Cryptoviral Extortion: A virus based approach

S.Manoj Kumar#1, M.Ravi Kumar*2
#Dept.of IT (MCA)
G M R Institute of Technology, Rajam, Andhra Pradesh, India

**Dept. of IT (MCA)*
G M R Institute of Technology Rajam, Andhra Pradesh, India

***Abstract*— As we know that traditionally, "Cryptography" is used for information processing and communications, it helps people to store information securely and it is used very frequently for private communications. but Cryptovirology is the study of applications of cryptography to build the malicious software (malware). It is an investigation, how modern cryptographic tools and paradigms can be used to strengthen, develop and improve new malware attacks. This is a forward engineering discipline that can be used for attacking rather than defending. In this paper we present the clear process of "how the crypto virus can damage the victim's system, based on Extortion mechanism" with showing the live scenario that causes the loss of access to information, loss of control and loss of money also. Here we discuss and explain some of the latest events regarding to this cryproviral extortion like GPcode and Conflicker. This paper also suggests some of the countermeasures, mechanisms to defend and prevent such attacks. Even if the attacker's actions on the host machine are being monitored, it cannot be controlled the host system completely. By knowing that the exact scenario what exactly hacker follow to spoil our system or network using this cryptoviral Extortion method .we can anticipate or guesses the opponent's or attackers next move and can able to provide some of the safe guards initially.**

***Keywords*—cryptovirus, snatching, public-key cryptography, kleptography, cryptanalysis, Gpcode, Malware, Deniable Password Snatching (DPS), cryptoviral extortion.**

I. INTRODUCTION

Cryptography has been used for defensive purposes. In the public eye, the word cryptography is virtually synonymous with security. It is a means to an end, a way to send e-mail privately and purchase items securely on-line. Ciphers defend against a passive eavesdropper. Crypto virology extends beyond finding protocol failures and design vulnerabilities. . Public-key cryptography is very essential for the attacks that based on cryptovirology. Crypto virology attacks have been devised to: give malware enhanced privacy and be more Robust against reverse-engineering, give the attacker enhanced anonymity when Communicating with deployed malware to improve the ability to steal data, improve the ability to carry out extortion, Enable new types of denial-of-service; enable fault-tolerance in distributed crypto viral attacks, and so on. This field also encompasses covert attacks in which the attacker secretly steals private information such as private keys.

This field was actually introduced with the observation that the public-key cryptography can be used to break the symmetry between what an antivirus analyst knows regarding a virus and what the virus writer. The former can only see a public key whereas the latter can see a public key and corresponding private key as well. The first attack that was identified in this field is the "cryptoviral extortion". The field includes hidden attacks in which the attacker secretly steals private information like private keys. In the cryptoviral extortion attack a malware hybrid encrypts the plaintext from the victim's system using the public key of the attacker. The attacker demands some form of payment from the victim as ransom in return for the plaintext that is held hostage. In the public eye, the word cryptography is virtually synonymous with security. It is a means to an end, a way to send e-mail privately and purchase items securely on-line.

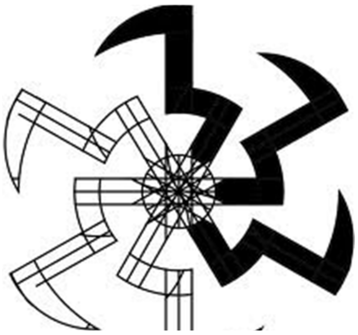

Fig 1 Skeletal of Crypto Virus

To reduce the risk of being get attacked or infected by a cryptovirus, some of the counter measures are described in this paper. Many of the attacks described in this paper can be avoided with existing antiviral mechanisms and a tool, since cryptoviruses propagate in the similarly as traditional viruses does.

