

Malware Analysis Report

PMAT - Practical Malware Analysis & Triage

Course Final



Ransomware.wannacry.exe

Table of Contents

| | |
|---|-----------|
| Table of Contents | 2 |
| Executive Summary | 3 |
| High-Level Technical Summary | 4 |
| Malware Composition | 6 |
| Ransomware.wannacry.exe..... | 6 |
| Unpacked executables..... | 6 |
| PKZIP file..... | 6 |
| Basic Static Analysis | 7 |
| Basic Dynamic Analysis | 15 |
| Advanced Static Analysis | 22 |
| Advanced Dynamic Analysis | 26 |
| Indicators of Compromise | 28 |
| Network Indicators..... | 28 |
| Host-based Indicators..... | 30 |
| Rules & Signatures | 36 |
| Appendices | 37 |
| A. Yara Rules..... | 37 |
| B. Bitcoin Wallet analysis..... | 38 |
| C. List of file extensions..... | 40 |

Executive Summary

WannaCry is a ransomware worm that targets Windows OS. Once launched, it encrypts files on the computer, changes the desktop wallpaper to indicate the successful infection of the machine, and presents a software interface displaying a ransom note. The ransom note provides instructions on where to send the Bitcoin payment in order to regain access to the encrypted files.

Additionally, WannaCry possesses persistence mechanisms, enabling it to remain on the target machine even after a reboot, and worm capabilities, allowing it to attempt the spread to other IP addresses.

It is important to note that this malware includes a killswitch mechanism. When successfully connected to a specific URL, the malware doesn't execute its malicious actions.

YARA signature rules are attached in Appendix A.

High-Level Technical Summary

| | |
|-----------|--|
| File name | Ransomware.wannacry.exe |
| md5 | db349b97c37d22f5ea1d1841e3c89eb4 |
| sha1 | e889544aff85ffaf8b0d0da705105dee7c97fe26 |
| sha256 | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c |

This particular sample of WannaCry is distributed as a 32-bit executable file and requires administrative privileges to execute its malicious actions.

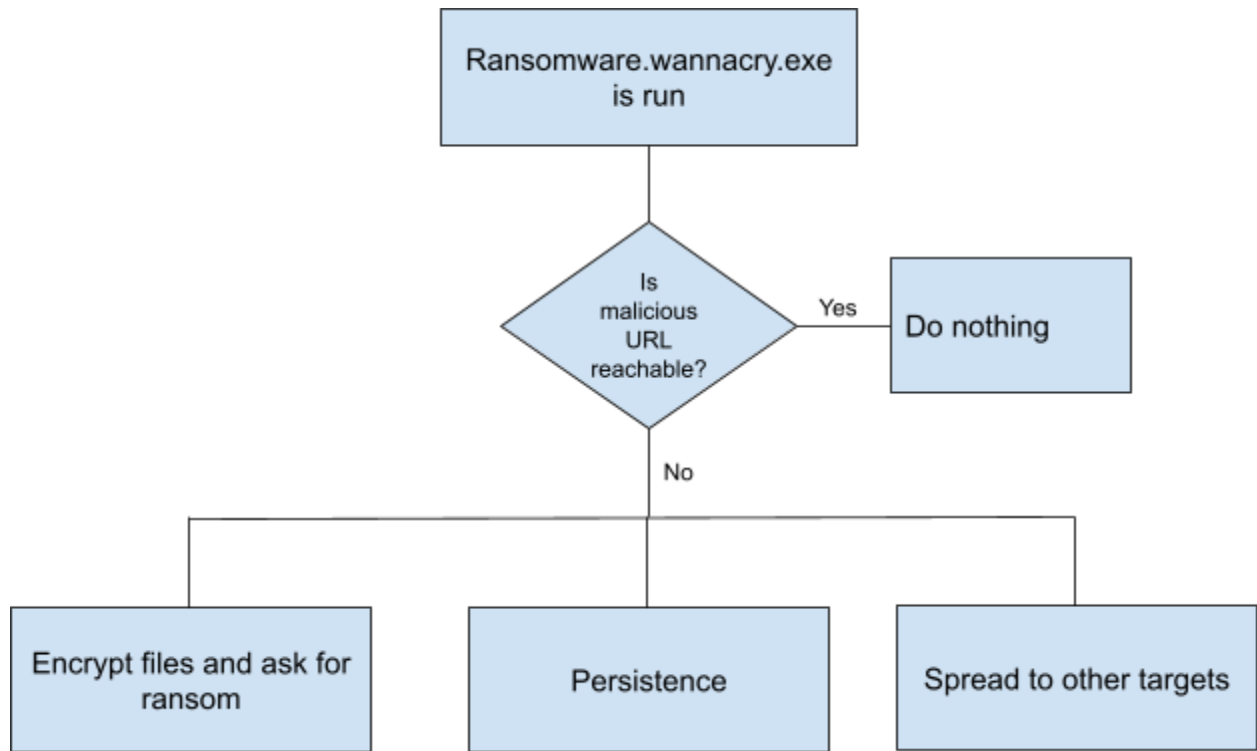
As a first step, it attempts to establish a connection with the URL **“hxxp[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com”**. If it receives a response from this domain, the malware terminates its routine and remains inactive. Essentially, it acts as a kill-switch.

If the domain is unreachable. (e.g. it doesn't exist), the program proceeds to execute its main function. This involves unpacking additional executables hidden within the file, one of which is an encryptor. Utilizing the Microsoft Enhanced RSA and AES Cryptographic Provider libraries, this encryptor encrypts the files on the targeted machine.

Subsequently, the malware changes the desktop wallpaper, replacing it with an image containing a message that explains the successful infection and provides instructions for recovery.

Additionally, it installs a decryptor program on the desktop, which is executed shortly after the infection. The decryptor program includes the ransom note and instructions on how to make the ransom payment and decrypt the files on the system. The program also displays two timers, indicating the deadlines for the ransom amount to double and the final deadline to pay the ransom and recover the files.

In terms of its worm capabilities, this malware initiates multiple connections to various IP addresses on port 445, which is commonly used for the SMB protocol. It exploits the EternalBlue vulnerability to propagate its infection.



Malware Composition

This WannaCry sample consists of the following components:

Ransomware.wannacry.exe

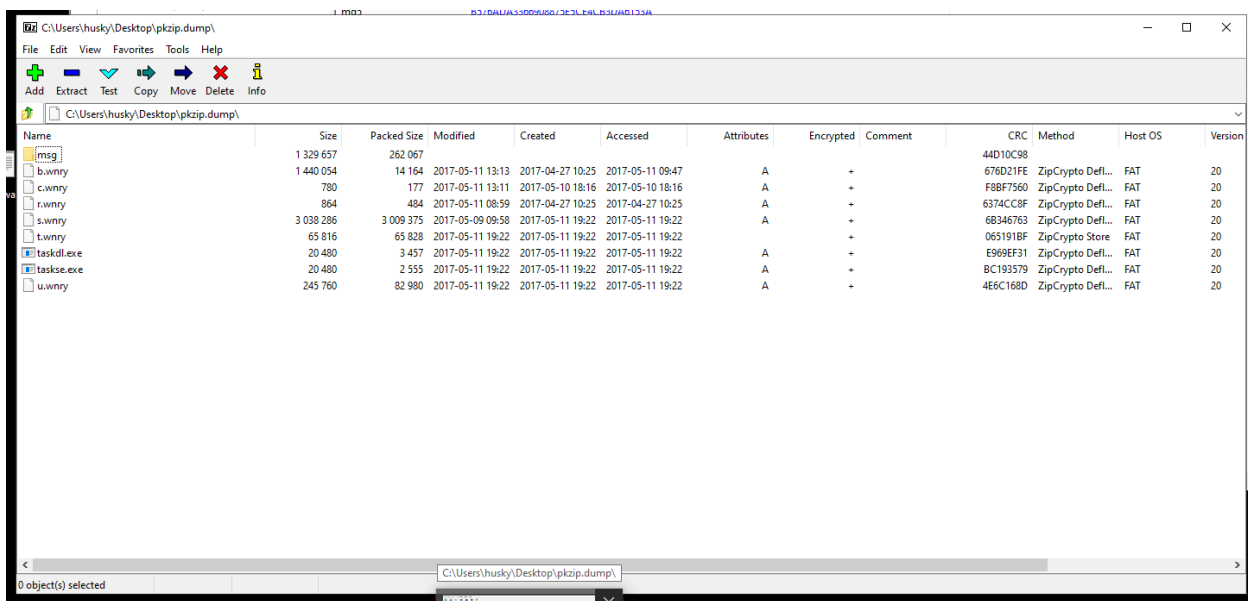
This is the initial executable that is executed when clicked or launched.

Unpacked executables

There's an executable found inside the resources section of the original executable, and additional executables within it.

PKZIP file

Contained inside the unpacked executable, there's a password protected zip file. It contains a folder named "msg" that appears to contain translations of the ransom note. Additionally, the zip file includes two executables (taskdl.exe and taskse.exe) along with supplementary files..



Basic Static Analysis

The basic static analysis of the sample was conducted using FLOSS, capa, and PEStudio. Each program's unique characteristics were utilized to gather comprehensive information about the sample.

During the analysis, several strings were identified that exhibited indications of potentially malicious activity:

| | |
|---|---|
| WanaCrypt0r | name of the malware itself |
| icacls . /grant Everyone:F /T /C /Q | command-line command used to change control access to files and folders |
| attrib +h . | command used to set the current folder as "hidden" |
| Microsoft Enhanced RSA and AES Cryptographic Provider | cryptography capabilities |
| hxxp[:]//]www[.]iuqerfsodp9ifjaposdfj hgosurijfaewrwegwea[.]com | the (defanged) URL |
| taskdl.exe taskse.exe diskpart.exe lhdfrgui.exe | some filenames |
| C:\%s\qeriuwjhrf | suspicious folder name |
| WriteFile CreateFileA CreateProcessA | examples of API calls found in the sample |
| str_%s -m securit_00431330r | command (part of it) |
| u.wnry | one of many .wnry file names |
| 13AM4VW2dhxYgXeQepoHkHSQuy6 NgaEb94 | The bitcoin wallet used in this sample, found by searching through the strings after getting the wallet address during the basic dynamic analysis |

| | |
|---|--|
| 115p7UMMngojl1pMvkpHijcRdfJNXj6LrLn 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw | Two other bitcoin wallets shown in strings and floss together with the main one, above. These 2 weren't used in the sample. Please check the appendices. |
| \\172.16.99.5\IPC\$ \\192.168.56.20\IPC\$ | SMB shares |
| cmd.exe /c "%s" | a command |

CAPA found some indicators that would prove correct during the dynamic analysis, like the communication and cryptography abilities, installation of files and creation of processes for persistence.

Here are the screenshots of the results:

| ATT&CK Tactic | ATT&CK Technique |
|-----------------|--|
| DEFENSE EVASION | Obfuscated Files or Information::Indicator Removal from Tools [T1027.005] |
| DISCOVERY | File and Directory Discovery [T1083] System Information Discovery [T1082] |
| EXECUTION | System Network Configuration Discovery [T1016] Shared Modules [T1129] |
| PERSISTENCE | System Services::Service Execution [T1569.002] Create or Modify System Process::Windows Service [T1543.003] |

| MBC Objective | MBC Behavior |
|--------------------------|---|
| ANTI-BEHAVIORAL ANALYSIS | Debugger Detection::Timing/Delay Check GetTickCount [B0001.032] Debugger Detection::Timing/Delay Check QueryPerformanceCounter [B0001.033] |
| ANTI-STATIC ANALYSIS | Execution Guardrails::Runs as Service [E1480.m07] |
| COMMAND AND CONTROL | Disassembler Evasion::Argument Obfuscation [B0012.001] C2 Communication::Receive Data [B0030.002] C2 Communication::Send Data [B0030.001] |
| COMMUNICATION | HTTP Communication::Create Request [C0002.012] HTTP Communication::Open URL [C0002.004] Socket Communication::Connect Socket [C0001.004] Socket Communication::Create TCP Socket [C0001.011] Socket Communication::Create UDP Socket [C0001.010] Socket Communication::Get Socket Status [C0001.012] Socket Communication::Initialize Winsock Library [C0001.009] Socket Communication::Receive Data [C0001.006] Socket Communication::Send Data [C0001.007] Socket Communication::Set Socket Config [C0001.001] Socket Communication::TCP Client [C0001.008] |
| CRYPTOGRAPHY | Generate Pseudo-random Sequence::Use API [C0021.003] |
| DATA | Compression Library [C0060] |
| EXECUTION | Install Additional Program [B0023] |
| FILE SYSTEM | Read File [C0051] |
| PROCESS | Create Thread [C0038] Terminate Process [C0018] Terminate Thread [C0039] |

| CAPABILITY | NAMESPACE |
|--|---|
| check for time delay via GetTickCount | anti-analysis/anti-debugging/debugger-detection |
| check for time delay via QueryPerformanceCounter | anti-analysis/anti-debugging/debugger-detection |
| contain obfuscated stackstrings | anti-analysis/obfuscation/string/stackstring |
| receive data (5 matches) | communication |
| send data (5 matches) | communication |
| connect to URL | communication/http/client |
| get socket status | communication/socket |
| initialize Winsock library | communication/socket |
| set socket configuration | communication/socket |
| create UDP socket (4 matches) | communication/socket/udp/send |
| act as TCP client | communication/tcp/client |
| generate random numbers via WinAPI | data-manipulation/prng |
| contain a resource (.rsrc) section | executable/pe/section/rsrc |
| extract resource via kernel32 functions | executable/resource |
| contain an embedded PE file | executable/subfile/pe |
| get file size | host-interaction/file-system/meta |
| move file | host-interaction/file-system/move |
| read file | host-interaction/file-system/read |
| get number of processors | host-interaction/hardware/cpu |
| get networking interfaces | host-interaction/network/interface |
| terminate process | host-interaction/process/terminate |
| run as service | host-interaction/service |
| create service | host-interaction/service/create |
| modify service | host-interaction/service/modify |
| start service | host-interaction/service/start |
| create thread (4 matches) | host-interaction/thread/create |
| terminate thread | host-interaction/thread/terminate |
| link function at runtime | linking/runtime-linking |
| linked against ZLIB | linking/static/zlib |
| inspect section memory permissions | load-code/pe |
| parse PE exports | load-code/pe |
| parse PE header | load-code/pe |
| persist via Windows service | persistence/service |

