**Use of Cryptology in Ransomware**

October 22, 2017 by Theresa Nguyen

You’ve done it. You either downloaded a file, opened a Hyperlink in your email, or accidently click on an advertisement containing malware. Except, it is more threatening, demanding payment through Bitcoin to decrypt your personal and critical files. You got seventy-two hours to pay the attackers before you lose your files forever. The countdown begins. Will you pay the attackers to get your files back?

First, there are some terms that needs to be cleared up: malware and ransomware. For those of you who are unfamiliar, malware may be annoying or malicious. It intends to infiltrate and damage a computer system without the owner’s knowledge. Ransomware, on the other hand, aims to steal its victim’s information. It notifies the user that they have been attacked. The victim’s hard drive and files have been encrypted. Then, the attacker will demand some sort of payment, usually through Bitcoin, to restore the computer to its previous state. Though, chances of restoration by the attacker are unlikely.

**What is Bitcoin and Why?**

Since the rise of Bitcoin, ransomware attacks have become quite profitable. What is bitcoin? As stated by Wikipedia, “Bitcoin is a worldwide cryptocurrency and digital payment system.” You can store an online wallet, trade with other currencies, and spend bitcoin, yet each transaction is anonymous. Thus, the mix of malware, encryption, and bitcoin makes the perfect situation for the attacker.

**A Little Background: Crypto-Ransomware**

The term Crypto-Ransomware is an umbrella term used to categorized ransomware that used cryptology in its malic deeds. These ransomwares fully intends to kidnap your data. The malware can enter the targeted organization or individual through “backdoors”—current malware on the system--or Trojans, which are malwares disguise in emails or advertisements. Once in the system, encryption is used to capture the victim’s data and disrupt critical system files. The ransomware communicates back to its command and control server. A command and control server is where attackers are able to coordinate the actions of infected computers on a compromised web server. Thus, attackers ultimately hold full control to delete your data and the key to decrypt it.

Generally, these attackers use a duel encryption, symmetric and asymmetric encryption, for performance and convenience. In symmetric encryption, there is a single secret key that is used in both encryption and decryption. The benefits of this encryption is its performance. As for asymmetric encryption, there is a private key that is known by the owner, and the public key may be known to anyone else. The public key is used in encryption while the private key is used in decryption. Asymmetric encryption is great as it is convenient for the attacker to keep one key instead of multiple keys for each victim. To achieve the best performance, crypto-ransomware used both symmetric and asymmetric encryption.

Unfortunately, there are multiple ransomware spreading rampant on the Internet. Thus, this will be a survey on a few ransomwares. These ransomwares will be compared to each other from least to extremely malicious.

**FSociety Ransomware**

Inspired by the show Mr.Robot, this ransomware is still in its early stages of development. At the moment, it is harmless. It tricks users into clicking its files by disguising itself with the Adobe PDF file icon. Without careful look at the file’s extension, a victim will click on the .exe file. The file is activated and encrypts files using an AES encryption. Additionally, an RSA key is then created to decrypt them.

Based on EDA2—the open source code to create ransomware, the malware will perform a broad search through a computer’s file system with its function call “walk\_\_drive()”. Then, it locates specific files to encrypt. Encrypted files are modified with “.fs0ciety” extension. Finally, the ransomware demands payment through Bitcoin through its own sub-function and changes the desktop background to the logo of the hacking group in Mr.Robot.

It has been reported that the instructions for payment appear to be incomplete. The ransom, overall, simply encrypts a few files with a simple encryption and locks them. Even so, it does contain the potential to be dangerous in the future.

**CryptoLocker**

It is rumored that this ransomware appeared in September 2013, targeting Windows computers. Concealing itself via email, CryptoLocker uses a Trojan horse to infect a victim’s computer. It is different from the usual ransomware. It allows infected computers and its software to continue working, but gaining access to personal files, documents, photos, etc. are unlikely as they are now encrypted with an RSA public-key encryption. The key to unlock the files is not located on the infected computer. Rather, the only copy is on the attacker’s server.

