SoK: Ransomware: Categories, infection vectors, traits, attack structure and mitigations

Omer Mujtaba, 40137495
CIISE, Concordia University
Montreal, Canada
o_mujtab@encs.concordia.ca

***Abstract*—Ransomwares are a global threat today, starting from the 'AIDS Trojan' in 1989 till the most recent 'Tycoon' the cyber extortion world has seen many variants; each being more advanced and lethal from its predecessor. They are alone responsible for millions of dollars in losses to the global economy, making them the game-changer for many cyber criminals and APT groups.**

Ransomwares started off being opportunistic attacks with the mere intentions of locking the user from its computer causing a DOS, to being more complex cryptographic attacks, encrypting all or most of user data and denying user from accessing it, to the blend of both; by locking and encrypting at the same time making it the most efficient of all. The end goal is monetary gains which were limited to eGift cards in the beginning, but later pivoted towards digital cash or Bitcoins. To thrive against such attacks, it is mandatory to be aware of ransomwares, how they are delivered, what is the structure of the attack and best practices to keep individuals and enterprises save.

In this report we will present with classification of ransomwares, their infection vectors, traits and attack structure, and mitigations. Moreover, the report will also analyze WannaCry ransomware and its lifecycle.

***Keywords*—Ransomware, Locker, Crypto, WannaCry, infection vectors, traits, attack structure, best practices, mitigations**

I. Introduction

In today's world, 'user data' is the most precious entity for an individual or an organization. Therefore, cyber criminals, and Advanced persistent groups (i.e. APTs) are after it round the clock. Cyber-crime has continued to grow with the attackers getting more innovative every passing day [1]. Typically, the motivation behind are the monetary gains and the influx of digital currency served as the paradise. One of the hottest and most feared cyber-attack is the ransomware, as the damage caused by these types of attacks seems to be computationally impossible to revert. Here the adversary leverages top-notch cryptographic algorithms to encrypt victim's data which can be only decrypted through the key provided by the adversary upon receiving the ransom which is usually in from of Bitcoins. As the ransomware matured, the target audience pivoted from being single victims to enterprises where the data in question is of more sensitive in nature hence the success rate is much higher [2]. Moreover, one-click solutions like Ransomware-as-a-service depicts the heights of success in this landscape; these can be used by anyone to build their own version easily. [3] [4]

Ransomware are not new; they have been around for quite a while. The first ever ransomware was created by Dr. Joseph Popp in 1989. It was named the 'AIDS Trojan' or 'PC Cyborg Trojan' and got distributed over a floppy disk during a health conference about AIDS [5]. The ransomware effected over twenty thousand computers. Earlier versions did not made use of the encryption, they were more sort of locker-ware where the infected system is locked from the user access without damaging any of the user data. As ransomware evolved, industry standard encryption techniques started showing up, now the goal was not to lock the system but to encrypt all or most of the user files and make them inaccessible. Enterprises, hospitals and individual users must know how vulnerable they are to these types of attack. Therefore, familiarity with diverse categories and infection vectors is evident in order to perform competent mitigations and preventions.

Owing to abovementioned, this paper briefly presents the categories of ransomwares based on objectives, techniques and extent of damage, infection vectors, and the mitigations proposed by academics, researchers and cyber firms. The rest of the paper is organized as follows: Section II classifies ransomware among two major categories, Section III talks about multiple infection vectors, whereas attack structure for ransomware is stated in Section IV, Section V takes WannaCry as a case-study to describe the lifecycle of a ransomware. At last, Section VI provides with mitigation and best practices to protect against the ransomwares.

II. Classification

In 2018, over 545,231 malware variants were reported, 100,907 were target at the consumer, whereas 444,259 were targeted at the enterprises [6]. Ransomwares can be broadly classified among two categories i.e. Locker and Crypto.

A. Locker Ransomware

Locker ransomware as the name suggests locks the device and deny user access without modifying any files on the system. A ransom message is typically displayed across the screen that demands payment; access is only granted once the ransom is paid.

An example of the locker ransomware is 'Reveton' that appeared in 2012, it locked the users' computer and prevented them from logging back in. In addition, it displayed a message that was pretended to be from FBI or National police. The

message said that the user was caught doing illegal activities such as child pornography or piracy, and to avoid any further action they must pay a fine. [7]

B. Crypto Ransomware

Crypto ransomware uses highly sophisticated cryptography algorithms to quietly search and encrypt users' files and later ask for a ransom to get the decryption key. Crypto ransomware can either encrypt the complete hard-disk or they can search for specific file extensions like .doc, .jpg, .pdf etc., these files usually tend to contain valuable and/or personal data that affects the user the most.

