Journal of Convergence for Information Technology
Vol. 8. No. 1, pp. 139-145, 2018

ISSN 2586-1816
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2018.8.1.139

Ransomware attack analysis and countermeasures of defensive aspects

Sunghyuck Hong*, Jin-a Yu
Division of Information & Communication, Baekseok University

랜섬웨어 공격분석 및 방어적 측면의 대응방안

홍성혁*, 유진아
백석대학교 정보통신학부

Abstract Ransomeware is a kind of malware. Computers infected with Ransomware have limited system access. It is a malicious program that must provide a money to the malicious code maker in order to release it. On May 12, 2017, with the largest Ransomware attack ever, concerns about the Internet security environment are growing. The types of Ransomware and countermeasures to prevent cyber terrorism are discussed. Ransomware, which has a strong infectious nature and has been constantly attacked in recent years, is typically in the form of Locky, Petya, Cerber, Samam, and Jigsaw. As of now, Ransomware defense is not 100% free. However, it can counter to Ransomware through automatic updates, installation of vaccines, and periodic backups. There is a need to find a multi-layered approach to minimize the risk of reaching the network and the system. Learn how to prevent Ransomware from corporate and individual users.

Key Words : Ransomware, Malicious code infection path, AES & RSA encryption, Drive-by-Download, Malicious code

요 약 랜섬웨어란 악성코드의 일종이다. 랜섬웨어에 감염된 컴퓨터는 시스템 접근이 제한된다. 이를 해제하기 위해서는 악성 코드 제작자에게 대가를 제공해야 한다. 최근 최대 규모의 랜섬웨어 공격이 발생함에 따라 인터넷 보안 환경에 대한 우려가 점점 커지고 있다. 랜섬웨어에 대한 종류와 사이버테러 피해를 막기 위한 대응 방안을 알아본다. 강력한 감염성을 가지며 최근에도 끊임없이 공격해오는 랜섬웨어는 대표적으로 Locky, Petya, Cerber, Samam, Jigsaw가 있고, 점점 공격 패턴이 진화중이며 요구 결제 금액 또한 증가하고 있다. 현재로써 랜섬웨어 방어는 100% 특효약이 있는 것이 아니다. 하지만 자동업데이트, 백신설치, 주기적 백업을 통해 랜섬웨어에 대응 할 수 있다. 본 연구에서는 네트워크와 시스템에 도달하지 못하도록 다층적인 접근 방법을 제시하여, 기업과 개인 사용자들의 랜섬웨어 예방 방법을 제시하였다.

주제어 : 랜섬웨어, 악성코드 감염경로, AES&RSA 암호화, Drive-by-Download, 악성코드

1. Introduction

As the web evolves, so does the scale of cyber attacks. KISA released its Top 7 Cyber Attack Outlook Report in 2017. The report calls for caution of An attack customized to Korea, Targeted attacks through common software, Mass distribution of various types of Ransomware, Cyber terrorism about social infrastructure, Intelligence of large-scale malicious code infection technique, Increased risk for mobile financial services, and the weapon transformation of Zombie-infected thing internet devices, As a whole in industry[1].

Among them, the most issue cyber attack in 2017 is

*This paper was supported by 2017 Baekseok University research fund.

*Corresponding Author : Sunghyuck Hong(sunghyuck.hong@gmail.com)

Received January 31, 2018 Revised Febuary 08, 2018
Accepted February 20, 2018 Published February 28, 2018

considered to be Ransomware. Ransomware was popular in Russia. and the fraud of using Ransomware has increased around the world. Security software development company McAfee released more than 250,000 copies of Ransomware samples collected during the first quarter of 2013, this is twice as many as last year. Extensive cyber attacks through encryption have begun to spike through Trojan horses such as Cryptolocker and Cryptowall[2].

On May 12, 2017, the largest Ransomware attack ever happened, which became a major global issue. Ransomware called WannaCry, which uses the United States National Security Agency's hacking tool, infected more than 150,000 computers around the world one day after the dissemination, causing the terror of cyber terrorism.

In chapter 2 of this study, we describe the Ransomware and Ransomware attack flow and principle, symmetric key & public key algorithm, Ransomware type, infection symptom, damage case. Chapter 3 describes various forms of Ransomware infection, Chapter 4 deals with Ransomware prevention. The final chapter finish with a conclusion to the study[3].

