Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 1; January-March, 2016, pp. 30-32

http://www.krishisanskriti.org/Publication.html

Elliptic Curve Deffie Hellman(ECDH) Encryption and Ransomware: A Survey

Rhyme Upadhyaya

M.Tech Research Student BIT Mesra Ranchi, India
E-mail: rhyme.u7@gmail.com

Abstract—*The emergence of cyber hackjacking threat in the new form in cyberspace is known as ransomware or cryptovirus. Imposing serious threats, ransomware victimizes Internet users by hijacking user files, encrypting them, and then demanding payment in exchange for the decryption key. Behavior-based detection and signature-based detection are popular approaches to malware analysis. This research aims in a detailed anatomy of ransomware, algorithm implied on the working of the malware, typical traits of the locker malware and discusses in details the encryption algorithms deployed for its workthrough. Actions are executed in two phases.First phase, the program modifies data to infect the compromised computer. Second phase, the locker bot waits for specific triggering events, to become active. It blocks the task manager, command prompt and other cardinal executables, a thread checks for their existence every few milliseconds, killing them if present. It is an intrusion based on Social Engineering attacks.*

1. INTRODUCTION

CTB Locker is financially motivated ransomware that encrypts user files and demands payment in Bitcoin or Moneypak payment cards. It is propagated through spam emails purporting to come from shipping companies or regarding business processes, can be dropped by other malware, disseminated through thumb drives, or transmitted through Yahoo! Messenger. CryptoLocker exploits features of public key (key distribution) and private key (efficient encryption of large amounts of data) cryptography as part of its ransom scheme. When CryptoLocker infects a computer, it attempts to connect with one of several pre-configured malicious websites (generically known as a Command and Control (C&C) server). The C & C server generates an RSA public/private key pair, and passes the public key to the CryptoLocker malware on the infected computer.

2. RELATED WORKS

Behavior-based malware detection approach has a greater potential in identifying previously unknown instances of malicious software is stated by [1] Holography: a behavior-based profiler for malware analysis by Shih-Yao Dai, Fyodor, Ming-Wei Wu, Huang and Yen Kuo.The accuracy of this approach relies on techniques to profile and recognize accurate behavior models. They have proposed an automated analysis platform to track and log all actions of malicious software running on an infected computer. It can be deduced that actions of legitimate software may be mistakenly considered as a malicious intention. Therefore, an insufficient supply of abnormal behavior models can lead to high false positive and/or false negative rates of detection. It is important to design an automatic, system-wide, and fine-grained tool that can provide security researchers with the ability to efficiently extract abnormal behavior models from malicious programs. Based on reverse-engineering while not focused on analysis methodology, a technical review is done at [2] Comparative analysis of various ransomware virii by Alexandre Gazet, at different levels, quality of code, malwares' functionalities and analysis of cryptographic primitives.Almost 20 years ago, in 1989, a malware named AIDS Trojan was rampant and made some victims.The infection had been propagated via post mail:a disk called "AIDS Information Introductory Diskette" being sent is also discussed. Ajjan, A in [3] Next-Generation Fake Antivirus states that ransomware threat might be in the form of a fake antivirus message pop up.Whereas Luo, Xin, and Qinyu Liao study in their paper [4] Awareness Education as the key to Ransomware prevention , theoretical comparison of ransomware with other malware. Ransomwares are induced through Internet like other computer virus such as Trojan horse, worms, and spyware**.** Unlike viruses, Trojan horse virus is a type of virus that doesn't replicate itself. Trojans get into a computer by hiding inside other software, such as an email attachment or download. They are destructive programs that masquerade as benign applications.Again, Kirda, Engin in[5] Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, discuss different classes of ransomware attacks with multiple levels of sophistication share very similar characteristics from a file system perspective, due to the nature of these attacks.

