Cryptovirology: Malicious Cryptography Ransomware Based Approach

[1]Payal Jain, [2]Kanchan Vaishnav

[1]Department of Computer Science and Engineering,
MGM's Jawaharlal Nehru Engineering College,
Aurangabad, Maharashtra, India

[2]Department of Computer Science and Engineering,
MGM's Jawaharlal Nehru Engineering College
Aurangabad, Maharashtra, India

Abstract - Cryptography is a boon to information processing and communications as it helps to store information and private communication securely so cryptography can be used defensively. Cryptovirology is one of the applications of cryptography which shows that how cryptography can be used offensively. Offensive means it attacks on system due to which information leakage, loss of confidentiality can occur. In these powerful attacks attacker encrypts the victim's data, asks for ransom and release data after hostage. This paper will introduce you with cryptovirological attacks and its types in detail. This paper will also suggest some countermeasures to prevent your system from such attacks.

Keywords - Malicious, Cryptovirology, Cryptography, Public-key cryptography, Ransomware, GPcode, Security, attack.

1. Introduction:

Cryptography is basically used for security purpose. Cryptography deals with encryption that means conversion of information from readable form to apparent nonsense. The essential aspect of cryptography is public-key cryptography. Cryptography loses its destination without public key and private key because cryptography often uses these keys for information and communication security. Cryptovirology is an application of cryptography which shows how the cryptography can be used in offensive manner. These attacks are also known as Ransomware attacks. The first cryptovirological attack was "Cryptoviral extortion", detected by Adam Young and Moti Young in 1996. In this attack, attacker steals the victim's private key then using attacker's public key it encrypts the victim's files and asks him for some amount as ransom to return these files. This field uses the cryptographic techniques along with computer virus and Trojan horse technology.[1] Encryption in viruses is a part of polymorphism which can be achieved by splitting the virus into three different section-Cryptographic key, Decryptor code and functional part of virus. When the virus creates a new copy of itself, it selects a new cryptographic key, encrypts the main functional part of itself with that new key and generates a new implementation of decryptor load as a result. When the virus executes the decryptor code runs and uses the key to decrypt the main functional part of the virus which then takes control[1]. To prevent over system or computer networks from such attacks we should try to analyze what attackers might do once they break into system.

2 Backgrounds:

Cryptography:

There are mainly two aspects in cryptography-
Symmetric key cryptography and Asymmetric key cryptography.

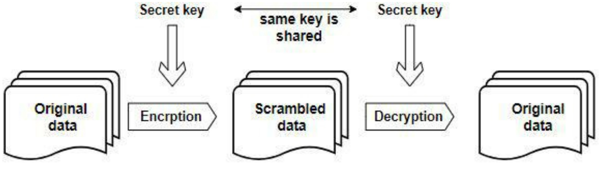

Fig 1: Symmetric key cryptography

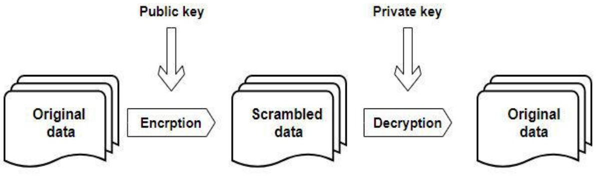

Fig 2: Asymmetric key cryptography

In symmetric key cryptography both sender and receiver shares the same key of encryption and decryption, whereas in asymmetric key cryptography, encryption key is public and decryption key is private.

Kleptography:

Kleptography is subfield of cryptovirology. It deals with stealing information securely. This attack uses asymmetric key cryptography technique.

Cryptanalysis:

Cryptanalysis deals with study of hidden information of the system. It is used to branch cryptographic security and gain access to the contents of encrypted message even if the cryptographic key is unknown.