Initially, symmetric encryption techniques were used to encrypt the data. They didn't do quite well as the key must be stored inside the malicious code which can be easily retrieved by reverse engineering. Later, attackers started using asymmetric or public-key encryption techniques, here the public key was hardcoded inside the malicious code, which is used to encrypt the data, whereas the private key is kept with the adversary which they only reveal upon the ransom being paid. Today, encryption standards like RSA and AES are used in the wild [8]. Modern ransomwares have introduced the concept of command and control (C2) which is usually a botnet of compromised hosts hidden behind a TOR network owned by the adversary. Due to advancement in antivirus solutions and the placement of sophisticated signature-based indictors of compromise [5], ransomware scripts usually do not contain the actual malware inside. Upon infecting the system, the scripts communicate with the C2 network and downloads the actual payload and keys for encryption [8].

Any example of crypto ransomware is Petya, it first appeared in 2016. The ransomware encrypts the entire hard drive by encrypting the Master file table (MFT), making file access impossible. Petya spread through a fake job application email with an infected Dropbox link. Petya resurged with a new alias GoldenEye in 2017, this time targeting larger enterprises such as oil producers, nuclear plants and banks. It infected over 2000 targets and caused millions in loses. [9]

III. Infection Vectors

Attackers use several techniques to install the ransomware on users' computers, several common techniques are discussed below:

A. Phishing/SPAM emails

The primary infection vector for ransomware is through malicious emails, attackers will use techniques such as spear phishing to send a malicious email with a link or an attachment to the malware. They will somehow lure the victims into opening the file which in turns downloads the malware, and the systems get compromised. In cases, such as P2P networks, ransomwares are strong enough to spread across multiple systems.

B. Exploit Kit

Exploit kits are such toolkits that are capable to automate the exploitation of a software vulnerability. Attackers will inject rogue advertisements on reputable websites to attract large audiences, the advertisement will direct the user to the attacker's malicious website. The exploit kit (e.g., Magnitude, Angler, Neutrino, and Nuclear [10]) identifies vulnerabilities in the browser. If it is found vulnerable it will leverage that to download the ransomware. Stats shows that 20% of exploits in Angler are related to Internet Explorer whereas 75% are of Adobe Flash. [11]. 'WannaCry' ransomware fell under exploit kit, it propagated through a dropper component named as Eternal Blue that identifies vulnerability in the SMB protocol, it enabled the attackers to infect all unpatched and vulnerable windows machines. [12] [13]

C. Downloaders and Trojan Botnets

Downloaders that downloads the software from the software-hosting website will often have a hidden functionality to download the malware without user notice or consent.

D. Malvertising

Malicious advertising is a method using by attackers to inject malicious advertisements in trusted websites. Often, there is no need to open the ad, the malvertised page will itself connect to several URL that will lead towards malware infection [14].

E. Traffic Distribution Systems

Traffic distribution systems – also known as TDS – buy and sell web traffic and are used to direct web users from one website to another. Attackers buy this traffic to direct users to their website that contains the exploit kit, if the exploit kit successfully exploits the vulnerability in the victims's computer it can be easily infected with the malware.

IV. Traits and Attack Structure

Just like other malwares, ransomwares present number of distinct traits. They can be organized in six categories listed below:

- Payload persistence - It is evident for a ransomware to be persistent. It is achieved by leveraging the startup folder. Usually the trick is to either place an executable or scheduling a startup task.
- Prevent system restore - A ransomware will always prevent the system from rolling back to changes, this is achieved by deleting any shadow copy saves.
- Stealth - Stealth is the key for a ransomware to avoid any detection and cause maximum damage, it will achieve this by injecting itself into legitimate process or name executable file after other popular process.
- Environment mapping - Ransomware will analyze the system they affect, this lets them determine the targets' value, check if it is a real computer or a virtual environment, and if there are any other possible victims that can be affected over the network.

- Network Connection - Earlier ransomware had everything baked into them, but nowadays, modern ransomware will require an internet connection to download the payloads and communicate with the C2 servers.
- Escalation of privilege - A ransomware will always try to access the root or admin privileges, it is done by either exploiting possible vulnerabilities, or by using techniques such as clickjacking.