Some findings from PESTudio:

| | | | | |
|------------|---|---|--------------|--|
| 0x0001F027 | x | - | desktop | GetUserObjectInformation |
| 0x0000DDFB | x | - | cryptography | CryptAcquireContext |
| 0x0000DE14 | x | - | cryptography | CryptGenRandom |
| 0x0000DF2 | x | - | cryptography | rand |
| 0x0000E022 | x | - | cryptography | srand |
| 0x0032B15D | x | - | cryptography | CryptReleaseContext |
| 0x0032B233 | x | - | cryptography | rand |
| 0x0032B23C | x | - | cryptography | srand |
| 0x0032C982 | x | - | cryptography | CryptGenKey |
| 0x0032C98E | x | - | cryptography | CryptDecrypt |
| 0x0032C99E | x | - | cryptography | CryptEncrypt |
| 0x0032C9AE | x | - | cryptography | CryptDestroyKey |
| 0x0032C9BE | x | - | cryptography | CryptImportKey |
| 0x0032C9CE | x | - | cryptography | CryptAcquireContext |
| 0x0001F647 | - | - | windowing | GetLastActivePopup |

API calls showing cryptographic abilities

| property | value |
|------------------|--|
| md5 | 1EBDC36976DD611E1A9E221A88E6858E |
| sha1 | 7B5A93CD7DB3DDC7FF48C6E3C7EEFCA46807462E |
| sha256 | 2F3FC51546ADA848DFC8E775554C0DE3689D6FAE7BA4BF3D40E3C8DEC68B277B |
| file-type | executable |
| date | empty |
| language | English-US |
| code-page | Unicode UTF-16, little endian |
| CompanyName | Microsoft Corporation |
| FileDescription | Microsoft® Disk Defragmenter |
| FileVersion | 6.1.7601.17514 (win7sp1_rtm.101119-1850) |
| InternalName | lhdfgui.exe |
| LegalCopyright | © Microsoft Corporation. All rights reserved. |
| OriginalFilename | lhdfgui.exe |
| ProductName | Microsoft® Windows® Operating System |
| ProductVersion | 6.1.7601.17514 |

One of the strings found using FLOSS seems to be the original filename of the sample

| Version | I | XXXXXXXXXX | Version | Size | Size % | Language | Signature |
|---------|------|------------|--------------------------|---------|---------|------------|---|
| R | 1831 | 0x000320A4 | executable (cpu: 32-bit) | 3514368 | 94.39 % | English-US | 4D 5A 90 00 03 00 00 00 04 00 00 00 FF ... MZ |

PEStudio shows an executable inside the .rsrc section of the file, called R.1831

PEView - C:\Users\husky\Desktop\Ransomware.wannacry.exe.malz

File View Go Help

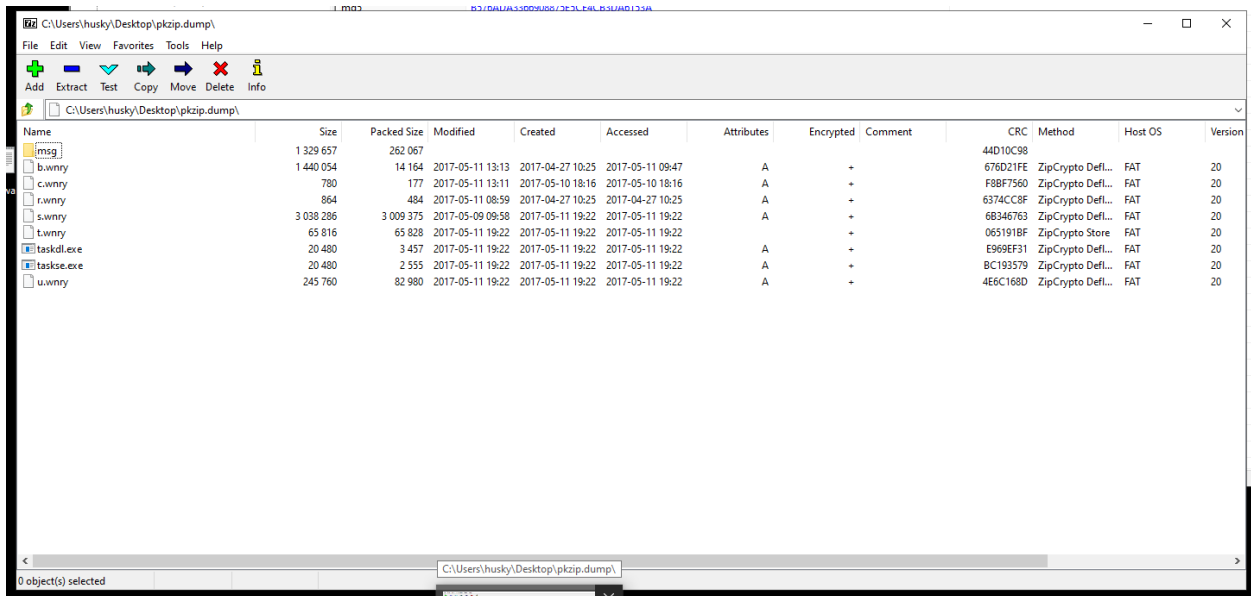
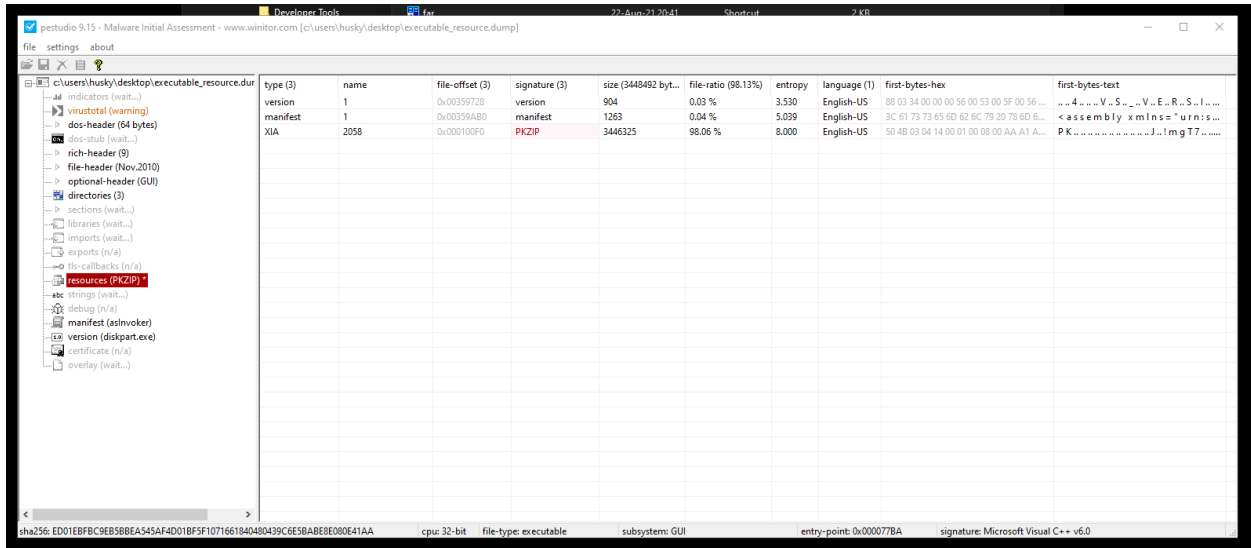
Ransomware.wannacry.exe.malz

- IMAGE_DOS_HEADER
- MS-DOS Stub Program
- IMAGE_NT_HEADERS
 - IMAGE_SECTION_HEADER .text
 - IMAGE_SECTION_HEADER .rdata
 - IMAGE_SECTION_HEADER .data
 - IMAGE_SECTION_HEADER .rsrc
- SECTION .text
- SECTION .rdata
- SECTION .data
- SECTION .rsrc
 - IMAGE_RESOURCE_DIRECTORY Type
 - IMAGE_RESOURCE_DIRECTORY NameID
 - IMAGE_RESOURCE_DIRECTORY Language
 - IMAGE_RESOURCE_DATA_ENTRY
 - IMAGE_RESOURCE_DIRECTORY_STRING
 - R 0727 0409
 - VERSION 0001 0409

| pFile | Raw Data | Value | |
|----------|-------------------------|-------------------------|-----------------------|
| 000320A4 | 4D 5A 90 00 03 00 00 00 | 04 00 00 00 FF FF 00 00 | MZ |
| 000320B4 | B8 00 00 00 00 00 00 00 | 40 00 00 00 00 00 00 00 |@..... |
| 000320C4 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 000320D4 | 00 00 00 00 00 00 00 00 | 00 00 00 00 F8 00 00 00 |F8..... |
| 000320E4 | 0E 1F BA 0E 00 B4 09 CD | 21 B8 01 4C CD 21 54 68 |!..L.ITh |
| 000320F4 | 69 73 20 70 72 6F 67 72 | 61 6D 20 63 61 6E 6E 6F | is program canno |
| 00032104 | 74 20 62 65 20 72 75 6E | 20 69 6E 20 44 4F 53 20 | t be run in DOS |
| 00032114 | 6D 6F 64 65 2E 0D 0D 0A | 24 00 00 00 00 00 00 00 | mode.....\$..... |
| 00032124 | E0 C5 3A D1 A4 A4 54 82 | A4 A4 54 82 A4 A4 54 82 |T...T...T... |
| 00032134 | DF B8 58 82 A6 A4 54 82 | CB BB 5F 82 A5 A4 54 82 |X...T...T... |
| 00032144 | 27 B8 5A 82 A0 A4 54 82 | CB BB 5E 82 AF A4 54 82 |Z...T...A...T... |
| 00032154 | CB BB 50 82 A0 A4 54 82 | 67 AB 09 82 A9 A4 54 82 |P...T...g...T... |
| 00032164 | A4 A4 55 82 07 A4 54 82 | 92 82 5F 82 A3 A4 54 82 |U...T...T...T... |
| 00032174 | 63 A2 52 82 A5 A4 54 82 | 52 69 63 68 A4 A4 54 82 | c.R...T.Rich...T... |
| 00032184 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032194 | 00 00 00 00 00 00 00 00 | 50 45 00 00 4C 01 04 00 |PE...L... |
| 000321A4 | 41 8F E7 4C 00 00 00 00 | 00 00 00 00 E0 00 0F 01 | A...L..... |
| 000321B4 | 0B 01 06 00 00 70 00 00 | 00 20 35 00 00 00 00 00 |p...5..... |
| 000321C4 | BA 77 00 00 00 10 00 00 | 00 80 00 00 00 00 40 00 | w.....@..... |
| 000321D4 | 00 10 00 00 00 10 00 00 | 04 00 00 00 00 00 00 00 | |
| 000321E4 | 04 00 00 00 00 00 00 00 | 00 A0 35 00 00 10 00 00 |5..... |
| 000321F4 | 00 00 00 00 02 00 00 00 | 00 00 10 00 00 10 00 00 | |
| 00032204 | 00 00 10 00 00 10 00 00 | 00 00 00 00 10 00 00 00 | |
| 00032214 | 00 00 00 00 00 00 00 00 | A8 D5 00 00 64 00 00 00 |d... |
| 00032224 | 00 00 01 00 A0 9F 34 00 | 00 00 00 00 00 00 00 00 |4..... |
| 00032234 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032244 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032254 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032264 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032274 | 00 80 00 00 D8 01 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032284 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032294 | 2E 74 65 78 74 00 00 00 | E0 69 00 00 00 10 00 00 |text...i..... |
| 000322A4 | 00 70 00 00 00 10 00 00 | 00 00 00 00 00 00 00 00 |p..... |
| 000322B4 | 00 00 00 00 20 00 00 60 | 2E 72 64 61 74 61 00 00 |rdata... |
| 000322C4 | 70 5F 00 00 00 80 00 00 | 00 60 00 00 00 80 00 00 |p..... |
| 000322D4 | 00 00 00 00 00 00 00 00 | 00 00 00 00 40 00 00 40 |@...@... |
| 000322E4 | 2E 64 61 74 61 00 00 00 | 58 19 00 00 00 E0 00 00 |data...X..... |
| 000322F4 | 00 20 00 00 00 E0 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032304 | 00 00 00 00 40 00 00 C0 | 2E 72 73 72 63 00 00 00 |@...rsrc... |
| 00032314 | A0 9F 34 00 00 00 01 00 | 00 A0 34 00 00 00 01 00 |4...4..... |
| 00032324 | 00 00 00 00 00 00 00 00 | 00 00 00 00 40 00 00 40 |@...@... |
| 00032334 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032344 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00032354 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |

Further confirmation of the executable inside the resources section, this time shown in the PEView tool

The following screenshots show the executable inside R.1831 (that had a PKZIP file inside itself) and the content of that ZIP file:



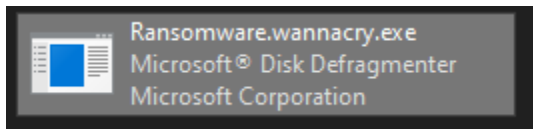
| property | value | value | value | value |
|------------------------------|---|--|--|--|
| name | .text | .rdata | .data | .rsrc |
| md5 | C7613102E2ECEC5DCEFC14... | D8037D744B539326C06E897... | 22A8598DC29CAD7078C291E94612CE26 | 12E1BD7375D82CCA3A51CA48FE22D1A9 |
| entropy | 6.135 | 3.504 | 6.100 | 7.995 |
| file-ratio (99.89%) | 0.99 % | 0.11 % | 4.29 % | 94.50 % |
| raw-address | 0x00001000 | 0x0000A000 | 0x0000B000 | 0x00032000 |
| raw-size (3719168 bytes) | 0x00009000 (36864 bytes) | 0x00001000 (4096 bytes) | 0x00027000 (159744 bytes) | 0x0035B000 (3518464 bytes) |
| virtual-address | 0x00401000 | 0x0040A000 | 0x0040B000 | 0x00710000 |
| virtual-size (6718034 bytes) | 0x00008BCA (35786 bytes) | 0x00000998 (2456 bytes) | 0x0030489C (3164316 bytes) | 0x0035A454 (3515476 bytes) |
| entry-point | 0x00009A16 | - | - | - |
| characteristics | 0x60000020 | 0x40000040 | 0xC0000040 | 0x40000040 |
| writable | - | - | x | - |
| executable | x | - | - | - |
| shareable | - | - | - | - |
| discardable | - | - | - | - |
| initialized-data | - | x | x | x |
| uninitialized-data | - | - | - | - |
| unreadable | - | - | - | - |
| self-modifying | - | - | - | - |
| virtualized | - | - | - | - |
| file | - | - | executable, offset: 0x0000B020, size: 5263716 | executable, offset: 0x000320A4, size: 3514368 |
| file | - | - | executable, offset: 0x0000F080, size: 5297524 | n/a |
| file | - | - | executable, offset: 0x00013F94, size: 159744 | n/a |

| offset | size | value | comment |
|-------------|------|-------------|--|
| 0x0000312C4 | 42 | 0x0000312C4 | Microsoft Base Cryptographic Provider v1.0 |
| 0x000017E18 | 41 | 0x000017E18 | R6025\r\n- pure virtual function call\r\n |
| 0x0000004D | 40 | 0x0000004D | !This program cannot be run in DOS mode. |
| 0x0000B06D | 40 | 0x0000B06D | !This program cannot be run in DOS mode. |
| 0x0000F0CD | 40 | 0x0000F0CD | !This program cannot be run in DOS mode. |
| 0x000320F1 | 40 | 0x000320F1 | !This program cannot be run in DOS mode. |
| 0x00017CE8 | 40 | 0x00017CE8 | R6028\r\n- unable to initialize heap\r\n |
| 0x0038B90C | 40 | 0x0038B90C | 6.1.7601.17514 (win7sp1_rtm.101119-1850) |
| 0x0038C20C | 40 | 0x0038C20C | 6.1.7601.17514 (win7sp1_rtm.101119-1850) |

Additional screenshots from the basic static analysis:

| encoding (2) | size (bytes) | file-offset | blacklist (54) | hint (416) | group (18) | value (43891) |
|--------------|--------------|-------------|----------------|-------------|------------|---|
| ascii | 4 | 0x0000A85C | - | utility | - | time |
| ascii | 46 | 0x0003EEEE | - | utility | - | .inflate.1.1.3 Copyright 1995-1998 Mark Adler |
| ascii | 35 | 0x000415A0 | - | utility | - | icacls . /grant Everyone:F /T /C /Q |
| ascii | 11 | 0x000415C4 | - | utility | - | attrib +h . |
| ascii | 4 | 0x0034A0DD | - | utility | - | AT 8 |
| ascii | 4 | 0x00380703 | - | utility | - | At 1 |
| unicode | 8 | 0x0038B8D8 | - | utility | - | DiskPart |
| unicode | 12 | 0x0038B980 | - | utility | - | diskpart.exe |
| unicode | 12 | 0x0038BA44 | - | utility | - | diskpart.exe |
| ascii | 56 | 0x000313D0 | - | url-pattern | - | http://www.iuqerfsodp9ifajaposdfjhgosurijfaewrgwea.com |
| ascii | 2039 | 0x0001BBBE | - | size | - | h6agLCqPqVyXi2VQS8O6Yb9jBx54jY6KM+sz33NmS6TK8XIOk920s0E0aajOV |
| ascii | 1403 | 0x0001C41B | - | size | - | h54WFF9cGigWFE92bzmoD0UOaZIMdU2F4F2+6qn9/ZDSqJksnLlfbdOimA |

Example of interesting strings, some of which already mentioned previously



Malware disguises itself as a Disk utility in Windows

This malware sample is flagged on VirusTotal as malicious:



The image shows a VirusTotal analysis interface. On the left, a circular gauge displays a score of 68 out of 71. Below it, a 'Community Score' bar is partially filled. The main analysis area shows the file name 'lhdfgui.exe' and its SHA-256 hash: 24d004a104d4d54034dbcfc2a4b19a11f39008a575aa614ea04703480b1022c. The file size is 3.55 MB and it was last analyzed 2 days ago. A list of detected signatures includes: peexe, malware, macro-create-ole, runtime-modules, detect-debug-environment, checks-network-adapters, exploit, cve-2017-0147, long-sleeps, direct-cpu-clock-access, and checks-user-input. The file type is identified as EXE. At the top of the analysis area, a red notification states: '68 security vendors and 5 sandboxes flagged this file as malicious'. Navigation options like 'Reanalyze', 'Similar', and 'More' are visible in the top right.

Running the sample with administrator privileges would activate the payload only if there is no internet connection available (i.e. in the forensic environment inetsim is not active).

Wireshark and TCPView would show network activity. First, we see in Wireshark the attempts to connect to the killswitch domain:

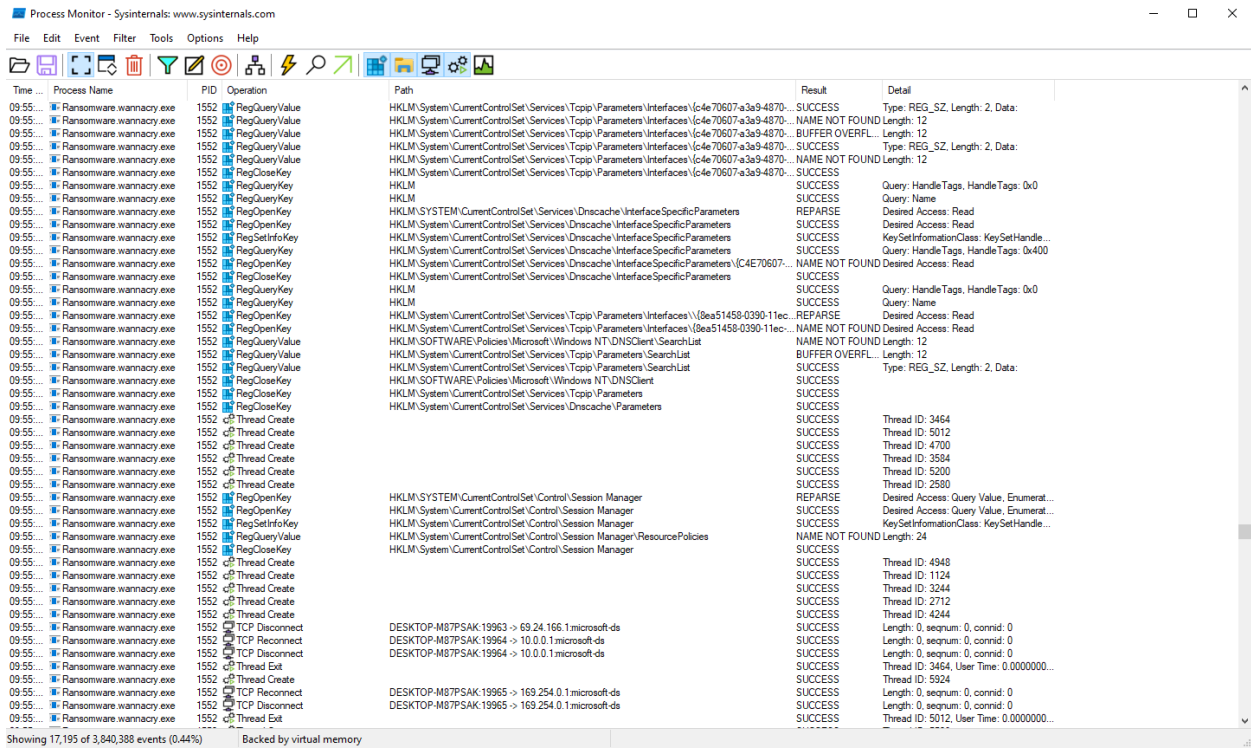
The screenshot shows the Wireshark interface with a network traffic capture. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The capture shows several DNS queries from 10.0.0.4 to 10.0.0.3 and back, along with ICMP 'Destination unreachable (Port unreachable)' responses. The packet list is as follows:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|-------------------|----------|--------|---|
| 1 | 0.000000 | PcsCompu_55:06:07 | PcsCompu_7d:a6:a5 | ARP | 42 | Who has 10.0.0.3? Tell 10.0.0.4 |
| 2 | 0.001336 | PcsCompu_7d:a6:a5 | PcsCompu_55:06:07 | ARP | 60 | 10.0.0.3 is at 08:00:27:7d:a6:a5 |
| 3 | 0.135212 | PcsCompu_7d:a6:a5 | PcsCompu_55:06:07 | ARP | 60 | Who has 10.0.0.4? Tell 10.0.0.3 |
| 4 | 0.135226 | PcsCompu_55:06:07 | PcsCompu_7d:a6:a5 | ARP | 42 | 10.0.0.4 is at 08:00:27:55:06:07 |
| 5 | 17.541821 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 6 | 17.542090 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 7 | 17.542164 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 8 | 17.542414 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 9 | 17.542480 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 10 | 17.542743 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 11 | 17.542799 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 12 | 17.543029 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 13 | 17.543079 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 14 | 17.543291 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 15 | 17.611432 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0xa625 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 16 | 17.611793 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 17 | 17.612430 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0xa625 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 18 | 18.627868 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0xa625 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 19 | 18.628333 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 20 | 18.628717 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0xa625 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrgw... |
| 21 | 22.516112 | PcsCompu_55:06:07 | PcsCompu_7d:a6:a5 | ARP | 42 | Who has 10.0.0.3? Tell 10.0.0.4 |
| 22 | 22.517377 | PcsCompu_7d:a6:a5 | PcsCompu_55:06:07 | ARP | 60 | 10.0.0.3 is at 08:00:27:7d:a6:a5 |

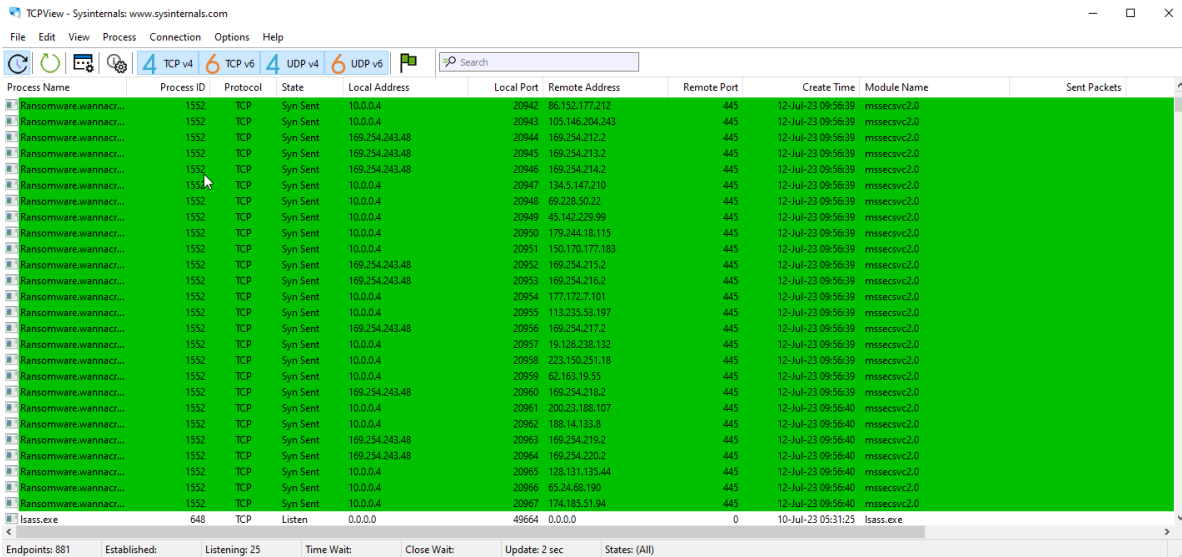
The packet details pane shows the selected packet (No. 1) with the following hex and ASCII data:

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{5DE24529-6A8E-414C-8A8E-1FF9F4B73334}, id 0
0000 08 00 27 7d a6 a5 08 00 27 55 06 07 08 06 00 01  ..'}.....'U.....
0010 08 00 06 04 00 01 08 00 27 55 06 07 0a 00 00 04  ..}'.....'U.....
0020 08 00 27 7d a6 a5 0a 00 00 03  ..}'... ..
```


Then, in ProcMon we see further operations (registry queries and modifications, DLL loading, threads creation, files and services creation, etc.). These operations eventually lead to the establishment of TCP connections for the purpose of spreading to other targets:



TCPView would also show the TCP connections to port 445, used by the SMB protocol:



TCP connections also caught in Wireshark:

The screenshot shows the Wireshark interface with a packet list and a packet details pane. The packet list shows various DNS queries and TCP connections. Packet 74 is highlighted, showing an ICMP destination unreachable message. The packet details pane shows the raw bytes of the frame.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------|--------------|----------|--------|---|
| 67 | 25.944954 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x0081 PTR 1.18.254.169.in-addr.arpa |
| 68 | 25.950233 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x634a PTR 1.19.254.169.in-addr.arpa |
| 69 | 25.951962 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xa19d PTR 1.20.254.169.in-addr.arpa |
| 70 | 26.005728 | 10.0.0.4 | 44.43.50.98 | TCP | 66 | 20002 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 71 | 26.673974 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0xfdcf PTR 66.27.44.89.in-addr.arpa |
| 72 | 26.701598 | 10.0.0.4 | 10.0.0.3 | DNS | 81 | Standard query 0x28df PTR 1.0.0.10.in-addr.arpa |
| 73 | 26.701694 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0xe65c PTR 1.0.254.169.in-addr.arpa |
| 74 | 26.702002 | 10.0.0.3 | 10.0.0.4 | ICMP | 109 | Destination unreachable (Port unreachable) |
| 75 | 26.710407 | 10.0.0.4 | 71.244.78.67 | TCP | 66 | 20012 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 76 | 26.710528 | 10.0.0.4 | 10.0.0.3 | DNS | 81 | Standard query 0x28df PTR 1.0.0.10.in-addr.arpa |
| 77 | 26.714207 | 10.0.0.4 | 10.0.0.3 | DNS | 86 | Standard query 0x4047 PTR 148.42.208.31.in-addr.arpa |
| 78 | 26.724655 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x69ba PTR 1.21.254.169.in-addr.arpa |
| 79 | 26.726261 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0x0e37 PTR 1.1.254.169.in-addr.arpa |
| 80 | 26.740819 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x6237 PTR 1.22.254.169.in-addr.arpa |
| 81 | 26.741069 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0x543c PTR 1.2.254.169.in-addr.arpa |
| 82 | 26.741131 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0x4997 PTR 1.3.254.169.in-addr.arpa |
| 83 | 26.743241 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xe918 PTR 1.23.254.169.in-addr.arpa |
| 84 | 26.747364 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xe9d8 PTR 1.24.254.169.in-addr.arpa |
| 85 | 26.749615 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xb996 PTR 1.25.254.169.in-addr.arpa |
| 86 | 26.753146 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0x8037 PTR 1.4.254.169.in-addr.arpa |
| 87 | 26.756525 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x0f91 PTR 1.26.254.169.in-addr.arpa |
| 88 | 26.768224 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xf423 PTR 1.27.254.169.in-addr.arpa |

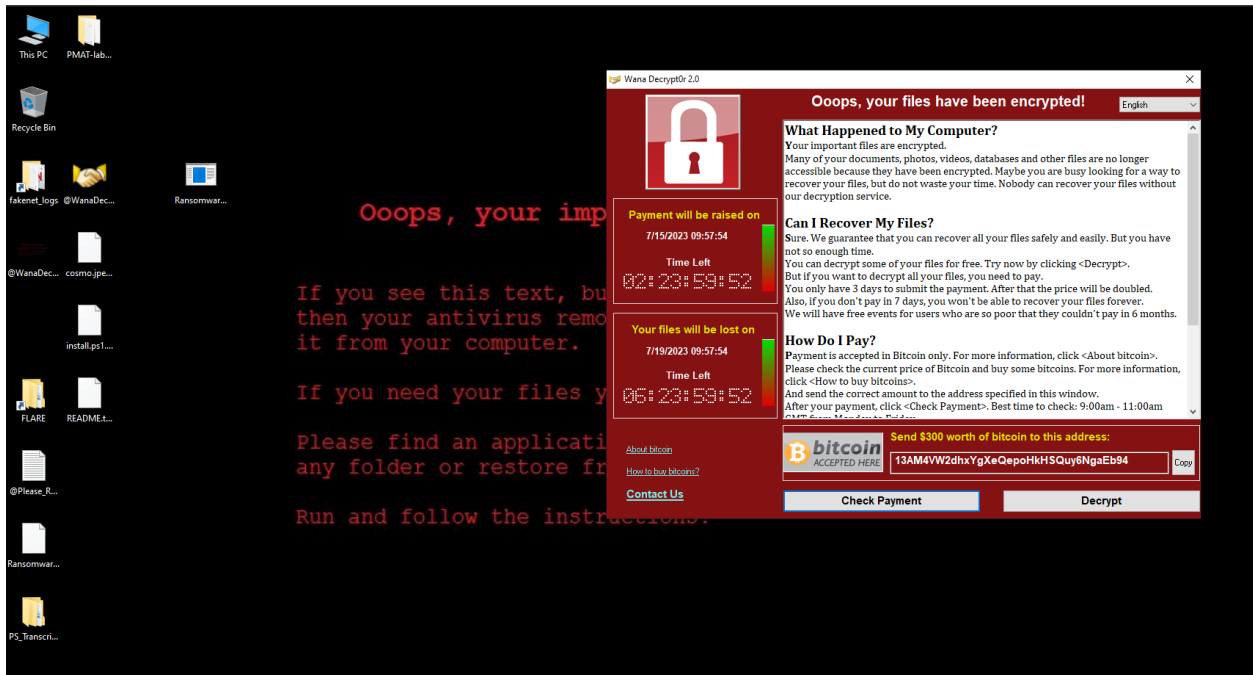
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{5DE24529-6A8E-414C-8A8E-1FF9F4873334}, id 0

```

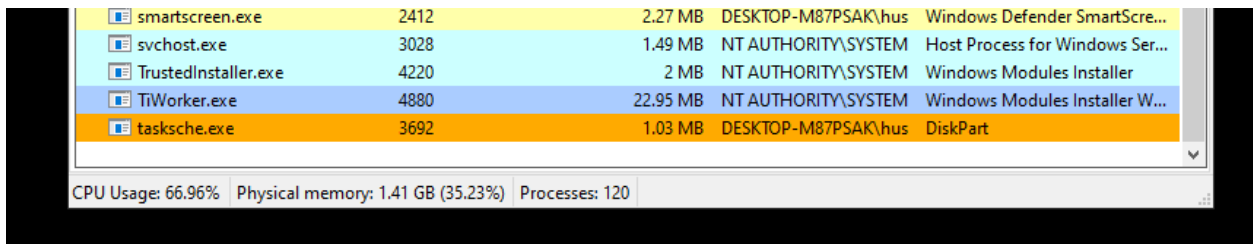
0000 08 00 27 7d a6 a5 08 00 27 55 06 07 08 06 00 01  ...}....'U.....
0010 08 00 06 04 00 01 08 00 27 55 06 07 0a 00 00 04  ....U.....
0020 08 00 27 7d a6 a5 0a 00 00 03  ...}..
  
```

Ethernet: <live capture in progress> | Packets: 3769 · Displayed: 3769 (100.0%) | Profile: Default

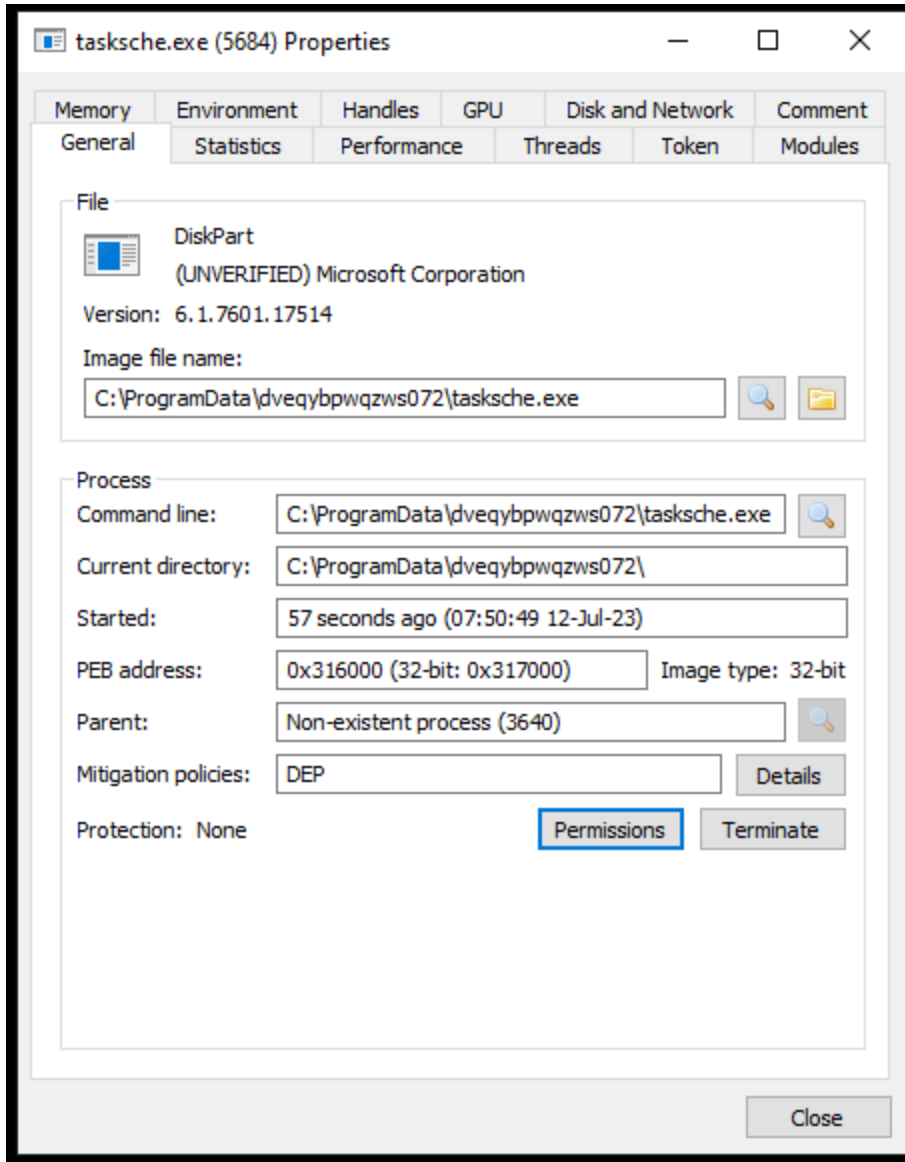
Then, we see files disappearing from the desktop, reappearing after a while with a different extension .wncry; we see the appearance of new files, the desktop wallpaper changing and also the GUI of the decryptor typical of this malware infection:



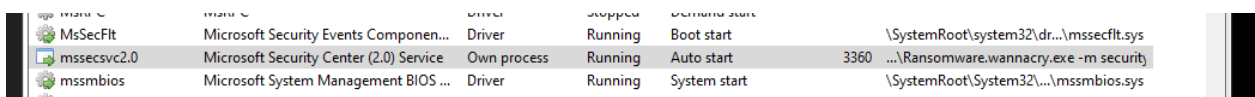
Here are some additional findings, after observing the malware during the dynamic analysis, using additional tools like Process Hacker 2 and the standard Windows Explorer:



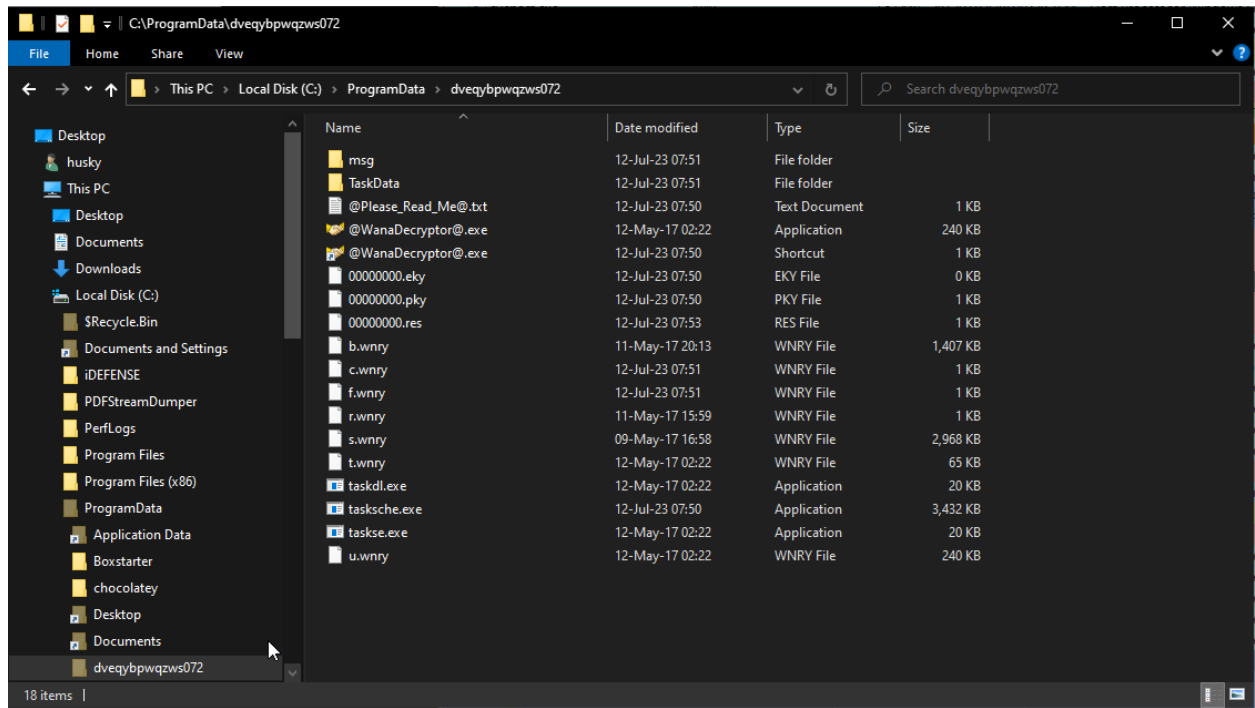
ProcessHacker: Here the malware poses as the DiskPart utility



ProcessHacker: We can see the hidden folder where the malware unpacked the additional executables and files



Process Hacker: service started by the malware, showing the command used to run it (part of it was found during the strings analysis)



The hidden folder on disk

Advanced Static Analysis

The advanced static analysis was conducted using Cutter, which at a first glance further confirmed the finding from the basic dynamic analysis. The initial step of the program involves checking the availability of the malicious URL identified in the strings and Wireshark logs.

Depending on the outcome of this check, the program would either remain inactive or initiate the malicious routine responsible for infecting the target.



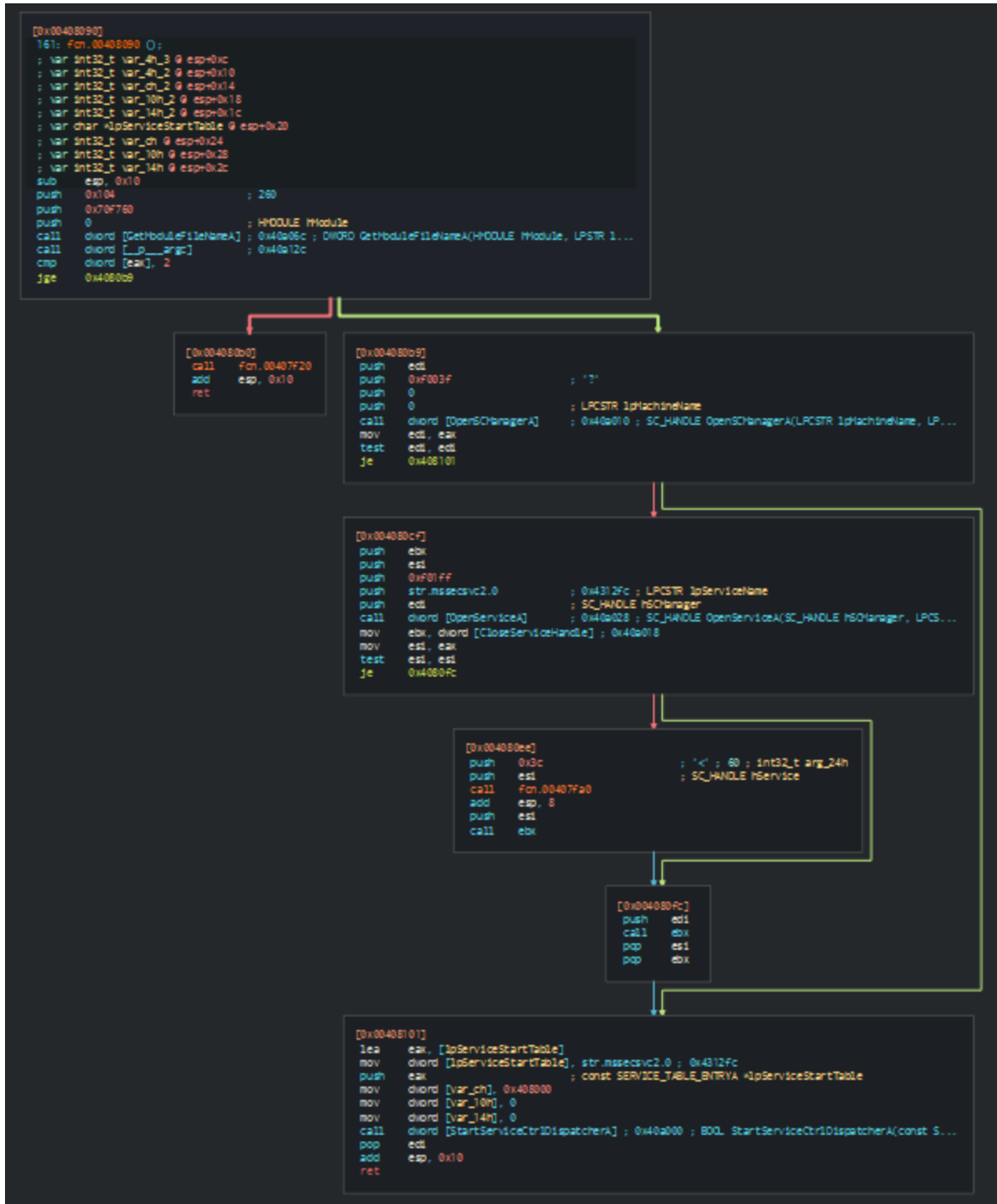
Overview of the main function