II. BACKGROUND

A. Cryptography

"Cryptography" is used to information processing and communications, because it allows people to store information securely and conduct private communications over long distances. There are mainly two aspects in cryptography algorithms and the key used [5]. The important encryption techniques are symmetric, asymmetric, hash function algorithms. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key of decryption. In asymmetric key cryptography, the encryption key is the public and decryption key is the private key or secret key individually.

B. *Cryptovirology*

Cryptovirology is the study of the applications of cryptography for implementation of malicious software [5]. 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.

C. *Kleptography*

"Kleptography" is the study of stealing the information more securely. A kleptographic attack is an attack in which a malware designer deploys an asymmetric backdoor. In this attack, there is an explicit distinction between confidentiality of the messages and awareness of the attack is taking place. A secure kleptographic attack is truly undetectable as long as the cryptosystem is a black-box [2]. A kleptographic attack is an asymmetric backdoor attack that can only used by the designer that carries out the attack. If reverse engineering detects the key generation code then he or she will get known that a kleptographic attack is underway.

D. C*ryptanalysis*

Cryptography is the science of making the secret unintelligible and cryptanalysis is the science of retrieving the secret from that unintelligible data for the further use [2].

E. *Crypto virus*

In computer security, a crypto virus is defined as a computer virus that contains and uses a public key. Usually the public key belongs to the author of the virus, though there are other possibilities as well. For instance, a virus or worm may generate and use its own Key pair at run-time [5]. Crypto viruses may utilize secret sharing to hide information and may communicate by reading posts from public bulletin boards. Crypto Trojans and crypto worms are the same as crypto viruses, except they are Trojan horses and worms, respectively.

Fig 2 Cryptovirus

III. ATTACKING METHODOLOGY OF CRYPTO VIRUS

A. *Cryptoviral Extortion [4]*

Crypto viral extortion is mechanism for the encrypted viruses which uses public key cryptography, in a denial of resources (DoR) attack which can be introduced by the crypto virus. It is a three-round protocol which is carried out by an attacker against the victim. The attack is generally carried out via a cryptovirus that uses a hybrid cryptosystem to encrypt data while deleting or overwriting the original data in the infecting process. The virus notifies its victim that the attack has occurred and states that the asymmetric cipher-text will be needed to restore the original data. If the victim ready to pay the ransom and transmitting the asymmetric cipher-text to the virus author then the virus author decrypts the cipher-text using the private key that only the virus author has. The virus author sends that symmetric key and corresponding initialization vector to the victim. These are then used to restore the data that was held ransom. The attack will be is ineffective if the data can be recovered from backups of victim's computer.

B. The Secret Sharing Virus

This type of attack shows how to implement a virus that is a very close approximation to the highly servile virus. Where as 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 analysed by antivirus analyst and could lose its power [6].

C. *Deniable Password Snatching*

In the DPS attack, the attacker first seeks to install a crypto Trojan into a target computer. Already it seems possible that the attacker is at the high risk of getting caught and most probably if he has installs the crypto Trojan manually. The attack is generally carried out by using a custom crypto virus designed by the attacker. The purpose of this whole is to allow the attacker to indirectly run code of his own Trojan without being blamed for installing it.

Among these above attacking techniques we mainly concentrate on the first technique i.e.,"Cryptoviral Extortion" the complete methods and tasks included in these techniques can be illustrated in following sections:

1) Cryptoviral Extortion Attack Scenarios:

Scenario 1 is a cryptoviral extortion protocol performed by encryption of the victim's data as ransom.

Scenario 2 is same as to Scenario 1 except for that the virus writer also demands the victim's encrypted text for decryption along with the ransom.

Scenario 3 explains a secret sharing cryptovirus. The attack works on network with infected hosts. In this attack asymmetric private key is divided into parts and shared among all infected network host.

Scenario 4 states the involvement of a cryptovirus in a Deniable Password Snatching (DPS) attack.