Cryptovirology:

Cryptovirology is the study of the applications of cryptography for implementation of harmful software. It is about, how modern cryptographic paradigms and tools can be used to strengthen, improve, and develop new malicious software attacks. Cryptovirology attacks have been categorized to: give enhanced privacy to the malware and be more robust against reverse-engineering, secondly give the attacker enhanced anonymity while communicating with deployed malware [1].

3. Cryptovirology attacking methodology:

3.1 Cryptoviral Extortion:

Cryptoviral extortion is file encrypting ransomware. This is the three round protocol or three step process as follows-

Key-pair generation: The attacker generates a key pair and the corresponding public key is placed in malware software. Attacker then sends the malware software to the victim[2].

Encryption of victim’s files: The malware generates the symmetric key and encrypts the victim’s data or file with the help of this symmetric key. It gives a small asymmetric cipher text and also a cipher text of victim’s data. A message is get displayed to the user which is about cipher text and ransom.

Decryption of victim’s file: Victim sends the amount with asymmetric cipher text to an attacker. After receiving the payment attacker decipher the asymmetric cipher text using his private key. Now attacker sends the plain text that is the original data to the victim.

3.2 The secret sharing virus:

This section shows how to implement a virus that is a very close approximation to the highly servile virus. Whereas in the above attack the virus author managed the keys and owned the private key and the virus itself will manage its private key. Since a virus holding a public key and managing its private key can be get analyzed by antivirus analyst and could lose its power [3]. It shows that how Public Key Cryptography can be used in a virus to encrypt information so that the user will not able to get it back. To decrypt held data it is necessary to store the private key somewhere so that encrypted data can be decrypted.

3.3 Deniable Password Snatching [3]:

In this attacks the attacker first install the crypto Trojan in target computer. Here, attacker is at the high risk of getting caught especially when he has installed the software manually. Thus attack is generally carried out by using custom cryptovirus which can be distributed using passive virus distribution channel. Purpose of this method is to allow the attacker to indirectly run code of his own Trojan without being blamed for installing it.

4. How do cryptovirological attacks happen?

4.1 GPCode:Gpcode is one of the typical cryptovirus which can be spread through email. This email has an MS word.doc file. It contains a malicious program known as Trojan-Dropper. On opening the .doc file; a malicious macro installs another Trojan –Trojan Downloader.Win32.Small.crb on the victim machine.

This Trojan then downloads GPCode from[skip].msk.ru/services.txt and installs it to the victim machine. GPCode scans all accessible directories and encrypts files with certain extensions such as .txt, .xls, .rar, .doc, .html, .pdf etc. [3]

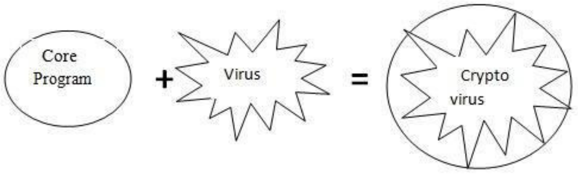

Fig 3: Cryptovirus attaching to the actual code

4.2 How GPCode spreads via Email:

The victim receives an email containing a

malicious link. If the victim clicks on the link or tries to open the attachment, a downloader will be placed on the victim's PC via infected website. Then that downloader installs the malware software on the PC. The malware then encrypts the entire hard disk content, personal files, and sensitive information. Everything, including data stored in cloud accounts synced on the PC. It can also encrypt data on other computers connected to the local network. [4]Then a window gets displayed which contains the information about the encryption of the content along with the ransom or payment details to get the data back.

