Practical Malware Analysis & Triage
Malware Analysis Report

WannaCry Ransomware Malware

Sep 2023 | Prinx | v1.0

Table of Contents

Executive Summary

File name	Ransomware.wannacry.exe
MD5 hash	DB349B97C37D22F5EA1D1841E3C89EB4
SHA1 hash	e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA256 hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

WannaCry is a ransomware malware sample first identified on May 11th, 2017 and quickly gained notoriety for its widespread and devastating impact on computer systems worldwide.

WannaCry is notable for its use of a worm-like behavior, which allowed it to spread rapidly across networks and infect a large number of computers.

It is a multistage attack starting with a dropper which unpacked a payload onto the target's system under the right conditions.

It is a C++-compiled ransomware that runs on the x32 Windows operating system.

When the virus is triggered, the files (come with a myriad of extensions) are encrypted and a ransom in bitcoin is demanded bitcoin.

Malware sample and hashes have been submitted to VirusTotal for further examination.

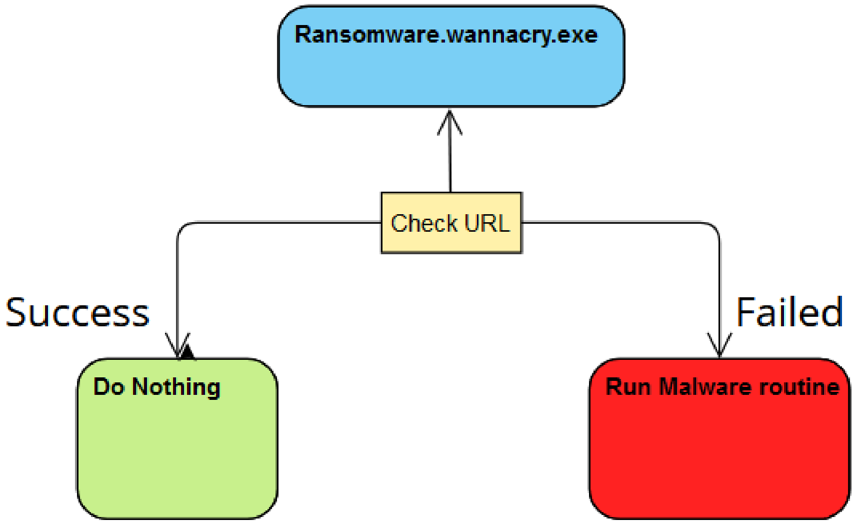
YARA signature rules are attached in Appendix A.

High-Level Technical Summary

The WannaCry ransomware comprises several components, including an initial dropper that contains an embedded encrypter. This encrypter component holds a decryption application called "Wana Decrypt0r 2.0," a password-protected zip file containing a copy of Tor, and various individual files with configuration data and encryption keys.

When the dropper runs, it first tries to establish a connection to the domain **http://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com** (acting as a "killswitch").
If successful, it exits.

If the connection fails, the dropper attempts to create a service named "mssecsvc2.0" with the DisplayName "Microsoft Security Center (2.0) Service".



The encrypter binary also includes a password-protected zip file (password: **WNcry@2ol7**), containing several files:

- A "**msg**" directory with Rich Text Format files used by the decrypter program.
- **b.wnry**, a bitmap file with decryption instructions.
- **c.wnry**, containing addresses and a link to download Tor.
- **r.wnry**, additional decryption instructions in English.
- **s.wnry**, a zip file containing the Tor software executable.
- **t.wnry**, encrypted using the "WANACRY!" header.
- **taskdl.exe** and taskse.exe, tools for file deletion and Remote Desktop Protocol (RDP) execution.
- **u.wnry**, the "@WanaDecryptor@.exe" decrypter file.

After dropping these files into its directory, WannaCry tries to hide and grant full access to all files by running specific commands. It does this by executing "attrib +h .", followed by "icacls . /grant Everyone:F /T /C /Q".

The WannaCry encrypter launches the embedded decrypter "@WanaDecryptor@.exe," displaying timers and ransom payment instructions in the victim's language. The ransom demands money in bitcoins to specified addresses, although only one address was observed in the analyzed sample (**13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94**).

If the ransom isn't paid before the first timer expires, the price doubles. After the second timer expires, the malware readme warns that the files will be unrecoverable without the decryption key. The encryption process leverages the Microsoft Enhanced RSA and AES Cryptographic Provider libraries.

Malware Composition

Wannacry consists of the following components:

File Name	SHA256 Hash
Ransomware.wannacry.exe	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
tasksche.exe	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
@WanaDecryptor@[.]exe	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
taskdl.exe	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
taskhsvc.exe	e48673680746fbe027e8982f62a83c298d6fb46ad9243de8e79b7e5a24dcd4eb
taskse.exe	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
Ransomware.wannacry.exe	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
tasksche.exe	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Ransomware.wannacry.exe

Initial file detonated

tasksche.exe

The payload unpacked from the dropper

@WanaDecryptor@[.]exe

The GUI application that is executed by tasksche after all files have been encrypted and handles ransom payment

taskdl.exe

SQL Client Configuration Utility EXE

taskhsvc.exe

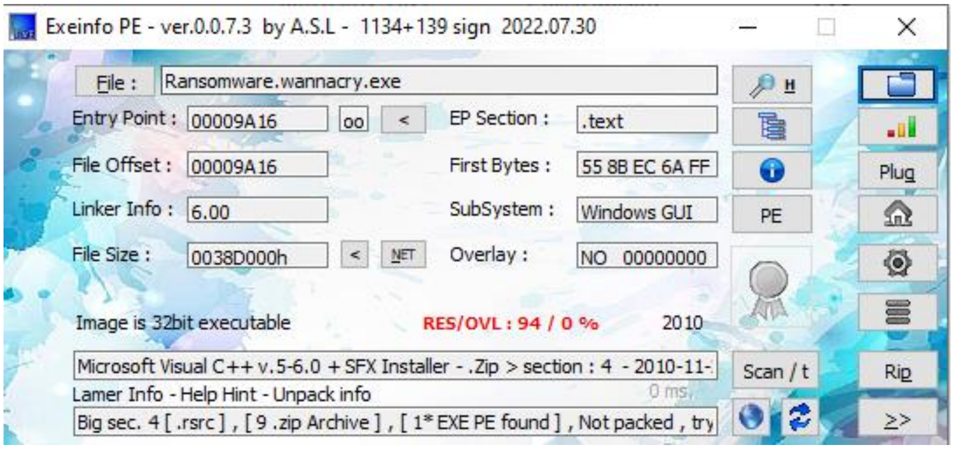
Handles communication to TOR URL and other TOR activities

taskse.exe

Waitfor - Wait/send a signal over a network

Basic Static Analysis

To determine which programming language the software was made in, we use “Exeinfo PE” and “DIE”.



Exeinfo PE - ver.0.0.7.3 by A.S.L - 1134+139 sign 2022.07.30

File : Ransomware.wannacry.exe

Entry Point : 00009A16

EP Section : .text

File Offset : 00009A16

First Bytes : 55 8B EC 6A FF

Linker Info : 6.00

SubSystem : Windows GUI

File Size : 0038D000h

Overlay : NO 00000000

Image is 32bit executable

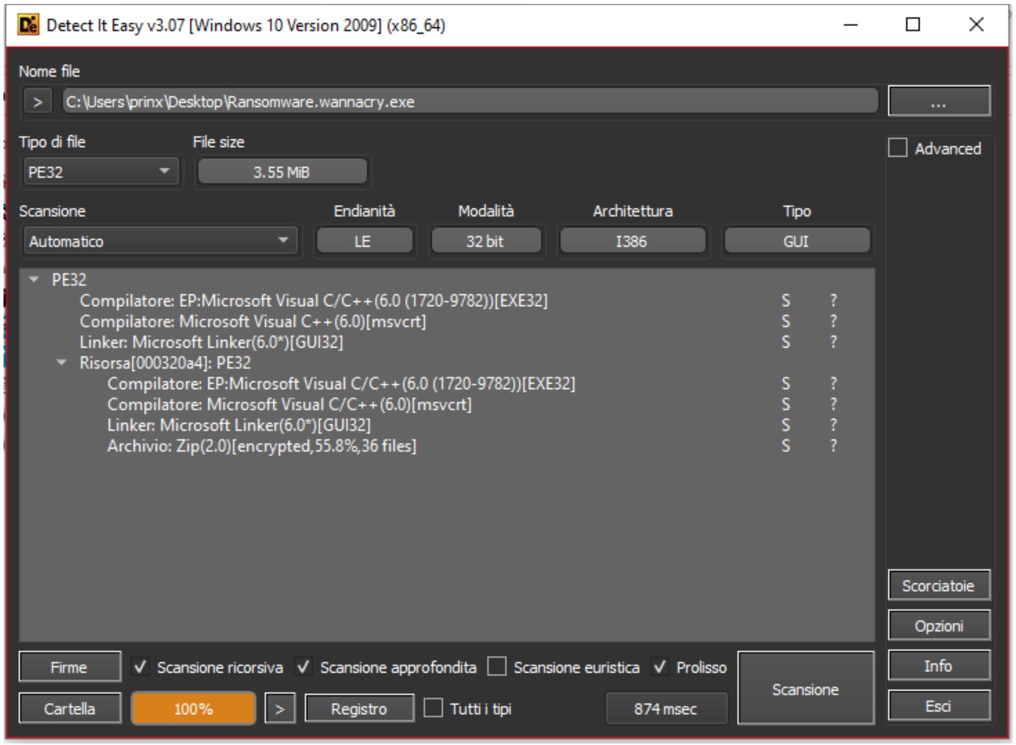
RES/OVL : 94 / 0 % 2010

Microsoft Visual C++ v.5-6.0 + SFX Installer - .Zip > section : 4 - 2010-11-

Lamer Info - Help Hint - Unpack info 0 ms.

Big sec. 4 [.rsrc] , [9 .zip Archive] , [1* EXE PE found] , Not packed , try

Exeinfo PE



Detect It Easy v3.07 [Windows 10 Version 2009] (x86_64)

Nome file: C:\Users\prinx\Desktop\Ransomware.wannacry.exe

Tipo di file: PE32

File size: 3.55 MiB

□ Advanced

Scansione: Automatico

Endianità: LE

Modalità: 32 bit

Architettura: I386

Tipo: GUI

```
PE32
    Compilatore: EP:Microsoft Visual C/C++(6.0 (1720-9782))[EXE32]        S    ?
    Compilatore: Microsoft Visual C++(6.0)[msvcrt]                         S    ?
    Linker: Microsoft Linker(6.0*)[GUI32]                                  S    ?
  Risorsa[000320a4]: PE32
        Compilatore: EP:Microsoft Visual C/C++(6.0 (1720-9782))[EXE32]    S    ?
        Compilatore: Microsoft Visual C/C++(6.0)[msvcrt]                  S    ?
        Linker: Microsoft Linker(6.0*)[GUI32]                             S    ?
        Archivio: Zip(2.0)[encrypted,55.8%,36 files]                      S    ?
```

☑ Scansione ricorsiva ☑ Scansione approfondita □ Scansione euristica ☑ Prolisso

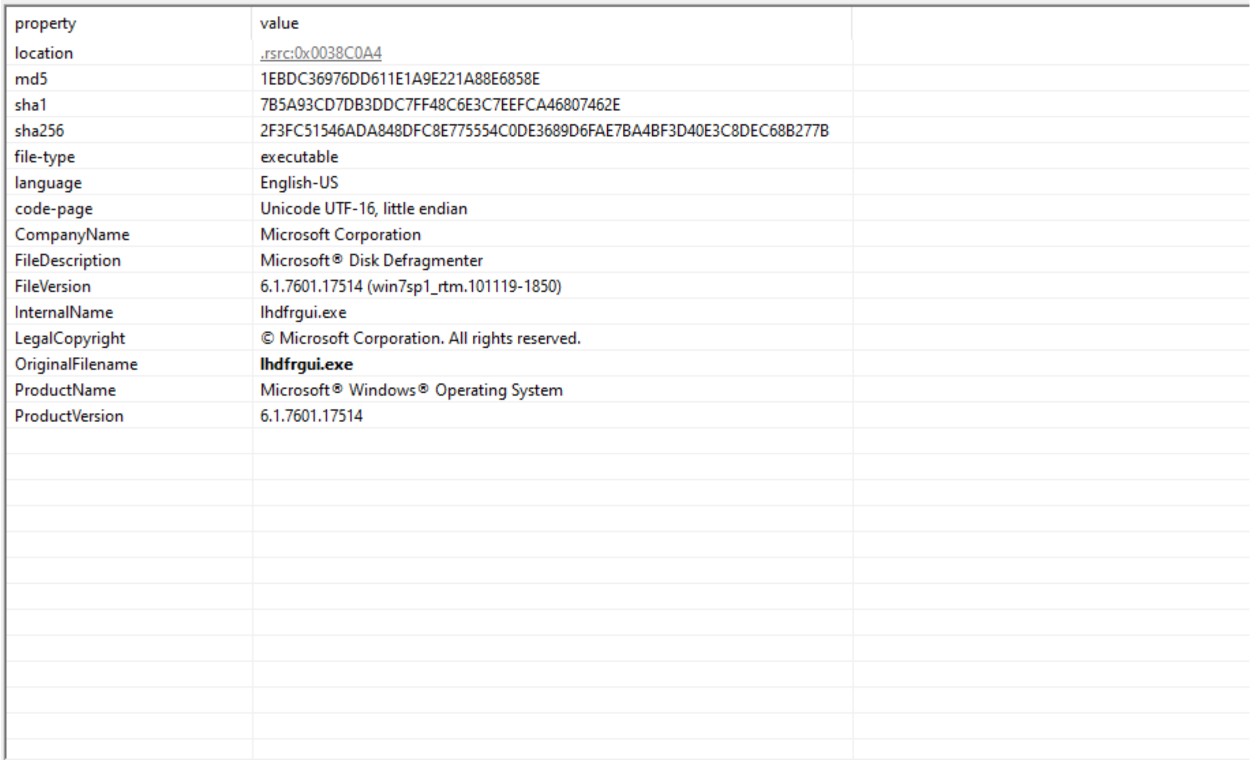
□ Tutti i tipi

100%

874 msec

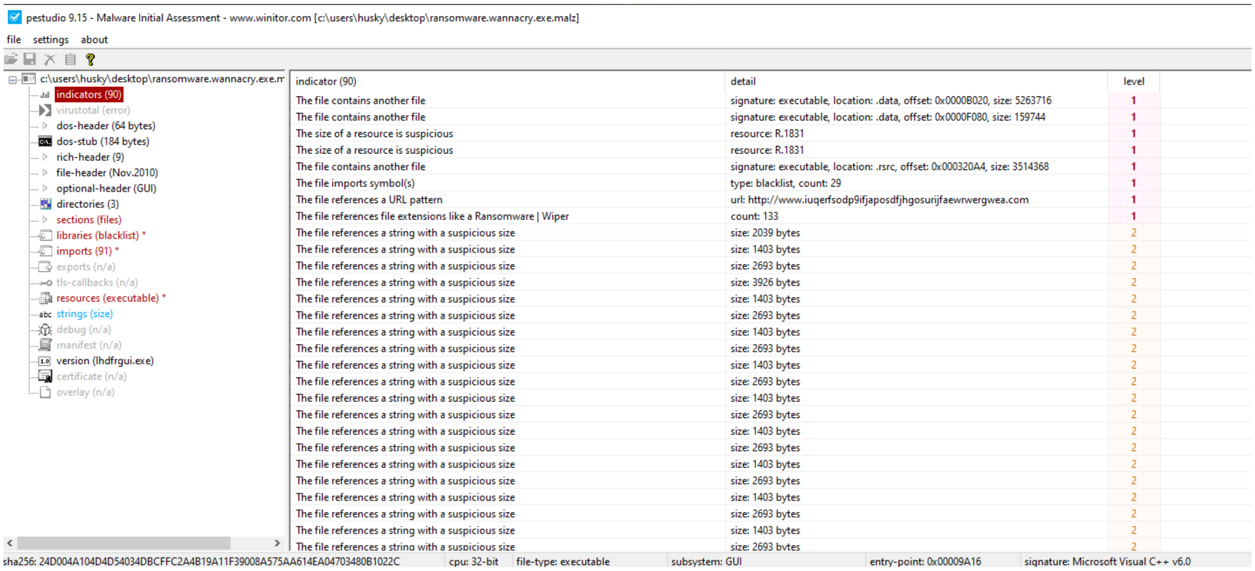
DIE – Detect It Easy

With “PEstudio” software we find General information son the virus like hash (md5, SHA1 and SHA256).



