**Name :** NUR FAHIMAH BT MOHD NASSIR

**Student ID :** 2015732433

**Subject** : ITT786 ADV NETWORK PROGRAMMING

**THE WANNACRY RANSOMWARE**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **NO** | **CONTENT** | **PAGE** |
| 1. | Introduction | 1 |
| 2. | Malware Versions / Variants | 1 |
| 3. | Technical Analysis: Encryption | 2 - 4 |
| 4. | Impact of the Attack | 4 - 5 |
| 5. | Step for Prevention | 5 - 6 |
| 6. | Defending Against Ransomware Generally | 6 |

**INTRODUCTION**

The world has experienced a massive global ransomware cyber-attack known as “WannaCrypt” or “WannaCry” (Ransom: Win32/WannaCrypt) since Friday, May 12 2017. Hundreds of thousands computers worldwide have been hit and affected more than 150 countries. WannaCry is far more dangerous than other common ransomware types because of its ability to spread itself across an organization’s network by exploiting a critical vulnerability in Windows computers, which was patched by Microsoft in March 2017 (MS17-010). The exploit, known as “Eternal Blue,” was released online in April in the latest of a series of leaks by a group known as the Shadow Brokers, who claimed that it had stolen the data from the Equation cyber espionage group.

The malware has the capability to scan heavily over TCP port 445 (Server Message Block/SMB), spreading similar to a worm, compromising hosts, encrypting files stored on them then demanding a ransom payment in the form of Bitcoin. It is important to note that this is not a threat that simply scans internal ranges to identify where to spread, it is also capable of spreading based on vulnerabilities it finds in other externally facing hosts across the internet.

Microsoft provided an emergency patch for older system versions on the day of the outbreak. This widespread attack is of high severity, and although the vulnerability being exploited by the attackers should have been patched a while back, many organizations have been hit and the count keeps rising. New versions and variants of this malware are constantly being released, making mitigation harder.

**MALWARE VERSIONS / VARIANTS**

The first version broke out on Friday 12 May and the identified malware variants are as follows:

• VARIANT 1: .wcry

• VARIANT 2: WCRY (+ .WCRYT for temp)

• VARIANT 3: .WNCRY (+ .WNCRYT for emp)

Another variant that was part of EternalBlue that silently mines cryptocurrency called Adylkuzz was released, this is a new media craze, obsessing about Internet security and the need for greater controls on the flow of information to keep us safe from Internet nasties.

**TECHNICAL ANALYSIS: ENCRYPTION**

Figure 1 shows the execution flow for the Wannacry malware where this ransomware can encrypt all of our files and then demand payment in bitcoins to decrypt the files.

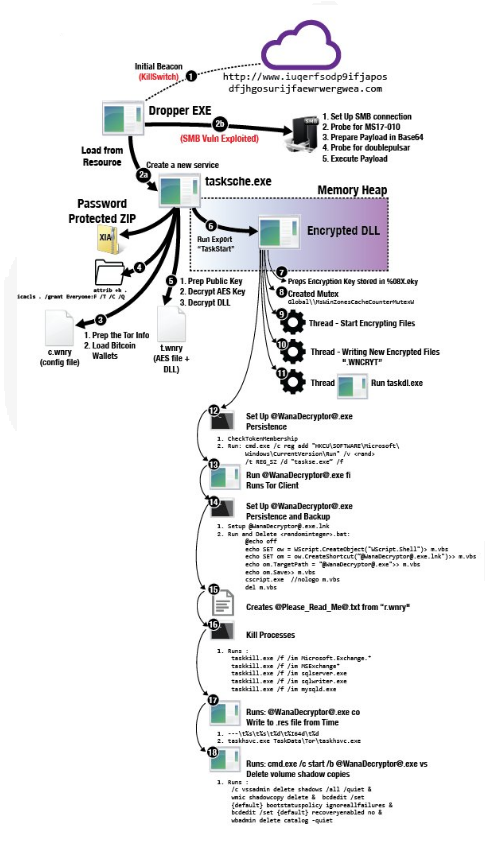


Figure 1. Wannacry Execution Flow

When a computer becomes infected with Wana Decrypt0r, the installer will extract an embedded file into the same folder that the installer is located in. This embedded resource is a password-protected zip folder that contains a variety of files that are used by and executed by WanaCrypt0r.

The WanaDecrypt0r loader will then extract the contents of this zip file into the same folder and perform some startup tasks. It will first extract localized version of the ransom notes into the msg folder. The currently supported languages are:

*Bulgarian, Chinese (simplified), Chinese (traditional), Croatian, Czech, Danish, Dutch, English, Filipino, Finnish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, Swedish, Turkish, Vietnamese.*

WanaCrypt0r will then download a TOR client from:

<https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip> and extract it into the TaskData folder.

This TOR client is used to communicate with the ransomware C2 servers at:

* 7ekbenv2riucmf.onion
* 7g7spgrzlojinas.onion
* xxlvbrloxvriy2c5.onion
* 76jdd2ir2embyv47.onion
* cwwnhwhlz52maqm7.onion

In order to prep the computer so that it can encrypt as many files as possible, WanaCrypt0r will now execute the command icacls . /grant Everyone:F /T /C /Q in order to change give everyone full permissions to the files located in the folder and subfolders under where the ransomware was executed. It then terminates processes associated with database servers and mail servers so it can encrypt databases and mail stores as well.

Now, Wana Decrypt0r is ready to start encrypting the files on the computer. When encrypting files, WanaDecrypt0r will scan all drives and mapped network drives for files that have one of the following extensions:

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

Finally, the installer will execute the @WanaDecryptor@.exe program so that the Wana Decryptor 2.0 lock screen will be displayed. This screen contains further information as to how the ransom can be paid and allows you to select one of the languages listed above. Once you see this screen and realize you are infected, it is important to terminate all the malware processes as Wana Decrypt0r will continue to encrypt new files as they are made.

The ransomware will also configure the Desktop wallpaper to display another ransom note as shown below:



Figure 2. Infected Desktop Wallpaper

**IMPACT OF THE ATTACK**

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including:

• temporary or permanent loss of sensitive or proprietary information.

• disruption to regular operations.

• financial losses incurred to restore systems and files.

• potential harm to an organization’s reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim’s money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

**STEP FOR PREVENTION**

* Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.
* Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
* Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.
* Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.
* Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.
* Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
* Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.
* Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
* Run regular penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical.
* Test your backups to ensure they work correctly upon use.

**DEFENDING AGAINST RANSOMWARE GENERALLY**

Precautionary measures to mitigate ransomware threats include:

• Ensure anti-virus software is up-to-date.

• Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.

• Scrutinize links contained in emails, and do not open attachments included in unsolicited emails.

• Only download software, especially free software - from sites you know and trust.

• Enable automated patches for your operating system and Web browser.