Just like the traits, ransomware usually tend to follow an attack structure although due to high volume of ransomware variants this does not apply to all of them.

Listed below are few common steps in a ransomware attack [15]:

1) Delivery: The first step for a ransomware is to get delivered to its intended audiences, attackers will use infection vectors discussed above to execute this phase.
2) Installation: Once the ransomware is delivered, next comes the installations. The malware will run its code to check if it is running on a real machine or a virtual environment, once it is determined that the machine is worth infecting it will establish itself in common Windows process like svchost.exe or lsass.exe to begin next phase i.e. Command and control.
3) Command and Control: C2 infrastructure is usually a botnet of compromised host which sits behind an anonymity network i.e. TOR. This is the most important step in the process, the ransomware tries to establish a connection with the command servers and awaits further instructions. In modern ransomwares, this is the stage where actual payload is delivered, along with other instructions. The instructions include types of files to encrypt, how long to wait before beginning the process, and whether the malware should continue to spread. In some cases, malware might report back the IP address, and information about operating system, installed browsers and antivirus software etc.
4) Encryption: Once the ransomware receives its keys for encryption and instructions about which files to encrypt. The actual damage starts immediately. The malware will iterate through all system directories and will encrypt every file that matches the instructions. Once the encryption is done, the ransomwares now tries to lock the system and make it persistent, this is done by creating a new desktop with limited functionality.
5) Extortion: An extortion message is displayed on the victims' screen here the language is based on the victim's location. It can either be a threat message pretended from some law enforcement accusing of child pornography or piracy, or a simple message stating that the system has been comprised and it can only be recovered once the ransom is paid which is usually in Bitcoins.

V. Case Study: WannaCry - Lifecylce of a ransomware

WannaCry (also known as WCry or WanaCryptor) is an example of crypto ransomware, the ransomware surfaced on 12 May 2017 [16] and affected over 300,00 systems spanning across 150 countries. The targeted sectors included healthcare, government, telecommunication and oil productions [16]. The ransomware is characterized as a self-propagating malware that spreads across internal and public networks by exploiting Microsoft's Server Message Block (SMB) protocol, MS17-010. The malware consists of two distinct modules, one provides with the ransomware functionality whereas the other is used to propagate using an exploit named as EternalBlue. The malware encrypts the files with a .wcry extension, and demands a ransom of $300-$600 in bitcoins [17].

TABLE I
WannaCry files characterstics

Filename	Description	File Type
mssecsvc.exe	Loader + Worm Component	EXE
tasksche.exe	Loader	EXE
Unavailable	Encryptor	DLL
@WanaDecryptor@.exe	Decryptor	EXE

Aforesaid, we will analyze the WannaCry ransomware in detail, including startup, installation, configuration, encryption and decryption.

A. Startup

The worm component of the malware starts its journey by attempting a connection to the following domain using the InternetOpenUrl function:

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

This domain is a kill-switch (see Appendix A). In other words, if the connection is successful, the malware halts its execution, else it will check for the number of arguments passed, if that is zero the malware continues its execution and registers itself as a "Microsoft Security Center (2.0) Service" mssecsvs2.0 process on the infected machine otherwise it will enter the service mode [18].

B. Installation

The ransomware undergoes following steps of installation.

1) Create and start a service named mssecsvc2.0.
2) Locates R resource, move it to the memory and write the data to C:\WINDOWS\tasksche.exe
3) Executes C:\WINDOWS\tasksche.exe with /i command.
4) Move C:\WINDOWS\tasksche.exe to C:\WINDOWS \qeriuwjhrf and replace the original file if exists.
5) Create an entry in Windows Registry with a unique identifier (8-15 random lowercase characters followed by 3 numbers e.g. midtxzggq900)
6) 'tasksche.exe' component writes itself having the random generated name to the AppData directory, and also writes itself to AutoRun to establish memory persistence.

C. Configuration

Once the malware is installed and persistence is maintained, now it's time for configuration. WannaCry will now undergo following configuration steps:

1) Load the XIA resource, decompress it, and write to %CD% (current directory).
2) Load config data from c.wnry file, choose and write one of the three available bitcoin address (see Appendix C).
3) Write updated config back to c.wnry file.
4) Set hidden attribute for working directory and grant full access to %CD% and its subdirectories.
5) Import hard-coded RSA private key (see Appendix B) from tasksche.exe process
6) Opens and read %CD%\t.wnry. The first 8 bytes of the file are checked to match the WANACRY! string.
7) Decrypt stored AES key in %CD%\t.wnry using the hard-coded private key.
8) Use the AES key to decrypt and load encryption DLL to the memory. This is the encryption component of the ransomware.