3. PUBLIC AND PRIVATE KEY CRYPTOGRAPHY

The art of writing secret codes for incognito data communication. There are two main types of cryptography in use today: private key or symmetric cryptography and public key or asymmetric cryptography. The primary difference

between the two methods is how many keys are used, as private key cryptography uses one key to both encrypt and decrypt the data, and public key cryptography uses two keys, with one key encrypting the data and a different, but mathematically-related key decrypting the data. Prior to the development of sophisticated, computer-generated algorithms, the most common type of cryptography was private key cryptography. Substitution algorithms are an early example of private key cryptography, because the same key that was used to encrypt the plaintext must be used in reverse to decrypt the encrypted text. In the current state of cryptography, private key algorithms are incorporated in complex computer programs instead of simple substitution schemes, and keys are expressed in bit lengths instead of, for example, number of character shifts. Technology has also led to the development of public key cryptography. There are several private key (symmetric) algorithms in use. One of the most common, is the Advanced Encryption Algorithm (AES) also the U.S. federal government standard. It is also known as the Rijndael Algorithm. Other private key algorithms include Blowfish, Data Encryption Standard (DES), and Triple DES. DES, the previous U.S. federal government standard, is no longer authorized for use by U.S. federal government agencies, as it was proved breakable through brute force techniques in 1999. Well known public key (asymmetric) algorithms include Diffie-Hellman (D-H), the Digital Signature Algorithm (DSA), and the Rivest, Shamir, Adleman (RSA) algorithm. Whitfield Diffie and Martin Hellman developed D-H, one of the earliest published public key algorithms, in 1976. The classic D-H algorithm requires key sizes from 1024 to 4096 bits, while Elliptic Curve D-H (ECDH) only requires key sizes from 160 to 512 bits.

4. PUBLIC VS PRIVATE KEY ALGORITHMS

The difference between private key and public key algorithms is the speed of encryption vs. ease of key distribution. Private key algorithms are very efficient at encrypting large amounts of bulk data. The weakness of private key algorithms is the logistics of key distribution. For example, if Bob decides to exchange encrypted data with Alice using a private key algorithm, then they must both be in possession of the key that is used to encrypt the data, since it will be required to decrypt the data. This means that Bob and Alice must set up a secure method for transmitting the key; emailing the key will not suffice. If the emailed key is intercepted, that interceptor (or anyone who possess the private key) will be able to decrypt any data the key was used to encrypt. This issue is compounded when the key must be shared among multiple people, as everyone will have access to the same key, increasing the opportunity for key theft. Public key algorithms are not as efficient at encrypting large amounts of bulk data, however, they do solve the key distribution issue. In public key cryptography, data encrypted by one key can only be decrypted by the mathematically related other key. Therefore, if Bob and Alice want to exchange encrypted data, and they do not have a secure method of getting a key to each other, they can opt to use a public key algorithm. In this example, Bob and Alice would each generate a "public/private key pair" with the algorithm they choose.

5. THE CTB LOCKER

CTB Locker is financially motivated ransomware that encrypts user files and demands payment in Bitcoin or Moneypak payment cards. It is propagated through spam emails purporting to come from shipping companies or regarding business processes, can be dropped by other malware, disseminated through thumb drives, or transmitted through Yahoo! Messenger.