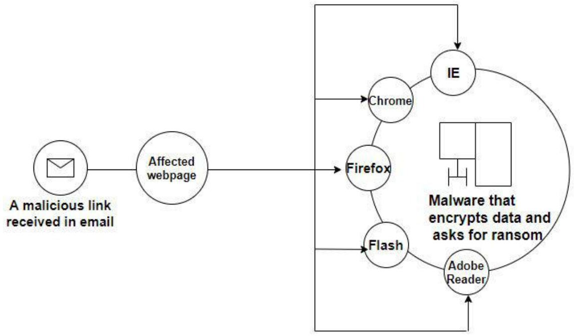
A malicious link received in email
Affected webpage
IE
Chrome
Firefox
Flash
Adobe Reader
Malware that encrypts data and asks for ransom

Fig 4: Key stages of ransomware attacks

5. Why ransomware often goes undetected by anti-virus:

Ransomware uses various tricks so that it remains hidden and also:

- Not get recognized by antivirus
- Not get detected by cyber security researchers
- Not get noticed by law enforcement agencies and their own malware author.

It uses following mechanism:

It uses anti-sandboxing mechanism so anti-virus will not pick it up. Security products often use VM's and sandboxes to execute potentially malicious code before it is approved to enter the organizational network. To avoid bypass security systems malware authors often design their code to detect isolated environments. Once such an environment is detected it may prevent the malicious code from running, or it may alter the malware's behavior to avoid exposing malicious activity while running in a VM. Virtual machine software is designed to mimic the hardware functionality of real hardware. But when doing so, some artifacts indicate that it is indeed a virtual machine and not a physical one. Malware authors take advantage of this design flaw and code the malware to detect virtual machine. This behavior is referred to as Anti-Sandbox or Anti-VM.[5]

6. The most notorious families of ransomware:

1. WannaCry:

On Friday, May 12, 2017, around 11 AM ET/3PM GMT, a ransomware attack of "unprecedented level" (Europol) started spreading WannaCry around the world. It used vulnerability in Windows that allowed it to infect victims PC's without them taking any action. Until May 24, 2017, the infection has affected over 200,000 victims in 150 countries and it keeps spreading.

2. CryptoLocker:

The original CryptoLocker was first discovered in May 2014. It was first targeted at windows based system. It generally spreads via email attachments. After downloaded it gets activated and encrypts certain file types using RSA public key, then demands for ransom. The cryptolocker word seems like Xerox and Kleenex and it has become almost synonymous with Ransomware. [6]

3. CryptoWall [6]:

After the downfall of CryptoLocker, the CryptoWall had gained its importance. Earlier it had appeared first in 2014 and its variants with a variety of names, including Cryptorbit, CryptoDefense, CryptoWall 2.0 and CryptoWall 3.0, among others. Like CryptoLocker, CryptoWall is distributed via spam or exploit kits.

4. Locky:

It was first spotted in 2016. This also get spreads via email having attachments of word documents containing malicious macros. When user opens that attachments it seems to be full of garbage and asks for enable the macros. After enabling the macros it downloads the Trojan and encrypts the file having that particular extension.

5. TeslaCrypt: This Ransomware was first detected in 2015. This malware generally tries to infect the gaming files. This malware usually encrypts the file which is smaller than 268 MB. Like other type of Ransomware, it uses an AES algorithm to encrypt files. Once vulnerability is exploited, TeslaCrypt installs itself in the Microsoft temp folder. [6]

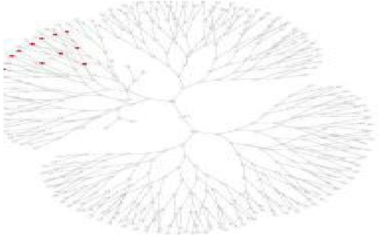

Fig 5: TeslaCrypt (replace original content with encrypted content) [7]

7. Statistics:

Statistics shows ransomware creators always target each kind of users as home users, business, public institutions and so on. They target general home users because they do not keep backups of their data. Also they are not much aware about the cyber security and still rely on antivirus to protect them from all threats, which is frequently ineffective in spotting and stopping ransomware. Ransomware attackers also targets the business data because they know that a successful infection can cause major business disruptions, which will increase their chances of getting paid because ransomware can affect not only computers but also servers and cloud-based file-sharing systems, going deep into a business's core. They targets public institutions because public institutions often use outdated software and equipment, which means that, the computer systems are packed with security holes just begging to be exploited.