```

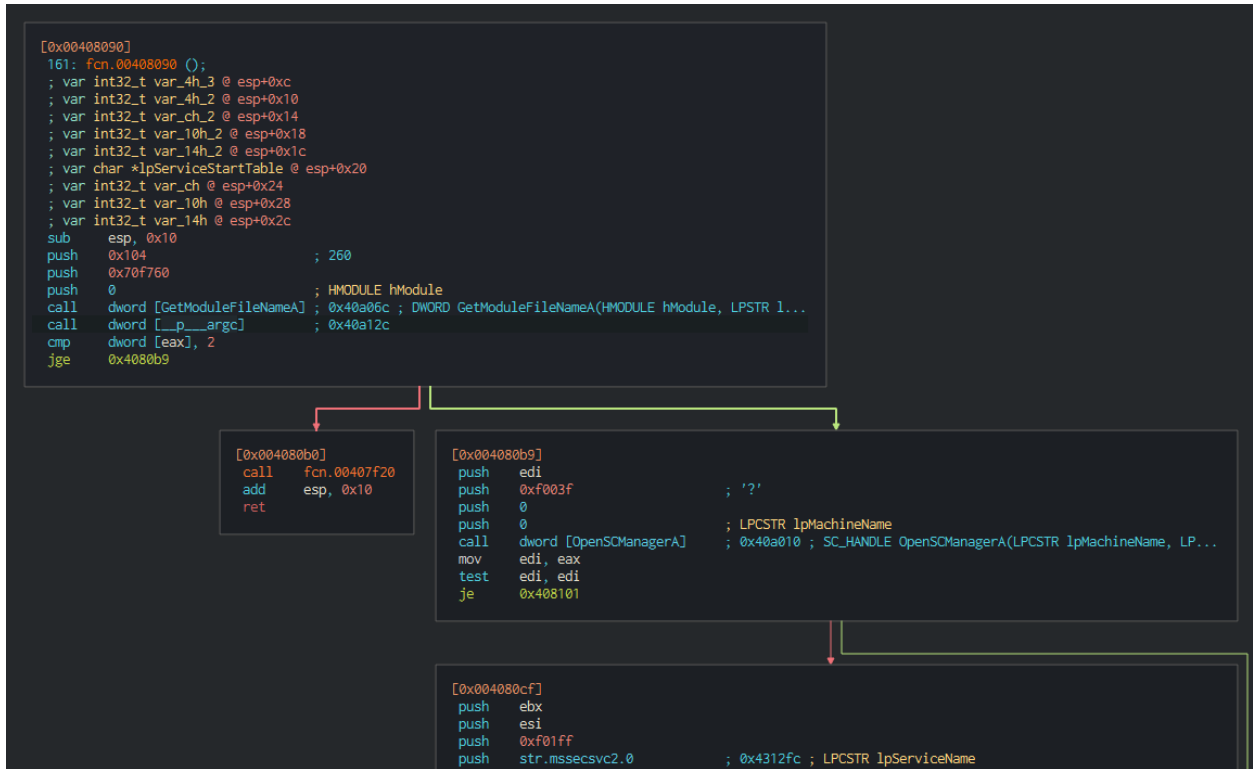
push esi
push edi
mov ecx, 0xe ; 14
mov esi, str.http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com ; 0x4313d0
lea edi, [var_8h]
xor eax, eax
rep movsd dword es:[edi], dword ptr [esi]
movsb byte es:[edi], byte ptr [esi]
mov dword [var_41h], eax
mov dword [var_45h], eax
mov dword [var_49h], eax
mov dword [var_4dh], eax
mov dword [var_51h], eax
mov word [var_55h], ax
push eax
push eax
push eax
push 1 ; 1
push eax
mov byte [var_6bh], al
call dword [InternetOpenA] ; 0x40a134
push 0
push 0x84000000
push 0
lea ecx, [var_14h]
mov esi, eax
push 0
push ecx
push esi
call dword [InternetOpenUrlA] ; 0x40a138
mov edi, eax
push esi
mov esi, dword [InternetCloseHandle] ; 0x40a13c
test edi, edi
jne 0x4081bc

```

Details of the main function, showing the three APIs used to connect to the malicious URL, the arguments passed to the APIs, including the URL itself.



Overview of the malicious routines.



Detail of the malicious function.

Advanced Dynamic Analysis

During the advanced dynamic analysis, there was additional confirmation and deeper understanding of the killswitch domain.

Using x32dbg, a breakpoint was set at address 00408140 (obtained from Cutter), which corresponds to the main section of the program where the killswitch URL was checked before proceeding further..