2. Ransomware

2.1 Ransomware

Ransomware is a kind of malicious software that infects Windows PC or server systems to restrict all access and requires some sort of expense to clear the infection. Because all access to the computer is restricted In order to release the restriction, the payment of money is made to the relevant Ransomware developer. Fig. 1 shows the process of Ransomeware attack. If there is Ransomware that is encrypted and can not be controlled, there is also Ransomware, which simply locks the screen and prompts the computer user to pay for the prompts. Because it is malicious code, it can be installed indiscriminately without user's consent. It occurs frequently in PC based on Windows operating system, but also occurs in mobile and Mac OS[4].

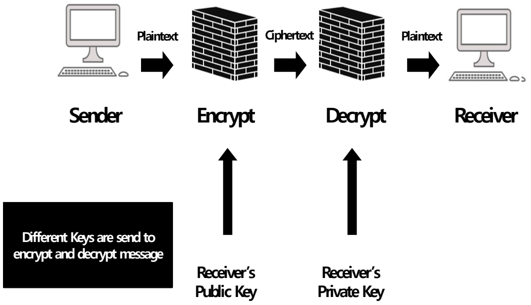

Fig. 1. Ransomware Attack Process

2.2 Ransomware attack flow

In general, Ransomware infects your computer in three steps. The first searches for files that the attacked user believes are important. The second encrypts the file. Typically, there are two ways to encrypt files : fixed key encryption and dynamic key encryption. Finally, move the encrypted file to the desktop so that the user can see it. After that, a message window will be displayed to guide the infection, and a restoration sum of money is required[5].

2.3 Ransomware attack method

Most of Ransomware uses file encryption method. In general, file encryption is used to protect files, but Ransonware can be seen as a bad example of using it to rob people of their money[6].

In order to proceed with encryption, a key to be used in encryption algorithms and algorithms is required. The public key algorithm and the symmetric key algorithm are examine, a representative encryption method.

2.3.1 Symmetric Key Encryption Algorithm

Fig. 2 shows symmetric-key algorithm. The symmetric key algorithm has the encryption key when proceeding with encryption and the same decryption key when proceeding with decryption. Typically, there is an AES algorithm. It is mainly used for personal file encryption and communication within unspecified groups. Although the speed is faster than the public key encryption algorithm, since the encryption key is the same as the decryption key, security becomes useless when the key is exposed[7].

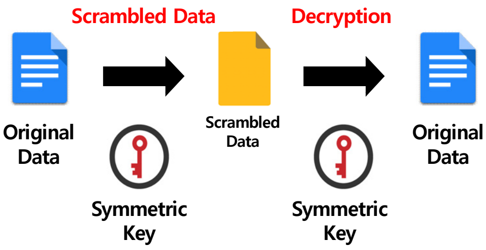

Fig. 2. Symmetric-key Algorithm

2.3.2 Public key Encryption Algorithm

Fig. 3 shows public-key cryptography. The public key algorithm has the different encryption key when proceeding with encryption and the different decryption key when proceeding with decryption. Typically, there is an RSA algorithm. Ron Rivest, Adi Shamir, and Leonard Adleman, and is named RSA following their respective names[8].

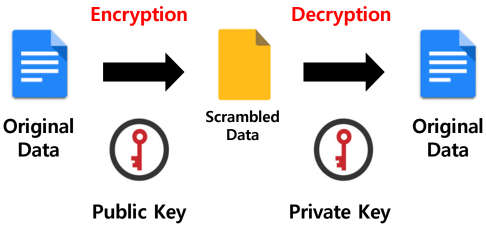

Fig. 3. Public-key Cryptography

The public key algorithm is divided into public key and private key. When a public key algorithm generates a key, a public key and a secret key are generated as a pair, anyone can see the public key, whereas the private key only needs to know the producer. Generally it is used to encrypt with the public key and decrypt the secret key. Because of this feature, the public key algorithm has the advantage of high security, but it has a drawback that it is slow. Generally, a public key encryption algorithm and a symmetric key encryption algorithm mixed to use.

2.4 Types of Ransomware and Infection Symptoms

Table 1 shows the features by Ransomware. Let's look at six varieties of Ransomware. NsbLocker targeted to attack all of the images, documents, executables, compression, and media files on the system. The original file is converted into an executable file after being backed up in an encoded form. Since it is not an AES or RSA type encryption, it is the weakest form of Ransomware because it does not require a decryption key[9].

