

Topic: Know More about Ransomware and Protect Your File Better

Mentor: Ming Chow

Student: Yucheng He

Abstract:

Ransomware is a specific kind of malware, which will restrict your access to your data in your computer via file encryption, and ask for fee to regain the access. As named 'year of ransomware', 2016 has seen rapid growth in Ransomware diffusion, transmission and ransom thieving. ^[1] Until the end of August, ransomware flow has increased more than 500% compared to 2015. ^[1] Ransomware has become one of most critical security problem now. It is better to know more about ransomware to protect your computer. In this paper, ransomware will be introduced in detail, including the definition, history, transmission methods and the profit-model of ransomware owner; the current status and statistics of ransomware will also be reported; the real cases of illustrated; the reason of rapid growth will be analyzed; and the technologies and methods for preventing from ransomware will be presented.

1. Introduction:

1.1 Preface:

In Sep. 2013, the SecureWorks CTU of Dell discover a ransomware named CryptoLocker, which was attached in the email to distributed in the network and would infected the computer and encrypted hundreds types of files including excel, database and images. It would ask victim for ransom about 300 dollars. According to statistics, in the first 100 days, CryptoLocker had infected 200 to 250 thousands of systems. ^[2]

In Aug. 2014, New York Times reported a ransomware named “ScarePackage” had infected 900 thousands Android devices in one month. This ransomware would not only access to the camera and phone, but also could pop out a message to accuse the user of device to diffuse pornographic contents. The victim had to pay about hundreds dollars of ransom to use the Android devices normally. ^[3]

In Dec. 2014, the researchers of Sophos and ESET found a self-replicating ransomware named VirLock, which would encrypt victim’s documents, images, audios, videos and compressed files, and lock device’s screen in the reason of copyright infringement to ask for 0.652 bitcoin as ransom.

For the traditional virus, the computer system or applications without the protection of anti-virus software may be infected by some malwares, but user can fix this by re-installing operating system or applications; for the Trojan, which would remote control user’s computer, user can disconnect the network to get rid of remote control of attacker, but for the ransomware, once user’s files was encrypted or user’s system was locked, and the files were very important to user, for examples: Comp116 final project, if I were the victim, I think I had to pay the ransom to get my final project report back. Especially in this year, there has been rapid growth in the infected devices, the variants of ransomware and the amount of ransom. It is time to take more attention of this specific malware: ransomware.

1.2 What is ransomware:

Ransomware is a kind of Malware, using methods of annoying, scaring or kidnapping user’s files

to make user cannot use data or system normally, and ask user for ransom. The files include documents, emails, databases, original codes, images, compressed files and many other types of files. The ransom usually is real currency or virtual currency like bitcoin. Generally speaking, the owner of ransomware would set a time limit for ransom, and the ransom would increase with the time going. Sometimes, even the ransom was paid; the victims could not use their systems or get their files back.

1.3 History of Ransomware:

The first ransomware virus should be AIDS Trojan (also called PC Cyborg) in 1989 created by Joseph L.Popp. The virus infected 20 thousands copies of soft disks and the disks were distributed to the attendees of the international AIDS conference. The Trojan used symmetric cryptography, so it was not difficult to use decryption tool to decrypt the key in reasonable times. Then 17 years later, another ransomware: Archievus was discovered. This was the first ransomware using asymmetric cryptography, so it is more difficult to decrypt and remove it. In 2011, because of the untraceable payment service, it was easier for the owners of ransomware to receive the ransom without exposure themselves. So after 2011, there have been hundreds of ransomware variants, such as Reveton, Cryptolocker, Locky and many other ransomwares. ^[4]

1.4 Type of Ransomware

Depending the blackmail methods, ransomware can be divided into three kinds:

1. Disturb user to use the system normally. Like PC Cyborg, this kind of ransomware would use the methods like locking the screen to compel user to pay ransom to use the system normally.
2. Scare user. Like FakeAV, this kind of ransomware would pretend to be anti-virus software, and warn the user some viruses were found in the system to decoy user to buy the fake anti-virus software. Or like Reveton, it would pretend to be the law enforcement agency and claim user has violated the law, and need to pay some ransom to avoid facing criminal charge.
3. Kidnap user's files. This is the most common ransomware nowadays. It would encrypt user's files using cryptographic algorithm and ask for ransom to decrypt them.

