransomware targets the backup files and folders on the victim's system and removes them to prevent restoring from backup. The unique feature of ransomware is it deletes the backup files , while the kind of malware don't bother to delete the backup file. Other kind of crimeware[6] are not so feasible than ransomware that it can easily attack successfully. The ransomware infects the user's machine using any of the typical methods , such as sending victims convincing email and encouraging them to run the attachment. It infects on the backup files so victim can't get the idea about the malware.

Phase 4:
File Encryption: Once the phase 3 has completed, the malware will perform a secure key exchange with the command and control (C2)[ ] server. Those encryption keys are used on the local system.
Phase 5:
User Notification and Cleanup: After removing the Backup files and encryption dirty work done, the demand instructions for extortion and payment are displayed. The victim is given time limit to pay, After that time the ransomware increases.

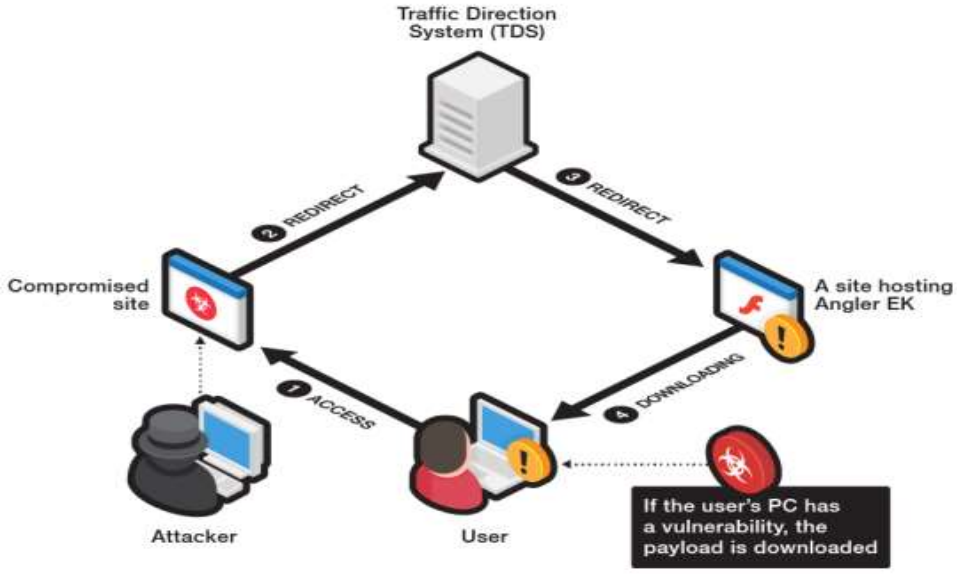

Fig : Architecture of Ransomware[7]

Fig shows the Architecture of Ransomware which include all the above phases.

IV. How to Protect Your Computer from Ransomware

Several antivirus companies have come up with ways to remove the virus, but that doesn't decrypt the files. Unfortunately, you don't have many options unless you have backups of your data, but you can protect your computer with some common sense.

First, don't ever download from a site that tells you software on your computer is outdated. Websites aren't able to detect outdated software unless you give the website permission to read your hard drive. If you think your software needs an update, go to the official product developer's site and download it directly from there.

Next, always keep the latest antivirus definitions installed on your computer to defend against all types of malware. The one main issue with ransomware is that once you get infected, there is nothing you can do to reverse the damage. It's better to be proactive with antivirus updates than wait until you've already become a victim.

Finally, always keep backups of your files. Hackers know that most people don't keep backups. Even some businesses fail to keep regular backups, and it's a big mistake that usually leads to some kind of data loss. Always keep regular backups in a safe place. Note that you can't keep them on your local hard drive, because these backups might also get encrypted. One safe place is keeping them in the cloud such as Google Drive or Microsoft's SkyDrive.

Viruses are becoming stronger and more resilient to common defenses. The best defense is to use common sense and avoid downloading executable files unless you absolutely need to. Keep your antivirus software updated and never installs software if you're unsure of its security.

V.Ransomware affects other device that computer.

There are ransomware that affect NAS (Network Attached Storage)[10] systems, Computer Servers, etc. For example, the database stored on the server of a financial website can be encrypted.

Ransomware also affect mobile/smart phones. These are generally disguised as free apps that provide premium services, adult content, or illegal services and entice users to install and try it on their phones. It locks the phone and demands a ransom to unlock it.

In the future, ransomware maybe written to affect any device connected to the Internet, especially the smart connected devices that have limited interface options, like in the IoT (Internet of Things) ecosystem.

Conclusion

This paper indicates the brief details of Ransomware . How Ransomware affects on computer system without money paid victim can't use the computer system . Ransomware is a malicious software that attacks on victim's confidential data.For this one can backup their data before this attack. The future enhancement of this paper is how to protect or provide some security tool/software from ransomware.

References

[1] Andronio, Nicoló, Stefano Zanero, and Federico Maggi. "HelDroid: dissecting and detecting mobile ransomware." *International Workshop on Recent Advances in Intrusion Detection*. Springer International Publishing, 2015.

[2] Scaife, Nolen, et al. "Cryptolock (and drop it): stopping ransomware attacks on user data." *Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on*. IEEE, 2016.

[3] Constantin, Lucian. "CryptoWall ransomware held over 600K computers hostage, encrypted 5 billion files." *PC-World. Tomado de www. pcworld. com/article/2600543/cryptowall-heldover-halfamillion-computers-hostageencrypted-5-billion-files. html* (2014).

[4] Luo, Xin, and Qinyu Liao. "Ransomware: A new cyber hijacking threat to enterprises." *Handbook of research on information security and assurance*(2009): 1-6.

[5] Valach, Anthony P. "What to Do After a Ransomware Attack." *Risk Management* 63.5 (2016): 12.

[6] Jakobsson, Markus, and Zulfikar Ramzan. *Crimeware: understanding new attacks and defenses*. Addison-Wesley Professional, 2008.

[7]https://www.ransomware+diagram&oq=ransomware+diagram&gs_l=serp

[8] J. Walter. Meet tox: Ransomware for the rest of us. https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/, 2015.

[9] H. Weisbaum. CryptoLocker crooks launch ‘customer service’ site. http://www.

cnbc.com/id/101195861, 2013.

[10] Co, Carl, et al. "Mechanism of action network attachment to moving membranes: barbed end capture by N-WASP WH2 domains." *Cell* 128.5 (2007): 901-913.