IJCSC 0973-7391 Volume 7 • Number 1 Sept 2015 - March 2016 pp. 224-227 available online at www.csjournalss.com

Ransomware: A Threat to Cyber security

Deneesha Kansagra[1], Malaram Kumhar[2], Dhaval Jha[3]
[1 2 3]Institute of Technology, Nirma University, Ahmedabad, India
15mcei10@nimauni.ac.in, malaram.kumhar@nirmauni.ac.in, dhaval.jha@nirmauni.ac.in

Abstract: All computer system using anti-virus that is because of threat against virus or malwares. Cybersecurity normally protect systems against all these viruses but as technology increasing the threat against technology also increasing. One of the new threat is Ransomware. It is a kind of virus which directly steal user's money or it forces victim to pay some Ransom in order to get the access of victim's original files. These all can be done through Cryptography. Fact is that cryptography is used to secure information but here Ransomware uses cryptography against it. Ransomware extort money from the victim by encrypting their valuable information. And to get back access of important files victim needs to pay some ransom. This paper tries to investigate the working of a Crypto Locker (Ransomware) and formal analysis of malware. This analysis leads to some conclusion concerning this phenomenon also few strength and weaknesses of money extort malware. This paper presents novel Ransomware, its encryption schema and some prevention, detection approaches.
KeyWords: Malware, Cyber Security, Ransomware, Cryptolocker, RSA algorithm.

1. Introduction

In early day's computer system users only aware of virus, spyware, Trojan Horses, warm etc. but in 1989 new variant of Trojan called "PC Cyborg" (AIDS Trojan)[4] which worn users by displaying message that user's license had expired and user requires to pay some money to unlock it. Cryptography used for that is symmetric cryptography which is easy to crack. But in Russia around 2005 new threat get reported to cybersecurity that is Ransomware variant (TROJ_CRYZIP.A) [4] which zipped files with password protection on users system and leave one notepad created Ransom note that inform users to get back password protected zipped files users need topay some written Ransom. Cryptography used for that is asymmetric that is stronger than symmetric.

In 2012 researcher noticed new Ransomware variants called Crypto Locker which is based on encryption uses asymmetric cryptography like RSA to encrypt files and also locking the systems [1]. But analysis shows latest Ransomware variants use AES + RSA encryption. That shows to unlock those encrypted files user need some key value which is only known to attacker. Attacker demands money in exchange of key value that's why it is named as Crypto Locker Ransomware [4].

RSA uses asymmetric key cryptography which holds public and private two keys. Public key known to everyone and Private Key kept secret by user. In RAS one key is used for encryption and another key is used for decryption. Where AES is based on symmetric key cryptography so it uses same key for encryption and decryption [7].

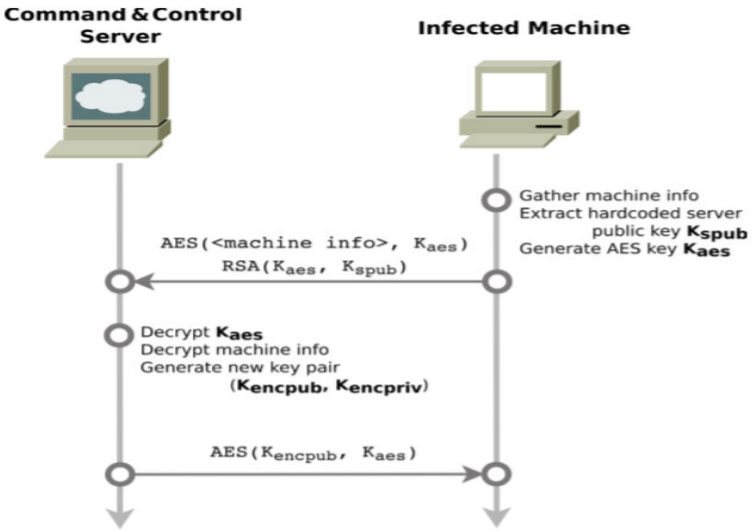

Figure 1: Crypto Locker and C&C protocol [7]

AES is used by Crypto Locker to encrypt files and file in which encryption key of AES is written is also encrypted by RAS public key. So to unlock files user need symmetric key which is protected by RSA so user first require private key of RSA and then which unlock the symmetric key stored file. This private key is not available [7].

Another face of Ransomware is used to lock the screen of infected system. It infects file like .dll , .exe, .xl etc.[4] these infected files are most critical files because removing those critical files (ex .dll) can crash a system.