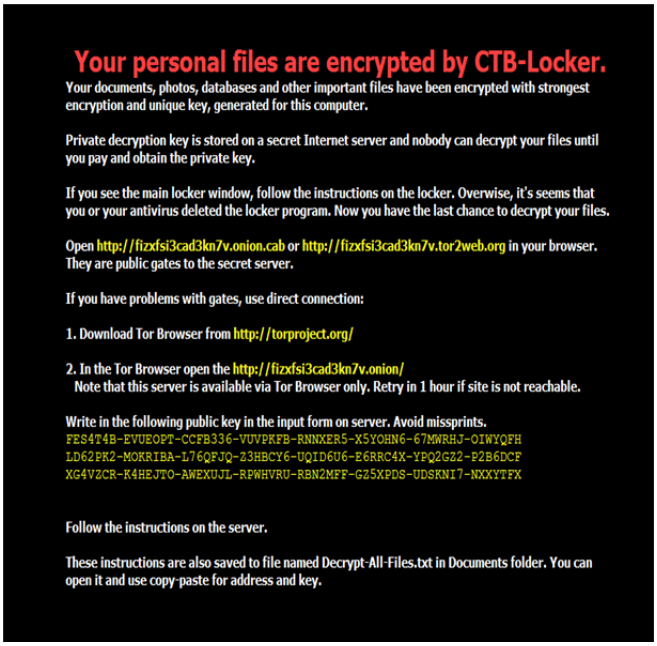

Fig. 1: A Ransomware Threat Message

CryptoLocker exploits features of public key (key distribution) and private key (efficient encryption of large amounts of data) cryptography as part of its ransom scheme. When CryptoLocker infects a computer, it attempts to connect with one of several pre-configured malicious websites (generically known as a Command and Control (C&C) server). The C & C server generates an RSA public/private key pair, and passes the public key to the CryptoLocker malware on the infected computer.

6. THE CTB LOCKER WORKING ALGORITHM

The CTB Locker uses Elliptic curve deffie hellman (ECDH) algorithm. Executes in four steps. Firstly, pair of private and public keys are generated. Second, shared secret key generated from your private key and other party's public key. Third, if both parties have exchanged public keys(not private key) and each has own private key, both will get same value. Fourth,

resulting shared secret key can be used as a key for any symmetric encryption algorithm.

7. THE CTB LOCKER ENCRYPTION

File compression using Zlib.Also file further encrypted using AES(Advanced Encryption Standard) with the hash SHA256(session shared) used as key.After encryption, the session public key is saved in the file while session private is not saved. The key generation process is defined in four steps. First, malware generates master-public+master-private key pairs. Second, master-private sent to server not saved in client. Third, for each file, new key pair session-public+session-private. Fouth, shared secret key calculated, session shared is ECDH(master-public, session-private).

8. CONCLUSION

In this manner, CryptoLocker uses the key distribution strength of public key cryptography to deliver a public key to the infected computer, and the efficiency of private key cryptography to encrypt the files. The public key is not used to actually encrypt the files; CryptoLocker uses the more efficient private key algorithm for that purpose. The public key, however, is used to encrypt the private keys that were responsible for the actual encryption of the files. Efficiency is not a factor for encrypting those keys, since the public key is only encrypting a short string (the private keys).After all files are encrypted, each extension's private key is further encrypted using public key algorithm and CTB Locker's C & C public key. Encrypted keys are stored in local key store. Ways to prevent the attack of the locker bot is summarized from this study as

- Educating users to verify the legitimacy of an email, since the emails used in ransomware scams originate from spoofed email accounts,
- Block traffic to known ransomware C&C server IP addresses at your network perimeter devices.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users to be cautious when clicking on links in emails coming from trusted sources.
- Ensure anti-virus software is installed and definitions are up to date.
- If infected with ransomware, remediate the infection via antivirus. Following the remediation, restore any encrypted files from backup or system restore points and volume shadow copies.

REFERENCES

[1] Dai, Fyodor, Ming-Wei Wu, Yennun Huang and Yen Kuo "Holography: a behavior-based profiler for malware analysis" *Softw. Pract. Exper.2012; 42:1107-1136, (13Oct, 2011) in Wiley Online Library* Documents

[2] Gazet, Alexandre. "Comparative analysis of various ransomware virii." *Journal in computer virology* 6.1 (2010): 77-90.

[3] AJJAN, A.Ransomware: Next-Generation Fake Antivirus.http://www.sophos.com/en-us/medialibrary/PDFs/technicalpapers/SophosRansomwareFakeAntivirus.pdf, 2013

[4] Luo, Xin, and Qinyu Liao. "Awareness Education as the key to Ransomware Prevention." *Information Systems Security* 16.4 (2007): 195-202.

[5] Kirda, Engin. "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks." *Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings*. Vol. 9148. *Springer, 2015.*