```
00408140 8BEC 50      sub esp,50
00408141 54        push esi
00408142 57        mov ecx,e
00408143 8B 0E000000 mov esi,ransomware.wannacry,4313D0
00408144 BE D0134300 test edi,dword ptr ss:[esp+4]
00408145 82C724 09    xor eax,ecx
00408146 33C0      movsb
00408147 44        movsb
00408148 894424 41    mov dword ptr ss:[esp+1],eax
00408149 894424 45    mov dword ptr ss:[esp+5],eax
0040814A 894424 49    mov dword ptr ss:[esp+9],eax
0040814B 894424 53    mov dword ptr ss:[esp+13],eax
0040814C 66894424 55 mov word ptr ss:[esp+17],eax
0040814D 50        push eax
0040814E 50        push eax
0040814F 6A 01     push 1
00408150 50        push eax
00408151 8B4424 4E    mov byte ptr ss:[esp+8],al
00408152 FF15 14444000 call dword ptr ds:[!InternetOpenA@]
00408153 6A 00     push 0
00408154 6A 00000084 push 84000000
00408155 50        push ecx
00408156 8B4424 14    mov ecx,dword ptr ss:[esp+14]
00408157 8BFF     mov esi,ecx
00408158 6A 00     push 0
00408159 6A 00     push 0
0040815A 51        push esi
0040815B FF15 38A14000 call dword ptr ds:[!InternetOpenA@]
0040815C 8BF8     mov esi,ecx
0040815D 8B35 3A140000 mov esi,dword ptr ds:[!InternetCloseHandle@]
0040815E 75 15     test edi,edi
0040815F 7F0E     call edi
00408160 6A 00     push 0
00408161 7F0E     call edi
00408162 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408163 57        mov edi,ecx
00408164 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408165 57        mov edi,ecx
00408166 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408167 57        mov edi,ecx
00408168 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408169 57        mov edi,ecx
0040816A 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040816B 57        mov edi,ecx
0040816C 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040816D 57        mov edi,ecx
0040816E 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040816F 57        mov edi,ecx
00408170 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408171 57        mov edi,ecx
00408172 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408173 57        mov edi,ecx
00408174 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408175 57        mov edi,ecx
00408176 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408177 57        mov edi,ecx
00408178 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408179 57        mov edi,ecx
0040817A 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040817B 57        mov edi,ecx
0040817C 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040817D 57        mov edi,ecx
0040817E 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040817F 57        mov edi,ecx
00408180 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408181 57        mov edi,ecx
00408182 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408183 57        mov edi,ecx
00408184 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408185 57        mov edi,ecx
00408186 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408187 57        mov edi,ecx
00408188 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408189 57        mov edi,ecx
0040818A 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040818B 57        mov edi,ecx
0040818C 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040818D 57        mov edi,ecx
0040818E 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040818F 57        mov edi,ecx
00408190 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408191 57        mov edi,ecx
00408192 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408193 57        mov edi,ecx
00408194 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408195 57        mov edi,ecx
00408196 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408197 57        mov edi,ecx
00408198 8B4424 08    mov ecx,dword ptr ss:[esp+8]
00408199 57        mov edi,ecx
0040819A 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040819B 57        mov edi,ecx
0040819C 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040819D 57        mov edi,ecx
0040819E 8B4424 08    mov ecx,dword ptr ss:[esp+8]
0040819F 57        mov edi,ecx
004081A0 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081A1 57        mov edi,ecx
004081A2 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081A3 57        mov edi,ecx
004081A4 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081A5 57        mov edi,ecx
004081A6 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081A7 57        mov edi,ecx
004081A8 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081A9 57        mov edi,ecx
004081AA 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081AB 57        mov edi,ecx
004081AC 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081AD 57        mov edi,ecx
004081AE 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081AF 57        mov edi,ecx
004081B0 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081B1 57        mov edi,ecx
004081B2 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081B3 57        mov edi,ecx
004081B4 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081B5 57        mov edi,ecx
004081B6 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081B7 57        mov edi,ecx
004081B8 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081B9 57        mov edi,ecx
004081BA 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081BB 57        mov edi,ecx
004081BC 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081BD 57        mov edi,ecx
004081BE 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081BF 57        mov edi,ecx
004081C0 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081C1 57        mov edi,ecx
004081C2 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081C3 57        mov edi,ecx
004081C4 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081C5 57        mov edi,ecx
004081C6 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081C7 57        mov edi,ecx
004081C8 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081C9 57        mov edi,ecx
004081CA 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081CB 57        mov edi,ecx
004081CC 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081CD 57        mov edi,ecx
004081CE 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081CF 57        mov edi,ecx
004081D0 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081D1 57        mov edi,ecx
004081D2 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081D3 57        mov edi,ecx
004081D4 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081D5 57        mov edi,ecx
004081D6 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081D7 57        mov edi,ecx
004081D8 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081D9 57        mov edi,ecx
004081DA 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081DB 57        mov edi,ecx
004081DC 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081DD 57        mov edi,ecx
004081DE 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081DF 57        mov edi,ecx
004081E0 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081E1 57        mov edi,ecx
004081E2 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081E3 57        mov edi,ecx
004081E4 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081E5 57        mov edi,ecx
004081E6 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081E7 57        mov edi,ecx
004081E8 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081E9 57        mov edi,ecx
004081EA 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081EB 57        mov edi,ecx
004081EC 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081ED 57        mov edi,ecx
004081EE 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081EF 57        mov edi,ecx
004081F0 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081F1 57        mov edi,ecx
004081F2 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081F3 57        mov edi,ecx
004081F4 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081F5 57        mov edi,ecx
004081F6 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081F7 57        mov edi,ecx
004081F8 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081F9 57        mov edi,ecx
004081FA 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081FB 57        mov edi,ecx
004081FC 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081FD 57        mov edi,ecx
004081FE 8B4424 08    mov ecx,dword ptr ss:[esp+8]
004081FF 57        mov edi,ecx
```

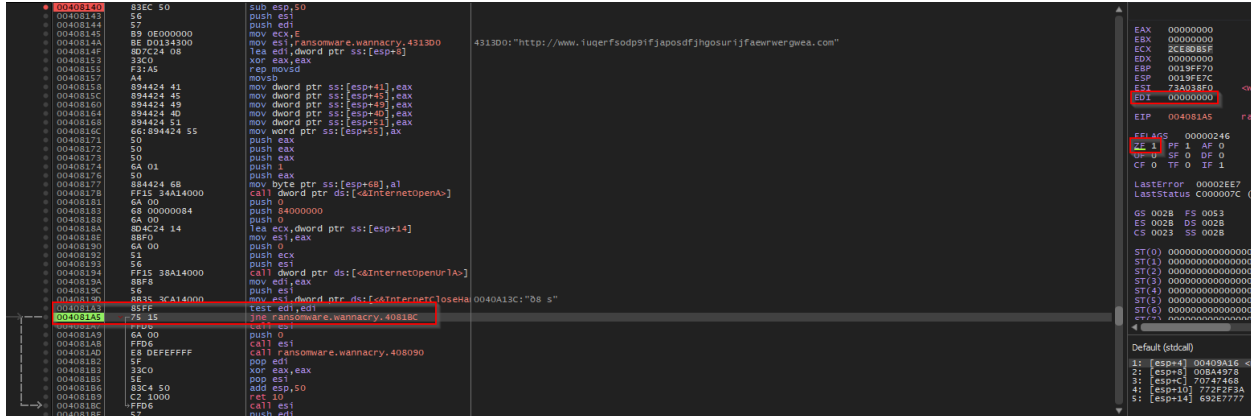
From that point, it was possible to meticulously follow the execution and validate the program's behavior, which can be summarized as follows:

- The malicious URL is inaccessible (either due to the non-existence of the domain in the wild or the absence of an active inetsim service in the forensic environment).
- ZF (Zero Flag) is already set to 1.
- The program establishes a connection to the URL.
- No response is received from the URL, resulting in EAX being set to 0.
- EAX is then copied to EDI, making EDI also 0.
- The program performs a test on EDI against EDI, resulting in 0 (since 0 and 0 = 0).
- ZF remains set to 1 since the result of the test function is 0.
- JNE (Jump if Not Equal) will not jump to the end of the program because ZF is not 0. This means that it will instead go through the malicious routine as explained in the Advanced Static Analysis section.

Note: For this summary, I have chosen to omit the details of the API calls shown in the screenshot and focus solely on the specific set of instructions

relevant to this particular killswitch behavior.

The following screenshot highlights the points of interest, at the moment where the jump is about to (not) be taken:



In this case, the program will proceed with the remaining instructions and eventually reach the call at address 004081AD, which points to the malicious function located at 00408090 (as indicated in the previous screenshot and also in the Cutter screenshot provided earlier in this report).

It is important to note that modifying the JNE instruction to JE would allow the malware to execute its malicious payload even if the URL is unreachable (for example, by patching the binary using Cutter). Similarly, during debugging with x32dbg, changing the ZF to 0 could lead to a similar outcome, enabling the execution of the malicious payload.

Indicators of Compromise

Network Indicators

Connection to the URL:

hxxp[://]www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 5) is a DNS Standard query from 10.0.0.4 to 10.0.0.3. Subsequent packets (Nos. 6-19) are ICMP Destination unreachable (Port unreachable) responses from 10.0.0.3 to 10.0.0.4. The packet list pane shows the following data:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|-------------------|----------|--------|--|
| 1 | 0.000000 | PcsCompu_55:06:07 | PcsCompu_7d:a6:a5 | ARP | 42 | Who has 10.0.0.3? Tell 10.0.0.4 |
| 2 | 0.001336 | PcsCompu_7d:a6:a5 | PcsCompu_55:06:07 | ARP | 60 | 10.0.0.3 is at 08:00:27:7d:a6:a5 |
| 3 | 0.135212 | PcsCompu_7d:a6:a5 | PcsCompu_55:06:07 | ARP | 60 | Who has 10.0.0.4? Tell 10.0.0.3 |
| 4 | 0.135226 | PcsCompu_55:06:07 | PcsCompu_7d:a6:a5 | ARP | 42 | 10.0.0.4 is at 08:00:27:55:06:07 |
| 5 | 17.541821 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 6 | 17.542090 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 7 | 17.542164 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 8 | 17.542414 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 9 | 17.542480 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 10 | 17.542743 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 11 | 17.542799 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 12 | 17.543029 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 13 | 17.543079 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0x261f A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 14 | 17.543291 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 15 | 17.611432 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0xa625 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 16 | 17.611793 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 17 | 17.612430 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0xa625 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 18 | 18.627868 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0xa625 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 19 | 18.628333 | 10.0.0.3 | 10.0.0.4 | ICMP | 137 | Destination unreachable (Port unreachable) |
| 20 | 18.628717 | 10.0.0.4 | 10.0.0.3 | DNS | 109 | Standard query 0xa625 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com |
| 21 | 22.516112 | PcsCompu_55:06:07 | PcsCompu_7d:a6:a5 | ARP | 42 | Who has 10.0.0.3? Tell 10.0.0.4 |
| 22 | 22.517377 | PcsCompu_7d:a6:a5 | PcsCompu_55:06:07 | ARP | 60 | 10.0.0.3 is at 08:00:27:7d:a6:a5 |

The packet details pane shows the selected packet (No. 5) as a DNS Standard query (0x261f A) for www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com. The packet bytes pane shows the raw data in hexadecimal and ASCII format.

Connections to several IP addresses on port 445:

Wireshark interface showing network traffic capture. The packet list pane displays various DNS queries and one ICMP message. The packet bytes pane shows the raw data for the selected ICMP packet.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------|--------------|----------|--------|---|
| 67 | 25.944954 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x0081 PTR 1.18.254.169.in-addr.arpa |
| 68 | 25.950233 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x634a PTR 1.19.254.169.in-addr.arpa |
| 69 | 25.951962 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xa19d PTR 1.20.254.169.in-addr.arpa |
| 70 | 26.005728 | 10.0.0.4 | 44.43.50.98 | TCP | 66 | 20002 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 71 | 26.673974 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0xfcd4 PTR 66.27.44.89.in-addr.arpa |
| 72 | 26.701598 | 10.0.0.4 | 10.0.0.3 | DNS | 81 | Standard query 0x28df PTR 1.0.0.10.in-addr.arpa |
| 73 | 26.701694 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0xe65c PTR 1.0.254.169.in-addr.arpa |
| 74 | 26.702002 | 10.0.0.3 | 10.0.0.4 | ICMP | 109 | Destination unreachable (Port unreachable) |
| 75 | 26.710407 | 10.0.0.4 | 71.244.78.67 | TCP | 66 | 20012 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 76 | 26.710528 | 10.0.0.4 | 10.0.0.3 | DNS | 81 | Standard query 0x28df PTR 1.0.0.10.in-addr.arpa |
| 77 | 26.714207 | 10.0.0.4 | 10.0.0.3 | DNS | 86 | Standard query 0x4047 PTR 148.42.208.31.in-addr.arpa |
| 78 | 26.724655 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x69ba PTR 1.21.254.169.in-addr.arpa |
| 79 | 26.726261 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0x0e37 PTR 1.1.254.169.in-addr.arpa |
| 80 | 26.740819 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x6237 PTR 1.22.254.169.in-addr.arpa |
| 81 | 26.741069 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0x543c PTR 1.2.254.169.in-addr.arpa |
| 82 | 26.741131 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0x4997 PTR 1.3.254.169.in-addr.arpa |
| 83 | 26.743241 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xe918 PTR 1.23.254.169.in-addr.arpa |
| 84 | 26.747364 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xe9d8 PTR 1.24.254.169.in-addr.arpa |
| 85 | 26.749615 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xb996 PTR 1.25.254.169.in-addr.arpa |
| 86 | 26.753146 | 10.0.0.4 | 10.0.0.3 | DNS | 84 | Standard query 0x8037 PTR 1.4.254.169.in-addr.arpa |
| 87 | 26.756525 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0x0f91 PTR 1.26.254.169.in-addr.arpa |
| 88 | 26.768224 | 10.0.0.4 | 10.0.0.3 | DNS | 85 | Standard query 0xf423 PTR 1.27.254.169.in-addr.arpa |

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{5DE24529-6A8E-414C-8A8E-1FF9F4B73334}, id 0

```

0000 08 00 27 7d a6 a5 08 00 27 55 06 07 08 06 00 01  ...}....U.....
0010 08 00 06 04 00 01 08 00 27 55 06 07 0a 00 00 04  ...}....U.....
0020 08 00 27 7d a6 a5 0a 00 00 03  ...}....
    