property	value
location	.rsrc:0x0038C0A4
md5	1EBDC36976DD611E1A9E221A88E6858E
sha1	7B5A93CD7DB3DDC7FF48C6E3C7EEFCA46807462E
sha256	2F3FC51546ADA848DFC8E775554C0DE3689D6FAE7BA4BF3D40E3C8DEC68B277B
file-type	executable
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	lhdfrgui.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	**lhdfrgui.exe**
ProductName	Microsoft® Windows® Operating System
ProductVersion	6.1.7601.17514

PEView – General Info



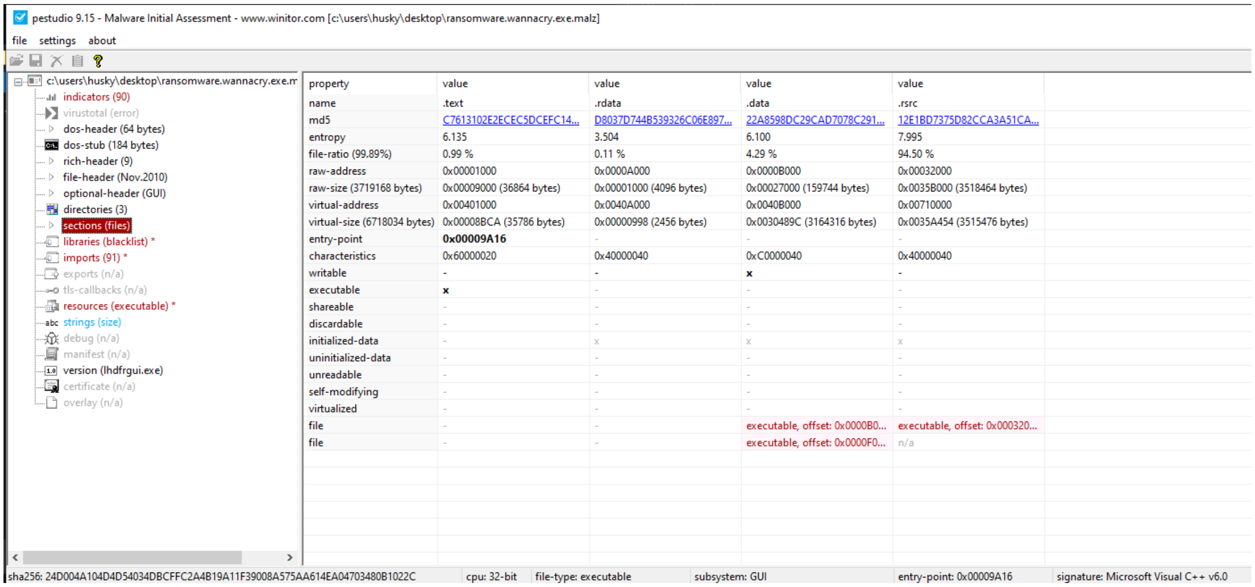
pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\husky\desktop\ransomware.wannacry.exe.malz]

```
c:\users\husky\desktop\ransomware.wannacry.exe.m
  indicators (90)
  virustotal (error)
  dos-header (64 bytes)
  dos-stub (184 bytes)
  rich-header (9)
  file-header (Nov.2010)
  optional-header (GUI)
  directories (3)
  sections (files)
  libraries (blacklist) *
  imports (91) *
  exports (n/a)
  tls-callbacks (n/a)
  resources (executable) *
  strings (size)
  debug (n/a)
  manifest (n/a)
  version (lhdfrgui.exe)
  certificate (n/a)
  overlay (n/a)
```

indicator (90)	detail	level
The file contains another file	signature: executable, location: .data, offset: 0x0000B020, size: 5263716	1
The file contains another file	signature: executable, location: .data, offset: 0x0000F080, size: 159744	1
The size of a resource is suspicious	resource: R.1831	1
The size of a resource is suspicious	resource: R.1831	1
The file contains another file	signature: executable, location: .rsrc, offset: 0x000320A4, size: 3514368	1
The file imports symbol(s)	type: blacklist, count: 29	1
The file references a URL pattern	url: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	1
The file references file extensions like a Ransomware | Wiper	count: 133	1
The file references a string with a suspicious size	size: 2039 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2
The file references a string with a suspicious size	size: 3926 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2
The file references a string with a suspicious size	size: 1403 bytes	2
The file references a string with a suspicious size	size: 2693 bytes	2

sha256: 24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00009A16 | signature: Microsoft Visual C++ v6.0

There are executable sections

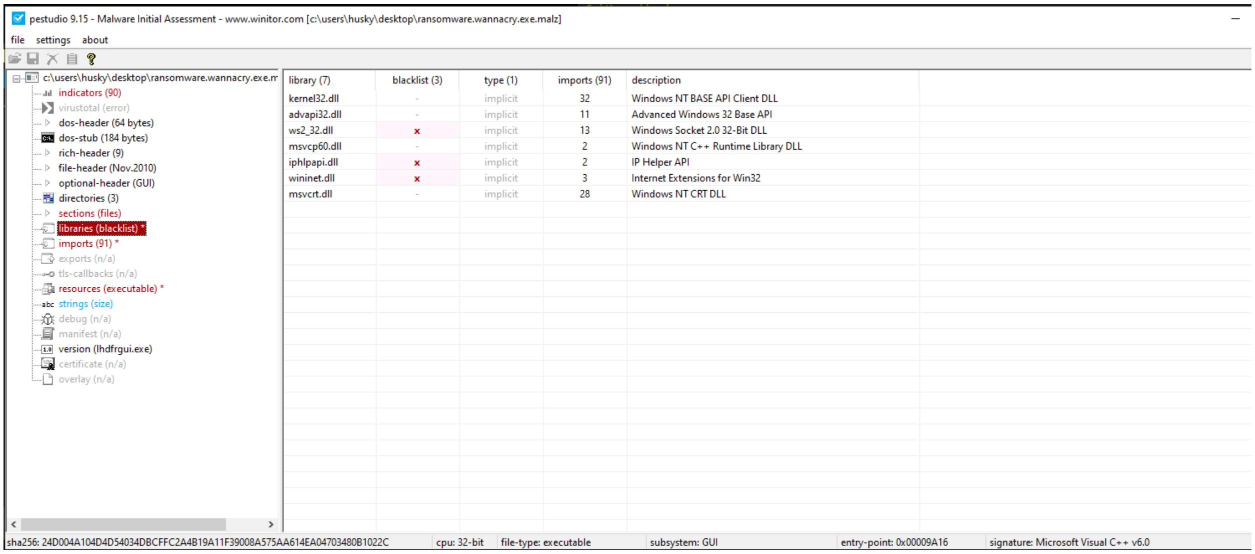


pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\husky\desktop\ransomware.wannacry.exe.malz]

```
c:\users\husky\desktop\ransomware.wannacry.exe.m
  indicators (90)
  virustotal (error)
  dos-header (64 bytes)
  dos-stub (184 bytes)
  rich-header (9)
  file-header (Nov.2010)
  optional-header (GUI)
  directories (3)
  sections (files)
  libraries (blacklist) *
  imports (91) *
  exports (n/a)
  tls-callbacks (n/a)
  resources (executable) *
  strings (size)
  debug (n/a)
  manifest (n/a)
  version (lhdfrgui.exe)
  certificate (n/a)
  overlay (n/a)
```

property	value	value	value	value
name	.text	.rdata	.data	.rsrc
md5	C7613102E2ECEC5DCEFC14...	D8037D744B539326C06E897...	22A8598DC29CAD7078C291...	12E1BD7375D82CCA3A51CA...
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: 0x0000B0...	executable, offset: 0x000320...
file	-	-	executable, offset: 0x0000F0...	n/a

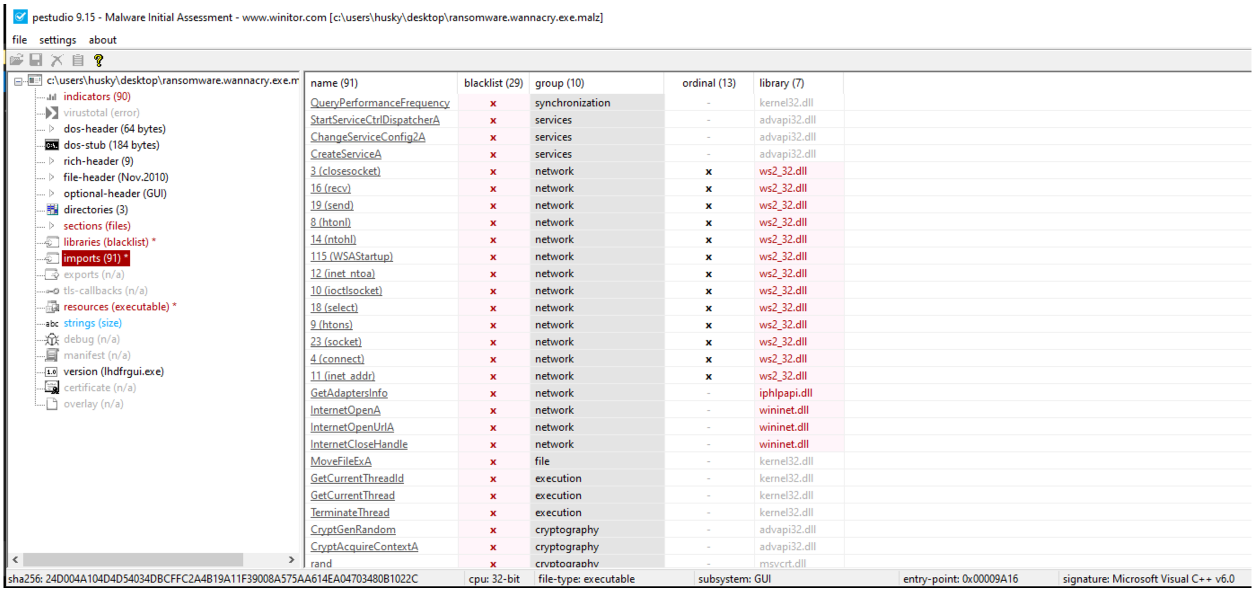
sha256: 24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00009A16 | signature: Microsoft Visual C++ v6.0



pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\husky\desktop\ransomware.wannacry.exe.malz]

library (7)	blacklist (3)	type (1)	imports (91)	description
kernel32.dll	-	implicit	32	Windows NT BASE API Client DLL
advapi32.dll	-	implicit	11	Advanced Windows 32 Base API
ws2_32.dll	x	implicit	13	Windows Socket 2.0 32-Bit DLL
msvcp60.dll	-	implicit	2	Windows NT C++ Runtime Library DLL
iphlpapi.dll	x	implicit	2	IP Helper API
wininet.dll	x	implicit	3	Internet Extensions for Win32
msvcrt.dll	-	implicit	28	Windows NT CRT DLL

sha256: 24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00009A16 | signature: Microsoft Visual C++ v6.0

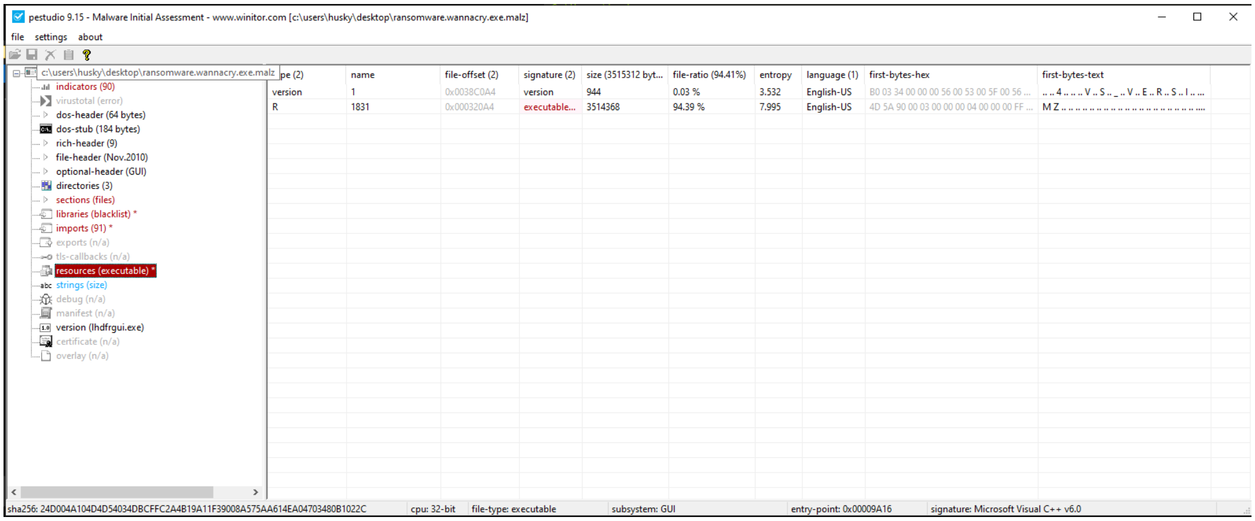


pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\husky\desktop\ransomware.wannacry.exe.malz]

name (91)	blacklist (29)	group (10)	ordinal (13)	library (7)
QueryPerformanceFrequency	x	synchronization	-	kernel32.dll
StartServiceCtrlDispatcherA	x	services	-	advapi32.dll
ChangeServiceConfig2A	x	services	-	advapi32.dll
CreateServiceA	x	services	-	advapi32.dll
3 (closesocket)	x	network	x	ws2_32.dll
16 (recv)	x	network	x	ws2_32.dll
19 (send)	x	network	x	ws2_32.dll
8 (htonl)	x	network	x	ws2_32.dll
14 (ntohl)	x	network	x	ws2_32.dll
115 (WSAStartup)	x	network	x	ws2_32.dll
12 (inet_ntoa)	x	network	x	ws2_32.dll
10 (ioctlsocket)	x	network	x	ws2_32.dll
18 (select)	x	network	x	ws2_32.dll
9 (htons)	x	network	x	ws2_32.dll
23 (socket)	x	network	x	ws2_32.dll
4 (connect)	x	network	x	ws2_32.dll
11 (inet_addr)	x	network	x	ws2_32.dll
GetAdaptersInfo	x	network	-	iphlpapi.dll
InternetOpenA	x	network	-	wininet.dll
InternetOpenUrlA	x	network	-	wininet.dll
InternetCloseHandle	x	network	-	wininet.dll
MoveFileExA	x	file	-	kernel32.dll
GetCurrentThreadId	x	execution	-	kernel32.dll
GetCurrentThread	x	execution	-	kernel32.dll
TerminateThread	x	execution	-	kernel32.dll
CryptGenRandom	x	cryptography	-	advapi32.dll
CryptAcquireContextA	x	cryptography	-	advapi32.dll
rand	x	cryptography	-	msvcrt.dll

sha256: 24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00009A16 | signature: Microsoft Visual C++ v6.0

There is an executable resource.



