MALWARE ANALYSIS OF WANNACRY RANSOMWARE

IE4032
Information Cyberwarfare
4th Year, 2nd Semester

Submitted to:

Sri Lanka Institute of Information Technology

Submitted by:
J.A.Y.N Jayasinghe – IT17037198

NOVEMBER 27, 2020

This is a Malware Analysis walkthrough of the WannaCry Ransomware. This document will be going through the steps to setup an analysis lab, precautions to take before beginning the analysis, and tools used to perform static and dynamic analysis of the malware.

WannaCry Introduction

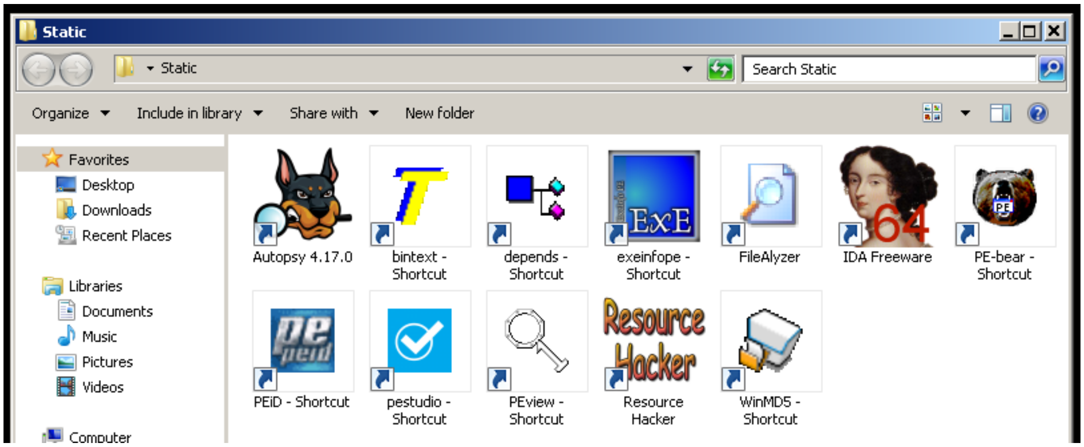
The WannaCry malware is a Ransomware that infects a computer by encrypting all files stored in the machine and demanding a ransom to be paid if the user wants their files to be decrypted.

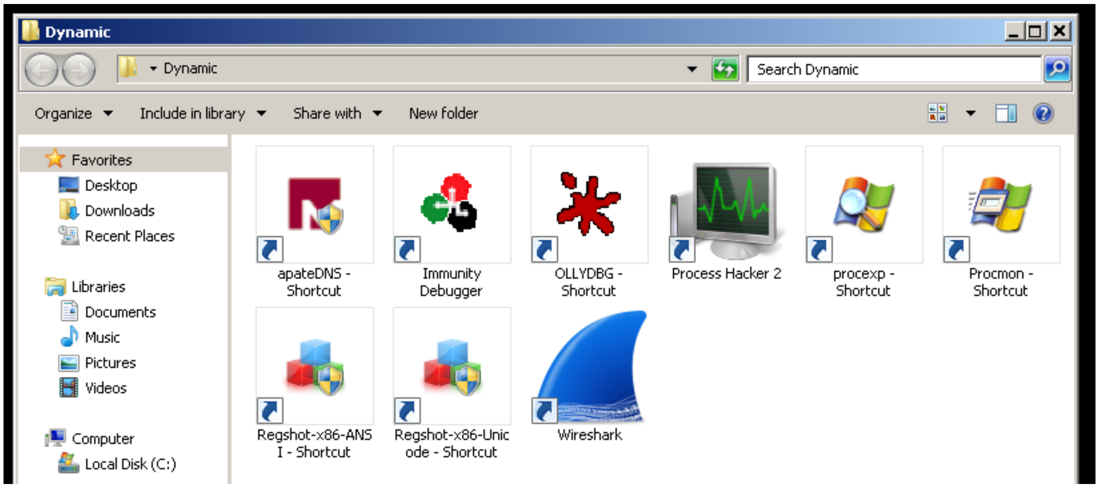
The beta was discovered on the 9th of February 2017, followed by Wannacry v1.0 on the 28th of March 2017. A second attack of the malware, WannaCry v2.0 began on the 12th of May 2017.

In the first week, WannaCry had infected at least 250,000 computers in more that 150 countries. According to Wcrypt tracker, over 500,000 systems are now affected. A ransom of $300 was demanded from victims, a demand which doubles after 3 days. If the ransom is not paid within 7 days, the files will be permanently deleted.

Lab Setup

The Analysis lab that will be used in this walkthrough is a Windows 7 Ultimate (SP2) Virtual machine running in Virtual Box. The analysis tools installed are shown below:





Static Analysis tools:

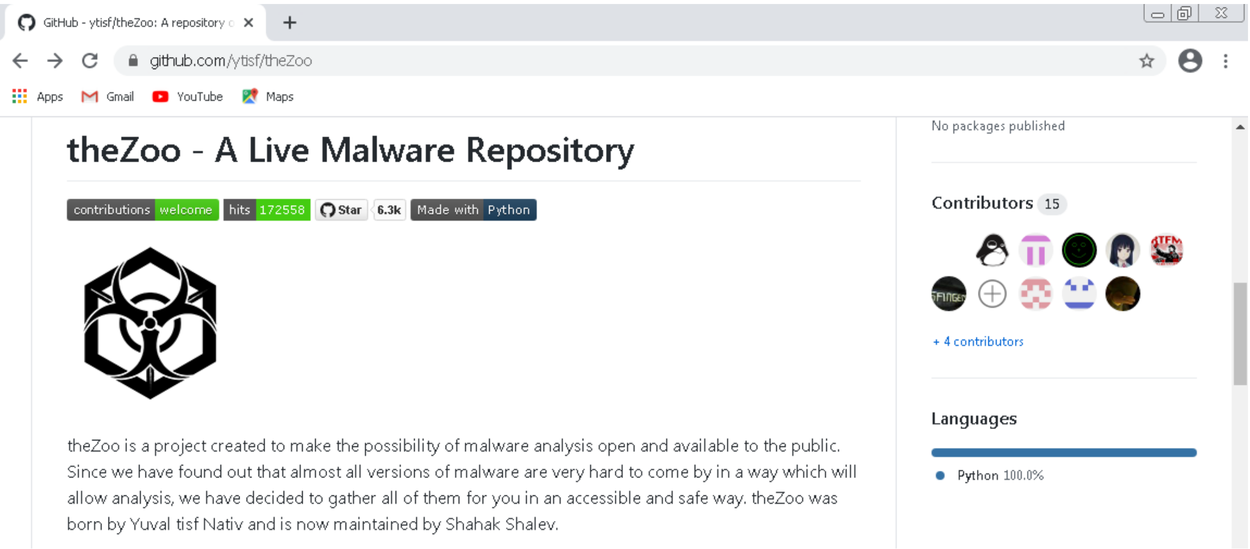
- Autopsy
- Bintext
- Dependency Walker
- EXEinfo PE
- FileAlyzer
- IDA
- PE-bear
- PEid
- PE Studio
- PE view
- Resource Hacker
- WinMD5

Dynamic Analysis tools:

- ApateDNS
- Immunity Debugger
- OllyDBG
- Process Hacker
- Process Explorer
- Process Monitor
- Regshot
- Wireshark