```

TCPView - Sysinternals: www.sysinternals.com

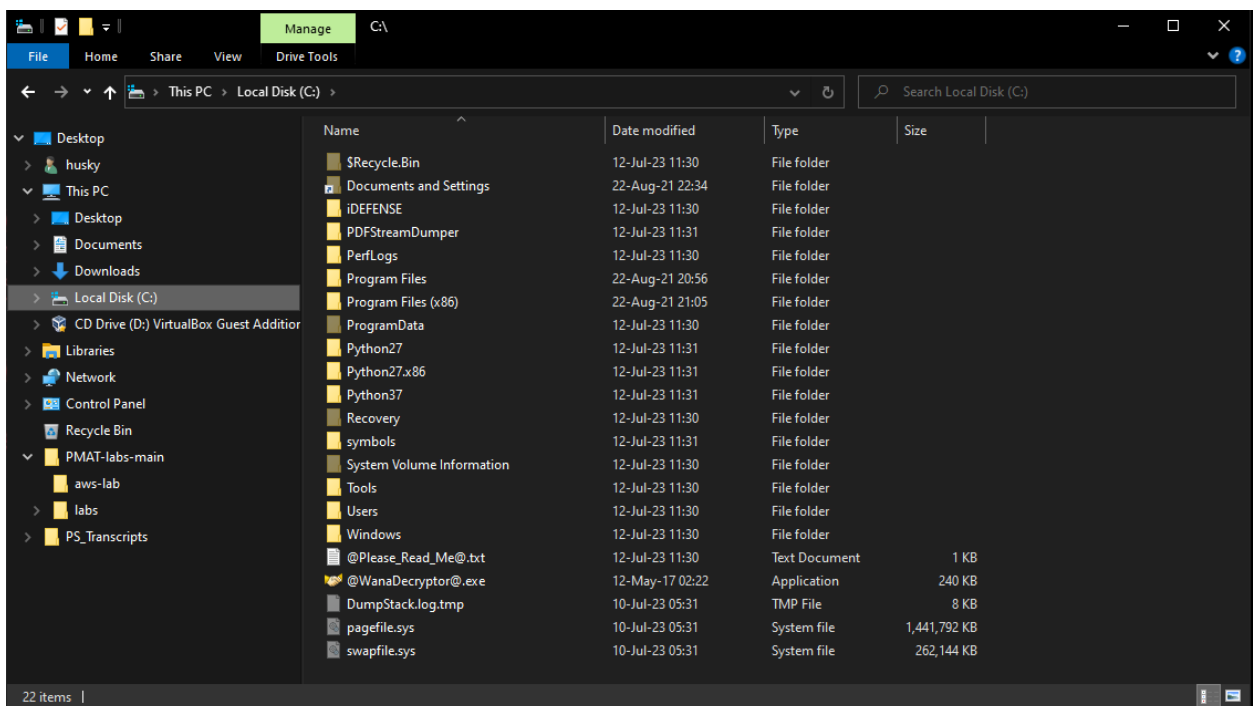
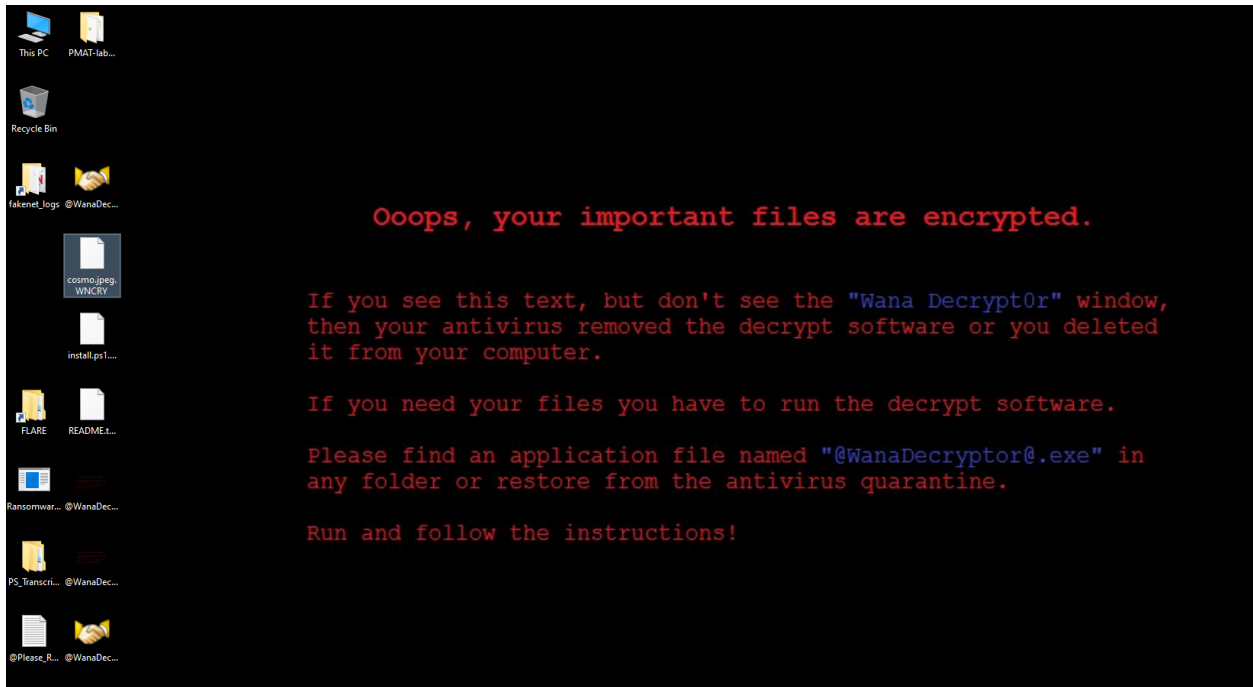
Process Name | Process ID | Protocol | State | Local Address | Local Port | Remote Address | Remote Port | Create Time | Module Name | Sent Packets

| | | | | | | | | | | |
|-------------------------|------|-----|----------|----------------|-------|-----------------|-----|--------------------|------------|--|
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20942 | 86.152.177.210 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20943 | 105.146.204.243 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20944 | 169.254.212.2 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20945 | 169.254.213.2 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20946 | 169.254.214.2 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20947 | 134.5.147.210 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20948 | 69.228.30.22 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20949 | 45.142.229.99 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20950 | 179.244.18.115 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20951 | 150.170.177.183 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20952 | 169.254.215.2 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20953 | 169.254.216.2 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20954 | 177.172.7.101 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20955 | 113.235.53.197 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20956 | 169.254.217.2 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20957 | 19.126.238.132 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20958 | 223.150.251.18 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20959 | 62.163.19.55 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20960 | 169.254.218.2 | 445 | 12-Jul-23 09:56:39 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20961 | 200.23.188.107 | 445 | 12-Jul-23 09:56:40 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20962 | 188.14.133.8 | 445 | 12-Jul-23 09:56:40 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20963 | 169.254.219.2 | 445 | 12-Jul-23 09:56:40 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 169.254.243.48 | 20964 | 169.254.220.2 | 445 | 12-Jul-23 09:56:40 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20965 | 128.131.135.44 | 445 | 12-Jul-23 09:56:40 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20966 | 65.24.68.190 | 445 | 12-Jul-23 09:56:40 | mssecsv2.0 | |
| Ransomware.wannacry.exe | 1552 | TCP | Syn Sent | 10.0.0.4 | 20967 | 174.185.51.94 | 445 | 12-Jul-23 09:56:40 | mssecsv2.0 | |
| lsass.exe | 648 | TCP | Listen | 0.0.0.0 | 49664 | 0.0.0.0 | 0 | 10-Jul-23 05:31:25 | lsass.exe | |

Endpoints: 881 | Established: | Listening: 25 | Time Wait: | Close Wait: | Update: 2 sec | States: (All)

Host-based Indicators

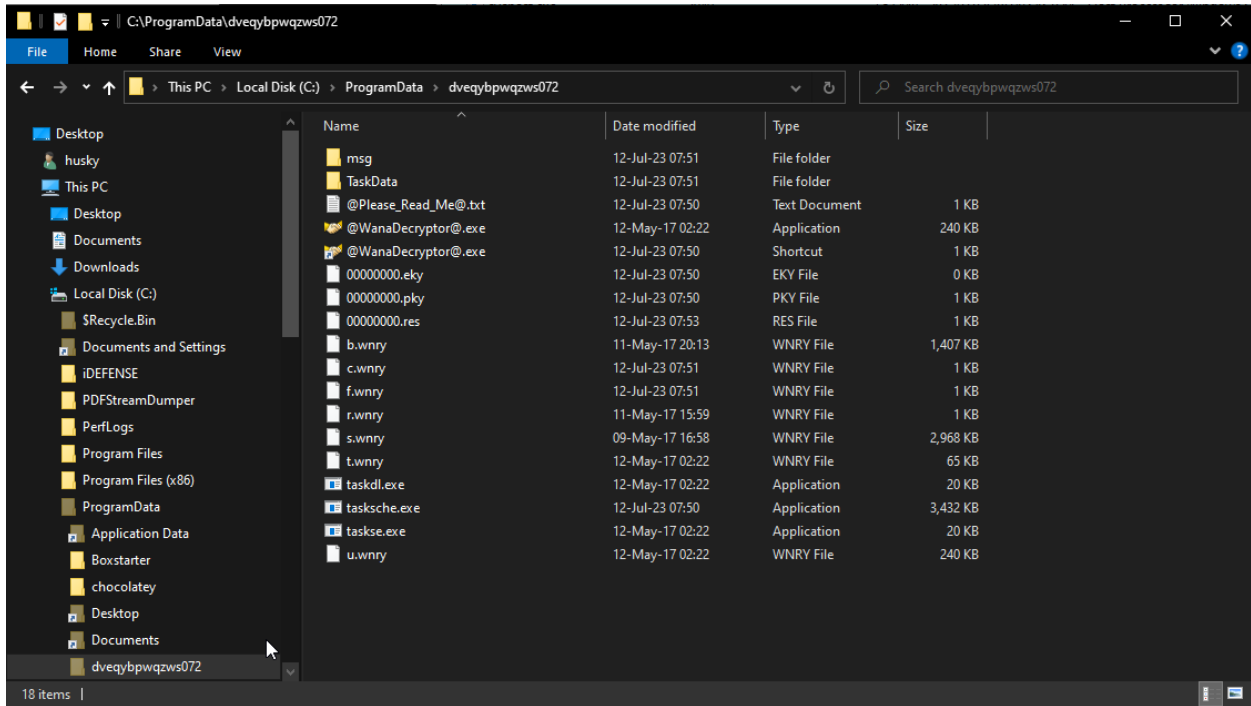
Desktop wallpaper changed, local files encrypted with extension .wncry, presence of new files on the desktop (and, in time, inside other folders as well):



Program loading on the foreground every few seconds:

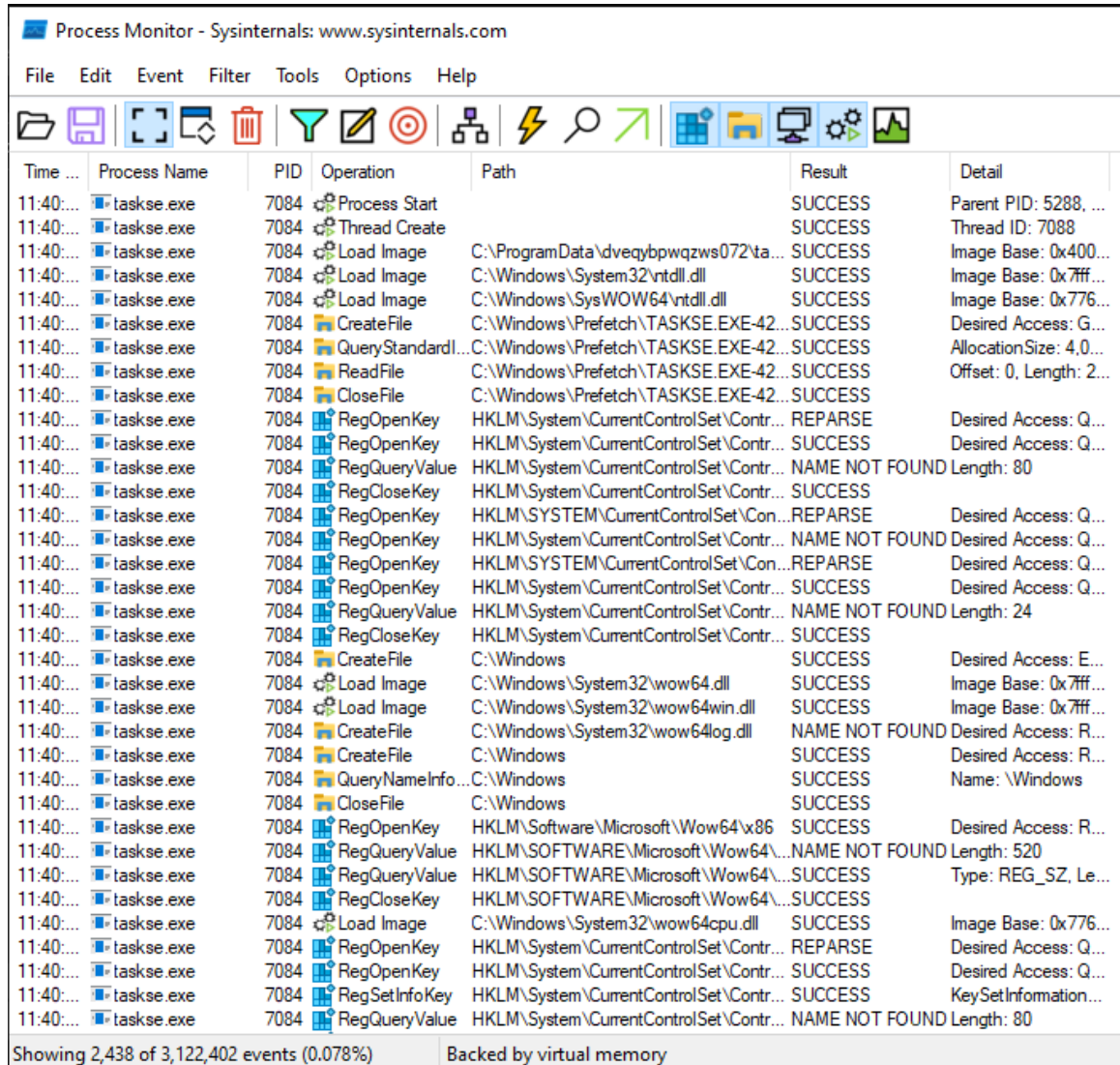


Creation of a new folder named “dveqybpwqzws072” inside C:\ProgramData\ containing malicious files. The folder and its content is set to Hidden:



New processes:

tasksche.exe / taskdl.exe / taskse.exe



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time ... | Process Name | PID | Operation | Path | Result | Detail |
|-----------|--------------|------|-------------------|--|----------------|-------------------------|
| 11:40:... | taskse.exe | 7084 | Process Start | | SUCCESS | Parent PID: 5288, ... |
| 11:40:... | taskse.exe | 7084 | Thread Create | | SUCCESS | Thread ID: 7088 |
| 11:40:... | taskse.exe | 7084 | Load Image | C:\ProgramData\dveqybpwqzws072\ta... | SUCCESS | Image Base: 0x400... |
| 11:40:... | taskse.exe | 7084 | Load Image | C:\Windows\System32\ntdll.dll | SUCCESS | Image Base: 0x7ff... |
| 11:40:... | taskse.exe | 7084 | Load Image | C:\Windows\SysWOW64\ntdll.dll | SUCCESS | Image Base: 0x776... |
| 11:40:... | taskse.exe | 7084 | CreateFile | C:\Windows\Prefetch\TASKSE.EXE-42... | SUCCESS | Desired Access: G... |
| 11:40:... | taskse.exe | 7084 | QueryStandardI... | C:\Windows\Prefetch\TASKSE.EXE-42... | SUCCESS | AllocationSize: 4,0... |
| 11:40:... | taskse.exe | 7084 | ReadFile | C:\Windows\Prefetch\TASKSE.EXE-42... | SUCCESS | Offset: 0, Length: 2... |
| 11:40:... | taskse.exe | 7084 | CloseFile | C:\Windows\Prefetch\TASKSE.EXE-42... | SUCCESS | |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | REPARSE | Desired Access: Q... |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... |
| 11:40:... | taskse.exe | 7084 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 80 |
| 11:40:... | taskse.exe | 7084 | RegCloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Desired Access: Q... |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... |
| 11:40:... | taskse.exe | 7084 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 24 |
| 11:40:... | taskse.exe | 7084 | RegCloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | |
| 11:40:... | taskse.exe | 7084 | CreateFile | C:\Windows | SUCCESS | Desired Access: E... |
| 11:40:... | taskse.exe | 7084 | Load Image | C:\Windows\System32\wow64.dll | SUCCESS | Image Base: 0x7ff... |
| 11:40:... | taskse.exe | 7084 | Load Image | C:\Windows\System32\wow64win.dll | SUCCESS | Image Base: 0x7ff... |
| 11:40:... | taskse.exe | 7084 | CreateFile | C:\Windows\System32\wow64log.dll | NAME NOT FOUND | Desired Access: R... |
| 11:40:... | taskse.exe | 7084 | CreateFile | C:\Windows | SUCCESS | Desired Access: R... |
| 11:40:... | taskse.exe | 7084 | QueryNameInfo... | C:\Windows | SUCCESS | Name: Windows |
| 11:40:... | taskse.exe | 7084 | CloseFile | C:\Windows | SUCCESS | |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\Software\Microsoft\Wow64\86 | SUCCESS | Desired Access: R... |
| 11:40:... | taskse.exe | 7084 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Wow64\... | NAME NOT FOUND | Length: 520 |
| 11:40:... | taskse.exe | 7084 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Wow64\... | SUCCESS | Type: REG_SZ, Le... |
| 11:40:... | taskse.exe | 7084 | RegCloseKey | HKLM\SOFTWARE\Microsoft\Wow64\... | SUCCESS | |
| 11:40:... | taskse.exe | 7084 | Load Image | C:\Windows\System32\wow64cpu.dll | SUCCESS | Image Base: 0x776... |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | REPARSE | Desired Access: Q... |
| 11:40:... | taskse.exe | 7084 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... |
| 11:40:... | taskse.exe | 7084 | RegSetInfoKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | KeySetInformation... |
| 11:40:... | taskse.exe | 7084 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 80 |

Showing 2,438 of 3,122,402 events (0.078%) Backed by virtual memory



| Time ... | Process Name | PID | Operation | Path | Result | Detail |
|-----------|--------------|------|-------------------|--|----------------|-------------------------|
| 11:40:... | taskdl.exe | 6672 | Process Start | | SUCCESS | Parent PID: 5288, ... |
| 11:40:... | taskdl.exe | 6672 | Thread Create | | SUCCESS | Thread ID: 6676 |
| 11:40:... | taskdl.exe | 6672 | Load Image | C:\ProgramData\dveqybpwqzws072\ta... | SUCCESS | Image Base: 0x400... |
| 11:40:... | taskdl.exe | 6672 | Load Image | C:\Windows\System32\ntdll.dll | SUCCESS | Image Base: 0x7ff... |
| 11:40:... | taskdl.exe | 6672 | Load Image | C:\Windows\SysWOW64\ntdll.dll | SUCCESS | Image Base: 0x776... |
| 11:40:... | taskdl.exe | 6672 | CreateFile | C:\Windows\Prefetch\TASKDL.EXE-D... | SUCCESS | Desired Access: G... |
| 11:40:... | taskdl.exe | 6672 | QueryStandardI... | C:\Windows\Prefetch\TASKDL.EXE-D... | SUCCESS | AllocationSize: 4.0... |
| 11:40:... | taskdl.exe | 6672 | ReadFile | C:\Windows\Prefetch\TASKDL.EXE-D... | SUCCESS | Offset: 0, Length: 2... |
| 11:40:... | taskdl.exe | 6672 | CloseFile | C:\Windows\Prefetch\TASKDL.EXE-D... | SUCCESS | |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | REPARSE | Desired Access: Q... |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... |
| 11:40:... | taskdl.exe | 6672 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 80 |
| 11:40:... | taskdl.exe | 6672 | RegCloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Desired Access: Q... |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... |
| 11:40:... | taskdl.exe | 6672 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 24 |
| 11:40:... | taskdl.exe | 6672 | RegCloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | |
| 11:40:... | taskdl.exe | 6672 | CreateFile | C:\Windows | SUCCESS | Desired Access: E... |
| 11:40:... | taskdl.exe | 6672 | Load Image | C:\Windows\System32\wow64.dll | SUCCESS | Image Base: 0x7ff... |
| 11:40:... | taskdl.exe | 6672 | Load Image | C:\Windows\System32\wow64win.dll | SUCCESS | Image Base: 0x7ff... |
| 11:40:... | taskdl.exe | 6672 | CreateFile | C:\Windows\System32\wow64log.dll | NAME NOT FOUND | Desired Access: R... |
| 11:40:... | taskdl.exe | 6672 | CreateFile | C:\Windows | SUCCESS | Desired Access: R... |
| 11:40:... | taskdl.exe | 6672 | QueryNameInfo... | C:\Windows | SUCCESS | Name: \Windows |
| 11:40:... | taskdl.exe | 6672 | CloseFile | C:\Windows | SUCCESS | |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\Software\Microsoft\Wow64\x86 | SUCCESS | Desired Access: R... |
| 11:40:... | taskdl.exe | 6672 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Wow64\... | NAME NOT FOUND | Length: 520 |
| 11:40:... | taskdl.exe | 6672 | RegQueryValue | HKLM\SOFTWARE\Microsoft\Wow64\... | SUCCESS | Type: REG_SZ, Le... |
| 11:40:... | taskdl.exe | 6672 | RegCloseKey | HKLM\SOFTWARE\Microsoft\Wow64\... | SUCCESS | |
| 11:40:... | taskdl.exe | 6672 | Load Image | C:\Windows\System32\wow64cpu.dll | SUCCESS | Image Base: 0x776... |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | REPARSE | Desired Access: Q... |
| 11:40:... | taskdl.exe | 6672 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | Desired Access: Q... |
| 11:40:... | taskdl.exe | 6672 | RegSetInfoKey | HKLM\System\CurrentControlSet\Contr... | SUCCESS | KeySetInformation... |
| 11:40:... | taskdl.exe | 6672 | RegQueryValue | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Length: 80 |

Showing 880 of 3,518,350 events (0.025%)

Backed by virtual memory

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time ... | Process Name | PID | Operation | Path | Result | Detail |
|-----------|--------------|------|--------------------|--------------------------------------|----------------|-------------------------|
| 11:40:... | tasksche.exe | 5288 | CreateFile | C:\ProgramData\dveqybpwqzws072\00... | SUCCESS | Desired Access: G... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\ProgramData\dveqybpwqzws072\00... | SUCCESS | Offset: 0, Length: 1... |
| 11:40:... | tasksche.exe | 5288 | CloseFile | C:\ProgramData\dveqybpwqzws072\00... | SUCCESS | |
| 11:40:... | tasksche.exe | 5288 | CreateFile | C:\ | SUCCESS | Desired Access: S... |
| 11:40:... | tasksche.exe | 5288 | QueryFullSizeln... | C:\ | SUCCESS | TotalAllocationUnit... |
| 11:40:... | tasksche.exe | 5288 | CloseFile | C:\ | SUCCESS | |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,276,044,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,286,530,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,297,016,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,307,502,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,317,987,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,328,473,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,338,959,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,349,445,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,359,930,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,370,416,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,380,902,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,391,388,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,401,873,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,412,359,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,422,845,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,433,331,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,443,816,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,454,302,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,464,788,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,475,274,... |
| 11:40:... | tasksche.exe | 5288 | CreateFile | C:\ProgramData\dveqybpwqzws072\00... | NAME NOT FOUND | Desired Access: R... |
| 11:40:... | tasksche.exe | 5288 | CreateFile | C:\ProgramData\dveqybpwqzws072\00... | NAME NOT FOUND | Desired Access: R... |
| 11:40:... | tasksche.exe | 5288 | CreateFile | C:\ | SUCCESS | Desired Access: S... |
| 11:40:... | tasksche.exe | 5288 | QueryFullSizeln... | C:\ | SUCCESS | TotalAllocationUnit... |
| 11:40:... | tasksche.exe | 5288 | CloseFile | C:\ | SUCCESS | |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,485,760,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,496,245,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,506,731,... |
| 11:40:... | tasksche.exe | 5288 | WriteFile | C:\Windows\Temp\hibsys.WNCRYT | SUCCESS | Offset: 10,517,217,... |

Showing 755 of 3,800,541 events (0.019%) Backed by virtual memory

New service:

mssecsvc2.0

| name | description | type | status | start | path |
|-------------|---|-------------|---------|--------------|---|
| MsSecFt | Microsoft Security Events Componen... | Driver | Running | Boot start | \SystemRoot\system32\dr...\mssecflt.sys |
| mssecsvc2.0 | Microsoft Security Center (2.0) Service | Own process | Running | Auto start | 3360 ...\\Ransomware.wannacry.exe -m security |
| mssmbios | Microsoft System Management BIOS ... | Driver | Running | System start | \SystemRoot\System32\...mssmbios.sys |

Rules & Signatures

A full set of YARA rules is included in Appendix A.

URL:

hxxp[:]//]www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

Strings:

WanaCrypt0r

.wnry

C:\%s\qeriuwjhrf

taskdl.exe

taskse.exe

tasksche.exe

115p7UMMngojl1pMvkpHijcRdfJNXj6LrLn

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

WANACRY!

\\172.16.99.5\IPC\$

\\192.168.56.20\IPC\$

Appendices

A. Yara Rules