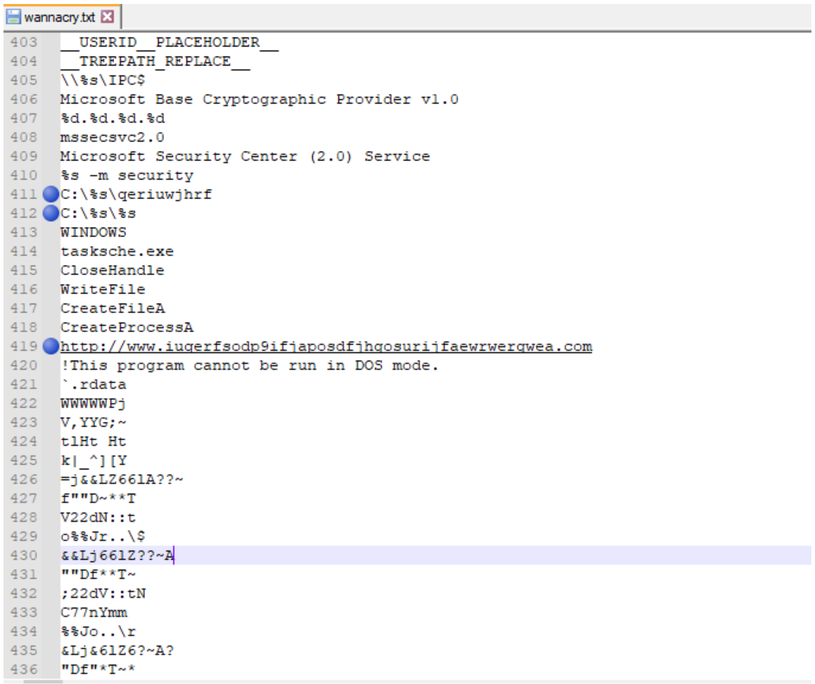
pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\husky\desktop\ransomware.wannacry.exe.malz]

c:\users\husky\desktop\ransomware.wannacry.exe.malz
- indicators (90)
- virustotal (error)
- dos-header (64 bytes)
- dos-stub (184 bytes)
- rich-header (9)
- file-header (Nov.2010)
- optional-header (GUI)
- directories (3)
- sections (files)
- libraries (blacklist) *
- imports (91) *
- exports (n/a)
- tls-callbacks (n/a)
- resources (executable) *
- strings (size)
- debug (n/a)
- manifest (n/a)
- version (lhdfrgui.exe)
- certificate (n/a)
- overlay (n/a)

pe (2)	name	file-offset (2)	signature (2)	size (3515312 byt...	file-ratio (94.41%)	entropy	language (1)	first-bytes-hex	first-bytes-text
version	1	0x0038C0A4	version	944	0.03 %	3.532	English-US	B0 03 34 00 00 00 56 00 53 00 5F 00 56 ...	.. .. 4 .. .. .. V .. S .. _ .. V .. E .. R .. S .. I .. ...
R	1831	0x000320A4	executable...	3514368	94.39 %	7.995	English-US	4D 5A 90 00 03 00 00 00 04 00 00 00 FF ...	M Z .. ..

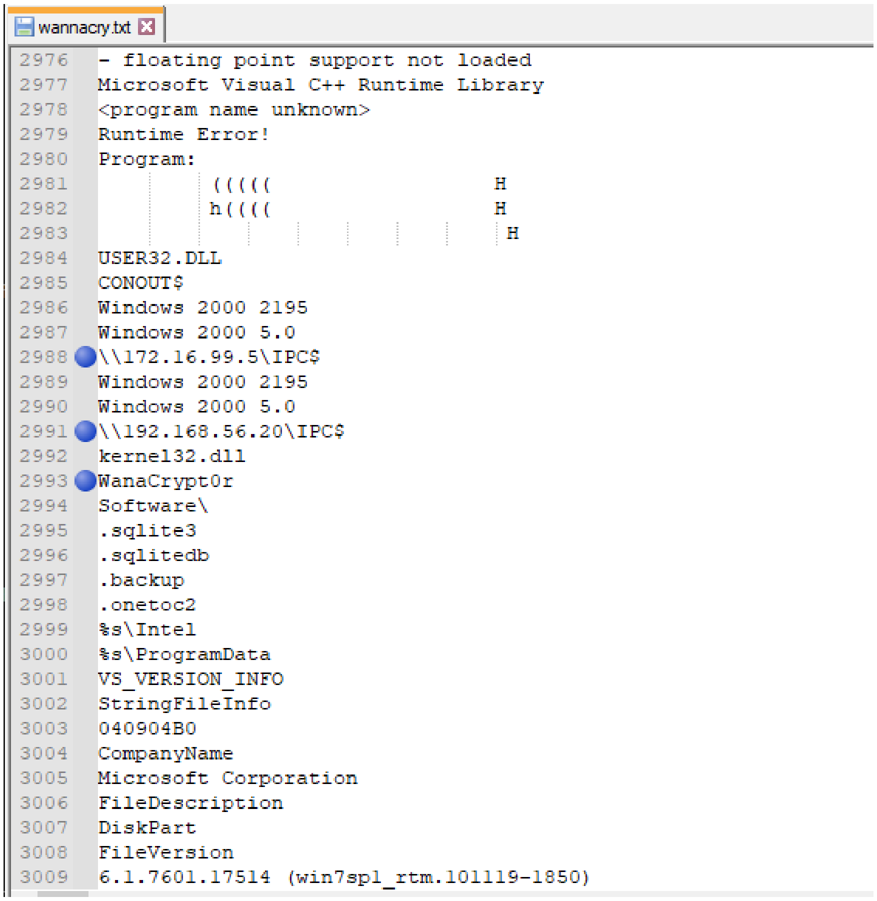
sha256: 24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00009A16 | signature: Microsoft Visual C++ v6.0

The Floss utility is used to determine potential "strings" in the binary file. And we found some interesting ones

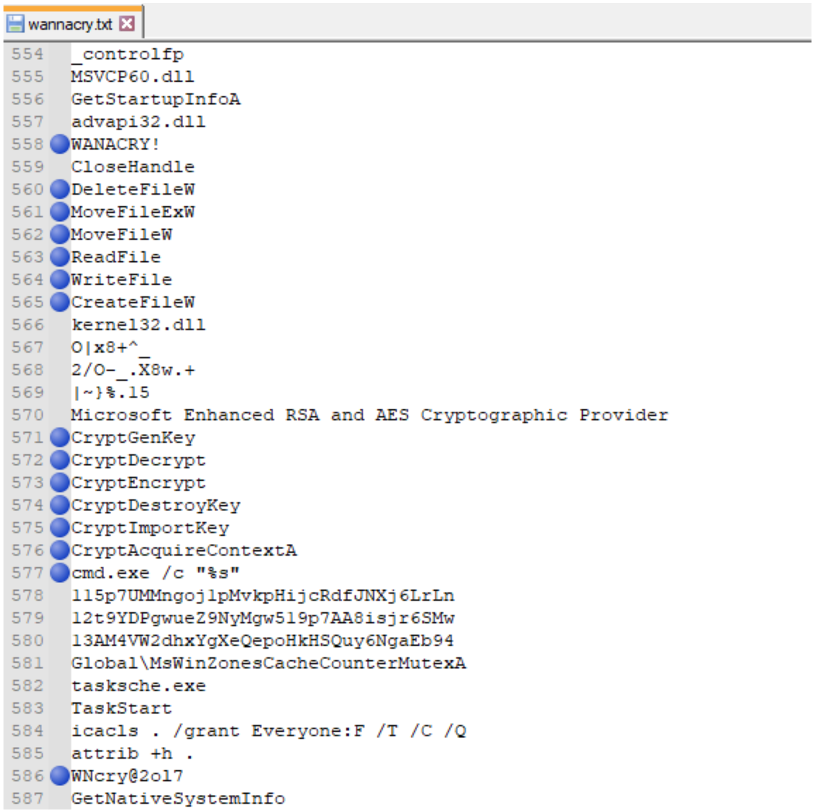


wannacry.txt

```
__USERID__PLACEHOLDER__
__TREEPATH_REPLACE__
\\%s\IPC$
Microsoft Base Cryptographic Provider v1.0
%d.%d.%d.%d
mssecsvc2.0
Microsoft Security Center (2.0) Service
%s -m security
C:\%s\qeriuwjhrf
C:\%s\%s
WINDOWS
tasksche.exe
CloseHandle
WriteFile
CreateFileA
CreateProcessA
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
!This program cannot be run in DOS mode.
`.rdata
WWWWWPj
V,YYG;~
tlHt Ht
k|_^][Y
=j&&LZ66lA??~
f""D~**T
V22dN::t
o%%Jr..\$
&&Lj66lZ??~A
""Df**T~
;22dV::tN
C77nYmm
%%Jo..\r
&Lj&6lZ6?~A?
"Df"*T~*
```



```
- floating point support not loaded
Microsoft Visual C++ Runtime Library
<program name unknown>
Runtime Error!
Program:
         (((((                 H
         h((((                 H
                                H
USER32.DLL
CONOUT$
Windows 2000 2195
Windows 2000 5.0
\\172.16.99.5\IPC$
Windows 2000 2195
Windows 2000 5.0
\\192.168.56.20\IPC$
kernel32.dll
WanaCrypt0r
Software\
.sqlite3
.sqlitedb
.backup
.onetoc2
%s\Intel
%s\ProgramData
VS_VERSION_INFO
StringFileInfo
040904B0
CompanyName
Microsoft Corporation
FileDescription
DiskPart
FileVersion
6.1.7601.17514 (win7sp1_rtm.101119-1850)
```

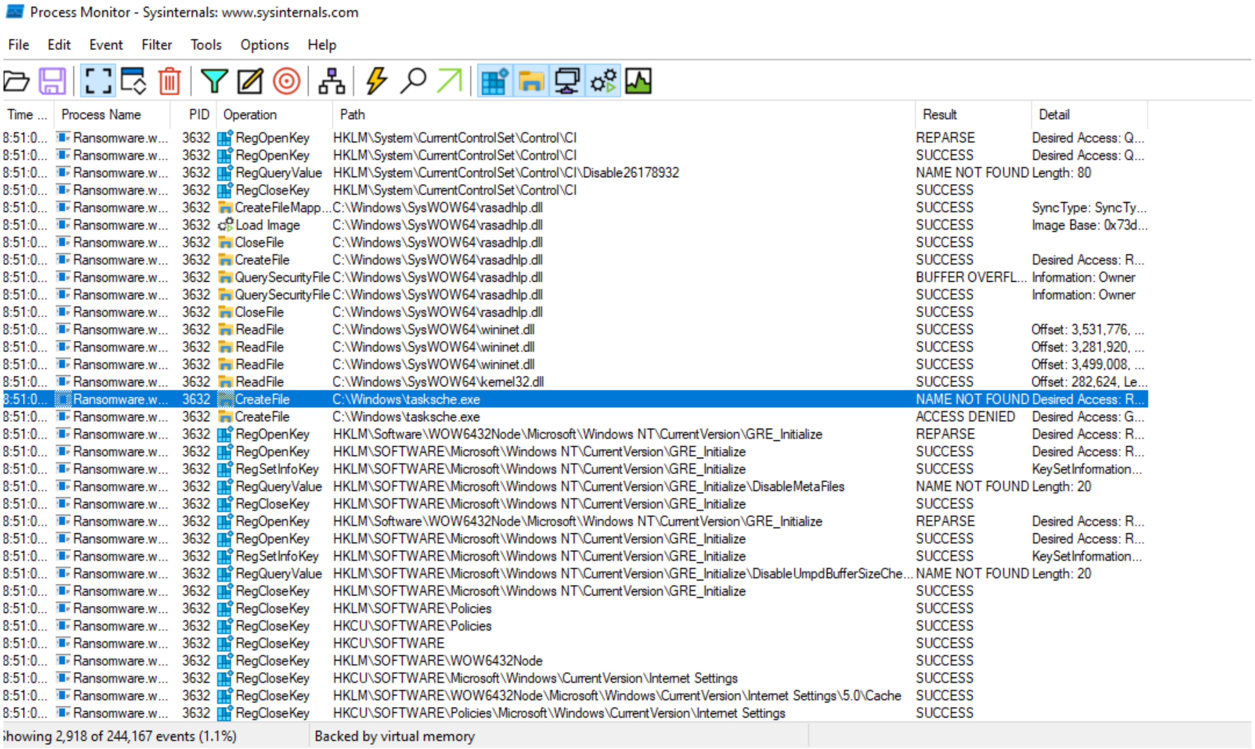


```
_controlfp
MSVCP60.dll
GetStartupInfoA
advapi32.dll
WANACRY!
CloseHandle
DeleteFileW
MoveFileExW
MoveFileW
ReadFile
WriteFile
CreateFileW
kernel32.dll
O|x8+^_
2/O-_.X8w.+
|~}%.15
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Global\MsWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
icacls . /grant Everyone:F /T /C /Q
attrib +h .
WNcry@2ol7
GetNativeSystemInfo
```

Basic Dynamic Analysis

Running the malware without administrator privileges will not activate the malicious payload, which includes file encryption and spreading to other targets.