Comparing these three kinds of ransomware, the third one is the most harmful and most common in recent days. It use encryption method to restrict the user's access to their data, and hard to decrypt it. Usually there are five stages in the infection of this kind ransomware.^[5] First, once the victim's computer was infected by ransomware, ransomware would install itself and change the setting of operating system to start automatically every time the victim's computer boots up. Second, the ransomware would contact the owner of the ransomware, and told the owner, the victim's computer had been infected. Third, the owner server and the ransomware client would conduct the handshake to identify each other and the server would generate two keys by cryptographic algorithm and send one key to ransomware and keep the other key in server. The key sent to ransomware would be used to encrypt the victim's files, and the key kept in server was used to decrypt the encrypted files. Fourth, once the ransomware received the key, ransomware would scan victim's files in computer and encrypted the files with specific file extensions, like jpg, txt and so on. The last stage, a notification would show in the screen with a time limit and the ransom need to be paid, usually the ransom would be paid in untraceable electronic payments such as bitcoin or gift cards. We will focus on this kind of ransomware in this paper.

1.5 Transmission Methods:

The transmission methods of ransomware are similar to Trojan's. Following are the main methods:

1. Transmit by Trojan on website. When user browse malicious website, ransomware would be downloaded by the browser and automatically running in the background.
2. Ransomware would be binding to other malware and transmit by other malware.
3. Transmit through the portable storage media, once user connect the device with the storage media, the ransomware in it would automatically run and lock the computer
4. Transmit through the attachment of email, once user download the attachment and open it, the ransomware would infect the computer

In recent days, ransomware are mainly using email to transmit. Usually, the ransomware were

hiding in the attachment or on the website of the link in the mail. The statistics of transmission method of ransomware in 2016 would be introduced in the paper.

2. To the Community

As introduced in the introduction, compared to the other malware, ransomware is more harmful and difficult to remove. And in 2016, which was named the 'year of ransomware', there have been more and more new ransomwares and more and more devices were infected. In this section, the statistics of ransomware in 2016 would be introduced and indicate the huge growth of ransomware, and it is the time we must learn about ransomware, and protect ourselves from ransomware.

2.1 Growth of Ransomwares:

As the summary from proofpoint.com,^[6] there was 600% growth of the number of ransomware families since December 2015 to June 2016. And in the first five months of 2016, there were 50 new ransomware families.^[7] And compared to the proportion of different type of ransomware before 2016, there is more than 95% of ransomwares found in 2016 are Crypto-ransomware,^[8] which means 2016's ransomware are the most malicious ransomware. So actually, 2016 is the year of Crypto-Ransomware.

2.2 Growth of Infection:

From the Symantec report of ransomware in 2016,^[8] there has been huge growth in the devices being infected by ransomware. Only in March 2016, there was more than 56,000 ransomware infection reported. Even organizations have better security protection compare to normal user, almost half of the organizations have been attacked by ransomware, and more than 40% of ransomware victims are organizations, which means ransomware is hard to prevent and detect. Another important improve of ransomware is, not only windows OS has been attacked by ransomware, there are more and more ransomware infections in Mac OS and mobile devices. We can image, with the technology of ransomware get better and better, it can be true that all kinds of platforms may be infected by ransomware.

2.3 Growth of Ransom:

Compared to the average ransom of 2014 (372 dollars) and 2015 (294 dollars), the average ransom in 2016's ransomware attack has increased to 679 dollars. ^[9] As shown in 2.2, organizations victims have become more and more in 2016. Even only 5% of all the victims would pay ransom to the criminal, reported by the CNN, ^[10] there have been 209 million ransom paid by businesses and institutions to unlock their data, and at this rate there will be a total 1 billion for this year or more in actually, since not all the organizations would report the criminal.