```
rule WannaCry {  
  
    meta:  
        last_updated = "2023-07-12"  
        author = "Harpocrat3s"  
        description = "Detects WannaCry"  
        sha256 =  
"24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c"  
        // Providing the file's hash to pinpoint which strain of the  
malware this rules works on  
  
    strings:  
        $string1 = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"  
    ascii  
        $string2 = "WanaCrypt0r" ascii  
        $string3 = "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94" ascii  
        $string4 = "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn" ascii  
        $string5 = "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw" ascii  
        $string6 = "C:\\%s\\qeriuwjhrf" ascii  
        $string7 = "taskdl.exe" ascii  
        $string8 = "taskse.exe" ascii  
        $string9 = "tasksche.exe" ascii  
  
    condition:  
        any of ($string*)  
}
```

B. Bitcoin Wallet analysis

As every operation on the bitcoin blockchain is recorded, it was possible to check the history of the wallet used on this sample, but also to confirm that the other two strings found in the sample were indeed bitcoin wallets that also received funds in a similar fashion of the main wallet.

This further confirms the suspicion that other malware samples of WannaCry could use the other two wallets for a similar operation.

Here are the screenshots of the summary for the 3 bitcoin wallets found in the strings.

Further analysis could be done investigating where the funds were sent from these wallets, and investigate and correlate the other wallets with other strains of malwares (WannaCry or others), potentially finding out additional operations of the threat actor that originally developed this malware.

We can see that the total sum of money sent on the 3 wallets is 1,677,868 USD. It's not sure at this point if all the funds were due to WannaCry or if the wallets were used in other malware campaigns. Further investigation is required, but it's outside the scope of this analysis.

13AM4-aEb94 USD

Base58 (P2PKH)

Bitcoin Address
13AM4VW2dhxYgXeQepoHKHSQuy6NgaEb94

Bitcoin Balance
0.32843048 • \$10,073.10

| | Wallet | Chart |
|---|--|--|
| Summary | | |
| This address has transacted 143 times on the Bitcoin blockchain. It has received a total of 20.07353352 BTC \$615,663 and has sent a total of 19.74510304 BTC \$605,590. The current value of this address is 0.32843048 BTC \$10,073.10. | Total Received ● 20.07353352 BTC \$615,663 | Total Sent ● 19.74510304 BTC \$605,590 |
| | Transactions ● 143 | Total Volume ● 39.81863656 BTC \$1,221,254 |



115p7-6LrLn

USD

Base58 (P2PKH)

Bitcoin Address
115p7UMMngoj1pMvvpHjicRdfJNXj6LrLn

Bitcoin Balance
0.46702392 • \$14,323.82

Wallet

Chart

Summary

This address has transacted 124 times on the Bitcoin blockchain. It has received a total of 14.87769994 BTC \$456,305 and has sent a total of 14.41067602 BTC \$441,981 The current value of this address is 0.46702392 BTC \$14,323.82.

Total Received ●
14.87769994 BTC
\$456,305

Transactions ●
124

Total Sent ●
14.41067602 BTC
\$441,981

Total Volume ●
29.28837596 BTC
\$898,286



12t9Y-r6SMw

USD

Base58 (P2PKH)

Bitcoin Address
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Bitcoin Balance
1.92169961 • \$59,126.05

Wallet

Chart

Summary

This address has transacted 248 times on the Bitcoin blockchain. It has received a total of 19.69282998 BTC \$605,900 and has sent a total of 17.77113037 BTC \$546,774 The current value of this address is 1.92169961 BTC \$59,126.05.

Total Received ●
19.69282998 BTC
\$605,900

Transactions ●
248

Total Sent ●
17.77113037 BTC
\$546,774

Total Volume ●
37.46396035 BTC
\$1,152,675

C. List of file extensions

In the strings there's what looks like a list of file extensions that are encrypted by the malware:

| | | |
|-----------|--------|---------|
| .der | .accdb | .asf |
| .pfx | .mdb | .avi |
| .key | .dbf | .mov |
| .crt | .odb | .mp4 |
| .csr | .frm | .3gp |
| .p12 | .myd | .mkv |
| .pem | .myi | .3g2 |
| .odt | .ibd | .flv |
| .ott | .mdf | .wma |
| .sxw | .ldf | .mid |
| .stw | .sln | .m3u |
| .uot | .suo | .m4u |
| .3ds | .cpp | .djvu |
| .max | .pas | .svg |
| .3dm | .asm | .psd |
| .ods | .cmd | .nef |
| .ots | .bat | .tiff |
| .sxc | .ps1 | .tif |
| .stc | .vbs | .cgm |
| .dif | .dip | .raw |
| .slk | .dch | .gif |
| .wb2 | .sch | .png |
| .odp | .brd | .bmp |
| .otp | .jsp | .jpg |
| .sxd | .php | .jpeg |
| .std | .asp | .vcd |
| .uop | .java | .iso |
| .odg | .jar | .backup |
| .otg | .class | .zip |
| .sxm | .mp3 | .rar |
| .mml | .wav | .tgz |
| .lay | .swf | .tar |
| .lay6 | .fla | .bak |
| .asc | .wmv | .tbk |
| .sqlite3 | .mpg | .bz2 |
| .sqlitedb | .vob | .PAQ |
| .sql | .mpeg | .ARC |

.aes
.gpg
.vmx
.vmdk
.vdi
.sldm
.sldx
.sti
.sxi
.602
.hwp
.snt
.onetoc2
.dwg
.pdf
.wk1
.wks
.123
.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