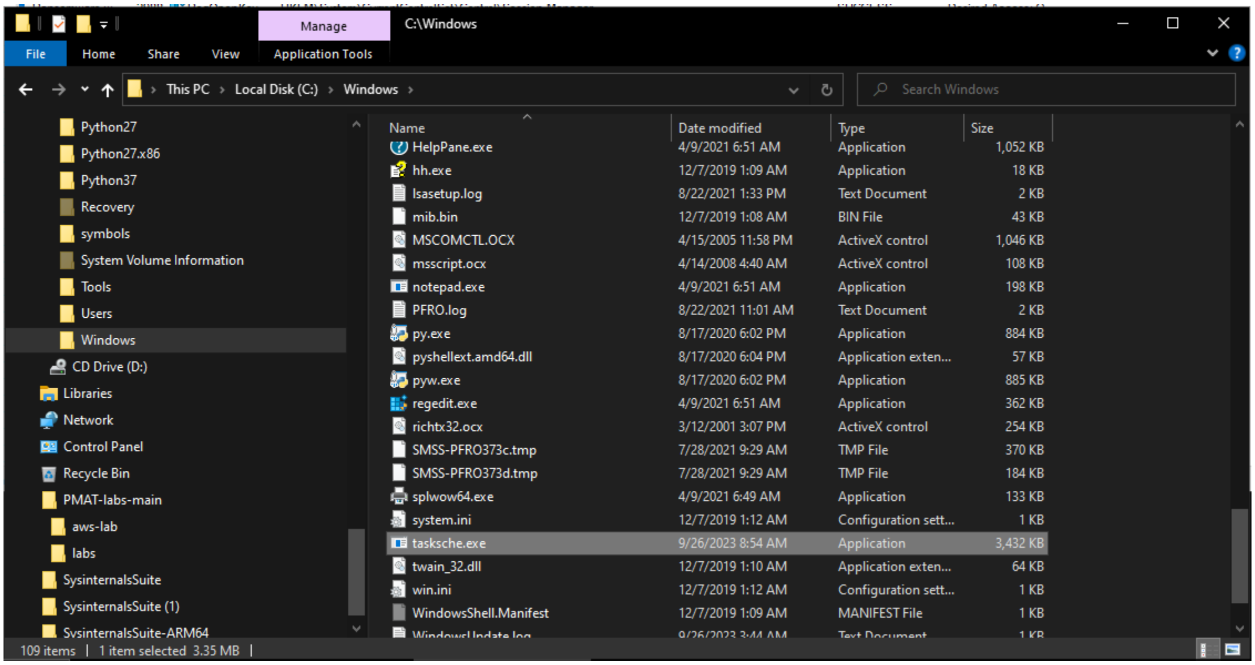
Without Administrator privileges



Time ...	Process Name	PID	Operation	Path	Result	Detail
8:51:0...	Ransomware.w...	3632	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: Q...
8:51:0...	Ransomware.w...	3632	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: Q...
8:51:0...	Ransomware.w...	3632	RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND	Length: 80
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
8:51:0...	Ransomware.w...	3632	CreateFileMapp...	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	SyncType: SyncTy...
8:51:0...	Ransomware.w...	3632	Load Image	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	Image Base: 0x73d...
8:51:0...	Ransomware.w...	3632	CloseFile	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	
8:51:0...	Ransomware.w...	3632	CreateFile	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	Desired Access: R...
8:51:0...	Ransomware.w...	3632	QuerySecurityFile	C:\Windows\SysWOW64\rasadhlp.dll	BUFFER OVERFL...	Information: Owner
8:51:0...	Ransomware.w...	3632	QuerySecurityFile	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	Information: Owner
8:51:0...	Ransomware.w...	3632	CloseFile	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	
8:51:0...	Ransomware.w...	3632	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 3,531,776, ...
8:51:0...	Ransomware.w...	3632	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 3,281,920, ...
8:51:0...	Ransomware.w...	3632	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 3,499,008, ...
8:51:0...	Ransomware.w...	3632	ReadFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Offset: 282,624, Le...
8:51:0...	Ransomware.w...	3632	CreateFile	C:\Windows\tasksche.exe	NAME NOT FOUND	Desired Access: R...
8:51:0...	Ransomware.w...	3632	CreateFile	C:\Windows\tasksche.exe	ACCESS DENIED	Desired Access: G...
8:51:0...	Ransomware.w...	3632	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	REPARSE	Desired Access: R...
8:51:0...	Ransomware.w...	3632	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: R...
8:51:0...	Ransomware.w...	3632	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	KeySetInformation...
8:51:0...	Ransomware.w...	3632	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles	NAME NOT FOUND	Length: 20
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	
8:51:0...	Ransomware.w...	3632	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	REPARSE	Desired Access: R...
8:51:0...	Ransomware.w...	3632	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: R...
8:51:0...	Ransomware.w...	3632	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	KeySetInformation...
8:51:0...	Ransomware.w...	3632	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableUmpdBufferSizeChe...	NAME NOT FOUND	Length: 20
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKLM\SOFTWARE\Policies	SUCCESS	
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKCU\SOFTWARE\Policies	SUCCESS	
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKCU\SOFTWARE	SUCCESS	
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKLM\SOFTWARE\WOW6432Node	SUCCESS	
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache	SUCCESS	
8:51:0...	Ransomware.w...	3632	RegCloseKey	HKCU\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	

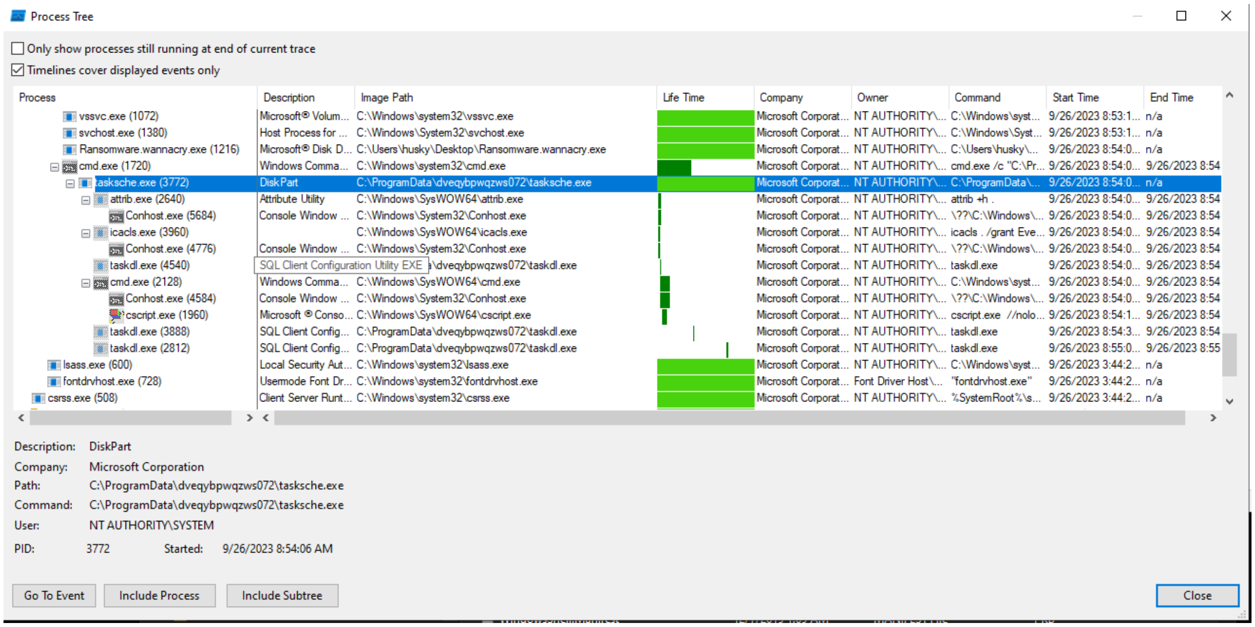
Showing 2,918 of 244,167 events (1.1%)   Backed by virtual memory

With Administrator privileges



Name	Date modified	Type	Size
HelpPane.exe	4/9/2021 6:51 AM	Application	1,052 KB
hh.exe	12/7/2019 1:09 AM	Application	18 KB
lsasetup.log	8/22/2021 1:33 PM	Text Document	2 KB
mib.bin	12/7/2019 1:08 AM	BIN File	43 KB
MSCOMCTL.OCX	4/15/2005 11:58 PM	ActiveX control	1,046 KB
msscript.ocx	4/14/2008 4:40 AM	ActiveX control	108 KB
notepad.exe	4/9/2021 6:51 AM	Application	198 KB
PFRO.log	8/22/2021 11:01 AM	Text Document	2 KB
py.exe	8/17/2020 6:02 PM	Application	884 KB
pyshellext.amd64.dll	8/17/2020 6:04 PM	Application exten...	57 KB
pyw.exe	8/17/2020 6:02 PM	Application	885 KB
regedit.exe	4/9/2021 6:51 AM	Application	362 KB
richtx32.ocx	3/12/2001 3:07 PM	ActiveX control	254 KB
SMSS-PFRO373c.tmp	7/28/2021 9:29 AM	TMP File	370 KB
SMSS-PFRO373d.tmp	7/28/2021 9:29 AM	TMP File	184 KB
splwow64.exe	4/9/2021 6:49 AM	Application	133 KB
system.ini	12/7/2019 1:12 AM	Configuration sett...	1 KB
tasksche.exe	9/26/2023 8:54 AM	Application	3,432 KB
twain_32.dll	12/7/2019 1:10 AM	Application exten...	64 KB
win.ini	12/7/2019 1:12 AM	Configuration sett...	1 KB
WindowsShell.Manifest	12/7/2019 1:09 AM	MANIFEST File	1 KB
WindowsUpdate.log	9/26/2023 3:44 AM	Text Document	1 KB

109 items | 1 item selected 3.35 MB |

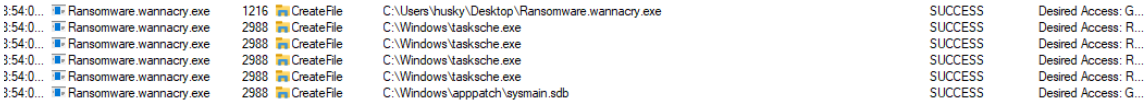


□ Only show processes still running at end of current trace

☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
vssvc.exe (1072)	Microsoft® Volum...	C:\Windows\system32\vssvc.exe		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	9/26/2023 8:53:1...	n/a
svchost.exe (1380)	Host Process for ...	C:\Windows\System32\svchost.exe		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\Syst...	9/26/2023 8:53:1...	n/a
Ransomware.wannacry.exe (1216)	Microsoft® Disk D...	C:\Users\husky\Desktop\Ransomware.wannacry.exe		Microsoft Corporat...	NT AUTHORITY\...	C:\Users\husky\...	9/26/2023 8:54:0...	n/a
cmd.exe (1720)	Windows Comma...	C:\Windows\system32\cmd.exe		Microsoft Corporat...	NT AUTHORITY\...	cmd.exe /c "C:\Pr...	9/26/2023 8:54:0...	9/26/2023 8:54
tasksche.exe (3772)	DiskPart	C:\ProgramData\dveqybpwqzws072\tasksche.exe		Microsoft Corporat...	NT AUTHORITY\...	C:\ProgramData\...	9/26/2023 8:54:0...	n/a
attrib.exe (2640)	Attribute Utility	C:\Windows\SysWOW64\attrib.exe		Microsoft Corporat...	NT AUTHORITY\...	attrib +h .	9/26/2023 8:54:0...	9/26/2023 8:54
Conhost.exe (5684)	Console Window ...	C:\Windows\System32\Conhost.exe		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\...	9/26/2023 8:54:0...	9/26/2023 8:54
icacls.exe (3960)		C:\Windows\SysWOW64\icacls.exe		Microsoft Corporat...	NT AUTHORITY\...	icacls . /grant Eve...	9/26/2023 8:54:0...	9/26/2023 8:54
Conhost.exe (4776)	Console Window ...	C:\Windows\System32\Conhost.exe		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\...	9/26/2023 8:54:0...	9/26/2023 8:54
taskdl.exe (4540)	SQL Client Configuration Utility EXE	\dveqybpwqzws072\taskdl.exe		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	9/26/2023 8:54:0...	9/26/2023 8:54
cmd.exe (2128)	Windows Comma...	C:\Windows\SysWOW64\cmd.exe		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	9/26/2023 8:54:0...	9/26/2023 8:54
Conhost.exe (4584)	Console Window ...	C:\Windows\System32\Conhost.exe		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\...	9/26/2023 8:54:0...	9/26/2023 8:54
cscript.exe (1960)	Microsoft ® Conso...	C:\Windows\SysWOW64\cscript.exe		Microsoft Corporat...	NT AUTHORITY\...	cscript.exe //nolo...	9/26/2023 8:54:1...	9/26/2023 8:54
taskdl.exe (3888)	SQL Client Config...	C:\ProgramData\dveqybpwqzws072\taskdl.exe		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	9/26/2023 8:54:3...	9/26/2023 8:54
taskdl.exe (2812)	SQL Client Config...	C:\ProgramData\dveqybpwqzws072\taskdl.exe		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	9/26/2023 8:55:0...	9/26/2023 8:55
lsass.exe (600)	Local Security Aut...	C:\Windows\system32\lsass.exe		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	9/26/2023 3:44:2...	n/a
fontdrvhost.exe (728)	Usermode Font Dr...	C:\Windows\system32\fontdrvhost.exe		Microsoft Corporat...	Font Driver Host\...	"fontdrvhost.exe"	9/26/2023 3:44:2...	n/a
csrss.exe (508)	Client Server Runt...	C:\Windows\system32\csrss.exe		Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\s...	9/26/2023 3:44:2...	n/a