Downloading the Malware

“TheZoo” is a Github repository that contains a collection of malware all in one location for the purpose of making them easy to obtain for analysts. The repository can be accessed using www.github.com/ytisf/theZoo



theZoo - A Live Malware Repository

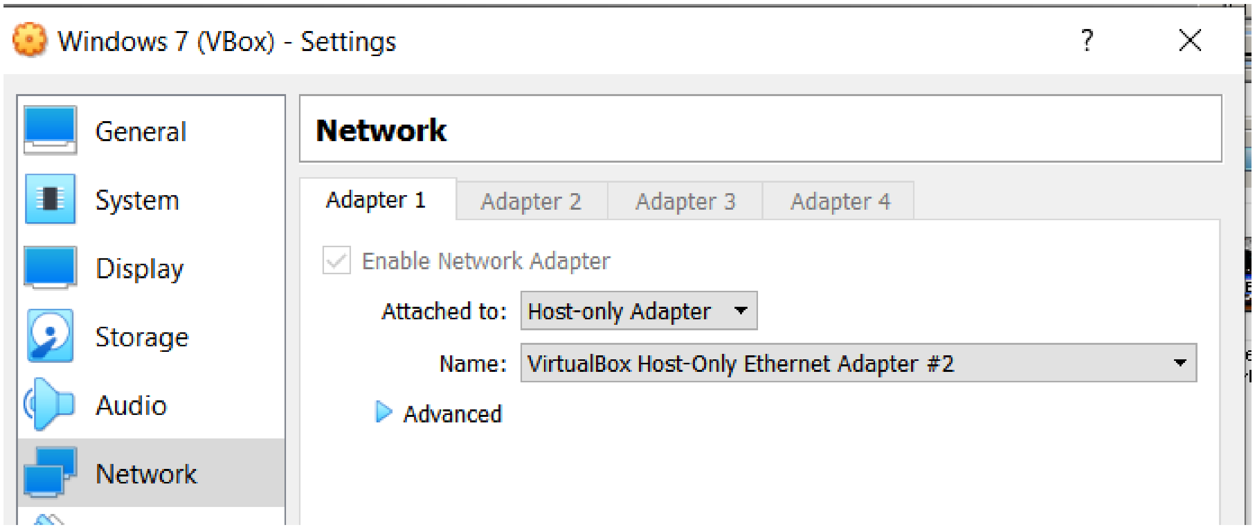
theZoo is a project created to make the possibility of malware analysis open and available to the public. Since we have found out that almost all versions of malware are very hard to come by in a way which will allow analysis, we have decided to gather all of them for you in an accessible and safe way. theZoo was born by Yuval tisf Nativ and is now maintained by Shahak Shalev.

In this repository, the Wannacry ransomware can be downloaded through the path:

theZoo/malwares/Binaries/Ransomware.WannaCry/ Ransomware.WannaCry.zip

Note that in this archived form it cannot infect any machine. It can be extracted using the password “infected”, but **before extracting the ransomware, the following precautions must be taken**.

- Remove any shared folders between the host and the VM.
- Uninstall VBox Guest Additions/ VMware Tools.
- Take a snapshot of the VM before running the malware.
- Set the Network Adapter to Host-only Adapter.



☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #2

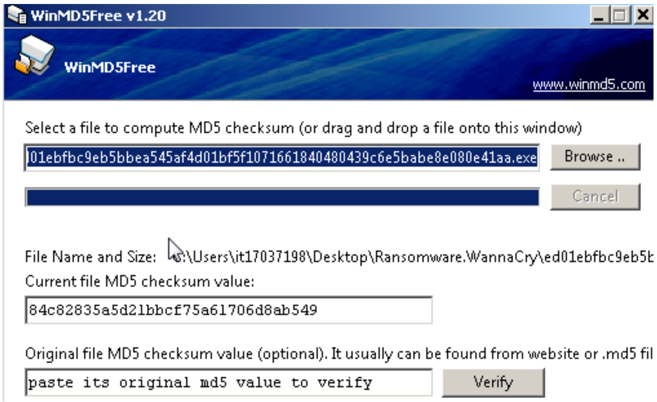
These settings will make sure that there is no connection between the VM and the Host machine so that the malware will not spread outside the Analysis Lab.

Static Analysis

Static Analysis is analyzing the malware without actually running it. This mainly consists of analyzing the PE header, Strings, and Process flows.

VirusTotal Results

The first thing we can do to analyze the malware is to see if it has been already been analyzed by antivirus software. To do this we can use the WinMD5 tool to obtain the MD5 checksum of the PE file, and search this hash in www.virustotal.com.



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

```
]01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
```

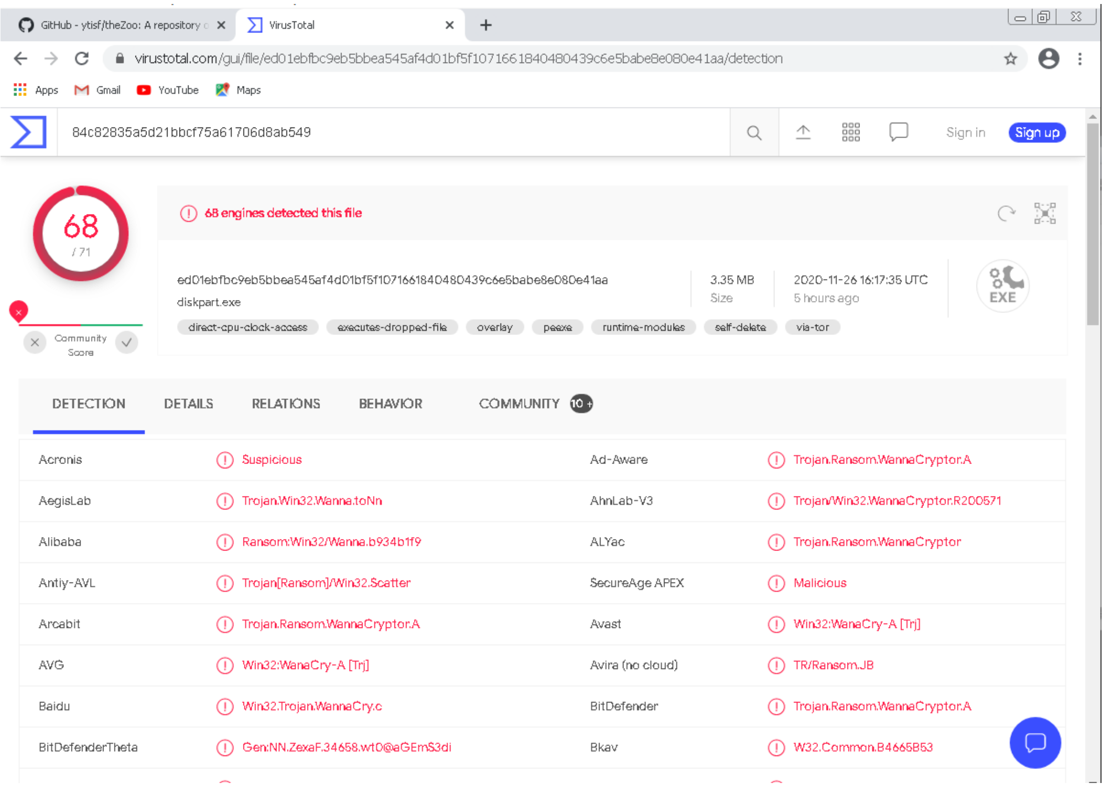
File Name and Size: C:\Users\it17037198\Desktop\Ransomware.WannaCry\ed01ebfbc9eb5b

Current file MD5 checksum value:

```
84c82835a5d21bbcf75a61706d8ab549
```

Original file MD5 checksum value (optional). It usually can be found from website or .md5 fil

```
paste its original md5 value to verify
```



virustotal.com/gui/file/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa/detection

84c82835a5d21bbcf75a61706d8ab549

68 / 71

68 engines detected this file

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
diskpart.exe

3.35 MB
Size

2020-11-26 16:17:35 UTC
5 hours ago

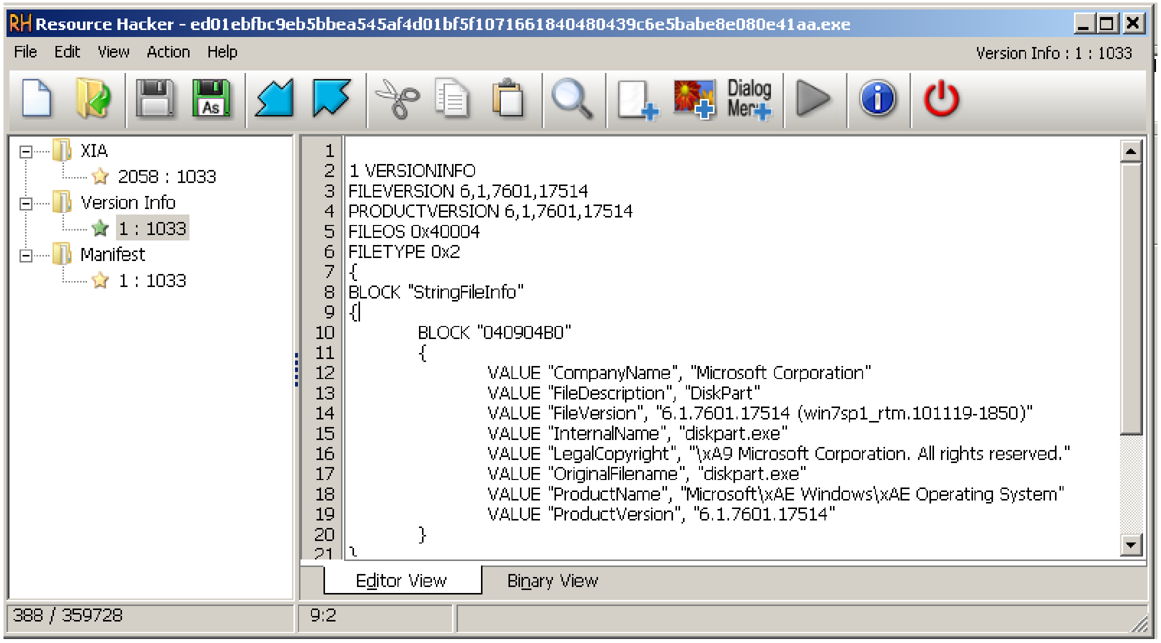
direct-cpu-clock-access · executes-dropped-file · overlay · peexe · runtime-modules · self-delete · via-tor