2.4 To Pay or Not To Pay?

As mentioned before, there is only 5% of the victims would try to pay the ransom to unlock their computers. This maybe because of the following reasons: first, for the normal users, their data or files are not that important compared to the amount of ransom, so most of the users may decide to not pay the ransom, and just re-install their system to remove the ransomware; second, for the organizations, I think most of them should have backup of their data in somewhere else, so they can recover their data easily; third, even you paid the ransom, there are high possibilities, you cannot fully recover your data, so most victims chose not pay the ransom. But even you didn't pay ransom; you still have lost in losing the data or spending time to fix the computers.

2.5 To the Community Conclusion

Since the rampant growth of ransomware and the potential damage ransomware can have, all the network users should better to know more about the ransomware, and this is the significance of this paper.

3. Things behind Ransomware

There are three types of ransomware as discussed before, which are two non-encrypting ransomware and one encrypting ransomware. Since the encrypting ransomware has more odious effect on victims, this section will focus on encrypting ransomware, such as Locky and CryptLocker family.

3.1 How Encrypting Ransomware Works:

By analysis of a ransomware source code example ^[11] and some real case ^[12], the general mechanism of encrypting ransomware can be discovered.

First part is how the computer would be infected by ransomware. Usually, there are three kinds of transmission methods as described in the introduction section of this paper. They are email, malicious website and exploit kit with ransomware. Email can contain attachment with ransomware program in it, then when the user download the attachment and open it (actually if user double click it, it would run the program), then the ransomware would be triggered and infect the program. Email can also contain malicious link, either to a malicious website or to download or execute some malicious program, this is the same as the malicious website transmission method. Another method is through the exploit kit. When victim execute the malicious exploit kit, the ransomware in the exploit kit will be activated and infect the computer. These three methods are the most common methods and more than 80% of infections are through these three methods. ^[9]

Second part is how encrypting ransomware encrypts the victim's files. From the 'my-Little-Ransomware' open source code on Github, the ransomware will first create the key or keys used for encrypting and decrypting files, in the example: AES was used for the cryptographic algorithm. Then the ransomware will scan all the files in the file system, and find the specific files with specific file extensions. Then the ransomware will encrypt the files with the key generated, and at the same time, the ransomware would show the message of instruction for paying ransom to decrypt the files.

The last part is how to pay the ransom. Before the virtual currency appeared, the ransom is usually paid with the mailing the check or transfer money to some untraceable account. In recent years, with the development of bitcoin, most of the ransomware only accept the bitcoin because of the untraceable property of the bitcoin account. This is the safest method for the attacker to receive the ransom.

The last part is how ransomware would decrypt the files. Usually when ransom was paid, the decrypting key would be sent to the victim and the victim can use this key to decrypt the files. The key can be stored and sent through some public server, such as Google Doc (for the example ransomware) or C&C server. And with the help of this server, it is hard to trace the attacker.

3.2 Why Ransomware Grow so Fast:

First reason is the great profit of the ransomware. The developer of ransomware can get incredible amount of money from the ransom victim paid. From the statistics in section 2, there would be 1 billion dollars ransom for the ransomware in this year. The attacker can use the money to develop the new ransomware family to get more money.

Second reason is the payment method of ransom is safe. Using bitcoin as the payment method, there is no way for the law enforcement agency to find the attacker. It is just like the most kidnap scenario in the movie, the police usually cannot catch the criminals when they were getting the ransom. It is safe for the criminal, so the criminal would like to keep using ransomware.

Third reason is encrypting ransomware is hard to crack. Ransomware takes the advantage of cryptographic algorithms that are almost impossible to break in the limit time. So it is impossible for the victim to decrypt the encrypted files without knowing the key. So the victim has to pay the ransom to recover their files, otherwise, victim will lost their files.