IV. Latest Events

A. *Gpcode [6]*

This Trojan modifies data on the victim system so that the victim cannot use the data or it prevents the computer from functioning correctly. Once the data has been encrypted, the user will receive demand for ransom. The ransom demand states to send the money to the attacker, on the receipt of this, the virus writer will send a program to the victim to restore the original data or restore his computer's performance. Gpcode is one of the classic cryptovirus. Another classic cryptovirus is Virus.Win32.Gpcode.ag. It partially uses the version of 660-bit RSA (RSA private key) and encrypts files in many different extensions and overwrites or removes the original one. It tells victim to email a given mail ID if the he desires the decryptor of data to regain the original data. If attacker contacted by email, the victim will be asked to pay a certain amount of money as ransom in return for the decryptor of data.

- Virus uses cryptography for extortion.
- Files in the infected computer are encrypted.
- Asks for a fee to decrypt the files.
- Virus spreads through email.

1) How Gpcode spreads...:

Email message:

Dear customer!

We are very much glad to be as our customer. We are really thankful to you for choosing our service. We need your valuable feedback about out services this will really helpful to providing better services further. That's why please fill out the attached feedback form based on your views and opinions related to our services and send that form.

Sincerely,
Shanon fedo
Head of the Marketing Dept
Armway Home needs Agency Pvt.Ltd

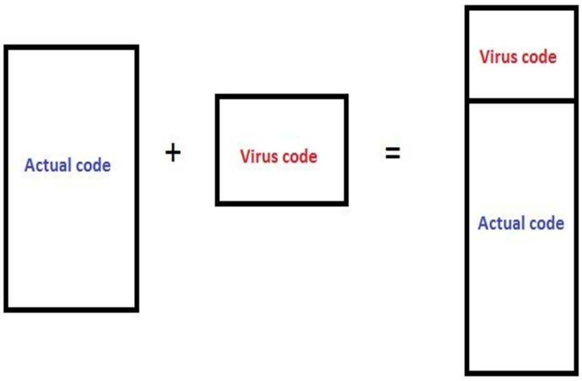

Fig 3 How the cryptovirus attaching to the actual code

- This email has an MS word .doc file called feedback.doc attached. File contains a malicious program called Trojan-Dropper.MSWord.Tored.a.
- On opening that feedback.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.

2) How GPcode attacks the victim's system:

Scans all accessible directories and encrypts files with certain extensions such as .txt, .xls, .rar, .doc, .html, .pdf etc. Also encrypts mail client databases. Gpcode and the other Trojans self destruct. Leave behind a file in each directory which has an encrypted file with README.txt.

3) *Cryptanalysis***:**

- Initially 56-bit RSA key was used.
- 660-bit key was cracked by Kaspersky Labs.
- The technique used was never published (trade secret!)
- Now, GPcode uses 1024-bit.

B. Conflicker

Conficker is also nicknamed as Downup, Downadup and Kido, is a computer worm targeted to the Microsoft Windows operating systems that was detected in November 2008 for first time. It makes use of the flaws in Windows software and make Dictionary attack on administrator passwords to co-opt system and link them into a virtual computer that can be commanded remotely by attacker. Conficker has since spread very rapidly into what is now known as the largest computer worm infection since the 2003 SQL Slammer, with more than seven million government, business and home computers in over two hundred countries now in its control. The worm has been usually difficult to detect because of its combined use of many advanced malware tools and techniques [7] [6].

1) TimeLine:

- Win32/Conficker.A -November 21, 2008.
- Win32/Conficker.B - December 29, 2008.
- Win32/Conficker.C - February 20, 2009.
- Win32/Conficker.D - March 4, 2009.
- Win32/Conficker.E - April 8, 2009.

2) Initial Infection:

Variants A, B, C and E exploit vulnerability in the Server Service on Windows computers. In the source computer, the worm runs an HTTP server on a port between 1024 and 10000. The target shell code connects back to this HTTP server to download a copy of the worm in DLL form, which it then attaches to a running service.

