Ransomware 101: Understanding the Business Model

Amien Harisen

Master of Information Technology, Swiss German University, The Prominence Tower, Jalan Jalan Sutera Barat Kav 15, Alam Sutera, Tangerang 15143, Indonesia

Abstract

WannaCrypt Ransomware outbreak in 2017 shocked everyone in the term of the spreading and damage it caused. WannaCry Ransomware keep us reminded that the impact of ransomware attack is devastating and costly. Crypto Wall alone racked up around $324 million in 2016 (Trend Micro, 2016), while WannaCry tally not yet to be confirmed, since its spreading in 150 countries including Indonesia within its infection spreading in 2017. Since its modern outbreak in 2014, ransomware produce one word to the cybercriminal operator, profit. In this paper, we will breakdown how the ransomware works, the history of ransomware, and why it is one of the profitable main fronts for the cybercriminal.

Keywords: Ransome; WannaCry, WannaCrypt; Cyber Extortion; Cyber Criminal;

1. Introduction

Ransomware is a category of malicious software which, when run, disables the functionality of a computer in some way (Symantec, 2012). When it’s running its lock the affected computer and depends on the type of ransomware, they encrypt all the files with strong encryption until the owner of the computer pay some ransom (mostly by bit coin) to the attacker. Paying the ransom unfortunately does not guarantee the files would be come back and safe to the owner (Checkpoint, 2017).

Ransomware it’s not a new threat in cyber security, since its first occurrence appears in 2005, different kind of ransomware appeared and impacted the users in different way. Still these kinds of threat usually treated lightly by the end user, because 71% of the ransomware spread are from spam email (Trend Micro, 2016). The devastating impact of ransomware was estimated USD 1 billion in 2016, and it cost USD 209 millions alone in the first 3 month of 2016 in the USA (CarbonBlack, 2016).

This paper will be divided into multiple chapter, chapter 1 would be the introduction, chapter 2 consist of the history of the ransomware, chapter 3 would be the methodology of how ransomware infected the victim, chapter 4 would be the business model of ransomware, how the monetization system works, and chapter 5 would be the conclusion and how to mitigate the ransomware attack.

2. Ransomware History & Type

According to Carbon Black, Ransomware is not new, its 30 years old malicious software that suddenly became a trend because of cybercriminal using it as a business model to easily extort money from victim (CarbonBlack, 2016).

2.1 Ransomware History

The first model of ransomware ever recorded was dubbed AIDS (AIDS Info Desk) Trojan that were encrypting files in diskette back in 1989 also known as “PC Cyborg Trojan” because if the user needs to regain access, they would have to send USD 189 to PC Cyborg Corp. at a post office box in Panama (U. Shalvi, 2016). The initial creation of ransomware in that day was unsuccessful since the owners of a computer are small and exclusive, and AIDS had flaw in their function since they are using symmetrical encryption.

The reign of modern ransomware creation was emerged in the year of 2005, with the appearance of Archives, the first ransomware that implement the asymmetric encryption, and its growing from there. The brief rundowns of well-known ransomware are shown below (CarbonBlack, 2016) (U. Shalvi, 2016):