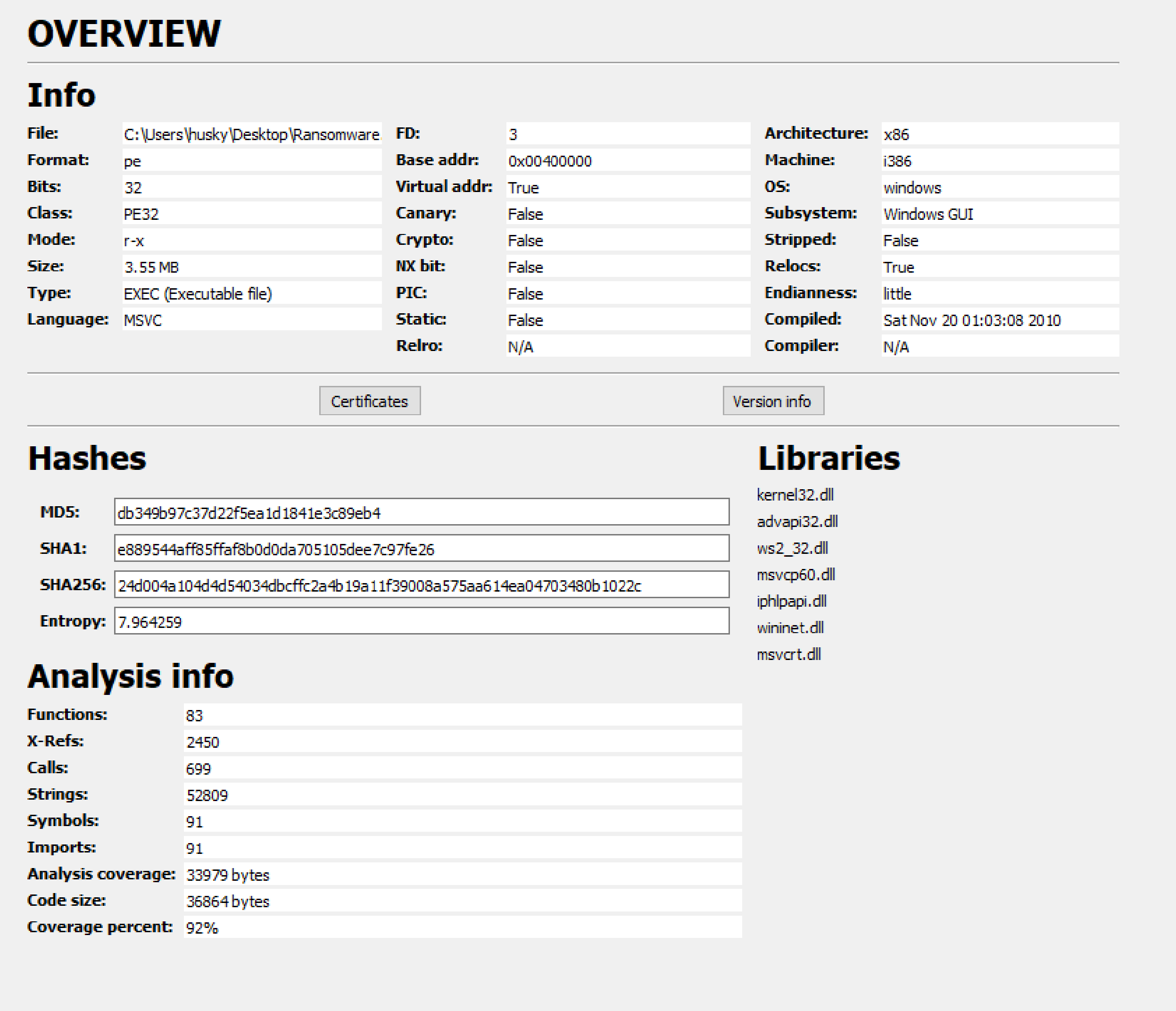
Description: DiskPart
Company: Microsoft Corporation
Path: C:\ProgramData\dveqybpwqzws072\tasksche.exe
Command: C:\ProgramData\dveqybpwqzws072\tasksche.exe
User: NT AUTHORITY\SYSTEM
PID: 3772 Started: 9/26/2023 8:54:06 AM



```
3:54:0...  Ransomware.wannacry.exe   1216  CreateFile   C:\Users\husky\Desktop\Ransomware.wannacry.exe   SUCCESS   Desired Access: G...
3:54:0...  Ransomware.wannacry.exe   2988  CreateFile   C:\Windows\tasksche.exe                          SUCCESS   Desired Access: R...
3:54:0...  Ransomware.wannacry.exe   2988  CreateFile   C:\Windows\tasksche.exe                          SUCCESS   Desired Access: R...
3:54:0...  Ransomware.wannacry.exe   2988  CreateFile   C:\Windows\tasksche.exe                          SUCCESS   Desired Access: R...
3:54:0...  Ransomware.wannacry.exe   2988  CreateFile   C:\Windows\tasksche.exe                          SUCCESS   Desired Access: R...
3:54:0...  Ransomware.wannacry.exe   2988  CreateFile   C:\Windows\apppatch\sysmain.sdb                  SUCCESS   Desired Access: G...
```

Advanced Static Analysis

We use “Cutter” disassembler to follow the flow of the binary code



OVERVIEW

Info

File:	C:\Users\husky\Desktop\Ransomware	**FD:**	3	**Architecture:**	x86
Format:	pe	**Base addr:**	0x00400000	**Machine:**	i386
Bits:	32	**Virtual addr:**	True	**OS:**	windows
Class:	PE32	**Canary:**	False	**Subsystem:**	Windows GUI
Mode:	r-x	**Crypto:**	False	**Stripped:**	False
Size:	3.55 MB	**NX bit:**	False	**Relocs:**	True
Type:	EXEC (Executable file)	**PIC:**	False	**Endianness:**	little
Language:	MSVC	**Static:**	False	**Compiled:**	Sat Nov 20 01:03:08 2010
		Relro:	N/A	**Compiler:**	N/A

Hashes

MD5:	db349b97c37d22f5ea1d1841e3c89eb4
SHA1:	e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA256:	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Entropy:	7.964259

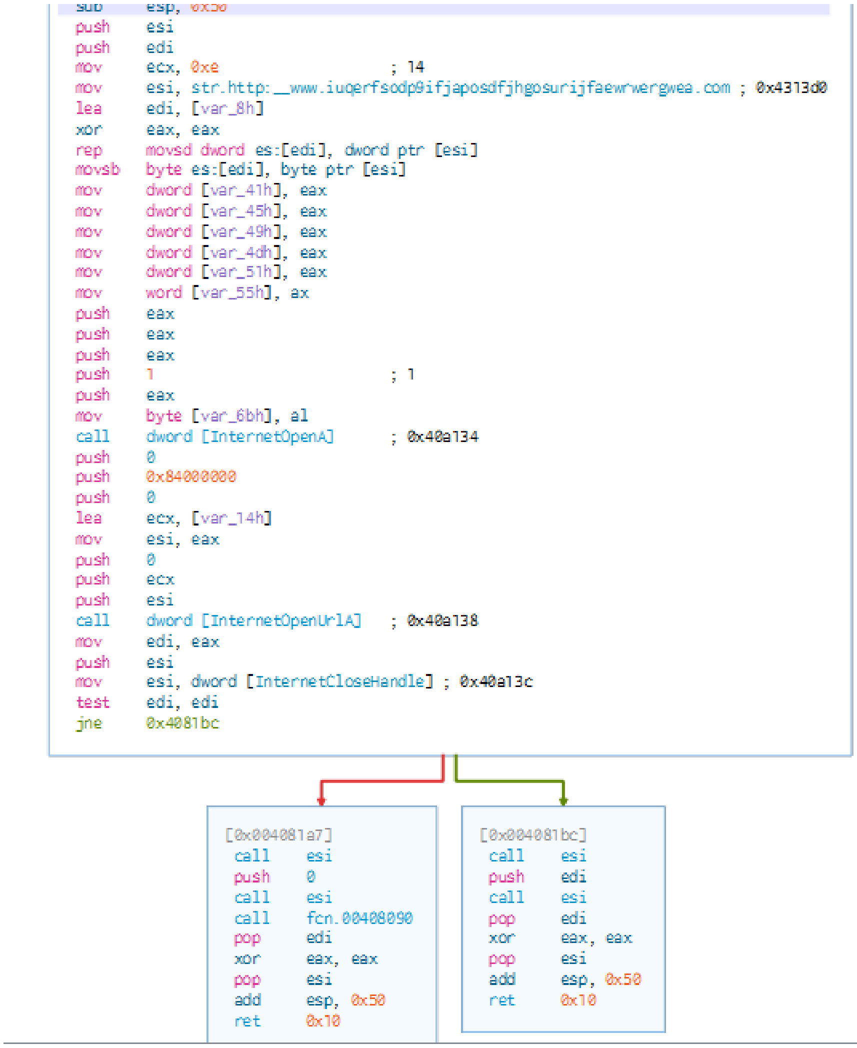
Libraries

kernel32.dll
advapi32.dll
ws2_32.dll
msvcp60.dll
iphlpapi.dll
wininet.dll
msvcrt.dll

Analysis info

Functions:	83
X-Refs:	2450
Calls:	699
Strings:	52809
Symbols:	91
Imports:	91
Analysis coverage:	33979 bytes
Code size:	36864 bytes
Coverage percent:	92%

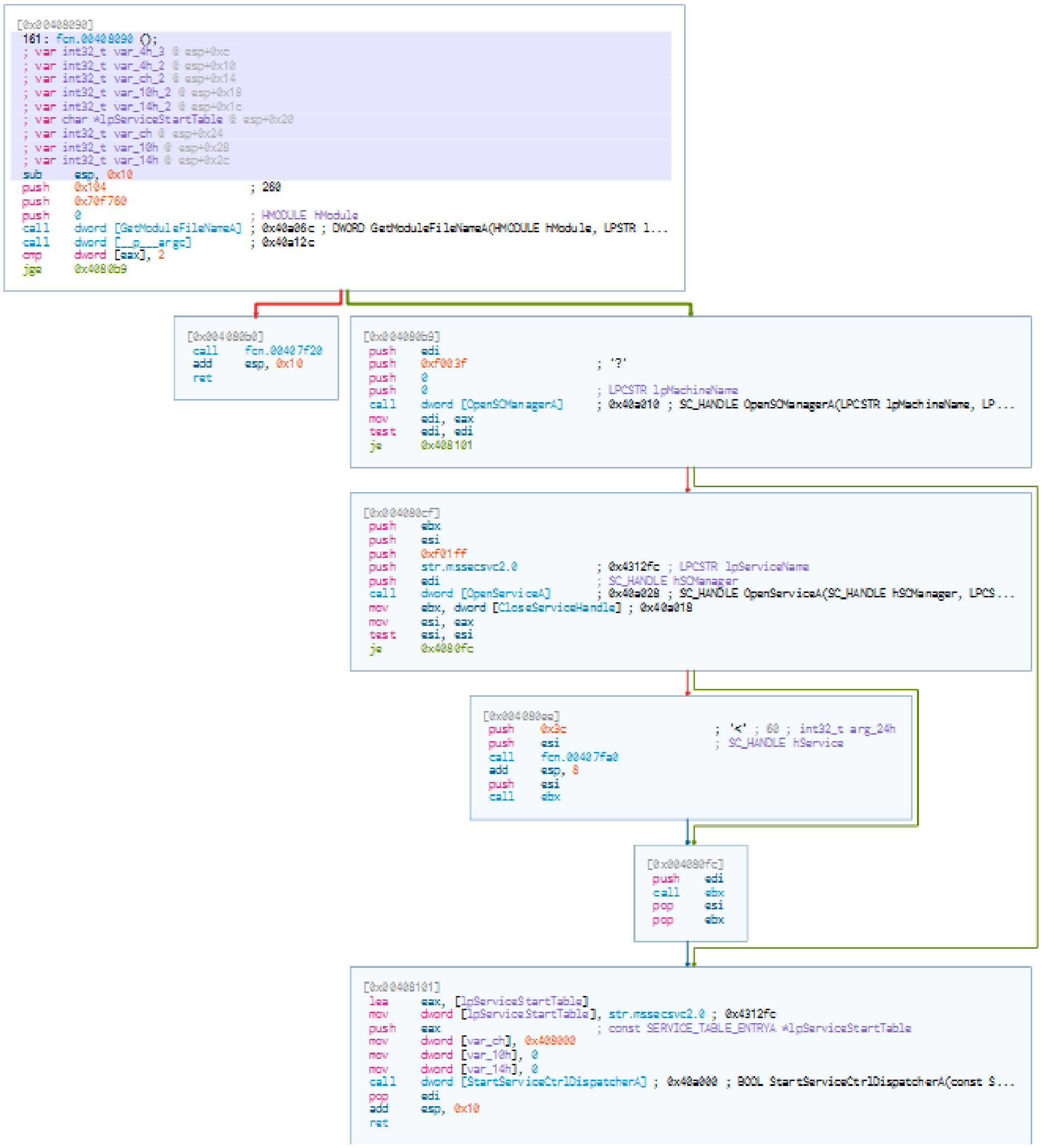
In the main function, the binary check is the callback url exists and try to connect.
If successful, it exits.
If the connection fails, the dropper attempts to create a service named "mssecsvc2.0" with the DisplayName "Microsoft Security Center (2.0) Service



```
sub     esp, 0x50
push    esi
push    edi
mov     ecx, 0xe                   ; 14
mov     esi, str.http:__www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.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
```

```
[0x004081a7]
 call    esi
 push    0
 call    esi
 call    fcn.00408090
 pop     edi
 xor     eax, eax
 pop     esi
 add     esp, 0x50
 ret     0x10
```

```
[0x004081bc]
 call    esi
 push    edi
 call    esi
 pop     edi
 xor     eax, eax
 pop     esi
 add     esp, 0x50
 ret     0x10
```



```
[0x00408090]
161: fcn.00408090 ();
; var int32_t var_4h_3 @ esp+0xc
; var int32_t var_4h_2 @ esp+0x10
; var int32_t var_ch_2 @ esp+0x14
; var int32_t var_10h_2 @ esp+0x18
; var int32_t var_14h_2 @ esp+0x1c
; var char *lpServiceStartTable @ esp+0x20
; var int32_t var_ch @ esp+0x24
; var int32_t var_10h @ esp+0x28
; var int32_t var_14h @ esp+0x2c
sub     esp, 0x10
push    0x104                        ; 260
push    0x70f760
push    0                            ; HMODULE hModule
call    dword [GetModuleFileNameA]   ; 0x40a06c ; DWORD GetModuleFileNameA(HMODULE hModule, LPSTR l...
call    dword [__p___argc]           ; 0x40a12c
cmp     dword [eax], 2
jge     0x4080b9
```

```
[0x004080b0]
call    fcn.00407f20
add     esp, 0x10
ret
```

```
[0x004080b9]
push    edi
push    0xf003f                      ; '?'
push    0
push    0                            ; LPCSTR lpMachineName
call    dword [OpenSCManagerA]       ; 0x40a010 ; SC_HANDLE OpenSCManagerA(LPCSTR lpMachineName, LP...
mov     edi, eax
test    edi, edi
je      0x408101
```

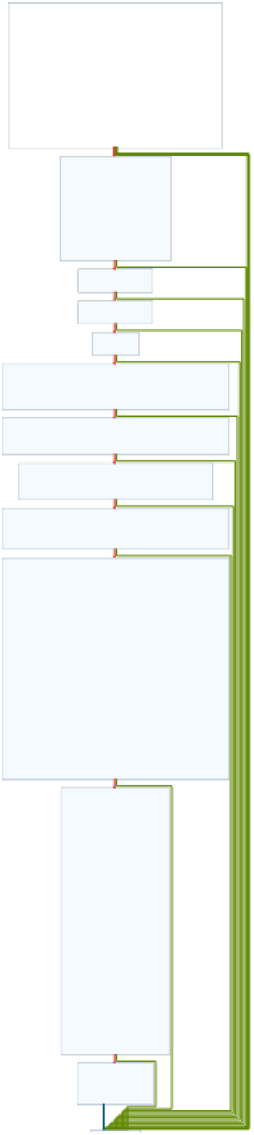
```
[0x004080cf]
push    ebx
push    esi
push    0xf01ff
push    str.mssecsvc2.0              ; 0x4312fc ; LPCSTR lpServiceName
push    edi                          ; SC_HANDLE hSCManager
call    dword [OpenServiceA]         ; 0x40a028 ; SC_HANDLE OpenServiceA(SC_HANDLE hSCManager, LPCS...
mov     ebx, dword [CloseServiceHandle] ; 0x40a018
mov     esi, eax
test    esi, esi
je      0x4080fc
```

```
[0x004080ee]
push    0x3c                         ; '<' ; 60 ; int32_t arg_24h
push    esi                          ; SC_HANDLE hService
call    fcn.00407fa0
add     esp, 8
push    esi
call    ebx
```

```
[0x004080fc]
push    edi
call    ebx
pop     esi
pop     ebx
```

```
[0x00408101]
lea     eax, [lpServiceStartTable]
mov     dword [lpServiceStartTable], str.mssecsvc2.0 ; 0x4312fc
push    eax                          ; const SERVICE_TABLE_ENTRYA *lpServiceStartTable
mov     dword [var_ch], 0x408000
mov     dword [var_10h], 0
mov     dword [var_14h], 0
call    dword [StartServiceCtrlDispatcherA] ; 0x40a000 ; BOOL StartServiceCtrlDispatcherA(const S...
pop     edi
add     esp, 0x10
ret
```