D. Encryption

Now that the malware is configured, it will now start the encryption process as follows:

TABLE II
WANNACRY CONFIGURATION FILES

Filename	Description
00000000.res	TOR/C2 information
00000000.pky	Public RSA key
00000000.eky	Encrypted private RSA key

1) TaskStart export component is invoked, and creates a mutex named "MsWinZonesCacheCounterMutexA" and reads the contents of c.wnry.
2) If mutex exists or c.wnry is not present, the malware halts, else the malware will go ahead and created a mutex named "MsWinZonesCacheCounterMutexA0", reads the content from c.wnry file and create three additional config files i.e. 00000000.res, 00000000.pky, and 00000000.eky.
3) Load and check 00000000.pky and 00000000.dky files exists, if the files does not exists it will generate a new key pair of RSA 2048-bit keys.
4) Export victims' public RSA key to 00000000.pky file.
5) Export victims' private RSA key and encrypt with additional hard-coded RSA public key and store as 00000000.eky file.
6) Destroy private key to eliminate any possible recovery.
7) Enumerate every 3 seconds and start encryption process on any new drive, moreover, iterate through all directories and subdirectories to search file extensions of interest (see Appendix D.)
8) Encrypt each file with public RSA key which is encrypted with a 16-byte symmetric AES key. Encrypted files are renamed and appended with .wncry extension.
9) Launch a parallel thread that calls taskse.exe process every 30s and enumerate active RDP sessions on connected remote machines.
10) Launch another thread with @WanaDecryptor@.exe file, fetch updated bitcoin address from server and update c.wnry file.
11) Copy u.wrny to @WanaDecryptor@.exe and create @WanaDecryptor@.exe.lnk.
12) Create and write content of r.wnry to @Please_Read_Me@.txt
13) Copies @Please_Read_Me@.txt and @WanaDecryptor@.exe to every encrypted directory.
14) Once encryption is complete and Microsoft Exchange, SQLServer, and SQLWriter processes are killed.
15) Copy b.wnry to @WanaDecryptor@.bmp and place it in each user's desktop folder, as well as a copy of @WanaDecryptor@.exe.

At last, a window (Fig. 1) is displayed to the user indicating that files have been encrypted and a ransom must be duly paid in order to receive the decryption key and recover the lost data.

Fig. 1. WannaCry message

E. Decryption

The malware communicates with an onion server using a TOR running on local host TCP port 9050. The malware will now register the affected system with the onion server, transfer the encryption keys and delete any shadow volume. Once the user pays the ransom, the malware obtains corresponding RSA private keys from the onion server and decrypts the files.

VI. MITIGATION AND BEST PRACTICES

As discussed in the above mentioned case study, ransomwares can be a nightmare for enterprises and individuals. Enterprises have had paid millions in ransoms [8] which makes it evident that prevention is better. The fundamental reason of

prevention rather than mitigating the effects is; getting rid of ransomware does not restore the data. Therefore, it is in the best interest to keep it away from the systems at the entry point. Third-party pivots (i.e. emails, malvertising and social engineering) and Direct attack via vulnerability exploitation are two of the most common ways a ransomware enters the system.

A. Third-party Pivots

Emails are the vital source of communication for enterprises and individuals. Attackers will often try to leverage them to deliver ransomware to victims. The most effective way to secure is to introduce strong spam filter and intelligence-based intrusion detection systems. Spam filters should be implemented on the network level, whereas intelligence-based IDS should be applied at the host level. IDS should be able to detect and prevent ransomware payloads identified using digital signatures and also malicious link that might redirect to external links. The links can also be provided to spam filter to improve its policies.

The spam filters and detection systems are only as good as the signatures and IOCs provided to them; therefore, it is crucial that trainings should be provided on individual level to mitigate these risks. Employees should be trained with the attackers' intentions and the ways they try to affect the systems. Afterall, a ransomware hiding behind a link or in an attachment will remain inactive as long as it is clicked.