Another reason is the ransomware is easy to infect the computers. The transmission methods are various and the new ransomware species keep appearing. As a result, it is hard for the anti-virus application to detect all kinds of the ransomware.

4. How to Protect Ourselves

Since most organizations have security department, in this section, we are focused on the protection of normal user.

a. The best way to defeat ransomware is backup the system regularly and frequently, and stores the backup into other separate storage device. It is not safe to store the backup in cloud, because some ransomware will also encrypt the files in the cloud.

b. Keep the software and OS in the computer up to date. Most malware could use the vulnerability of software and system to infect the devices. The updates of OS and software usually would fix the vulnerability and reduce the risk of infection of ransomware.

c. Add the websites that trusted into bookmark and use bookmark to access these websites through bookmark. It is much safer to use the bookmark to access the website compared to use

the link in some website or in the email.

d. Do not open the attachment or click the link in the email from untrusted email address. It's better to add the trusted email address into contact, so it is easier to figure out the trusted and untrusted emails.

e. Scan the whole disk of computer by anti-virus software regularly. Although the anti-virus software cannot detect the very new ransomware, but it can detect most of ransomwares, which have been reported.

All these steps can protect user from the ransomware in a certain degree, but what more important to against ransomware is increasing the knowledge of ransomware and developing a good habit of using network safely.

5. Conclusion

Ransomware actually is not new to us, but the transmission methods are more and more covert, and the technology involved in ransomware are more and more mature. This means the developers of ransomware are trying to develop the more and more unpredictable variant of ransomware. Compared to anytime before, it is time to know better about ransomware and protect your computer from infection by ransomware. With better knowledge about it, we can protect ourselves from infection by ransomware.

6. Support Material

The support material is the Poster.

Reference:

- [1]. M.Khatri “Ransomware Statistics – Growth of Ransomware in 2016”, Aug. 2016, From <http://blogs.systweak.com/2016/08/ransomware-statistics-growth-of-ransomware-in-2016/>
- [2]. Keith Jarvis, SecureWorks “Threat Analysis – CryptoLocker Ransomware”, Dec. 2013, From <https://www.secureworks.com/research/cryptolocker-ransomware>
- [3]. Nicole Perloth, New York Times, “Android Phones Hit by Ransomware”, Aug. 2014, From http://bits.blogs.nytimes.com/2014/08/22/android-phones-hit-by-ransomware/?_r=0
- [4]. Ryan Francis, “The History of Ransomware”, Jul. 2016, From <http://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html>
- [5]. “Anatomy of a Crypto-Ransomware Attack”, From <https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-anatomy-crypto-ransomware-infographic.pdf>
- [6]. “Quarterly Threat Summary: Apr – Jun 2016” From proofpoint.com https://www.proofpoint.com/sites/default/files/quarterly_threat_summary_apr-jun_2016.pdf
- [7]. “By The Numbers: Ransomware Rising” Jun. 2016, From <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/by-the-numbers-ransomware-rising>
- [8]. “Ransomware and Business in 2016” From Symantec: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
- [9]. Jonathan Crowe, “Ransomware by the Numbers: Must-Know Ransomware Statistics 2016”, From <https://blog.barkly.com/ransomware-statistics-2016>
- [10]. David Fitzpatrick, Drew Griffin, “Cyber-Extortion Losses Skyrocket, Says FBI” From CNN.com <http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/>
- [11]. The my-Little-Ransomware source code from github: <https://github.com/aaaddress1/my-Little-Ransomware/>
- [12]. Bleeping Computer: <https://www.bleepingcomputer.com/forums/t/608773/list-of-ransomware-support-topics-faqs-and-news-articles/>
- [13]. O’Gorman, Gavin, and Geoff McDonald. Ransomware: a growing menace. Symantec Corporation, 2012.
- [14]. Abrams, Lawrence. "CryptoLocker ransomware information guide and FAQ." (2014).
- [15]. Luo, Xin, and Qinyu Liao. "Awareness Education as the key to Ransomware Prevention." Information Systems Security 16.4 (2007): 195-202.