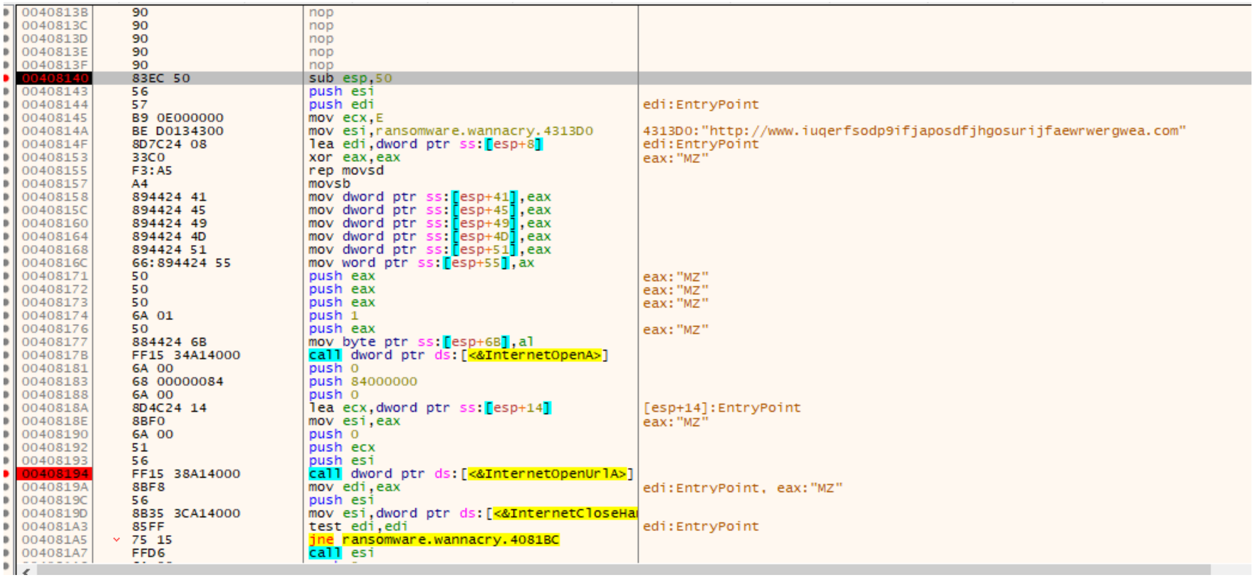
Encryption function.



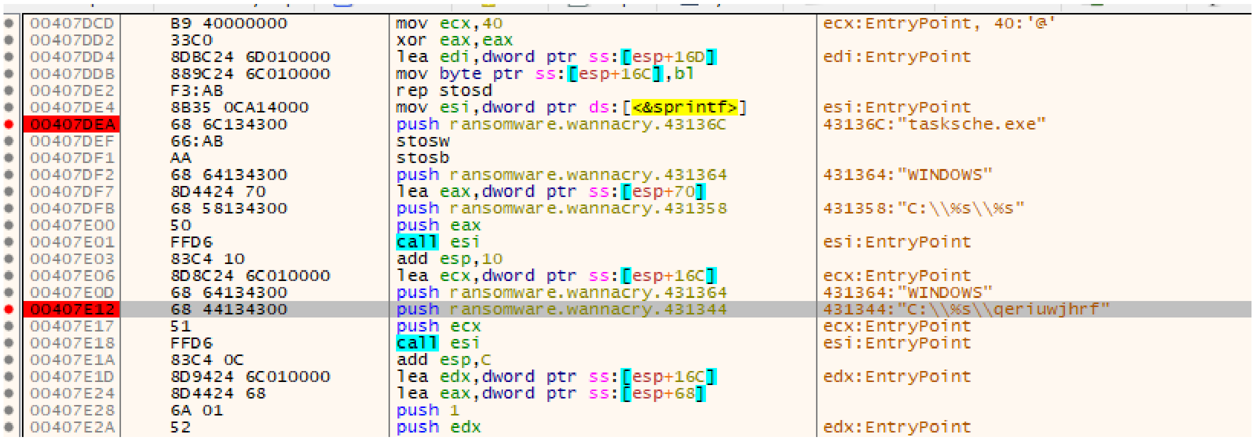
Advanced Dynamic Analysis

We use “x32dbg” debugger to analyze the binary code dynamically.

Main function.

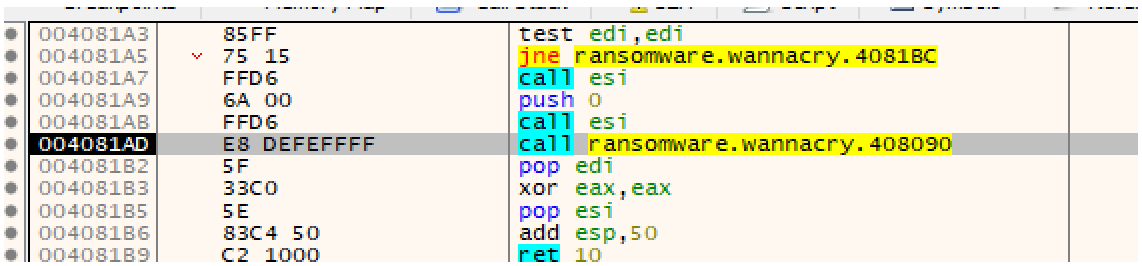


```
0040813B    90               nop
0040813C    90               nop
0040813D    90               nop
0040813E    90               nop
0040813F    90               nop
00408140    83EC 50          sub esp,50
00408143    56               push esi
00408144    57               push edi                                   edi:EntryPoint
00408145    B9 0E000000      mov ecx,E
0040814A    BE D0134300      mov esi,ransomware.wannacry.4313D0         4313D0:"http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
0040814F    8D7C24 08        lea edi,dword ptr ss:[esp+8]               edi:EntryPoint
00408153    33C0             xor eax,eax                                eax:"MZ"
00408155    F3:A5            rep movsd
00408157    A4               movsb
00408158    894424 41        mov dword ptr ss:[esp+41],eax
0040815C    894424 45        mov dword ptr ss:[esp+45],eax
00408160    894424 49        mov dword ptr ss:[esp+49],eax
00408164    894424 4D        mov dword ptr ss:[esp+4D],eax
00408168    894424 51        mov dword ptr ss:[esp+51],eax
0040816C    66:894424 55     mov word ptr ss:[esp+55],ax
00408171    50               push eax                                   eax:"MZ"
00408172    50               push eax                                   eax:"MZ"
00408173    50               push eax                                   eax:"MZ"
00408174    6A 01            push 1
00408176    50               push eax                                   eax:"MZ"
00408177    884424 6B        mov byte ptr ss:[esp+6B],al
0040817B    FF15 34A14000    call dword ptr ds:[<&InternetOpenA>]
00408181    6A 00            push 0
00408183    68 00000084      push 84000000
00408188    6A 00            push 0
0040818A    8D4C24 14        lea ecx,dword ptr ss:[esp+14]              [esp+14]:EntryPoint
0040818E    8BF0             mov esi,eax                                eax:"MZ"
00408190    6A 00            push 0
00408192    51               push ecx
00408193    56               push esi
00408194    FF15 38A14000    call dword ptr ds:[<&InternetOpenUrlA>]
0040819A    8BF8             mov edi,eax                                edi:EntryPoint, eax:"MZ"
0040819C    56               push esi
0040819D    8B35 3CA14000    mov esi,dword ptr ds:[<&InternetCloseHa
004081A3    85FF             test edi,edi                               edi:EntryPoint
004081A5    75 15            jne ransomware.wannacry.4081BC
004081A7    FFD6             call esi
```

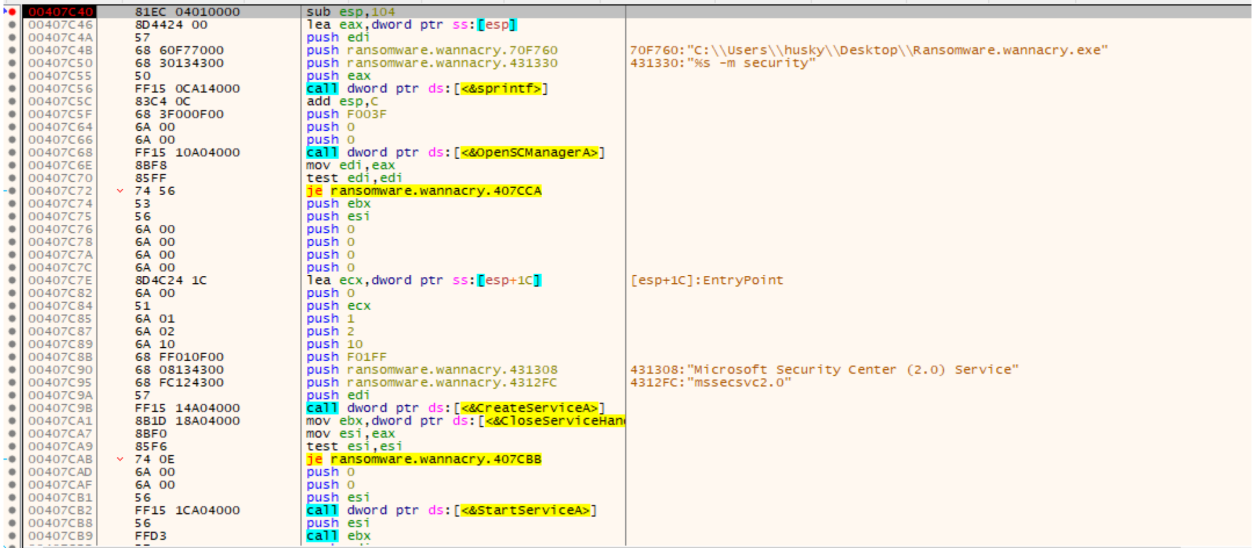


```
00407DCD    B9 40000000      mov ecx,40                                 ecx:EntryPoint, 40:'@'
00407DD2    33C0             xor eax,eax
00407DD4    8DBC24 6D010000  lea edi,dword ptr ss:[esp+16D]             edi:EntryPoint
00407DDB    889C24 6C010000  mov byte ptr ss:[esp+16C],bl
00407DE2    F3:AB            rep stosd
00407DE4    8B35 0CA14000    mov esi,dword ptr ds:[<&sprintf>]          esi:EntryPoint
00407DEA    68 6C134300      push ransomware.wannacry.43136C            43136C:"tasksche.exe"
00407DEF    66:AB            stosw
00407DF1    AA               stosb
00407DF2    68 64134300      push ransomware.wannacry.431364            431364:"WINDOWS"
00407DF7    8D4424 70        lea eax,dword ptr ss:[esp+70]
00407DFB    68 58134300      push ransomware.wannacry.431358            431358:"C:\\%s\\%s"
00407E00    50               push eax
00407E01    FFD6             call esi                                   esi:EntryPoint
00407E03    83C4 10          add esp,10
00407E06    8D8C24 6C010000  lea ecx,dword ptr ss:[esp+16C]             ecx:EntryPoint
00407E0D    68 64134300      push ransomware.wannacry.431364            431364:"WINDOWS"
00407E12    68 44134300      push ransomware.wannacry.431344            431344:"C:\\%s\\qeriuwjhrf"
00407E17    51               push ecx                                   ecx:EntryPoint
00407E18    FFD6             call esi                                   esi:EntryPoint
00407E1A    83C4 0C          add esp,C
00407E1D    8D9424 6C010000  lea edx,dword ptr ss:[esp+16C]             edx:EntryPoint
00407E24    8D4424 68        lea eax,dword ptr ss:[esp+68]
00407E28    6A 01            push 1
00407E2A    52               push edx                                   edx:EntryPoint
```

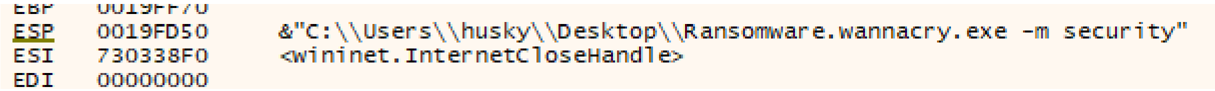
Function 00408090



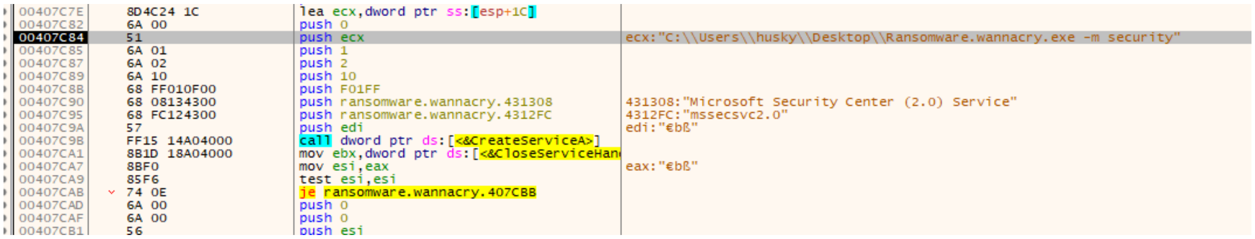
```
004081A3    85FF          test edi,edi
004081A5    75 15         jne ransomware.wannacry.4081BC
004081A7    FFD6          call esi
004081A9    6A 00         push 0
004081AB    FFD6          call esi
004081AD    E8 DEFEFFFF   call ransomware.wannacry.408090
004081B2    5F            pop edi
004081B3    33C0          xor eax,eax
004081B5    5E            pop esi
004081B6    83C4 50       add esp,50
004081B9    C2 1000       ret 10
```