B. Vulnerability Exploitation

WannaCry, one of the deadliest ransomware propagated through a vulnerability in the SMB protocol of Window 7 and earlier. Attackers are now well aware of the intrusion detection and antivirus system in place and they tend to search for other alternatives. They tend to find loopholes and backdoors in the targeted system by exploiting any found vulnerabilities in the system. These vulnerabilities are usually seen in unpatched, old or misconfigured systems. The only mitigations for this is to have policies in place for recurring vulnerability assessments and penetration tests. Any known or found vulnerability should be immediately reported and patched, this practice should be strictly implemented on both network devices and workstations.

C. Offline and Cloud Backups

If the data is backed up, there is no need to pay a ransom to get the data back. Instead, it can be recovered from the backups [15]. With that being said, it should be noted that multiple ransomwares encrypt locally connected backup systems, those files are placed in the current backup system which halts the restoration process completely. Morever, a ransomware might delay its revelation and encrypt days or months of data. Therefore, it is advised to keep multiple offline and cloud backups in place that can significantly reduce the risk of data loss.

VII. Conclusion

In conclusion, ransomware can be a traumatic for individuals and enterprises, as we discussed, attackers are getting smarter each passing day, use of modern cryptographic technologies is evident. As discussed in the WannaCry case study, ransomwares tend to be complex and extremely nifty. It is simply impossible to keep yourself or your enterprise secure by relying on the antivirus softwares; they are as good as the signatures and IOCs provided to them. Therefore, it compulsory for individuals and enterprises to keep their systems and devices up-to-date, moreover, trainings on individual levels can prove worthy in terms of securing from social engineering attacks.

References

[1] P. Hunton, "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model," *Computer Law Security Review*, vol. 25, pp. 528–535, 2009.

[2] W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the internet: Attacks, costs and responses," *Inf. Syst.*, vol. 36, no. 3, p. 675–705, May 2011. [Online]. Available: https://doi.org/10.1016/j.is.2010.11.003

[3] A. Young and M. Yung, "Cryptovirology: Extortion-based security threats and countermeasures," in *Proceedings of the 1996 IEEE Conference on Security and Privacy*, ser. SP'96. USA: IEEE Computer Society, 1996, p. 129–140.

[4] A. L. Young and M. Yung, "Cryptovirology: The birth, neglect, and explosion of ransomware," *Commun. ACM*, vol. 60, no. 7, p. 24–26, Jun. 2017. [Online]. Available: https://doi.org/10.1145/3097347

[5] I. Yaqoob, E. Ahmed, M. H. u. Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the internet of things," *Comput. Netw.*, vol. 129, no. P2, p. 444–458, Dec. 2017. [Online]. Available: https://doi.org/10.1016/j.comnet.2017.09.003

[6] "ISTR: Internet Security Threat Report," Symantec, Tech. Rep. Volume 24, 2019. [Online]. Available: https://docs.broadcom.com/doc/istr-24-2019-en

[7] P. Rubens, "Common Types of Ransomware," Mar. 2017. [Online]. Available: https://www.esecurityplanet.com/malware/types-of-ransomware.html

[8] A. Zimba and M. Chishimba, "Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures," *International Journal of Computer Network and Information Security*, vol. 11, pp. 26–39, 2019. [Online]. Available: http://mecs-press.com/ijcnis/ijcnis-v11-n1/IJCNIS-V11-N1-3.pdf

[9] K. Zetter, "4 Ways to Protect Against the Very Real Threat of Ransomware," *Wired*, May 2016. [Online]. Available: https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/

[10] J. C. Chen and B. Li, "Evolution of exploit kits - exploring past trends and current improvements," TrendMicro, Tech. Rep. [Online]. Available: https://331.cybersec.fun/exploit-kits.pdf

[11] N. Biasini, "Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually From Ransomware Alone." [Online]. Available: https://talosintelligence.com/angler-exposed

[12] R. Brewer, "Ransomware attacks: detection, prevention and cure," *Network Security*, vol. 2016, no. 9, pp. 5 – 9, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485816300861

[13] I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the internet of things," *Computer Networks*, vol. 129, pp. 444 – 458, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128617303468

[14] A. Bhardwaj, V. Avasthi, H. Sastry, and G. V. B. Subrahmanyam, "Ransomware Digital Extortion - A Rising New Age Threat," *Indian Journal of Science and Technology*, vol. 9, Apr. 2016. [Online]. Available: https://www.academia.edu/26701552/Ransomware_Digital_Extortion_-_A_Rising_New_Age_Threat

[15] M. H. Salvi and M. R. Kerkar, "Ransomware: A cyber extortion," *Asian Journal For Convergence In Technology (AJCT)*, vol. 2, no. 2, Dec. 2017. [Online]. Available: http://asianssr.org/index.php/ajct/article/view/55

[16] M. Akbanov and V. Vassilakis, "Wannacry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," *Journal of Telecommunications and Information Technology*, vol. 1, pp. 113–124, 04 2019.