Then, CryptoLocker provides the victim a short time limit –seventy-two hours or three days—to purchase the decryption key. Nevertheless, the victim should not pay the attackers as it is not guaranteed that the decryption key will be delivered.

**CryPy**

In late 2016, CryPy was discovered by Jakub Kroustek. This ransomware, written entirely in Python, hides its command and control server behind a compromised web server in Israel. It is composed of two main files: boot\_common.py and encryptor.py. boot\_common.py performs error-logging on Windows platform while encryptor.py locks down the files. Once infected, the computer’s registry policies are overwritten, system recovery tools are disabled, and boot status policy is set to ignore.

What is interesting about this ransomware is that it assigns a unique key or token to each file. After file encryption takes place, the names of the files are sent to the command and control (C&C) server. The C&C will then send back the new name for the file and its unique key that will be used to encrypt the file’s contents.

To inspire hope in the victim, the attackers will offer a few free unlocks to convince the victim of their “good intentions”. Attackers will continue their teasing before demanding full payment to prevent file deletion.

**WannaCry**

In May 2017, a ransomware attack spread worldwide. The culprit of the attack is WannaCry. From what is known, over 200,000 victims and 300,000 computers have been infected. WannaCry appeared after the USA’s National Security Agency found a vulnerability in Microsoft’s software—EternalBlue.

EternalBlue refers to the software vulnerability found on Microsoft’s Windows operating system earlier this year. The vulnerability originates from the Microsoft Server Message Block (SMB). The SMB provides a variety of services including: file sharing, printer sharing, giving access to remote Windows services, etc. Most dangerously, it allows applications to read and write to files if they are on the same network. It conducts its functions over TCP ports 139 and 445, leaving the WannaCry ransomware to scan for these ports. As a result, if a host if using one of these ports, it is now vulnerable. WannaCry ransomware takes advantage of this flaw and infects Windows machines by downloading itself on to the host—through a Trojan. Eventually, the WannaCry ransomware spreads itself on the network.

WannaCry ransomware uses an RSA-2048 algorithm. This particular algorithm encrypts data, but it is not decryptable. A perfect one-way street. Once encryption is finished, WannaCry notifies the infected user that the starting price for recovery is $300USD via Bitcoin. After seventy-two hours, the price doubles. Finally, after seven days, WannaCry begins file deletion. Best way to get files back is to hope that you have stored them in an external hard drive or on a cloud.

**What To Do Once Infected**

Do not pay them. It encourages the attackers. There is no guarantee that the attackers will give you back your data. Once you pay them, you become a regular target. The next ransom you will have to pay will not be cheap.

**Prevention**

* **Keep regular backups of your most important files**

Make sure these backups are stored offline. If they are online, well, they will be discovered.

* **Use an anti-virus program and keep it up to date**

By updating or running these anti-virus programs, they catch less malicious malwares that are hidden on your computer. They take away the chances of ransomwares entering via “backdoors”.

* **Keep your operating system up to date**
* You always get those annoying notifications to update the software or that there are new software updates that need to be installed. There is an important reason for that. With each update, the operating systems are patching up previous vulnerabilities in the software. These patches will prevent malware from entering your computer. They are not installing new features for you.
* **Review the access control settings on any network shares you have**

Don’t grant yourself or anyone else write access to files you only need to read.

Don’t grant yourself any access at all to files that you don’t need to see.

* **Do not give administrative rights**

You potentially give more power to the malware. Simply put.

**References**

Abrams, Lawrence. “The Week in Ransomware - September 9th 2016 - CryPy, CryLocker, Philadelphia, and More.” BleepingComputer, BleepingComputer.com, 10 Sept. 2016, [www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-9th-2016-crypy-crylocker-philadelphia-and-more/](http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-9th-2016-crypy-crylocker-philadelphia-and-more/)

Biddle, Susan. “Take It Easy, and Say Hi to This New Python Ransomware.” Fortinet Blog, 1 Sept. 2016, blog.fortinet.com/2016/09/01/take-it-easy-and-say-hi-to-this-new-python-ransomware?linkId=28324943

Bonderud, Douglas. “CryPy Ransomware Slithers Onto PCs With Unique, Python-Based Encryption.” Security Intelligence, 17 Oct. 2016, securityintelligence.com/news/crypy-ransomware-slithers-onto-pcs-unique-python-based-encryption/

Cassius Puodzius posted 13 Sep 2016 - 01:45PM. “How Encryption Molded Crypto-Ransomware.” WeLiveSecurity, 13 Sept. 2016, www.welivesecurity.com/2016/09/13/how-encryption-molded-crypto-ransomware/.