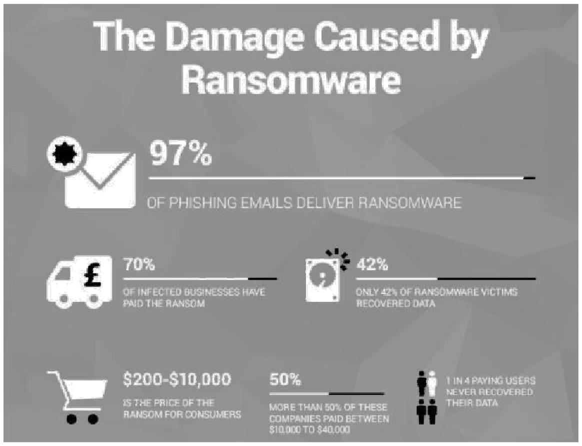

Fig 6: Effect of ransomware all over the world[4]

8. Countermeasures:

Here are some precautions to take care your system so that you cannot be a victim of ransomware attacks:

- Don't store important data only on pc.
- Maintain at least two backups of your data on external hard drive and on google drive.
- Use up to date operating systems and security tools.
- For daily use don't use administrator account on your pc, use guest account with minimum privileges
- Remove the following plugins from your browsers: Adobe Flash, Adobe Reader, Java and Silverlight. If you absolutely have to use them, set the browser to ask you if you want to activate these plugins when needed.
- Never open spam emails or emails from unknown senders.
- Never download attachments from spam emails or suspicious emails.
- Never click links in spam emails or suspicious emails.
- Use a reliable, paid antivirus product that includes an automatic update module and a real-time scanner.
- Understand the importance of having a traffic-filtering solutionthat can provide proactive anti-ransomware protection.

9. Conclusion:

It is demonstrated that how Cryptography can be used to build the malicious software programs that can be used in extortion-based attacks on computer system. Public-key cryptography is necessary for the attacker to take advantage over the owner of infected system. Also presented a set of measures that can be taken to minimize the risks of attack posed by the cryptovirology. We can conclude that from all these attacks that auditing and logging tools may inadequate for the law enforcement purposes against the attacker. The first step towards security of your system is, mechanisms and schemes to detect viruses before infection.

Acknowledgment:

For this paper we acknowledge and express our profound sense of gratitude and thanks to everybody who have been a source of inspiration during the paper preparation. Also, we would like to thank our peers who have been a constant source of encouragement and inspiration in every walk of life.

References:

[1] Shivale Saurabh Anandrao,"Cryptovirology: Virus Approach",International Journal of Network Security & its Application(IJNSA), Vol. 3, No. 4, July 2011.

[2] www.tothenew.com

[3] S. Manoj Kumar, M. Ravi Kumar,"Cryptoviral Extortion: A Virus Based Approach", International Journal of Computer Trends and Technology (IJCTT), volume 4, Issue 5–May.

[4] www.heimdalsecurity.com

[5] www.cyberbit.com

[6] S. Mahmudha Fasheem, P. Kanimozhi, B. Akora Murthy, "Detection and Avoidance of Ransomware", 2017 IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939.

[7] Nolen Scaife, Henry carter, Patrick Traynor, Kevin R.B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", 2016 IEEE 36th International Conference on Distributed Computing Systems.

First Author Payal Jain is a student at MGM's Jawaharlal Nehru Engineering College, BAMU University, Aurangabad. She is currently pursuing BE (Bachelor of Engineering) in Computer Science and Engineering. She is interested in Database Management System(DBMS), network security and programming as well.

Second Author Kanchan Vaishnav had completed Diploma in 2005 then she completed her BE in Information Technology with distinction in 2008. She also did ME in Computer Science in 2016. She had one paper presented and one paper published in international conference in 2016. She also has a teaching experience of 8 years.