Table 1. Features by Ransomware

	Division	Protocol	Encryption	Main target	Ransom
1	NsbLocker	TCP	POLYMORPHIC	DOC/EXE/IMAGE/MEDIA	250 USD
2	CTB Locker	HTTPS /TOR	AES, ECDH	DOC/IMAGE	0.5 USD
3	Crypto Locker	HTTP	AES, RSA	DOC/IMAGE	300 USD
4	CryptoWall	HTTP /TOR	RSA	DOC/IMAGE	500-1000 USD
5	TorrentLocker	HTTPS	AES	DOC/IMAGE	0.8 BTC
6	TeslaCrypt	HTTPS /TOR	AES, ECC	GAME/DOC/IMAGE	500-1000 USD

Cryptolocker is a malicious code found in 2013. All files in the computer, including files, are encrypted using RSA and AES keys to control access and require money in exchange for decryption. The computer slows down for no reason because it inflates the RAM to its fullest extent during the infection process. It counts down to 100 hours after the infection, but it deletes all files if you do not deposit in time.

Cryptolocker is a Website infection Ransomware found in 2014. The server's index page is replaced by a page created by the Ransomware developer, destroying the Web site. The decryption method is also a method of requesting the site operator for the cost and distributing the decryption key when the deposit is made[10].

CryptoWall is Ransomware that is infected through primarily spam mail. The latest version of CryptoMonkey 4.0 encrypts all file names and extension names of documents, pictures, media, etc. existing on the user's PC through the AES CBC 256Bit algorithm using the RSA-2048 key.

TorrentLocker is similar to Cryptolocker and CryptoWall. The difference is that "HKCU\Software\Bit Torrent Application\configuration" registers the encrypted file in the registry.

TeslaCrypt is similar in structure to Crytolocker, but it also encrypts game files such as profiles, save data, and maps. Install the malicious code on the user's PC using the vulnerability of Flash Player[11].

2.5 Ransomware damage cases

2.5.1 Wanakrai Ransomware also got a CGV

CJCGV said on the morning of the 15th that it was confirmed that the advertisement server that stored the ad before the movie screening in the theater was infected with Ransomware. An related persons of the company said, "Some of the theater's advertisement servers are infected with Ransomware at dawn and can not send commercials that are screened before the start of the movie. The server that saved the movie was not infected, so the screening was ongoing."

2.5.2 Internet Nayana infects Ransomware with 'APT attack'…

According to the government 's interim report, infection of The hosting company 'Internet Nayana' who paid a Bit Coin worth 1.3 billion won for the data recovery fee Ransomware was caused by a sophisticated intelligent continuous threat (APT) attack. Internet Nayana revealed that the overall security management system, including device security and server access control, was poor.

It is with this, 153 Internet Nayana servers were infected with Linux-based 'Erebus' Ransomware and more than 5,000 Web sites hosted by Web servers were damaged.

2.5.3 'Read the Internet articles and pay?

A victim who was asked 1BTC for in exchange for unlocking Ransomware-infected passwords was infected with Ransomware after reading entertainment articles on the internet as usual. The victim who only installed the vaccine and rarely updated, detected slowing computer while reading the entertainment articles. When victim shut down the internet window to reboot the computer, the wallpaper changed and the voice of a strange woman flowed out. When a frightened victim shuts down the computer and turns it back on, The victim was aware that he had been infected with Ransomware, which demand to have a large amount of money take as hostage data.

3. Various forms of Ransomware infection path

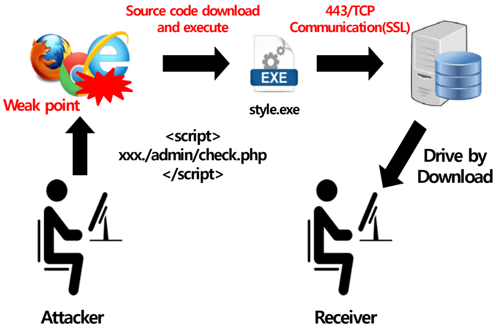
Source code download and execute
443/TCP Communication(SSL)
EXE
style.exe
Weak point
<script> xxx./admin/check.php </script>
Drive by Download
Attacker
Receiver

Fig. 4. Drive-by-Download Attack diagram

Ransomware can be infected in various ways. It can be infected with Ransomware by accessing a vulnerable Web site, and can be infected with spam mail and spear phishing, file sharing sites, and SNS[12]. Fig. 4 shows Drive-by-Download Attack diagram. The most dangerous is the unreliable site access. It is fatal that a simple site visit can be infected. Drive-by-download method is typical.