Acronis	Suspicious	Ad-Aware	Trojan.Ransom.WannaCryptor.A
AegisLab	Trojan.Win32.Wanna.toNn	AhnLab-V3	Trojan/Win32.WannaCryptor.R200571
Alibaba	Ransom:Win32/Wanna.b934b1f9	ALYac	Trojan.Ransom.WannaCryptor
Antiy-AVL	Trojan[Ransom]/Win32.Scatter	SecureAge APEX	Malicious
Arcabit	Trojan.Ransom.WannaCryptor.A	Avast	Win32:WanaCry-A [Trj]
AVG	Win32:WanaCry-A [Trj]	Avira (no cloud)	TR/Ransom.JB
Baidu	Win32.Trojan.WannaCry.c	BitDefender	Trojan.Ransom.WannaCryptor.A
BitDefenderTheta	Gen:NN.ZexaF.34658.wt0@aGEmS3di	Bkav	W32.Common.B4665B53

As shown in the above diagram, the Wannacry ransomware has been detected by 68 out of 71 antivirus tools in the VirusTotal database, meaning we are certain that this is a dangerous malware. The details tab will show various information such as its different hash values, file properties, various names, creation date, signature info etc. The community tab will show user comments on how the malware works and how dangerous it is.

PE File Analysis

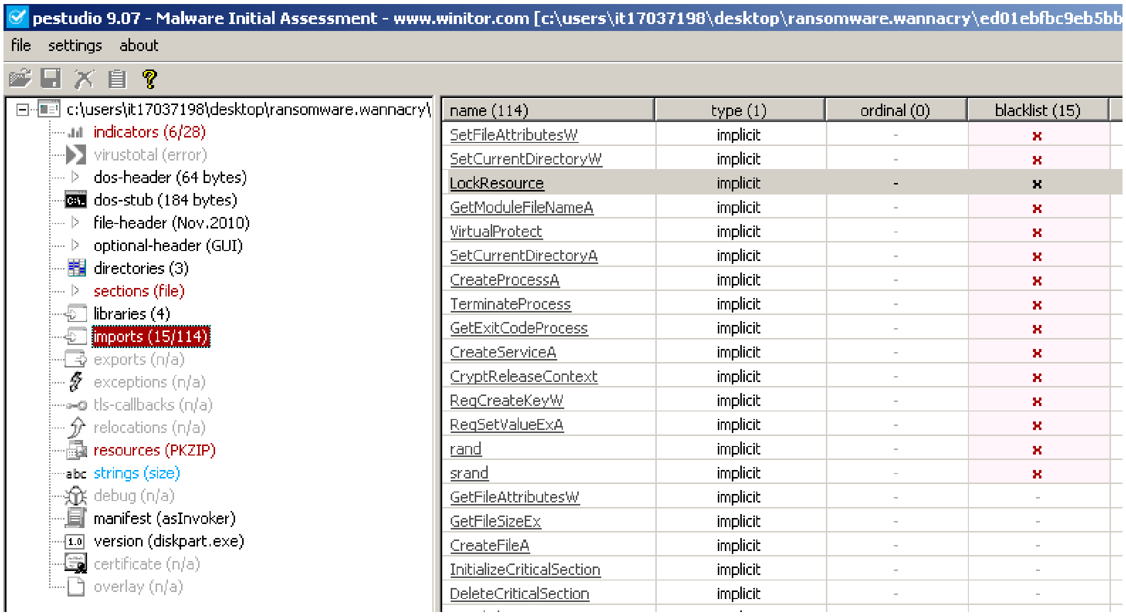
There are many tools that perform similar functions in terms of analyzing the PE file. We can first open our malware through Resource hacker as shown in the figure below.



```

1 VERSIONINFO
FILEVERSION 6,1,7601,17514
PRODUCTVERSION 6,1,7601,17514
FILEOS 0x40004
FILETYPE 0x2
{
BLOCK "StringFileInfo"
{
	BLOCK "040904B0"
	{
		VALUE "CompanyName", "Microsoft Corporation"
		VALUE "FileDescription", "DiskPart"
		VALUE "FileVersion", "6.1.7601.17514 (win7sp1_rtm.101119-1850)"
		VALUE "InternalName", "diskpart.exe"
		VALUE "LegalCopyright", "\xA9 Microsoft Corporation. All rights reserved."
		VALUE "OriginalFilename", "diskpart.exe"
		VALUE "ProductName", "Microsoft\xAE Windows\xAE Operating System"
		VALUE "ProductVersion", "6.1.7601.17514"
	}
}
```

As shown above, in Resource hacker we can obtain various information such as version information, which shows the original name for the malware which was “diskpart.exe”, as well as obtain access to the manifest file.

We can then analyze the PE header using many different tools, but let us analyze using PE Studio as it gives us pretty much all the information we can obtain through every other tool and presents it in a clear manner.



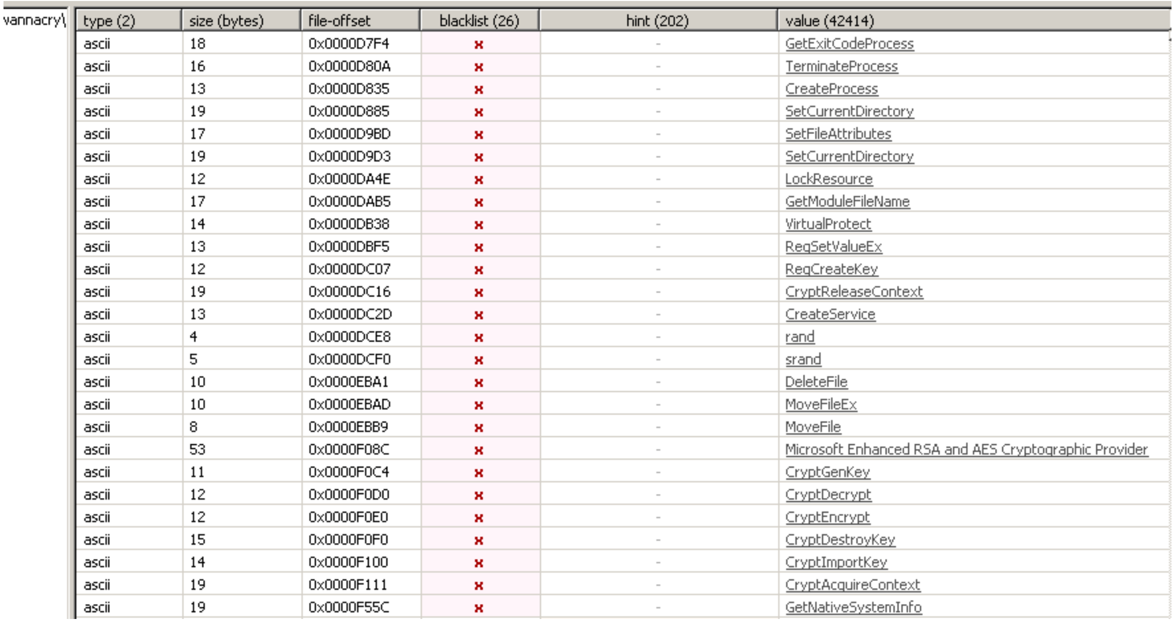
pestudio 9.07 - Malware Initial Assessment - www.winitor.com [c:\users\it17037198\desktop\ransomware.wannacry\ed01ebfbc9eb5bb

name (114)	type (1)	ordinal (0)	blacklist (15)
SetFileAttributesW	implicit	-	✗
SetCurrentDirectoryW	implicit	-	✗
LockResource	implicit	-	✗
GetModuleFileNameA	implicit	-	✗
VirtualProtect	implicit	-	✗
SetCurrentDirectoryA	implicit	-	✗
CreateProcessA	implicit	-	✗
TerminateProcess	implicit	-	✗
GetExitCodeProcess	implicit	-	✗
CreateServiceA	implicit	-	✗
CryptReleaseContext	implicit	-	✗
RegCreateKeyW	implicit	-	✗
RegSetValueExA	implicit	-	✗
rand	implicit	-	✗
srand	implicit	-	✗
GetFileAttributesW	implicit	-	-
GetFileSizeEx	implicit	-	-
CreateFileA	implicit	-	-
InitializeCriticalSection	implicit	-	-
DeleteCriticalSection	implicit	-	-

In PE Studio we can view all aspects of the PE header such as the file-header, optional-header, directories, sections, resources etc. The above figure shows the imports used by the PE file. PE studio has the option to sort them by "blacklist" which will show the potentially harmful imports among the lists. Here we can see the PE file uses imports such as SetFileAttributes, LockResouce, CreateProcess, TerminateProcess, RegCreateKey etc. which can give us clues to let us assume that this program will attempt to find and encrypt files.