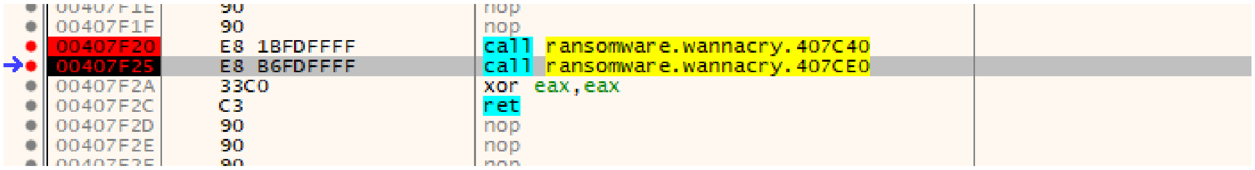
```
00407C40   81EC 04010000   sub esp,104
00407C46   8D4424 00       lea eax,dword ptr ss:[esp]
00407C4A   57              push edi
00407C4B   68 60F77000     push ransomware.wannacry.70F760            70F760:"C:\\Users\\husky\\Desktop\\Ransomware.wannacry.exe"
00407C50   68 30134300     push ransomware.wannacry.431330            431330:"%s -m security"
00407C55   50              push eax
00407C56   FF15 0CA14000   call dword ptr ds:[<&sprintf>]
00407C5C   83C4 0C         add esp,C
00407C5F   68 3F000F00     push F003F
00407C64   6A 00           push 0
00407C66   6A 00           push 0
00407C68   FF15 10A04000   call dword ptr ds:[<&OpenSCManagerA>]
00407C6E   8BF8            mov edi,eax
00407C70   85FF            test edi,edi
00407C72   74 56           je ransomware.wannacry.407CCA
00407C74   53              push ebx
00407C75   56              push esi
00407C76   6A 00           push 0
00407C78   6A 00           push 0
00407C7A   6A 00           push 0
00407C7C   6A 00           push 0
00407C7E   8D4C24 1C       lea ecx,dword ptr ss:[esp+1C]              [esp+1C]:EntryPoint
00407C82   6A 00           push 0
00407C84   51              push ecx
00407C85   6A 01           push 1
00407C87   6A 02           push 2
00407C89   6A 10           push 10
00407C8B   68 FF010F00     push F01FF
00407C90   68 08134300     push ransomware.wannacry.431308            431308:"Microsoft Security Center (2.0) Service"
00407C95   68 FC124300     push ransomware.wannacry.4312FC            4312FC:"mssecsvc2.0"
00407C9A   57              push edi
00407C9B   FF15 14A04000   call dword ptr ds:[<&CreateServiceA>]
00407CA1   8B1D 18A04000   mov ebx,dword ptr ds:[<&CloseServiceHan
00407CA7   8BF0            mov esi,eax
00407CA9   85F6            test esi,esi
00407CAB   74 0E           je ransomware.wannacry.407CBB
00407CAD   6A 00           push 0
00407CAF   6A 00           push 0
00407CB1   56              push esi
00407CB2   FF15 1CA04000   call dword ptr ds:[<&StartServiceA>]
00407CB8   56              push esi
00407CB9   FFD3            call ebx
```



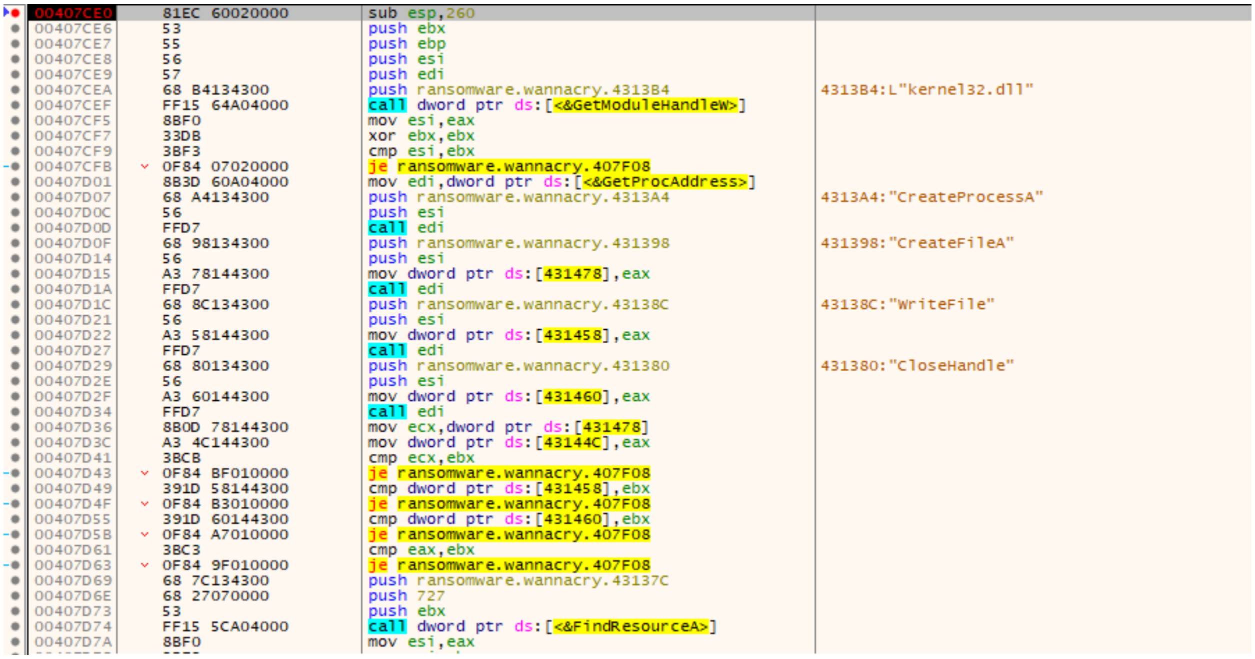
```
ESP   0019FD50   &"C:\\Users\\husky\\Desktop\\Ransomware.wannacry.exe -m security"
ESI   730338F0   <wininet.InternetCloseHandle>
EDI   00000000
```



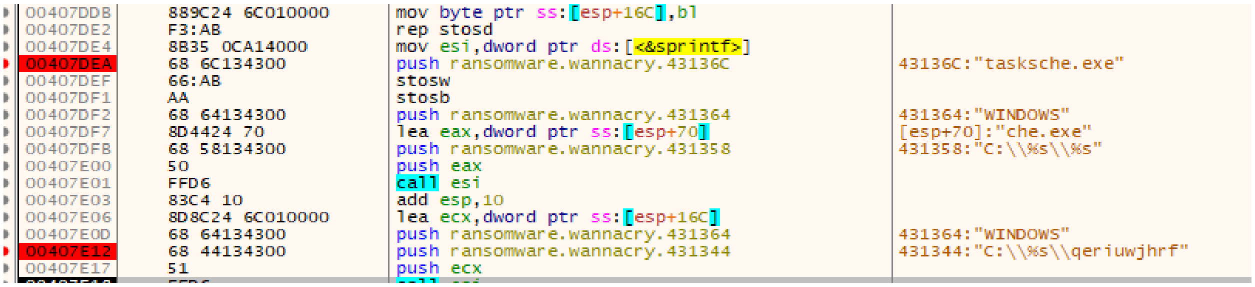
```
00407C7E   8D4C24 1C       lea ecx,dword ptr ss:[esp+1C]
00407C82   6A 00           push 0
00407C84   51              push ecx                                   ecx:"C:\\Users\\husky\\Desktop\\Ransomware.wannacry.exe -m security"
00407C85   6A 01           push 1
00407C87   6A 02           push 2
00407C89   6A 10           push 10
00407C8B   68 FF010F00     push F01FF
00407C90   68 08134300     push ransomware.wannacry.431308            431308:"Microsoft Security Center (2.0) Service"
00407C95   68 FC124300     push ransomware.wannacry.4312FC            4312FC:"mssecsvc2.0"
00407C9A   57              push edi                                   edi:"€bß"
00407C9B   FF15 14A04000   call dword ptr ds:[<&CreateServiceA>]
00407CA1   8B1D 18A04000   mov ebx,dword ptr ds:[<&CloseServiceHan
00407CA7   8BF0            mov esi,eax                                eax:"€bß"
00407CA9   85F6            test esi,esi
00407CAB   74 0E           je ransomware.wannacry.407CBB
00407CAD   6A 00           push 0
00407CAF   6A 00           push 0
00407CB1   56              push esi
```



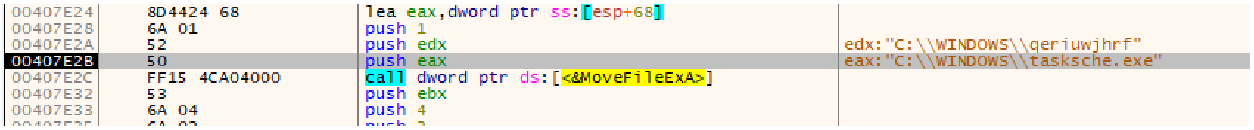
```
00407F1E    90            nop
00407F1F    90            nop
00407F20    E8 1BFDFFFF   call ransomware.wannacry.407C40
00407F25    E8 B6FDFFFF   call ransomware.wannacry.407CE0
00407F2A    33C0          xor eax,eax
00407F2C    C3            ret
00407F2D    90            nop
00407F2E    90            nop
```



```
00407CE0   81EC 60020000   sub esp,260
00407CE6   53              push ebx
00407CE7   55              push ebp
00407CE8   56              push esi
00407CE9   57              push edi
00407CEA   68 B4134300     push ransomware.wannacry.4313B4                 4313B4:L"kernel32.dll"
00407CEF   FF15 64A04000   call dword ptr ds:[<&GetModuleHandleW>]
00407CF5   8BF0            mov esi,eax
00407CF7   33DB            xor ebx,ebx
00407CF9   3BF3            cmp esi,ebx
00407CFB   0F84 07020000   je ransomware.wannacry.407F08
00407D01   8B3D 60A04000   mov edi,dword ptr ds:[<&GetProcAddress>]
00407D07   68 A4134300     push ransomware.wannacry.4313A4                 4313A4:"CreateProcessA"
00407D0C   56              push esi
00407D0D   FFD7            call edi
00407D0F   68 98134300     push ransomware.wannacry.431398                 431398:"CreateFileA"
00407D14   56              push esi
00407D15   A3 78144300     mov dword ptr ds:[431478],eax
00407D1A   FFD7            call edi
00407D1C   68 8C134300     push ransomware.wannacry.43138C                 43138C:"WriteFile"
00407D21   56              push esi
00407D22   A3 58144300     mov dword ptr ds:[431458],eax
00407D27   FFD7            call edi
00407D29   68 80134300     push ransomware.wannacry.431380                 431380:"CloseHandle"
00407D2E   56              push esi
00407D2F   A3 60144300     mov dword ptr ds:[431460],eax
00407D34   FFD7            call edi
00407D36   8B0D 78144300   mov ecx,dword ptr ds:[431478]
00407D3C   A3 4C144300     mov dword ptr ds:[43144C],eax
00407D41   3BCB            cmp ecx,ebx
00407D43   0F84 BF010000   je ransomware.wannacry.407F08
00407D49   391D 58144300   cmp dword ptr ds:[431458],ebx
00407D4F   0F84 B3010000   je ransomware.wannacry.407F08
00407D55   391D 60144300   cmp dword ptr ds:[431460],ebx
00407D5B   0F84 A7010000   je ransomware.wannacry.407F08
00407D61   3BC3            cmp eax,ebx
00407D63   0F84 9F010000   je ransomware.wannacry.407F08
00407D69   68 7C134300     push ransomware.wannacry.43137C
00407D6E   68 27070000     push 727
00407D73   53              push ebx
00407D74   FF15 5CA04000   call dword ptr ds:[<&FindResourceA>]
00407D7A   8BF0            mov esi,eax
```



```
00407DDB   889C24 6C010000   mov byte ptr ss:[esp+16C],bl
00407DE2   F3:AB             rep stosd
00407DE4   8B35 0CA14000     mov esi,dword ptr ds:[<&sprintf>]
00407DEA   68 6C134300       push ransomware.wannacry.43136C    43136C:"tasksche.exe"
00407DEF   66:AB             stosw
00407DF1   AA                stosb
00407DF2   68 64134300       push ransomware.wannacry.431364    431364:"WINDOWS"
00407DF7   8D4424 70         lea eax,dword ptr ss:[esp+70]      [esp+70]:"che.exe"
00407DFB   68 58134300       push ransomware.wannacry.431358    431358:"C:\\%s\\%s"
00407E00   50                push eax
00407E01   FFD6              call esi
00407E03   83C4 10           add esp,10
00407E06   8D8C24 6C010000   lea ecx,dword ptr ss:[esp+16C]
00407E0D   68 64134300       push ransomware.wannacry.431364    431364:"WINDOWS"
00407E12   68 44134300       push ransomware.wannacry.431344    431344:"C:\\%s\\qeriuwjhrf"
00407E17   51                push ecx
```

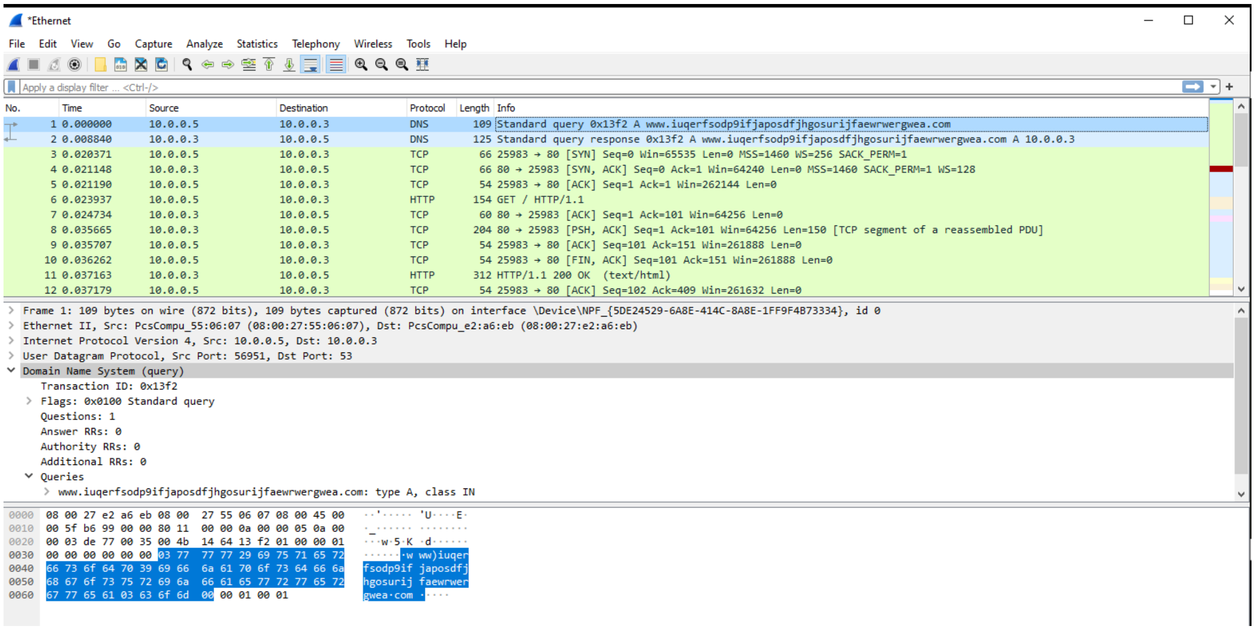


```
00407E24   8D4424 68       lea eax,dword ptr ss:[esp+68]
00407E28   6A 01           push 1
00407E2A   52              push edx                          edx:"C:\\WINDOWS\\qeriuwjhrf"
00407E2B   50              push eax                          eax:"C:\\WINDOWS\\tasksche.exe"
00407E2C   FF15 4CA04000   call dword ptr ds:[<&MoveFileExA>]
00407E32   53              push ebx
00407E33   6A 04           push 4
```