Drive-by-Download occurs when you visit a site in a web environment or click a pop-up window. Attackers use a variety of methods to hide malicious code and prevent it from being recognized by security software. Eventually users will not be aware and will agree to provide the attackers with the information[13]. This causes the browser to crash, allow the attacker to perform the desired action in the browser, such as reading or destroying data from the file system. and all the information on the network stored inside the computer is exposed to security risks. Users are always encouraged to keep their OS and security updates steady, running the antivirus program periodically is also one of the ways to deal with Ransomware[14].

The second path of infection is spam mail. If receive spam mails that are not clear from the provenance, malicious code is distributed through an attached file or URL. It's best not to open up strange e-mail as much as possible. But if you send spam mail by disguising it as something you can often see in everyday life such as 'year-end settlement guide', 'bank password change request' and 'mobile phone charge notice', It can be helpless. Users should never open an e-mail that is not clear from the provenance, attachments that require downloading should be checked for malware after downloading [15].

The third path of infection is file sharing. Downloading files via web hard and torrent (P2P) sites is the best environment to infect malicious code. Illegal P2P & Web hard downloading is prohibited, and it is recommended to share files via a secure method.

The fourth path of infection is SNS. In a typical SNS, Facebook, the spread of the Ransomware through the SVG (Scalable Vector Graphics) image of the photograph has been found. The SVG file is a file in which SNS, e-mail, text message, etc. are utilized because the graphic quality is maintained even when the image is enlarged or reduced. If you click on the SVG image file on your PC, Ransomware will download and run and Ransomware will become infected. Embedded Content Code, such as JavaScript, is included, which allows malicious code to run through a Web browser. Users do not download the SVG file, and it is necessary to security patch the SNS application[16-18].

4. Ransomware Prevention Plan

The damage caused by Ransomware is continuously increasing. In addition, Ransomware is targeted not only to individuals but also to corporations, and it is likely to expand to serious problems due to infection of important documents. Therefore, in this paper, we propose a defensive response method to minimize the damage of Ransomware.

The most important thing is always to update and keep all software up to date. Especially, in case of flash (Flash) which Ransomware can infiltrate, it is recommended to set automatic update.

The second is the use of trusted vaccine software and regular updates. Vaccines can detect and prevent infection with Ransomware and other malware, but documents that are already infected and encrypted can not be decrypted. It is also necessary to make sure that the vaccine is regularly checked and that engine updates are ongoing on a regular basis [19].

Third, it takes a habit of backing up important files periodically. It is a good idea to back up to a secure storage device such as USB, external hard disk, or cloud, not a disk inside the computer. If you are infected with Ransomware and important files are encrypted, you can recover the files that you have already backed up after formatting.

5. Conclusion

Ransomware is a kind of malicious software that infects Windows PC or server systems, restricts all access, and requires some sort of cost for disinfection. Ransomware includes CryptoLocker, NsbLocker, and CTBLocker. Ransomware can be infected in various path. It may be infected to Ransomware by accessing a security vulnerable Web site, or may be infected with spam mail and spear phishing, file sharing sites, and SNS. It is always important to update all software to the latest version to prevent Ransomware. It is also recommended to periodically back up important files, and users can increase their security awareness by building their knowledge of computers.

REFERENCES

[1] H. Y. Kim, D. J. Kang & Y. Yeom. (2017). Dynamic ransomware protection using deterministic random bit generator. *2017 IEEE Conference on Application, Information and Network Security.*
DOI : 10.1109/ains.2017.8270426

[2] L. D. Yu.. (2015). Threats and countermeasures of malware. *Journal of Convergence for Information Technology. 5(1),* 13-18.