Strings

We can analyze the strings in a program to obtain valuable information about its functionality. We can use the tool bintext to obtain all the strings used in this PE file. But PE Studio also provides a view of all the strings and goes even further to show the blacklisted strings which can be a massive time saver for analysts.

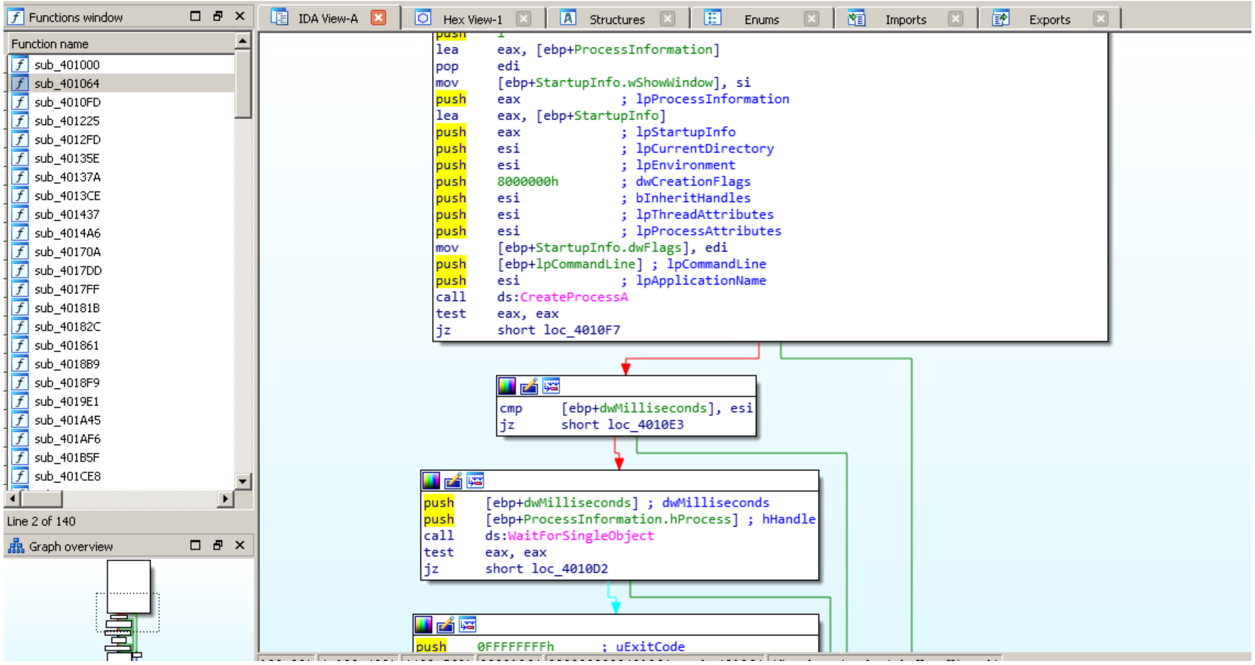


type (2)	size (bytes)	file-offset	blacklist (26)	hint (202)	value (42414)
ascii	18	0x0000D7F4	×	-	GetExitCodeProcess
ascii	16	0x0000D80A	×	-	TerminateProcess
ascii	13	0x0000D835	×	-	CreateProcess
ascii	19	0x0000D885	×	-	SetCurrentDirectory
ascii	17	0x0000D9BD	×	-	SetFileAttributes
ascii	19	0x0000D9D3	×	-	SetCurrentDirectory
ascii	12	0x0000DA4E	×	-	LockResource
ascii	17	0x0000DAB5	×	-	GetModuleFileName
ascii	14	0x0000DB38	×	-	VirtualProtect
ascii	13	0x0000DBF5	×	-	RegSetValueEx
ascii	12	0x0000DC07	×	-	RegCreateKey
ascii	19	0x0000DC16	×	-	CryptReleaseContext
ascii	13	0x0000DC2D	×	-	CreateService
ascii	4	0x0000DCE8	×	-	rand
ascii	5	0x0000DCF0	×	-	srand
ascii	10	0x0000EBA1	×	-	DeleteFile
ascii	10	0x0000EBAD	×	-	MoveFileEx
ascii	8	0x0000EBB9	×	-	MoveFile
ascii	53	0x0000F08C	×	-	Microsoft Enhanced RSA and AES Cryptographic Provider
ascii	11	0x0000F0C4	×	-	CryptGenKey
ascii	12	0x0000F0D0	×	-	CryptDecrypt
ascii	12	0x0000F0E0	×	-	CryptEncrypt
ascii	15	0x0000F0F0	×	-	CryptDestroyKey
ascii	14	0x0000F100	×	-	CryptImportKey
ascii	19	0x0000F111	×	-	CryptAcquireContext
ascii	19	0x0000F55C	×	-	GetNativeSystemInfo

The above figure shows the blacklisted strings as shown through PE Studio. These strings further support our assumption that the program works with cryptographic keys and file manipulation. Which is a telltale sign that this program might be a ransomware.

IDA

The IDA tool provides us with a flowchart-like representation of how the functions work in the program. The functions are shown in the assembly language, which can be analyzed to get a clearer understanding of what goes on in the program.



```
lea     eax, [ebp+ProcessInformation]
pop     edi
mov     [ebp+StartupInfo.wShowWindow], si
push    eax             ; lpProcessInformation
lea     eax, [ebp+StartupInfo]
push    eax             ; lpStartupInfo
push    esi             ; lpCurrentDirectory
push    esi             ; lpEnvironment
push    8000000h        ; dwCreationFlags
push    esi             ; bInheritHandles
push    esi             ; lpThreadAttributes
push    esi             ; lpProcessAttributes
mov     [ebp+StartupInfo.dwFlags], edi
push    [ebp+lpCommandLine] ; lpCommandLine
push    esi             ; lpApplicationName
call    ds:CreateProcessA
test    eax, eax
jz      short loc_4010F7
```

```
cmp     [ebp+dwMilliseconds], esi
jz      short loc_4010E3
```

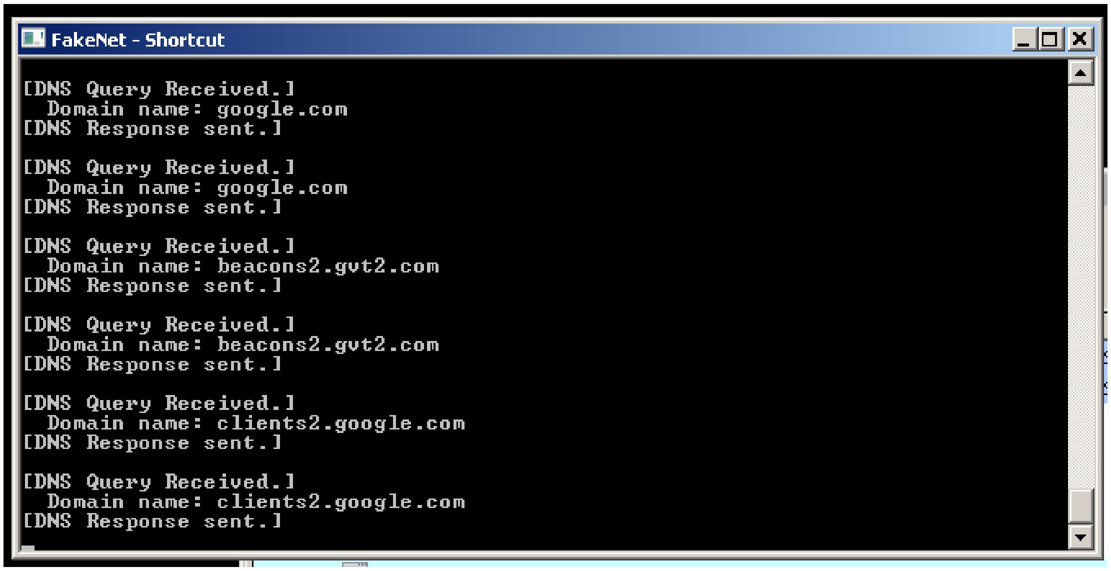
```
push    [ebp+dwMilliseconds] ; dwMilliseconds
push    [ebp+ProcessInformation.hProcess] ; hHandle
call    ds:WaitForSingleObject
test    eax, eax
jz      short loc_4010D2
```

```
push    0FFFFFFFFh      ; uExitCode
```