[17] A. Berry, R. Eitzman, and J. Homan, "WannaCry Malware Profile," May 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html

[18] M. Akbanov and V. Vassilakis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," *Journal of Telecommunications and Information Technology*, vol. 1, pp. 113–124, 2019. [Online]. Available: https://www.researchgate.net/publication/332088162_WannaCry_Ransomware_Analysis_of_Infection_Persistence_Recovery_Prevention_and_Propagation_Mechanisms

APPENDIX A
KILLSWITCH DOMAINS

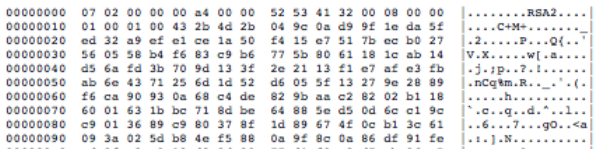
Following are the killswitch domains that can be found on a WannaCry sample:

- iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- ayylmaotjhsstasdfasdfasdfasdfasdfasdf.com
- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.test

APPENDIX B
WANNACRY BITCOIN ADDRESSES

- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

APPENDIX C
WANNACRY PRIVATE KEY



```
00000000  07 02 00 00 00 a4 00 00  52 53 41 32 00 08 00 00  |........RSA2....|
00000010  01 00 01 00 43 2b 4d 2b  04 9c 0a d9 9f 1e da 5f  |....C+M+.......|
00000020  ed 32 a9 ef e1 ce 1a 50  f4 15 e7 51 7b ec b0 27  |.2.....P...Q{..'|
00000030  56 05 58 b4 f6 83 c9 b6  77 5b 80 61 18 1c ab 14  |V.X.....w[.a....|
00000040  d5 6a fd 3b 70 9d 13 3f  2e 21 13 f1 e7 af e3 fb  |.j.;p..?.!......|
00000050  ab 6e 43 71 25 6d 1d 52  d6 05 5f 13 27 9e 28 89  |.nCq%m.R.._.'.(.|
00000060  f6 ca 90 93 0a 68 c4 de  82 9b aa c2 82 02 b1 18  |.....h..........|
00000070  60 01 63 1b bc 71 8d be  64 88 5e d5 0d 6c c1 9c  |`.c..q..d.^..l..|
00000080  c9 01 36 89 c9 80 37 8f  1d 89 67 4f 0c b1 3c 61  |..6...7...gO..<a|
00000090  09 3a 02 5d b8 4e f5 88  0a 9f 8c 0a 86 df 91 fe  |.:.].N..........|
000000a0  cd 9f a3 a0 13 d3 2d 30  77 d1 f0 a8 d7 ab 96 e5  |......-0w.......|
000000b0  48 96 37 03 69 64 97 06  5c 27 50 8c 91 76 67 85  |H.7.id..\'P..vg.|
000000c0  3a 6c 6a b2 59 12 0a 61  f2 a1 ee a8 24 c8 e4 b1  |:lj.Y..a....$...|
000000d0  11 6d d6 cc f7 8f 4c 5e  b0 55 84 81 6d 60 45 84  |.m....L^.U..m`E.|
000000e0  0f fc df f9 27 a5 52 c9  5b 06 28 a3 de 74 03 d6  |....'.R.[.(..t..|
000000f0  c7 72 66 dc be a4 1e ff  20 96 ed 51 84 00 cc 9c  |.rf..... ..Q....|
00000100  36 64 f2 85 4d cf 36 60  dd c8 b0 f1 91 db 7a 0b  |6d..M.6`......z.|
00000110  83 ee cf ef 19 d7 12 da  ae 86 d9 f9 0e be 02 af  |................|
00000120  78 f3 5b 49 be 0c 98 af  b5 5f d6 8a 4c 05 48 64  |x.[I....._..L.Hd|
00000130  9c 40 e1 1c f9 3c c4 e4  42 08 2d b2 b8 8a e6 0b  |.@...<..B.-.....|
00000140  6d df 93 cc 34 e8 48 30  93 5d df 8d 2e b3 3d 35  |m...4.H0.]....=5|