[3] M. Dave. (2016). *Beware-Ransomware!* River Publisher. http://pop.riverpublishers.com/opinions.php?id=4
DOI : 10.13052/popcas004

[4] Juggling Identities. (2009). *Four. Ideal Types of Crypto-Jewish Identity.* USA : Columbia University Press.

[5] Juggling Identities. (2009). *APT attacks and Countermeasures.* USA : Columbia University Press.

[6] A. K. Sood & R. Enbody. (2012). Targeted cyberattacks: a superset of advanced persistent threats. *IEEE security & privacy, 11(1),* 54-61.
DOI : 10.1109/msp.2012.90

[7] E. Sava & C. Yılmaz. (2015). A Generic Method for the Analysis of a Class of Cache Attacks: A Case Study for AES. *The Computer Journal, 58(10),* 2716-2737.
DOI : 10.1093/comjnl/bxv027

[8] P. Dixit, J. Zalke & S. Admane. (2017). Speed optimization of aes algorithm with hardware-software co-design. IEEE *2017 2nd International Conference for Convergence in Technology (I2CT).* IEEE : India.
DOI : 10.1109/i2ct.2017.8226237

[9] C. P. Pramod & M. Jaiswal. (2017). An advanced AES algorithm using swap and 400 bit data block with flexible S-Box in Cloud Computing. *2017 3rd International Conference on Computing, Communication and Automation (ICCCA).* IEEE : India.
DOI : 10.1109/ccaa.2017.8229888

[10] Y. Jeong, Y. Yon & J. Ku. (2017). Hash-chain-based IoT authentication scheme suitable for small and medium enterprises. *Convergence Society for SMB, 7(4),* 105-111.
DOI : 10.22156/cs4smb.2017.7.4.105

[11] M. S. Wamser & G. Sigl. (2017). Pushing the limits further : Sub-atomic AES. *2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC).* IEEE : United Arab Emirates.
DOI : 10.1109/vlsi-soc.2017.8203470

[12] S. L. Chikouche & N. Chikouche. (2017). An improved approach for lsb-based image steganography using AES algorithm. *2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B).* IEEE : Algeria.
DOI : 10.1109/icee-b.2017.8192077

[13] A. K. Sood & S. Zeadally. (2016). *Drive-By Download Attacks : A Comparative Study. IT Professional, 18(5),* 18-25.
DOI : 10.1109/mitp.2016.85

[14] M. Jodavi, M. Abadi & E. Parhizkar. (2015). DbDHunter : An ensemble-based anomaly detection approach to detect drive-by download attacks. *2015 5th International Conference on Computer and Knowledge Engineering (ICCKE).* IEEE : Iran.
DOI : 10.1109/iccke.2015.7365841

[15] J. Lee. (2017). A Study on gateway authentication protocol in IoT. *Convergence Society for SMB, 7(3),* 91-96.
DOI : 10.22156/cs4smb.2017.7.3.091

[16] Y. Takata, M. Akiyama, T. Yagi, T. Hariu & S. Goto. (2015). MineSpider : Extracting URLs from Environment-Dependent Drive-by Download Attacks. *2015 IEEE 39th Annual Computer Software and Applications Conference.* IEEE : Taiwan.
DOI : 10.1109/compsac.2015.76

[17] A. Yousefi, & S. M. Jameii. (2017). Improving the security of internet of things using encryption algorithms. *2017 International Conference on IoT and*

Application (ICIOT). IEEE : India.
DOI : 10.1109/iciota.2017.8073627

[18] M. S. Gu, Y. Z. Li. (2015). A Study of Countermeasures for Advanced Persistent Threats attacks by malicious code. *Journal of Convergence for Information Technology. 7(4),* 37-42.

[19] P. S. Shin, J. M. Kim. (2014). Security and Hacking on Wireless Networking for Small and Medium Business : Survey. *Journal of Convergence for Information Technology. 4(3),* 15-20.

홍 성 혁(Hong, Sung Hyuck) [정회원]

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2007년 9월 ~ 2012년 2월 : Texas Tech University, Office of International Affairs, Senior Programmer
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : Network Security
- E-Mail : sunghyuck.hong@gmail.com

유 진 아(Yu, Jin A) [학생회원]

- 2015년 3월 ~ 현재 : 백석대학교 정보통신학부 재학
- 관심분야 : Hacking, Secure Sensor Networks, Artificial intelligence
- E-Mail : ryujina0722@gmail.com