Dynamic Analysis

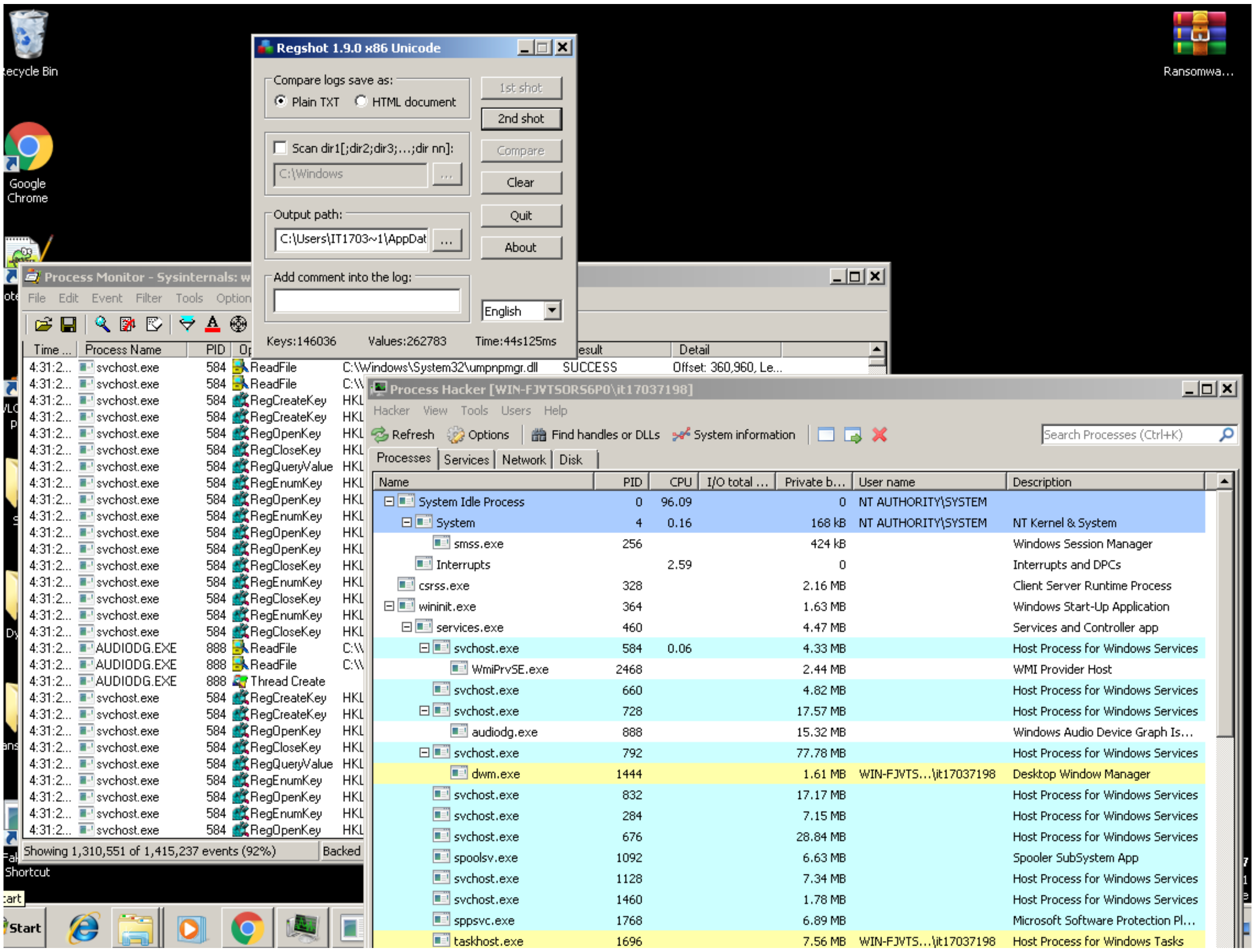
Dynamic analysis is analyzing the malware while it is running in the system. Before running the malware, we must set up all our analysis tools.

First, we must set up a program called fakenet, which is a windows tool that simulates a network connection in the system. Since we are disconnected from the internet in this analysis, this will help convince the malware that it is running on a machine with network connectivity.



```
[DNS Query Received.]
  Domain name: google.com
[DNS Response sent.]

[DNS Query Received.]
  Domain name: google.com
[DNS Response sent.]

[DNS Query Received.]
  Domain name: beacons2.gvt2.com
[DNS Response sent.]

[DNS Query Received.]
  Domain name: beacons2.gvt2.com
[DNS Response sent.]

[DNS Query Received.]
  Domain name: clients2.google.com
[DNS Response sent.]

[DNS Query Received.]
  Domain name: clients2.google.com
[DNS Response sent.]
```

Next, we will open up Regshot, Process hacker, and Process Monitor to analyze the behavior of processes after the malware is run. In Regshot, we will take the 1st shot before running the malware as shown below.



Regshot 1.9.0 x86 Unicode

```
Compare logs save as:  ● Plain TXT  ○ HTML document
☐ Scan dir1[;dir2;dir3;...;dir nn]:  C:\Windows
Output path:  C:\Users\IT1703~1\AppDat
Add comment into the log:
English
Keys:146036    Values:262783    Time:44s125ms
```

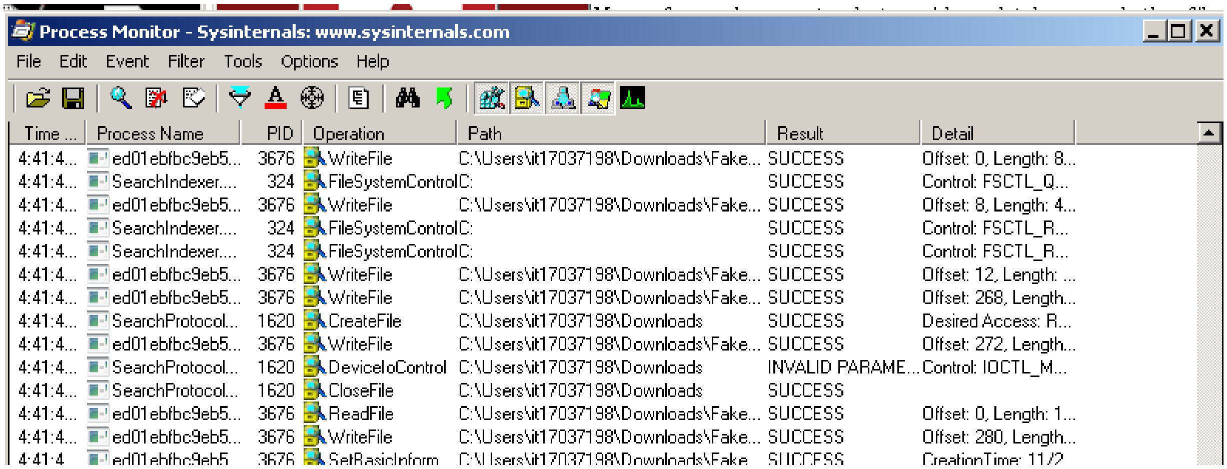
Process Monitor - Sysinternals

```
Time ...  Process Name   PID  Op
4:31:2... svchost.exe    584  ReadFile         C:\Windows\System32\umpnpmgr.dll  SUCCESS  Offset: 360,960, Le...
4:31:2... svchost.exe    584  ReadFile         C:\\
4:31:2... svchost.exe    584  RegCreateKey     HKL
4:31:2... svchost.exe    584  RegCreateKey     HKL
4:31:2... svchost.exe    584  RegOpenKey       HKL
4:31:2... svchost.exe    584  RegCloseKey      HKL
4:31:2... svchost.exe    584  RegQueryValue    HKL
4:31:2... svchost.exe    584  RegEnumKey       HKL
4:31:2... svchost.exe    584  RegOpenKey       HKL
4:31:2... svchost.exe    584  RegEnumKey       HKL
4:31:2... svchost.exe    584  RegOpenKey       HKL
4:31:2... svchost.exe    584  RegOpenKey       HKL
4:31:2... svchost.exe    584  RegCloseKey      HKL
4:31:2... svchost.exe    584  RegEnumKey       HKL
4:31:2... svchost.exe    584  RegCloseKey      HKL
4:31:2... svchost.exe    584  RegEnumKey       HKL
4:31:2... svchost.exe    584  RegCloseKey      HKL
4:31:2... AUDIODG.EXE    888  ReadFile         C:\\
4:31:2... AUDIODG.EXE    888  ReadFile         C:\\
4:31:2... AUDIODG.EXE    888  Thread Create
4:31:2... svchost.exe    584  RegCreateKey     HKL
4:31:2... svchost.exe    584  RegCreateKey     HKL
4:31:2... svchost.exe    584  RegOpenKey       HKL
4:31:2... svchost.exe    584  RegCloseKey      HKL
4:31:2... svchost.exe    584  RegQueryValue    HKL
4:31:2... svchost.exe    584  RegEnumKey       HKL
4:31:2... svchost.exe    584  RegOpenKey       HKL
4:31:2... svchost.exe    584  RegEnumKey       HKL
4:31:2... svchost.exe    584  RegOpenKey       HKL
Showing 1,310,551 of 1,415,237 events (92%)   Backed
```