00000150  e4 66 30 ad 8b e7 20 3d  e0 c9 d9 6c 36 4b 79 b9  |.f0... =...l6Ky.|
00000160  64 cd bc 5e 24 48 d4 88  90 1c 3d 17 4e 65 0c ec  |d..^$H....=.Ne..|
00000170  fb 1b 2b ec 5c c3 06 d6  6c 39 d8 6c 7e 23 9f 40  |..+.\...l9.l~#.@|
00000180  af 40 61 b4 fb b1 f6 82  cd a1 26 b8 8d c8 38 8f  |.@a.......&...8.|
00000190  94 03 4e fb bb ec 17 5e  dd 46 f7 e7 fb df 25 21  |..N....^.F....%!|
000001a0  ad 35 bd 9b 1d b5 01 3f  4e b0 20 b7 23 36 79 81  |.5.....?N. .#6y.|
000001b0  29 3c de e2 76 d7 e6 1f  9f ea 2d a5 c4 6a aa 40  |)<..v.....-..j.@|
000001c0  30 0d cc fe 58 e9 89 28  cb d7 e4 9c 7b b9 50 17  |0...X..(....{.P.|
000001d0  a7 31 21 3b b4 91 f3 84  a6 bd 9e 03 ca e9 cd ee  |.1!;............|
000001e0  4d 2b 29 fa 02 0f e7 2c  ae 30 bd 85 cc 2d 13 83  |M+)....,.0...-..|
000001f0  12 53 d3 f3 41 4e f5 23  d6 ce 5f 41 cd 81 7c 3b  |.S..AN.#.._A..|;|
00000200  f0 49 81 b8 ee 8d 35 3c  ba ec 92 c7 ee cf 24 63  |.I....5<......$c|
00000210  01 f3 4a f4 d9 da 8b e2  c0 a4 a5 7f da 8f 3c 50  |..J...........<P|
00000220  19 ec c2 33 5a 8f ee 7b  5a e9 83 7a 96 fd 94 4b  |...3Z..{Z..z...K|
00000230  69 50 9a d2 34 d1 09 61  45 96 7d d8 12 5e a8 ae  |iP..4..aE.}..^..|
00000240  7a c0 26 a5 6f d6 e5 64  93 03 13 a3 29 6d 03 24  |z.&.o..d....)m.$|
00000250  f7 c2 89 e9 46 46 72 ab  54 dc d8 c7 75 0f 2d 13  |....FFr.T...u.-.|
00000260  31 e7 6d 88 a1 3e a1 2d  be ff db 94 d1 bd 6d e3  |1.m..>.-......m.|
00000270  c2 55 c7 ca fb 2b 63 31  17 97 42 91 93 21 dd 53  |.U...+c1..B..!.S|
00000280  25 1d 64 c9 95 64 d9 b5  7a 9f a3 ca e2 0f 19 66  |%.d..d..z......f|
00000290  e4 04 b5 4d 6f 5d 33 76  1c e9 20 71 4b 22 e0 55  |...Mo]3v.. qK".U|
000002a0  5e 91 56 54 94 3c 36 3b  fd fe a1 62 d0 df d3 6e  |^.VT.<6;...b...n|
000002b0  95 8b e1 96 ce 4f 7c 78  38 2b 5e 5f 1b 8c 93 80  |.....O|x8+^_....|
000002c0  5a 6d 23 6f 6d f7 19 88  f1 8c 3d 52 1b d8 ab b4  |Zm#om.....=R....|
000002d0  d4 a0 88 0d ac fb 7a fa  c2 35 c4 a7 a9 50 62 4a  |......z..5...PbJ|
000002e0  ac 98 9b 30 e1 59 37 51  0c 6d 28 74 ac 11 d9 70  |...0.Y7Q.m(t...p|
000002f0  38 2c 35 d3 b8 d9 f1 b7  4f a1 34 36 8b 29 61 39  |8,5.....O.46.)a9|
00000300  35 00 70 de 73 e5 d5 1c  bb 5e b8 60 b6 70 49 85  |5.p.s....^.`.pI.|
00000310  79 65 46 7a 94 81 d6 cc  12 05 84 43 40 6d fc 77  |yeFz.......C@m.w|
00000320  55 8e 45 f8 3d b9 87 a7  89 d2 59 28 ce 16 9a 53  |U.E.=.....Y(...S|
00000330  dc 9d 82 93 ad b1 3c b9  a6 2d aa 9d 43 ec e2 7d  |......<..-..C..}|
00000340  ca 32 2f 4f 2d 5f 2e 58  38 77 2e 2b 1b 0a fa fe  |.2/O-_.X8w.+....|
00000350  79 5a 80 e1 8d 23 67 40  ff d3 d3 95 7a 14 be 93  |yZ...#g@....z...|
00000360  1b f8 ef 37 c2 ee c8 bf  59 3c 9c 5d 25 b6 44 ff  |...7....Y<.]%.D.|