- AIDS Trojan (1989), Infected 20k diskettes distributed at AIDS conference; symmetric cryptography; set in motion three decades of ransomware attacks.
- Archives (2005) is the first ransomware to use asymmetric encryption; encrypting every file in My Documents, and required users to make purchases from websites to obtain passwords to decrypt files.
• GP Code, It is an encryption Trojan, which initially spread via an email attachment appearing to be a job application which used a 660-bit RSA public key to encrypt the victim files.
• Reveton (2012), Spawned ‘police based’ ransomware including Urausy and Tohfy.
• CryptoLocker (2013), First cryptographic malware spread by downloads from a compromised website and/or business professionals in the form of email attachments.
• CryptorBit (2013), another ransomware that was discovered in December 2013. CryptorBit corrupts the first 1024 bytes of any data file, and it can bypass Group Policy Windows settings put in place to tackle against this kind of ransomware infection. It uses social engineering technique to get users to install the ransomware using a fake update. It uses Tor and Bit coin for a ransom payment.
• CryptoDefense (2014), Used Windows ‘built-in encryption CryptoAPI, 2048-bit RSA encryption & Tor/Bit coin for anonymity.
• Crypto Wall (2014), An improved version ransomware from creators of Crypto Defense; first to establish persistence behavior to the victim computer; According to an August 27 report from Dell Secure Works Counter Threat Unit (CTU): “CTU researchers consider Crypto Wall to be the largest and most destructive ransomware threat on the Internet as of this publication, and they expect this threat to continue growing.” More than 600,000 systems were infected between mid-March and August 24, with 5.25 billion files being encrypted. 1,683 victims (0.27%) paid a total $1,101,900 in ransom. The latest version of Crypto Wall is 4.0 and it was released in 2015.
• CTB Curve-Tor-Bit Coin Locker (2014), Suspected from Eastern European developer and targeted the Russian Mainland, it’s the first ransomware to communicate directly with a command center server in Tor Network as well as implement method deleting Volume Shadow Copies on Windows machines.
• Sypeng (2014), First Android-based ransomware.
• Koler (2014), Considered the first “Locker worm”
• SynoLocker (2014), this ransomware targeting Synology NAS devices. Using BitCoin for payment and TOR for anonymity.
• SimplLocker (2014), First ‘crypto-based’ ransomware for Android devices that encrypted files on simply locked phones
• Crypto Blocker (2014), A new ransomware variant emerged in July 2014. It only encrypts the files whose size is less than 100MB and will skip anything in Windows or Program Files. It uses AES rather than RSA encryption.
• OphionLocker (2014), It used ECC (Elliptic Curve Cryptography) public-key encryption. If the ransom was not paid within three days, the private key would be deleted.
• Pc Lock (2015),
• Locker Pin (2015),
• TeslaCrypt (2015),
• Chimaera (2015),
• LowLevel4 (2015),
• Vault Crypt (2015),
• 7ev3n (2015)
• Ransomeware32 (2016),
• Sam Sam (2016),
• Locky (2016),
• Petya (2016),
• KeRanger (2016),
• Maktub (2016),
• Jigsaw (2016),
• CryptXXX (2016),
• Power Ware (2016),
• ZCryptor (2016),
• WannaCrypt (2017)
2.2 Ransomware Type

There are three different ransomware which described below (Heimdal Security, 2017):

- Master Boot Record (MBR) Ransomware, its type of ransomware that overwrites the MBR of the entire hard drive, causing the victim OS (Windows) to crash. This is also the technique of getting around of any security products. If user try to reboot his PC, the modified MBR will prevent him from loading the OS (Windows) normally and instead greeted the victim with an ultimatum to pay up with a certain amount of money (usually in bit coins) or lose access to your files and computer forever (Trend Micro, 2016). Examples include Satana and Petya Ransomware.
- Locker Ransomware, is the type of ransomware that locked the victim out of their operating system, making it impossible to access their files and the OS itself. However, this kind of ransomware doesn’t encrypt the files of the victim, but still demand payment. Examples include WinLocker.
- Encrypting Ransomware, is the most popular and dangerous kind of ransomware which encrypt all the victim’s files with strong algorithms which in many case cannot be decrypted except they pay ransom or gain the master key. Examples include Locky, Crypt Locker, Wannacry, etc.

3. Ransomware Infection Methodology

The method of ransomware infection methods usually follows the same modus operandi used by cybercriminals to infect victims with any malware (Symantec, 2016). There several different methods that’s was popular among the cybercriminal such as:

3.1 Traffic Distribution Method (TDS)

This method implemented a site that hosted an exploit kit (Zeltser, 2015) to be ready for a victim that being redirected from the Traffic Distribution Service which cybercriminal bought from the TDS vendor. This method usually accompanied by a drive-by download method.

3.2 Malvertisement

Maladvertisement or malicious advertisement put a mislead or click bait advertisement to a site that hosted an exploit kit to infect the user that brave enough to click it.