Process Hacker [WIN-FJVTSORS6P0\it17037198]

```
Name                     PID   CPU    I/O total ...  Private b...  User name                   Description
System Idle Process        0   96.09                          0    NT AUTHORITY\SYSTEM
  System                   4    0.16                     168 kB    NT AUTHORITY\SYSTEM         NT Kernel & System
    smss.exe             256                             424 kB                                Windows Session Manager
  Interrupts                    2.59                          0                                Interrupts and DPCs
csrss.exe                328                            2.16 MB                                Client Server Runtime Process
wininit.exe              364                            1.63 MB                                Windows Start-Up Application
  services.exe           460                            4.47 MB                                Services and Controller app
    svchost.exe          584    0.06                    4.33 MB                                Host Process for Windows Services
      WmiPrvSE.exe      2468                            2.44 MB                                WMI Provider Host
    svchost.exe          660                            4.82 MB                                Host Process for Windows Services
    svchost.exe          728                           17.57 MB                                Host Process for Windows Services
      audiodg.exe        888                           15.32 MB                                Windows Audio Device Graph Is...
    svchost.exe          792                           77.78 MB                                Host Process for Windows Services
      dwm.exe           1444                            1.61 MB    WIN-FJVTS...\it17037198     Desktop Window Manager
    svchost.exe          832                           17.17 MB                                Host Process for Windows Services
    svchost.exe          284                            7.15 MB                                Host Process for Windows Services
    svchost.exe          676                           28.84 MB                                Host Process for Windows Services
    spoolsv.exe         1092                            6.63 MB                                Spooler SubSystem App
    svchost.exe         1128                            7.34 MB                                Host Process for Windows Services
    svchost.exe         1460                            1.78 MB                                Host Process for Windows Services
    sppsvc.exe          1768                            6.89 MB                                Microsoft Software Protection Pl...
    taskhost.exe        1696                            7.56 MB    WIN-FJVTS...\it17037198     Host Process for Windows Tasks
```

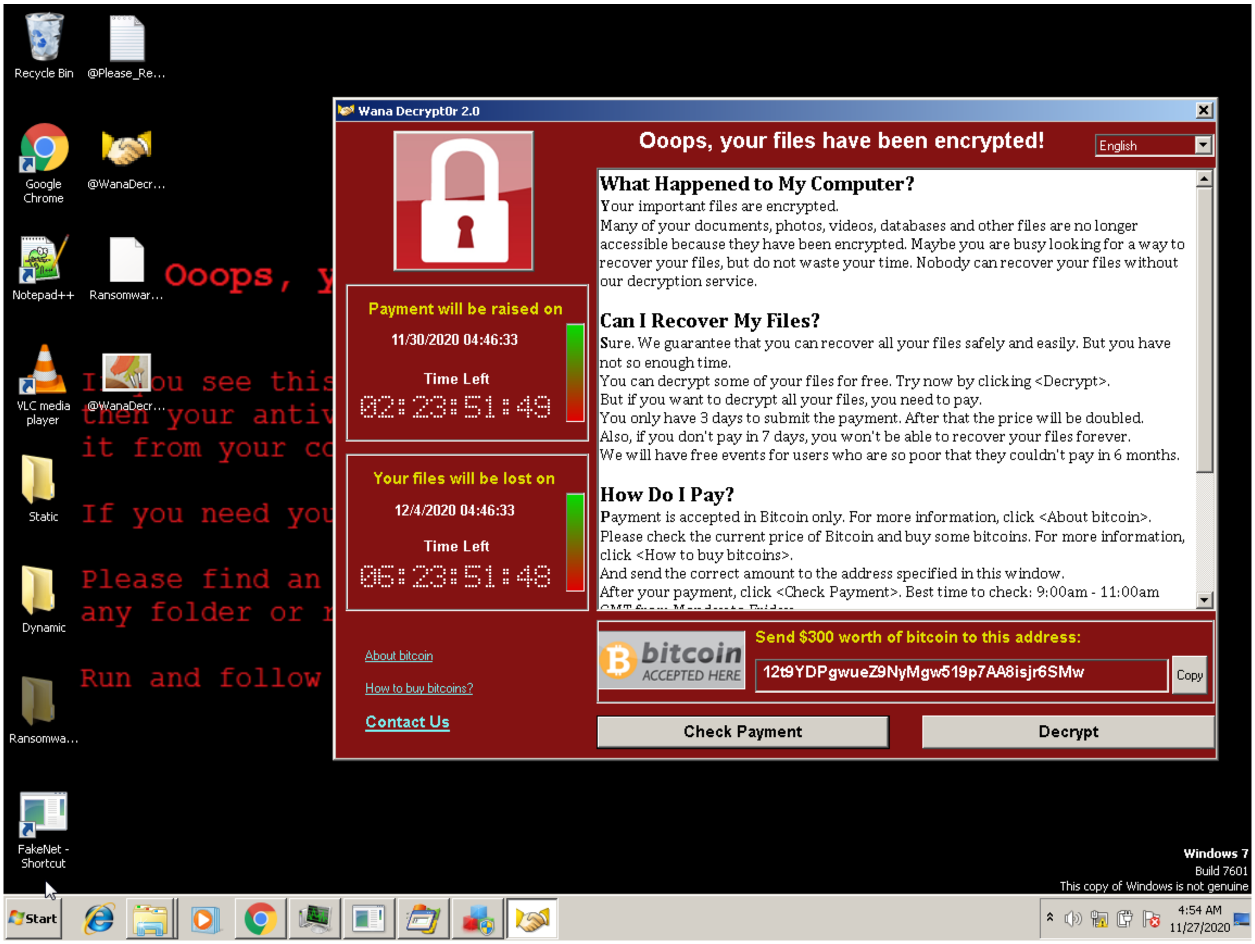
After preparing the tools, we are now ready to start the malware program. After starting the WannaCry Malware, if we take a look at Process Monitor, we can see the malware program going through all the files in the system and encrypting them as shown in the figure below.