“CryptoLocker.” Wikipedia, Wikimedia Foundation, 18 Oct. 2017, en.wikipedia.org/wiki/CryptoLocker

“CryptoLocker Ransomware – See How It Works, Learn about Prevention, Cleanup and Recovery.” Naked Security, 3 June 2014, nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/

Ducklin, Paul. “CryptoLocker Ransomware – See How It Works, Learn about Prevention, Cleanup and Recovery.” Naked Security, 3 June 2014, nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/

Fung, Brian. “What You Need to Know about Bitcoin after the WannaCry Ransomware Attack.” The Washington Post, WP Company, 15 May 2017, [www.washingtonpost.com/news/the-switch/wp/2017/05/15/what-you-need-to-know-about-bitcoin-after-the-wannacry-ransomware-attack/?utm\_term=.1eb412e2afd8](http://www.washingtonpost.com/news/the-switch/wp/2017/05/15/what-you-need-to-know-about-bitcoin-after-the-wannacry-ransomware-attack/?utm_term=.1eb412e2afd8)

GoldSparrow. “FSociety Ransomware.” Remove Spyware & Malware with SpyHunter - Enigma Software Group USA LLC, 26 Aug. 2016, [www.enigmasoftware.com/fsocietyransomware-removal/](http://www.enigmasoftware.com/fsocietyransomware-removal/)

Help Net Security. “Crypto-Ransomware Attacks Hit over 700,000 Users in One Year.” Help Net Security, 27 June 2016, [www.helpnetsecurity.com/2016/06/24/crypto-ransomware-attacks-hit-700000-users/](http://www.helpnetsecurity.com/2016/06/24/crypto-ransomware-attacks-hit-700000-users/)

Ido Naor, Noam Alon on October 13, 2016. 9:26 am. “CryPy: Ransomware behind Israeli Lines.” Securelist - Information about Viruses, Hackers and Spam, 13 Oct. 2016, securelist.com/crypy-ransomware-behind-israeli-lines/76318/

Islam, Ali. “SMB Exploited: WannaCry Use of ‘EternalBlue’ « Threat Research Blog.” FireEye, 26 May 2017, [www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html](http://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html)

News, Ransomware In the, and Fightransomware. “Ransomware Roundup: Mr. Robot Inspires New FSociety Ransomware Virus.” FightRansomware.com from Carbonite, fightransomware.com/ransomware-in-the-news/ransomware-roundup-mr-robot-inspires-new-fsociety-ransomware-virus/

Paganini, Pierluigi. “CryPy Ransomware Uses a Unique Key for Each Encrypted File.” Security Affairs, 16 Oct. 2016, securityaffairs.co/wordpress/52360/malware/crypy-ransomware.html

Rashid, Fahmida Y. “4 Reasons Not to Pay up in a Ransomware Attack.” InfoWorld, InfoWorld, 14 Mar. 2016, [www.infoworld.com/article/3043197/security/4-reasons-not-to-pay-up-in-a-ransomware-attack.html](http://www.infoworld.com/article/3043197/security/4-reasons-not-to-pay-up-in-a-ransomware-attack.html)

Symantec Security Response. “What You Need to Know about the WannaCry Ransomware.” Symantec Security Response, 12 May 2017, www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

“WannaCry Ransomware Attack.” Wikipedia, Wikimedia Foundation, 17 Oct. 2017, en.wikipedia.org/wiki/WannaCry\_ransomware\_attack

“WannaCry.” Malware Wiki, malware.wikia.com/wiki/WannaCry

Woodberg, Brad. “Malwre Command and Control Channels-a Journey into Darkness”. <https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Brad-Woodberg-Malware-Command-And-Control-Channels-A-Journey-Into-Darkness.pdf>