Icon

Description automatically generated

Practical Malware Analysis & Triage

Malware Analysis Report

WannaCry-Ransomware

January 2023 | Somita2415 AKA Alexi N. | v1.0

**Executive Summary**

**SHA256 HASH** 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

WannaCry ransomware is a crypto ransomware worm that attacks Windows PCs. It’s a form of malware that can spread from PC to PC across networks and then once on a computer it can encrypt critical files (the "crypto" part). The perpetrators then demand ransom payments to unlock those files.

The way WannaCry spreads is by using corporate networks to jump to other Windows systems. The only way for an infected user to access WannaCry encrypted files is if they have an external backup copy of those files.

WannaCry is written in C++ language and is a x32 bit program for Windows Operation system.

**Initial symptoms of infection:**

1.Background changes to black and red text with pad lock,

2.See WannaDecryptor.exe show up on the screen

3.Each of the file on the desktop is appended with the .WNCRY extension

Graphical user interface

Description automatically generated

**High-Level Technical Summary**

**WannaCry consists of 3 steps:**



1.Infection



2.Encryption



3.Ransom

**How it works:**

It first attempts to contact it’s kill-switch URL hxxp://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.local. If the URL is alive, it does not execute.

If the URL is not found, then the malware unpacks tasksche.exe and create a service to start tasksche.exe on startup. This executable encrypts all the files and shows a pop-up ransom window and change the background of the desktop. It also creates a random folder inside C:\ProgramData directory to store all the WannaCry files.

WannaCry ransomware exploits the EthernalBlue (a weakness in Microsoft Windows OS using a hack that was allegedly developed by the United States National Security Agency) vulnerability on port 445 (SMB) from a computer to other computers on the network.



No

Yes



Encrypt the hosts and hold for ransom

Create a service to run tasksche.exe from C:\ProgramData on startup

Create a random folder in C:\ProgramData that stores the payload

Run tasksche.exe

Scan for other host on the network on port 445



Unpack tasksche.exe

Execute Malware

Stop Execution

Is kill switch alive?

**Malware Composition**

WannaCry ransomware consists of the following components:

|  |  |
| --- | --- |
| File Name | SHA256 Hash |
| Ransomware.wannacry.exe | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c |
| Tasksche.exe | ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa |

**Ransomware.wannacry.exe:**

The initial executable that runs and checks the kill switch URL, if it is not alive, it will unpack tasksche.exe and vice versa.

**Tasksche.exe:**

This executable is used for persistence. It creates a random folder inside C:\ProgramData directory. After execution of malware a host computer, it will try to spread itself to other Windows OS using SMB protocol on port 445.

**Basic Static Analysis**

Using Floss and PEStudio for Basic Static Analysis

Graphical user interface, text, application

Description automatically generated



Using floss to extract strings:

Floss -n 8 Ransomware.wannacry.exe.malz > floss.ran.som.txt

We ca see service names used, kill switch URL and random paths.

Text

Description automatically generated

Icacls is used to modified access control on files, attrib +h is used to hide file attribute.

A screenshot of a computer

Description automatically generated with medium confidence

Using PEStudio 9.46 to display basic information about the executable.

**Basic Dynamic Analysis**

Using wireshark, inetsim, TCPView and procmon for Basic Dynamic Analysis

Graphical user interface, text, application

Description automatically generated

With inetsim on, the malware does not execute. Instead, it connects to the hxxp://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.local.

Graphical user interface, text, application

Description automatically generated with medium confidence

With inetsim off, the malware can not make a connection to the URL.

Graphical user interface, application, table, Excel

Description automatically generated



Using TCPView, the malware tries to connect to port 445(SMB) to infect other computers on the network.

Graphical user interface, text

Description automatically generated

Using procmon, we can see the creation of tasksche.exe



A screenshot of a computer

Description automatically generated



Graphical user interface, application

Description automatically generated

We can see new files created while old files are encrypted.

Graphical user interface, application

Description automatically generated



Still using procmon , We can see tasksche.exe creates a file with random name in C:\ProgramData directory. This folder is a staging area for WannaCry Ransomware.



Graphical user interface, text, application

Description automatically generated

In Task Manager, we can see the process name that is the same name as the random file name created by tasksche.exe

**Advanced Static Analysis**



Using Cutter



Graphical user interface, text

Description automatically generated



API Call reaches out to URL but there is nothing there, the zero flag will indicate that we jump to this side of the memory and run this function call.

API Call succeeds (reaches out to URL successfully) come to this part of the memory, clean up the arguments on the stack and return out of the program.

First API call to InternetOpenA



**Advanced Dynamic Analysis**

Using x32dbg



Graphical user interface, text, application

Description automatically generated

Breaking point is set at the URL

Will change from 0 to 1

X32dbg can be used to manipulate the control flow of the program. Therefore, with the inetsim running we can still execute the binary successfully by changing CF value from 0 to 1

**Indicators of Compromise**

Network-Based Indicators

Graphical user interface, text, application

Description automatically generated

Wireshark packet capture reaches out to the URL successfully.

Graphical user interface, text, application

Description automatically generated with medium confidence

Wireshark packet capture reaches out to the URL unsuccessfully.

Graphical user interface, application, table, Excel

Description automatically generated

TCPView shows that the infected host tries to reach out to the network on port 445.

Host-Based Indicators

Graphical user interface

Description automatically generated

Once infected, the screen above pop up, and all the files on the desktop are encrypted, new files are also created. Instruction on how to pay the ransom is also presented.

Text

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

**Rules & Signatures**

Yara Rule

**Graphical user interface, text, application

Description automatically generated**