Process Monitor - Sysinternals: www.sysinternals.com

```
Time ...  Process Name        PID   Operation           Path                                    Result           Detail
4:41:4... ed01ebfbc9eb5...   3676  WriteFile           C:\Users\it17037198\Downloads\Fake...   SUCCESS          Offset: 0, Length: 8...
4:41:4... SearchIndexer....   324  FileSystemControl   C:                                      SUCCESS          Control: FSCTL_Q...
4:41:4... ed01ebfbc9eb5...   3676  WriteFile           C:\Users\it17037198\Downloads\Fake...   SUCCESS          Offset: 8, Length: 4...
4:41:4... SearchIndexer....   324  FileSystemControl   C:                                      SUCCESS          Control: FSCTL_R...
4:41:4... SearchIndexer....   324  FileSystemControl   C:                                      SUCCESS          Control: FSCTL_R...
4:41:4... ed01ebfbc9eb5...   3676  WriteFile           C:\Users\it17037198\Downloads\Fake...   SUCCESS          Offset: 12, Length: ...
4:41:4... ed01ebfbc9eb5...   3676  WriteFile           C:\Users\it17037198\Downloads\Fake...   SUCCESS          Offset: 268, Length...
4:41:4... SearchProtocol...  1620  CreateFile          C:\Users\it17037198\Downloads           SUCCESS          Desired Access: R...
4:41:4... ed01ebfbc9eb5...   3676  WriteFile           C:\Users\it17037198\Downloads\Fake...   SUCCESS          Offset: 272, Length...
4:41:4... SearchProtocol...  1620  DeviceIoControl     C:\Users\it17037198\Downloads           INVALID PARAME...Control: IOCTL_M...
4:41:4... SearchProtocol...  1620  CloseFile           C:\Users\it17037198\Downloads           SUCCESS
4:41:4... ed01ebfbc9eb5...   3676  ReadFile            C:\Users\it17037198\Downloads\Fake...   SUCCESS          Offset: 0, Length: 1...
4:41:4... ed01ebfbc9eb5...   3676  WriteFile           C:\Users\it17037198\Downloads\Fake...   SUCCESS          Offset: 280, Length...
4:41:4... ed01ebfbc9eb5...   3676  SetBasicInform      C:\Users\it17037198\Downloads\Fake...   SUCCESS          CreationTime: 11/2...
```

The following figure shows the desktop after the malware has completely encrypted all files.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