2. How Ransomware get installed?

Ransomware gets entered into your system through some phishing attack or drive by download then it creates an exe file to run and flow of creation of an exe file is as follow:

- First it generate a key value which is unique from PC to PC. Parameters which required to create a key are computer name, processor information, volume serial, and operating system and hashed it suing MD5 algorithm. This hashed data used to uniquely identify the victim.[7]
- Secondly, identify if current process is running with admin privilege or not. If it is running with root privilege than malware continue its flow of execution

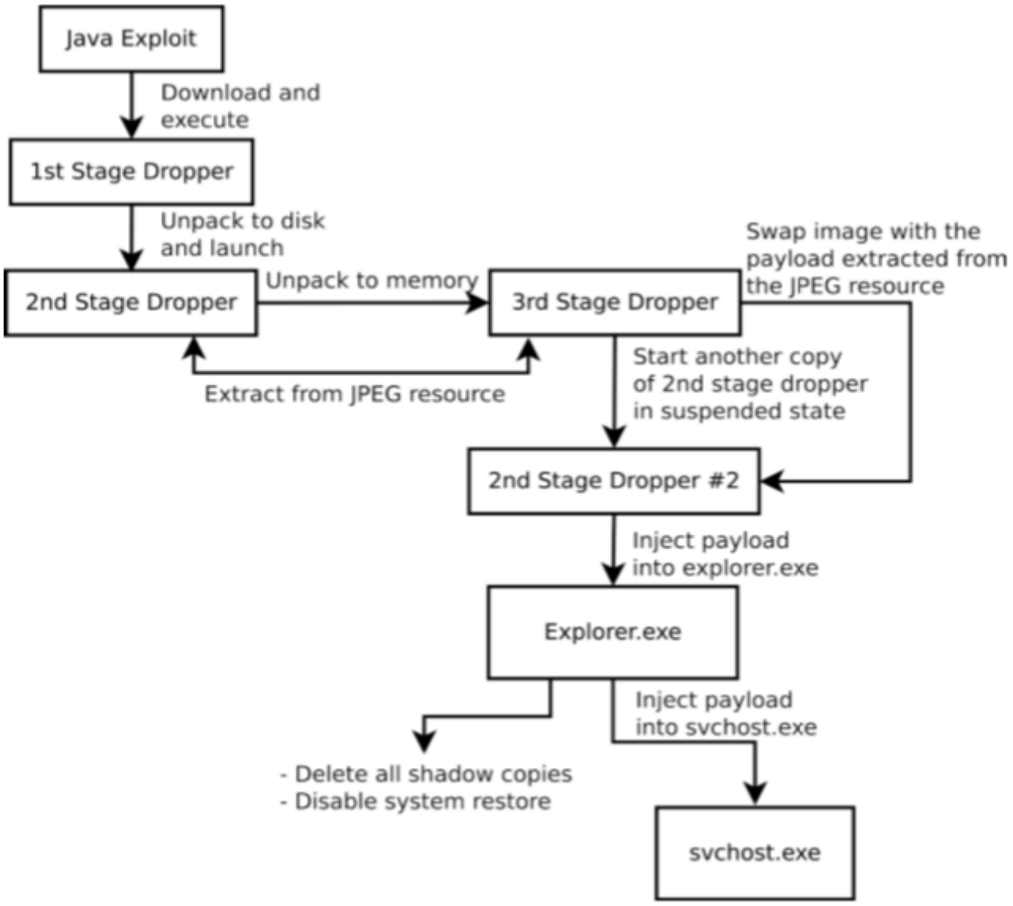

Figure 2: Cryptowall Infection workflow [7]

- Virus will copy itself into newly generated instance of explorer.exe
- Then it creates a new session and copy itself to newly allocated session of memory. And assign a new thread.
- Specific functions are called by this new thread.[7]
  - Deletion of shadow copy
  - Spawning new instance of svchost.exe and injecting code
  - Disabling common window services

- Different functions are loaded in new thread responsible for
  - File encryption
  - Uninstall/removal after malware has finished
  - Exec is generated by:
  - hex (RSA (Hex (MD5 (victim info))))[7]

Finally malware will attempt to copy itself to victim's startup folder

3. How Ransomware works?

Ransomware try to extort the money from the victim by encrypting files. Typically two function of Ransomware [6]

- Encrypt the documents or files
- Lock the computer to prevent normal usage.

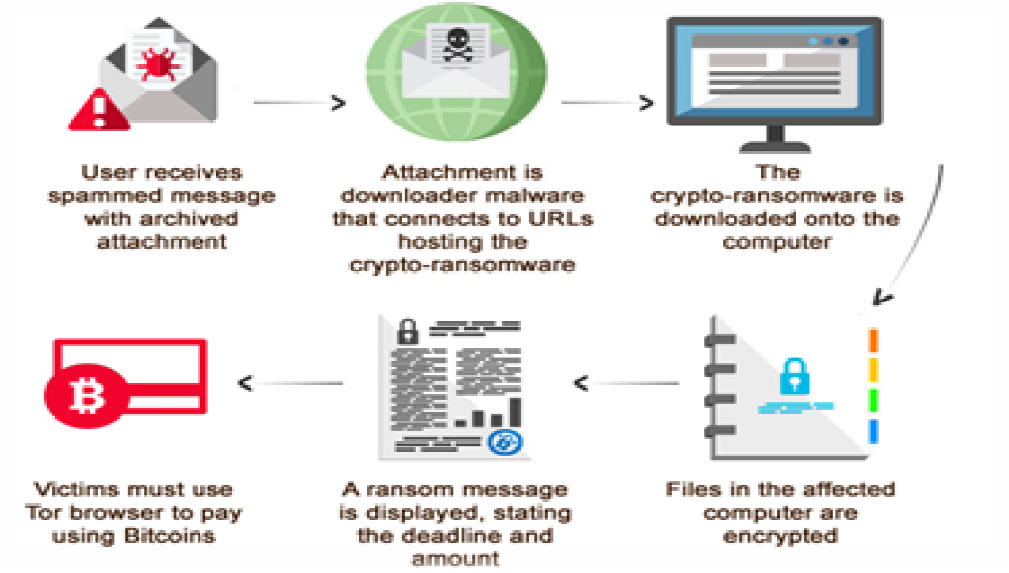

Figure 3: working of Ransomware [6]