00000370  6b 9b e9 b4 fd 59 85 ba  f1 3a 01 05 f1 3e 62 0d  |k....Y...:...>b.|
00000380  7f 1f e2 81 97 66 63 90  20 bb 96 b4 cf 44 c7 7c  |.....fc. ....D.|
00000390  7e 7d 25 2e 31 35 8b 2a  18 ab d2 41 c9 32 aa 4b  |~}%.15.*...A.2.K|
000003a0  ca ef 28 1d bf 2a 9c 1c  36 02 6b 02 0f a7 ed 10  |..(..*..6.k.....|
000003b0  c0 a0 da cf 09 72 59 5b  c6 3c f9 15 7f aa 22 00  |.....rY[.<....".|
000003c0  72 e0 a5 5c 79 06 6e 62  35 33 89 56 ab 5f f1 fd  |r..\y.nb53.V._..|
000003d0  93 62 4e 81 1e 3d fc 05  69 a4 2f 51 1b e2 c8 0e  |.bN..=..i./Q....|
000003e0  a6 86 a2 bf 9d a4 9c b3  dc 89 b3 e3 b0 f0 d7 60  |...............`|
000003f0  d6 6c de 69 1e c9 b0 02  85 96 d7 35 86 36 16 5b  |.l.i.......5.6.[|
00000400  e6 05 e1 f9 0b ed 25 80  e0 0a 04 c5 96 5d 34 6c  |......%......]4l|
00000410  4c f0 e0 c7 b7 8a 90 3c  98 a2 7a 92 ea 51 e9 05  |L......<..z..Q..|
00000420  ec 7d 3c c9 cd aa b6 66  b3 db 48 cf 7d fb 6d dd  |.}<....f..H.}.m.|
00000430  04 b9 1b 97 9e be e1 58  66 fd e9 70 ac f9 ff b6  |.......Xf..p....|
00000440  23 17 fd f0 35 0c 41 3a  38 9a 2f 3f 16 2a e8 a9  |#...5.A:8./?.*..|
00000450  73 30 7c 38 c9 c4 7e c6  68 a4 78 fe 6d 00 28 4e  |s0|8..~.h.x.m.(N|
00000460  33 87 e5 b6 c9 c5 3d ec  0e 92 03 eb 15 9b 38 73  |3.....=.......8s|
00000470  bf 0f c1 7b 5a 89 51 f1  97 71 f5 d5 ca 44 9f 87  |...{Z.Q..q...D..|
00000480  e7 dd 35 6d c0 1f cd 5b  93 c1 00 0e f1 a9 25 c8  |..5m...[......%.|
00000490  f6 e8 8b c7                                       |....|
```

APPENDIX D
WANNACRY TARGET FILES

```
.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .ott, .sxw, .stw, .uot, .3ds, .max, .3dm,
.ods, .ots, .sxc, .stc, .dif, .slk, .wb2, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm,
.mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .db, .dbf, .odb, .frm, .myd,
.myi, .ibd, .mdf, .ldf, .sln, .suo, .cs, .c, .cpp, .pas, .h, .asm, .js, .cmd, .bat, .ps1,
.vbs, .vb, .pl, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .rb, .java, .jar, .class, .sh, .mp3,
.wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2, .flv,
.wma, .mid, .m3u, .m4u, .djvu, .svg, .ai, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png,
.bmp, .vcd, .iso, .backup, .zip, .rar, .7z, .gz, .tgz, .tar, .bak, .tbk, .bz2, .PAQ, .ARC,
.aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .edb, .potm, .potx,
.ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm,
.dotx, .dotm, .dot, .docm, .docb, .jpg, .jpeg, .snt, .onetoc2, .dwg, .pdf, .wkl, .wks, .123,
.rtf, .csv, .txt, .vsdx, .vsd, .eml, .msg, .ost, .pst, .pptx, .ppt, .xlsx, .xls, .docx, .doc
```