11/30/2020 04:46:33

Time Left

02:23:51:49

Your files will be lost on

12/4/2020 04:46:33

Time Left

06:23:51:48

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Ooops, y

If you see this
then your antiv
it from your co

If you need you

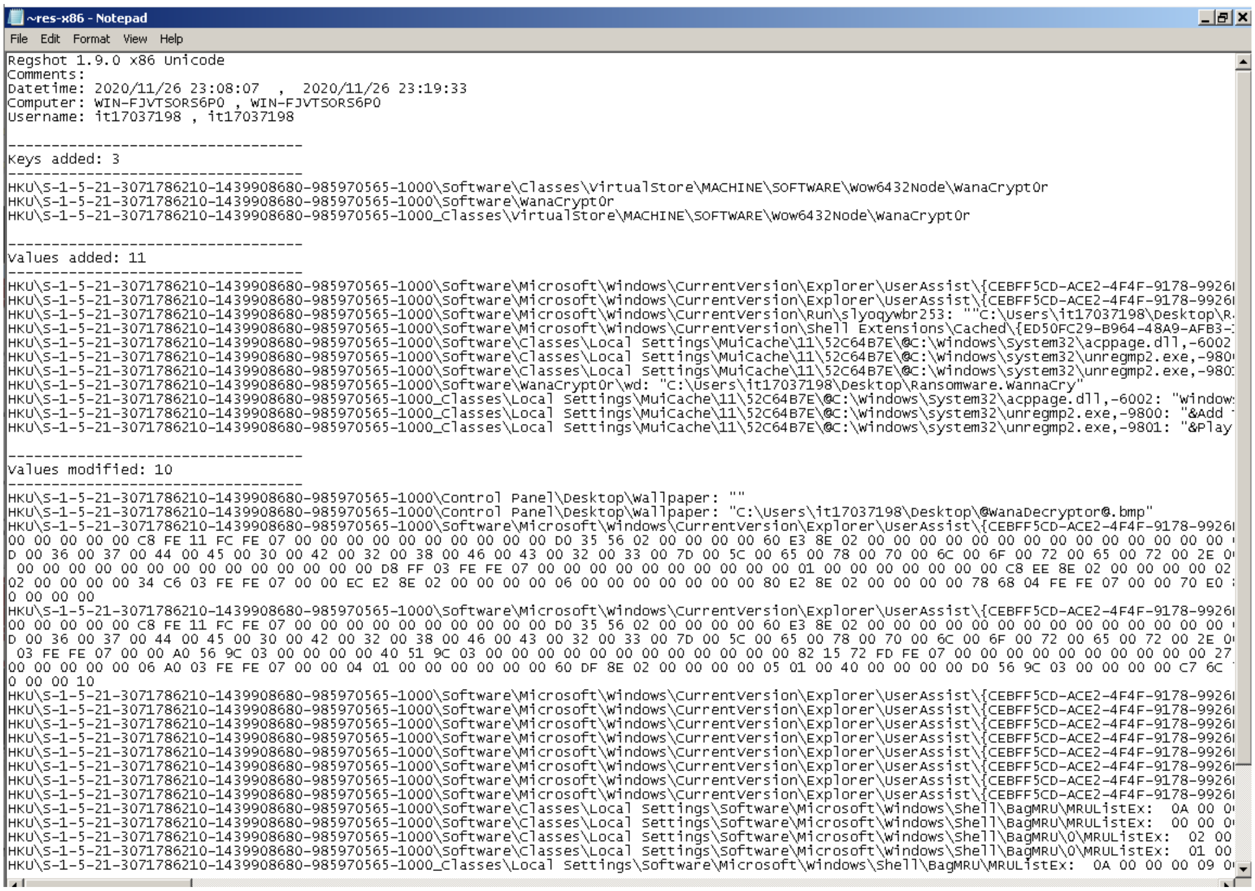
Please find an
any folder or r

Run and follow

Windows 7
Build 7601
This copy of Windows is not genuine

4:54 AM
11/27/2020

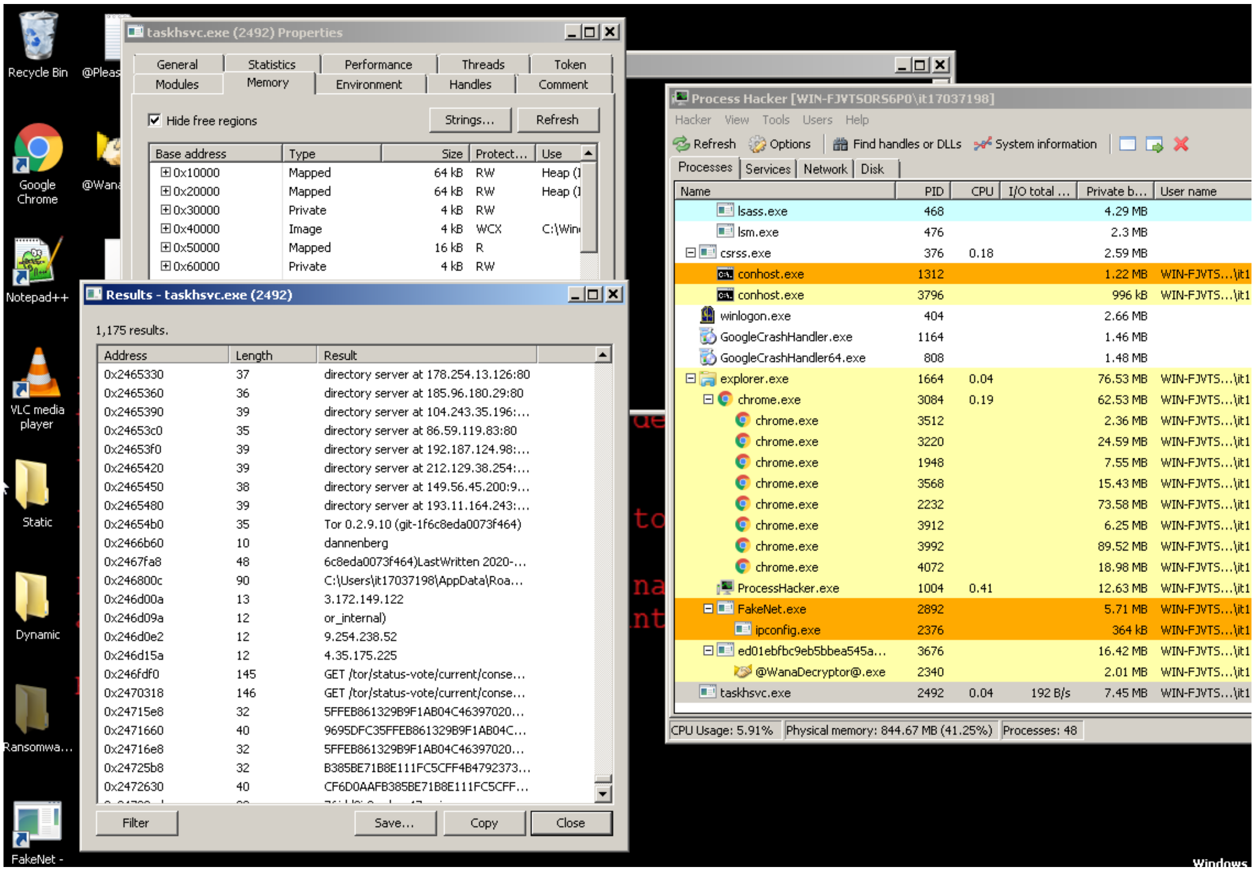
Now that the Malware has completed running, we can take our 2nd shot in Regshot and click the Compare button. This will open a notepad file that details the difference between the two shots. We can see that between the two shots, three WanaCryptor keys have been added, as well as some other information that could be valuable to analysts as shown in the figure below.



```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2020/11/26 23:08:07  ,  2020/11/26 23:19:33
Computer: WIN-FJVTSORS6P0 , WIN-FJVTSORS6P0
Username: it17037198 , it17037198

----------------------------------
Keys added: 3
----------------------------------
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Wow6432Node\WanaCrypt0r
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\WanaCrypt0r
HKU\S-1-5-21-3071786210-1439908680-985970565-1000_Classes\VirtualStore\MACHINE\SOFTWARE\Wow6432Node\WanaCrypt0r

----------------------------------
Values added: 11
----------------------------------
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Run\slyoqywbr253: ""C:\Users\it17037198\Desktop\R
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{ED50FC29-B964-48A9-AFB3-
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Classes\Local Settings\MuiCache\11\52C64B7E\@C:\Windows\System32\acppage.dll,-6002
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Classes\Local Settings\MuiCache\11\52C64B7E\@C:\Windows\system32\unregmp2.exe,-980
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Classes\Local Settings\MuiCache\11\52C64B7E\@C:\Windows\system32\unregmp2.exe,-980
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\WanaCrypt0r\wd: "C:\Users\it17037198\Desktop\Ransomware.WannaCry"
HKU\S-1-5-21-3071786210-1439908680-985970565-1000_Classes\Local Settings\MuiCache\11\52C64B7E\@C:\Windows\System32\acppage.dll,-6002: "Window
HKU\S-1-5-21-3071786210-1439908680-985970565-1000_Classes\Local Settings\MuiCache\11\52C64B7E\@C:\Windows\system32\unregmp2.exe,-9800: "&Add
HKU\S-1-5-21-3071786210-1439908680-985970565-1000_Classes\Local Settings\MuiCache\11\52C64B7E\@C:\Windows\system32\unregmp2.exe,-9801: "&Play

----------------------------------
Values modified: 10
----------------------------------
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Control Panel\Desktop\Wallpaper: ""
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Control Panel\Desktop\Wallpaper: "C:\Users\it17037198\Desktop\@WanaDecryptor@.bmp"
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
00 00 00 00 00 C8 FE 11 FC FE 07 00 00 00 00 00 00 00 00 00 00 D0 35 56 02 00 00 00 00 60 E3 8E 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
D 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 32 00 33 00 7D 00 5C 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 0
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D8 FF 03 FE FE 07 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 C8 EE 8E 02 00 00 00 00 02
02 00 00 00 00 34 C6 03 FE FE 07 00 00 EC E2 8E 02 00 00 00 00 06 00 00 00 00 00 00 80 E2 8E 02 00 00 00 00 78 68 04 FE FE 07 00 00 70 E0
0 00 00 00
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
00 00 00 00 00 C8 FE 11 FC FE 07 00 00 00 00 00 00 00 00 00 00 D0 35 56 02 00 00 00 00 60 E3 8E 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
D 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 32 00 33 00 7D 00 5C 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 0
 03 FE FE 07 00 00 A0 56 9C 03 00 00 00 00 40 51 9C 03 00 00 00 00 00 00 00 00 00 00 00 00 82 15 72 FD FE 07 00 00 00 00 00 00 00 00 00 27
00 00 00 00 00 06 A0 03 FE FE 07 00 00 04 01 00 00 00 00 00 00 60 DF 8E 02 00 00 00 00 05 01 00 40 00 00 00 00 D0 56 9C 03 00 00 00 00 C7 6C
0 00 00 10
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0A 00 0
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  00 00 0
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\MRUListEx:  02 00
HKU\S-1-5-21-3071786210-1439908680-985970565-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\MRUListEx:  01 00
HKU\S-1-5-21-3071786210-1439908680-985970565-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0A 00 00 00 09 0
```

Next, we can check the Process Hacker, where we can see that 3 new processes have been running: The PE file, @WanaDecryptor@.exe, and taskhsvc.exe. We can open each of these processes to view additional information, for example if we check the PE process and go to the memory tab > strings, we can view what file locations were opened by the process during the encryption process. The strings in the @WanaDecryptor@.exe process show the strings used in the interface of WannaCry that was shown in an above figure.

The most interesting strings are in taskhsvc.exe, where if we scroll through the strings as shown in the below figure, we can see various IP addresses, directory servers, as well as Tor addresses. These may be linked to the Command and Control centers used by WannaCry, which is used when paying the ransom.



Base address	Type	Size	Protect...	Use
⊞ 0x10000	Mapped	64 kB	RW	Heap (I
⊞ 0x20000	Mapped	64 kB	RW	Heap (I
⊞ 0x30000	Private	4 kB	RW	
⊞ 0x40000	Image	4 kB	WCX	C:\Win
⊞ 0x50000	Mapped	16 kB	R	
⊞ 0x60000	Private	4 kB	RW	

1,175 results.

Address	Length	Result
0x2465330	37	directory server at 178.254.13.126:80
0x2465360	36	directory server at 185.96.180.29:80
0x2465390	39	directory server at 104.243.35.196:...
0x24653c0	35	directory server at 86.59.119.83:80
0x24653f0	39	directory server at 192.187.124.98:...
0x2465420	39	directory server at 212.129.38.254:...
0x2465450	38	directory server at 149.56.45.200:9...
0x2465480	39	directory server at 193.11.164.243:...
0x24654b0	35	Tor 0.2.9.10 (git-1f6c8eda0073f464)
0x2466b60	10	dannenberg
0x2467fa8	48	6c8eda0073f464)LastWritten 2020-...
0x246800c	90	C:\Users\it17037198\AppData\Roa...
0x246d00a	13	3.172.149.122
0x246d09a	12	or_internal)
0x246d0e2	12	9.254.238.52
0x246d15a	12	4.35.175.225
0x246fdf0	145	GET /tor/status-vote/current/conse...
0x2470318	146	GET /tor/status-vote/current/conse...
0x24715e8	32	5FFEB861329B9F1AB04C46397020...
0x2471660	40	9695DFC35FFEB861329B9F1AB04C...
0x24716e8	32	5FFEB861329B9F1AB04C46397020...
0x24725b8	32	B385BE71B8E111FC5CFF4B4792373...
0x2472630	40	CF6D0AAFB385BE71B8E111FC5CFF...

Name	PID	CPU	I/O total ...	Private b...	User name
lsass.exe	468			4.29 MB	
lsm.exe	476			2.3 MB	
⊟ csrss.exe	376	0.18		2.59 MB	
conhost.exe	1312			1.22 MB	WIN-FJVTS...\it1
conhost.exe	3796			996 kB	WIN-FJVTS...\it1
winlogon.exe	404			2.66 MB	
GoogleCrashHandler.exe	1164			1.46 MB	
GoogleCrashHandler64.exe	808			1.48 MB	
⊟ explorer.exe	1664	0.04		76.53 MB	WIN-FJVTS...\it1
⊟ chrome.exe	3084	0.19		62.53 MB	WIN-FJVTS...\it1
chrome.exe	3512			2.36 MB	WIN-FJVTS...\it1
chrome.exe	3220			24.59 MB	WIN-FJVTS...\it1
chrome.exe	1948			7.55 MB	WIN-FJVTS...\it1
chrome.exe	3568			15.43 MB	WIN-FJVTS...\it1
chrome.exe	2232			73.58 MB	WIN-FJVTS...\it1
chrome.exe	3912			6.25 MB	WIN-FJVTS...\it1
chrome.exe	3992			89.52 MB	WIN-FJVTS...\it1
chrome.exe	4072			18.98 MB	WIN-FJVTS...\it1
ProcessHacker.exe	1004	0.41		12.63 MB	WIN-FJVTS...\it1
⊟ FakeNet.exe	2892			5.71 MB	WIN-FJVTS...\it1
ipconfig.exe	2376			364 kB	WIN-FJVTS...\it1
⊟ ed01ebfbc9eb5bbea545a...	3676			16.42 MB	WIN-FJVTS...\it1
@WanaDecryptor@.exe	2340			2.01 MB	WIN-FJVTS...\it1
taskhsvc.exe	2492	0.04	192 B/s	7.45 MB	WIN-FJVTS...\it1

CPU Usage: 5.91% Physical memory: 844.67 MB (41.25%) Processes: 48