When Crypto Locker installed on victims system it creates executable files in localAppData folde or in AppData folder.

Once malware gets entered in your system it looks for important files with extension .txt, .doc, .rft, .ppt, .chm, .cpp, .asm, .db, .zip, .jpg, .key, .mdb, .pgp .pdf etc and encrypt those files with RAS + AES algorithm so that owner of the file is unable to access them. [7] When you are trying to access those encrypted file pop-up is generated with demanding money to unlock your data. Ransom user need to pay through Bitcoin in most of the cases. Although by paying ransom it does not give any guarantee that you information or files are fully recovered.

Once attacker locates these files, he implements some methods. Firs , he moves all lcated files into one folder and compress it with password-protection zip parally removing original files. Second option, he can decrypt each and every files along with removing original ones.[5] Third one is that attacker moves all files into hidden folder but there is a risk of damage. After successful encryption it demads for some ransom to get password or key for the decryption.

4. Prevention

Ransomware uses asymmetric cryptography to lock files user require Private Key to unlock data and Private Key is only knows to cyber-criminal. As there is no solution for this Private Key users need to take some extra care to prevent their system being infected by Ransomware [1].

Any malware or ransomware successfully installed on any system if there is any patches or system is still running on older version although newer version is already published. So keep up to date system with all patches [3].

Secondly, some Anti-Ransomware tools are capable to report such a malicious malware. For that system need to use reputable anti-virus software and firewall as well after all malware which is going to infect is penetrate through firewall.

Malware try to enter in the system by phishing mail or spam mail. Avoid such mails because user one click can steal user's money [2]. It may be possible that malware get introduce by drive by download so download attachment from only trusted sources.

Make a formal habit of taking backup on regular interval bases [3]. Because when user try to boot system for removal of malware there may be possibility to loss all users' data. So backup is only option to store user's data safely and retrieve it whenever it needed.

5. Detecting Ransomware

Anti-Ransomware tool [10] is used to detect Ransomware. It uses proactive method in which Ransomware is detected in early stage before it is going to damage or encrypt files. Main advantage of this tool is that it is dependent on heuristics instead of signature. So. It can be able to detect all types of zero day attacks and most dangerous Ransomware variants. [9]

We can also sniff its tracks. We can predict behavior of malware. By checking how many files are changed during some interval of time and if it exceed the threshold then we assume that attack has been taken placed. Another method by comparing checksum we can get to know if our file is infected or not.

Malwarebytes Anti-Ransomware used advanced proactive technology to detect Ransomware. It runs in the background and identify the actions of Ransomware. It keeps on monitoring all the time and once it found any malicious activity than block that process before it has locked victim's files. Every Ransomware is blocked by this tool. [10]

6. Conclusion

Encryption algorithm which is used by Ransomware becoming more sophisticated in cyber environment. Unlocking or decryption of files is biggest challenge for Information system professionals and researchers.As there is no secure way to decrypt files without key it is better choice to take some prevention steps before it leads to attack. Proactively detection of Ransomware which is best solution to prevent system. Some awareness is also required to secure user's important documents being locked.

References

[1] "Remove CryptoLocker virus (Files Encrypted Ransomware).html", malwaretips.com

[2]X. Luo and Q. Liao, "Ransomware: A new cyber hijacking threat to enterprises," *Handbook of research on information security and assurance*, pp. 1–6, 2009.

[3]X. Luo and Q. Liao, "Awareness Education as the key to Ransomware Prevention," *Information Systems Security*, vol. 16, no. 4, pp. 195–202, 2007.

[4]A. Gazet, "Comparative analysis of various ransomware virii," *Journal in computer virology*, vol. 6, no. 1, pp. 77–90, 2010.

[5]G. M. Gavin O'Gorman, "ransomware-a-growing-menace," Symantec security Response.2012

[6] "Ransomware - Definition - Trend Micro USA." Available: http://www.trendmicro.com/vinfo/us/security/definition/Ransomware.

[7] Vadim Kotov and Mantej Singh Rajpal, "Understanding Crypto-Ransomware," Report, Bromiun,2014.

[8] "Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat", CyberThreatAlliance, 2015

[9]P. Belcher, "AES-128 Encryption Virus Removal," *Virus Removal*, 16-Feb-2016

[10] "Removing ransomware using the AntiRansomware Tool _ Trend Micro".com