3.3 SPAM Email

This method by far is the most successful method of delivering the malicious ransomware to the potential victim (Trend Micro, 2016; Trend Micro, 2016; Trend Micro, 2016). This old-fashioned method uses an email that looks like a legitimate email from victim’s boss, colleague or other legitimate services that point to a malicious site that host an exploit kit or using social engineering technique to leverage user to download or install malicious software.

3.4 Downloaders & Botnet

This method usually tricks the users to download a look alike legitimate software that in background download a secondary Trojan that infect the users.

3.5 Social Engineering & Self-Propagation

Some of ransomware has the ability to spread worm like method. WannaCry is the latest examples that utilize such techniques, as explained in the Microsoft Analysis report. Microsoft hasn’t found evidence of the exact initial entry vector used by this threat, but there are two scenarios that they believe are highly possible explanations for the spread of this ransomware (Microsoft, 2017):

- Arrival through social engineering emails designed to trick users to run the malware and activate the worm-spreading functionality with the SMB exploit
- Infection through SMB exploit when an unpatched computer is addressable from other infected machines
4. Ransomware Business Model & Monetization

4.1 Ransomware Traditional Business Model

FBI estimation in 2016 stated that ransomware would be cybercriminal $1 billion source of income in 2016 (CNN, 2016). This number achieved because 70% of the ransomware victim are choosing to pay the perpetrator in order to get their data back (IBM X-Force, 2016). The traditional business model is to send phishing mail to the company and public services agency such as hospital, mass transport operator, hotel, etc. This step is taken by cybercriminal to raise the chance of being paid, because of the nature of their business. However, cybercriminal targeted more on the medium and large company rather than small company by 50% (IBM X-Force, 2016).

After successfully infected the victim and encrypt the files, the cybercriminal is asking certain amount of money to the victim to a certain bit coin wallet.Bitcoin is a decentralized digital currency peer-to-peer payment network, meaning neither does it have central authority, nor does it have a central bank, and there are also a finite number of bit coins in the world (Bitcoin Organizations, 2017). Although it is not completely anonymous, there is an element of privacy involved in bit coin as well as it being almost impossible to counterfeit, immune to fraudulent chargeback’s and transactions being irreversible. This reason, as well as the global use of the currency, has led to concerns that it is a perfect currency for cybercriminals (Metro, 2017).

Ransomware outbreak is also one of the factors that raised the demand of crypto currency such as Bit coin (Vox Media, 2017). In 2017 Bit coin value raise in the breaking record of $ 2400 per 1 Bit coin, this number raised around 500% from the 2016 (BitStamp, 2017). With some ransomware have success rate around 40% (IBM X-Force, 2016), cybercriminal could be milking more from this kind of method in the future.

4.2 Ransomware As A Service

The cybercriminal doesn’t stop innovating only on creating a new and better ransomware, but also creating another business model regarding the ransomware. The Ransomware as a Service (RaaS) is a cybercriminal service to offer a profit sharing for a individual to take advantage of ransomware without having minimum or zero knowledge of technical ability such as programming to be able to launch a ransomware attack(Manky, 2013) (Trend Micro, 2016). This type of business model opens a new opportunity for insider threat or any individual that has money to purchase the ransomware and start the attack (Trend Micro, 2016).

There are currently two types of this kind of RaaS in the market, called Stampado and Jigsaw. This two is already sold in the underground market for any individual to purchase to as low as $39 (Trend Micro, 2016). Even Stampado has an online YouTube video to promote their ransomware.

5. Conclusion

In this paper, we learn about the history, evolution, infection method and the business model of the ransomware. The biggest ransomware outbreak in history is WannaCry that spread in 150 countries with hundreds of thousand computer infections. In order to handle this kind of cyber-attack, we need to work together as a team. Awareness is the most important things to be acquired since the most effective method to deliver the infection is through phishing. The second one would be patching management that needed to be enforcing, since the ransomware attack based on the vulnerability of the unpatched system. The third one would behave backup plan both online and offline, and taking steps to protect it.

The future of ransomware may infect your smart devices since most of technology innovations leads to such things, such as smart TV, smart refrigerator, etc. The challenge is how fast our security behavior adapts with such threat.

References