3) Payload Propagation

- Variant A generates a list of 250 domain names every day across five TLD's (top level domains).
- Variant B increases the number of TLD's to eight
- Variant C creates a named pipe, over which it can push URLs for downloadable payloads to other infected hosts on a local area network.
- Variant D generates a daily pool of 50000 domains across 110 TLDs, from which it randomly chooses 500 to attempt for that day.
- Variants D and E create an ad-hoc peer-to-peer network to push and pull payloads over the wider Internet.

4) Domain Name Generation:

Conficker implements its own random number generator. Selectively chooses between its own function generate _random () and system rand() function. A top-level domain (TLD) suffix chosen randomly between .com, .net, .org, .info, and .biz is then appended to the domain name. Conficker B includes additional TLD suffixes (.ws, .cn, .cc).

V. Countermeasures

There are several measures that can be taken to immensely reduce the risk of being get attacked or infected by a cryptovirus. Many of the attacks described in here can be avoided with existing antiviral mechanisms and a tool, since cryptoviruses propagate in the similarly as traditional viruses does. The first step toward this is, implementing mechanisms and schemes to detect viruses before infection or may be immediately following system infiltration [6].

1. Only passwords are weak to authenticate a host. Two level authentications, first with the biometric entity such as the users fingerprint, iris scan and second using the password.
2. Use of up-to-date anti-virus mechanism, as the crypto viruses spread similar to normal viruses does.
3. Provide an access control mechanism to cryptographic tools and API's of the system. This will helps virus analyst or the system administrator to identify suspicious cryptographic usage of the system component.
4. The direct memory monitoring is needed to catch self polymorphic encrypting, cryptoviruses.
5. Use of intrusion detection System and firewall to protect host in the network system and the stand alone systems. Use patches as they are made available to make system more secure.
6. On-line proactive anti-viral measures theoretic for now.
7. Access control to cryptographic tools
   If strong crypto ciphers and random number generators are available to user processes, then they are available to viruses.
8. Backups

VI. CONCLUSIONS

We have shown how Cryptography can be used to implement viruses that are able to perform extortion-based attacks on their hosts. Public-key cryptography is very much essential in enabling the virus-author to get an advantage over the victim system. We also suggested a set of counter measures that can be taken to minimize some sort of possibility to reduce the risks posed by the crypto virological attacks such as latest events like Gpcode and Conflicker. Finally, Cryptographic techniques and tools can be used to create a new class of viruses: Cryptoviruses in which the virus/Trojan writer need not be aware of all the cryptography tools and use of available functions (like API's) and a victim's point of view also, it is better to know the different types of attacks by the attacker to keep some of the safeguards to protect their system and networks from attacker. The goal of cryptanalysis is not to undo the honourable work of others, but to find vulnerabilities and fix them.

VII. ACKNOWLEDGMENT

We are thankful to GMR Institute of Technology, Rajam, AP, India and all our faculty members of Information Technology Department for their encouragement and whole hearted cooperation. I would like to thank Asst. Prof. M.Balajee for his guidance and valuable suggestions time to time. We are lucky to have god like Parents, they provided me very excellent moral support and Friends for their encouragement during this work.

VIII. REFERENCES

[1] "Malicious Cryptography Exposing Cryptovirology" by Adam Young Moti Yung , Wiley Publishing, Inc.

[2] http://en.wikipedia.org

[3] Shafiqul Abidin, Rajeev Kumar, Varun Tiwari," A Review Report on Cryptovirology and Cryptography" International Journal of Scientific & Engineering Research, Volume 3, Issue 11, November-2012 1 ISSN 2229-5518

[4] Adam Young and Moti Yung, Cryptovirology: Extortion-Based Security Threat and Countermeasures, Proceedings of the 1996 IEEE Symposium on Security and Privacy.

[5] Cryptovirology.com FAQ: http://www.cryptovirology.com/

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

[7] http://www.viruslist.com/en/viruses/encyclopedia?virusid=313 444