Indicators of Compromise

Network Indicators

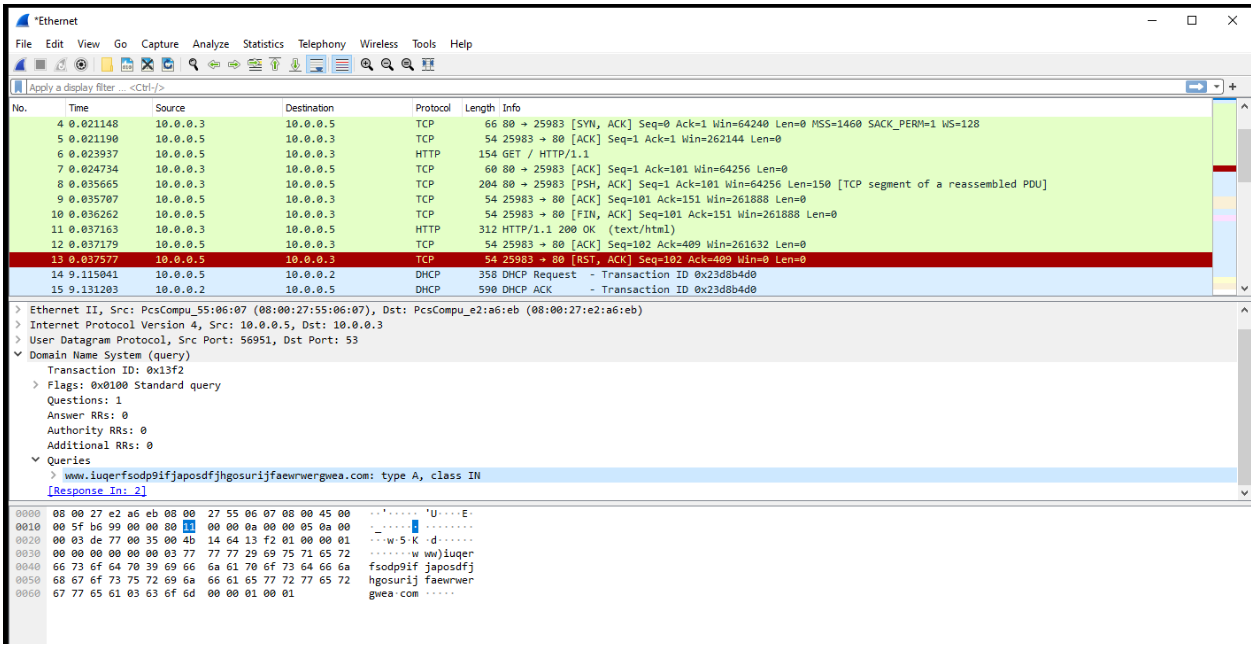
Wireshark analysis


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source    Destination Protocol Length Info
   1 0.000000  10.0.0.5  10.0.0.3    DNS       109 Standard query 0x13f2 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
   2 0.008840  10.0.0.3  10.0.0.5    DNS       125 Standard query response 0x13f2 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 10.0.0.3
   3 0.020371  10.0.0.5  10.0.0.3    TCP        66 25983 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   4 0.021148  10.0.0.3  10.0.0.5    TCP        66 80 → 25983 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
   5 0.021190  10.0.0.5  10.0.0.3    TCP        54 25983 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   6 0.023937  10.0.0.5  10.0.0.3    HTTP      154 GET / HTTP/1.1
   7 0.024734  10.0.0.3  10.0.0.5    TCP        60 80 → 25983 [ACK] Seq=1 Ack=101 Win=64256 Len=0
   8 0.035665  10.0.0.3  10.0.0.5    TCP       204 80 → 25983 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=150 [TCP segment of a reassembled PDU]
   9 0.035707  10.0.0.5  10.0.0.3    TCP        54 25983 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
  10 0.036262  10.0.0.5  10.0.0.3    TCP        54 25983 → 80 [FIN, ACK] Seq=101 Ack=151 Win=261888 Len=0
  11 0.037163  10.0.0.3  10.0.0.5    HTTP      312 HTTP/1.1 200 OK  (text/html)
  12 0.037179  10.0.0.5  10.0.0.3    TCP        54 25983 → 80 [ACK] Seq=102 Ack=409 Win=261632 Len=0
```

```
> Frame 1: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface \Device\NPF_{5DE24529-6A8E-414C-8A8E-1FF9F4B73334}, id 0
> Ethernet II, Src: PcsCompu_55:06:07 (08:00:27:55:06:07), Dst: PcsCompu_e2:a6:eb (08:00:27:e2:a6:eb)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.3
> User Datagram Protocol, Src Port: 56951, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x13f2
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN
```

```
0000  08 00 27 e2 a6 eb 08 00  27 55 06 07 08 00 45 00   ··'····· 'U····E·
0010  00 5f b6 99 00 00 80 11  00 00 0a 00 00 05 0a 00   ·_······ ········
0020  00 03 de 77 00 35 00 4b  14 64 13 f2 01 00 00 01   ···w·5·K ·d······
0030  00 00 00 00 00 00 03 77  77 77 29 69 75 71 65 72   ······w ww)iuqer
0040  66 73 6f 64 70 39 69 66  6a 61 70 6f 73 64 66 6a   fsodp9if japosdfj
0050  68 67 6f 73 75 72 69 6a  66 61 65 77 72 77 65 72   hgosurij faewrwer
0060  67 77 65 61 03 63 6f 6d  00 00 01 00 01            gwea·com ·····
```



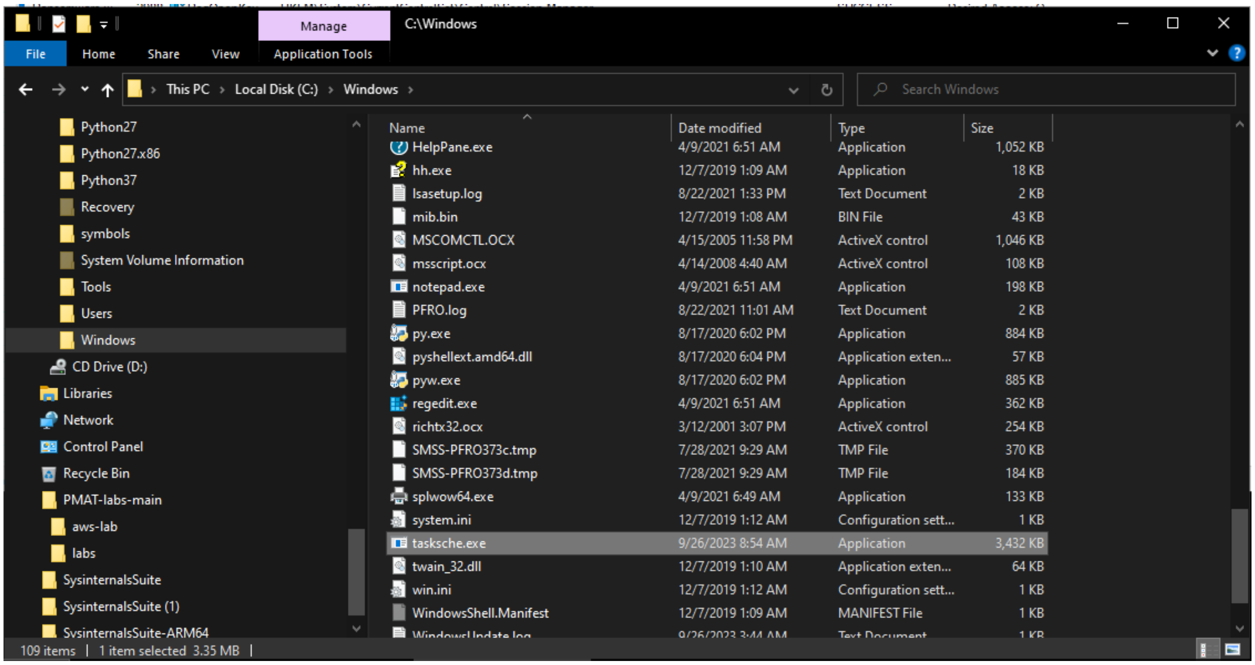
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source      Destination  Protocol Length Info
    4 0.021148   10.0.0.3    10.0.0.5     TCP        66 80 → 25983 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
    5 0.021190   10.0.0.5    10.0.0.3     TCP        54 25983 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
    6 0.023937   10.0.0.5    10.0.0.3     HTTP      154 GET / HTTP/1.1
    7 0.024734   10.0.0.3    10.0.0.5     TCP        60 80 → 25983 [ACK] Seq=1 Ack=101 Win=64256 Len=0
    8 0.035665   10.0.0.3    10.0.0.5     TCP       204 80 → 25983 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=150 [TCP segment of a reassembled PDU]
    9 0.035707   10.0.0.5    10.0.0.3     TCP        54 25983 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
   10 0.036262   10.0.0.5    10.0.0.3     TCP        54 25983 → 80 [FIN, ACK] Seq=101 Ack=151 Win=261888 Len=0
   11 0.037163   10.0.0.3    10.0.0.5     HTTP      312 HTTP/1.1 200 OK  (text/html)
   12 0.037179   10.0.0.5    10.0.0.3     TCP        54 25983 → 80 [ACK] Seq=102 Ack=409 Win=261632 Len=0
   13 0.037577   10.0.0.5    10.0.0.3     TCP        54 25983 → 80 [RST, ACK] Seq=102 Ack=409 Win=0 Len=0
   14 9.115041   10.0.0.5    10.0.0.2     DHCP      358 DHCP Request  - Transaction ID 0x23d8b4d0
   15 9.131203   10.0.0.2    10.0.0.5     DHCP      590 DHCP ACK      - Transaction ID 0x23d8b4d0
```

```
> Ethernet II, Src: PcsCompu_55:06:07 (08:00:27:55:06:07), Dst: PcsCompu_e2:a6:eb (08:00:27:e2:a6:eb)
> Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.3
> User Datagram Protocol, Src Port: 56951, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x13f2
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN
    [Response In: 2]
```

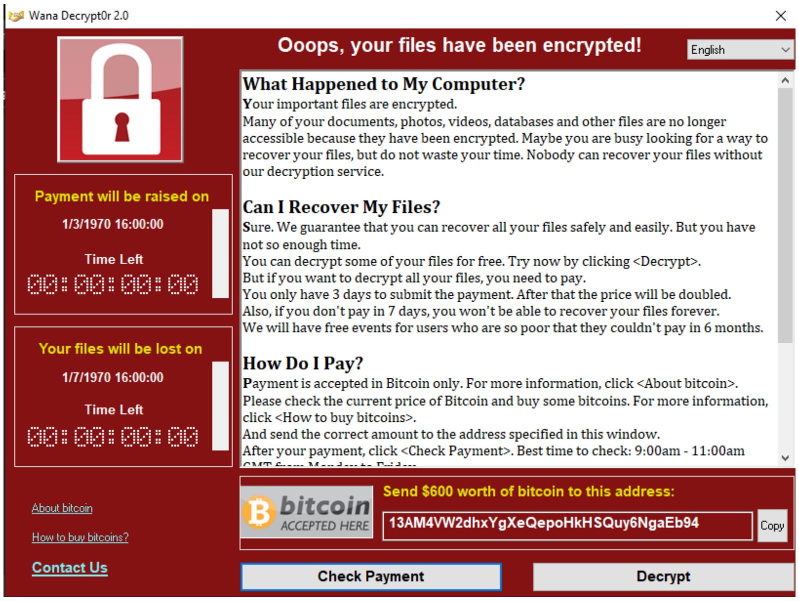
```
0000  08 00 27 e2 a6 eb 08 00  27 55 06 07 08 00 45 00   ··'····· 'U····E·
0010  00 5f b6 99 00 00 80 11  00 00 0a 00 00 05 0a 00   ·_······ ········
0020  00 03 de 77 00 35 00 4b  14 64 13 f2 01 00 00 01   ···w·5·K ·d······
0030  00 00 00 00 00 00 03 77  77 77 29 69 75 71 65 72   ·······w ww)iuqer
0040  66 73 6f 64 70 39 69 66  6a 61 70 6f 73 64 66 6a   fsodp9if japosdfj
0050  68 67 6f 73 75 72 69 6a  66 61 65 77 72 77 65 72   hgosurij faewrwer
0060  67 77 65 61 03 63 6f 6d  00 00 01 00 01            gwea·com ·····
```

Host-based Indicators



Name	Date modified	Type	Size
HelpPane.exe	4/9/2021 6:51 AM	Application	1,052 KB
hh.exe	12/7/2019 1:09 AM	Application	18 KB
lsasetup.log	8/22/2021 1:33 PM	Text Document	2 KB
mib.bin	12/7/2019 1:08 AM	BIN File	43 KB
MSCOMCTL.OCX	4/15/2005 11:58 PM	ActiveX control	1,046 KB
msscript.ocx	4/14/2008 4:40 AM	ActiveX control	108 KB
notepad.exe	4/9/2021 6:51 AM	Application	198 KB
PFRO.log	8/22/2021 11:01 AM	Text Document	2 KB
py.exe	8/17/2020 6:02 PM	Application	884 KB
pyshellext.amd64.dll	8/17/2020 6:04 PM	Application exten...	57 KB
pyw.exe	8/17/2020 6:02 PM	Application	885 KB
regedit.exe	4/9/2021 6:51 AM	Application	362 KB
richtx32.ocx	3/12/2001 3:07 PM	ActiveX control	254 KB
SMSS-PFRO373c.tmp	7/28/2021 9:29 AM	TMP File	370 KB
SMSS-PFRO373d.tmp	7/28/2021 9:29 AM	TMP File	184 KB
splwow64.exe	4/9/2021 6:49 AM	Application	133 KB
system.ini	12/7/2019 1:12 AM	Configuration sett...	1 KB
tasksche.exe	9/26/2023 8:54 AM	Application	3,432 KB
twain_32.dll	12/7/2019 1:10 AM	Application exten...	64 KB
win.ini	12/7/2019 1:12 AM	Configuration sett...	1 KB
WindowsShell.Manifest	12/7/2019 1:09 AM	MANIFEST File	1 KB
WindowsUpdate.log	9/26/2023 3:44 AM	Text Document	1 KB

109 items | 1 item selected 3.35 MB |



Ooops, your files have been encrypted!

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.

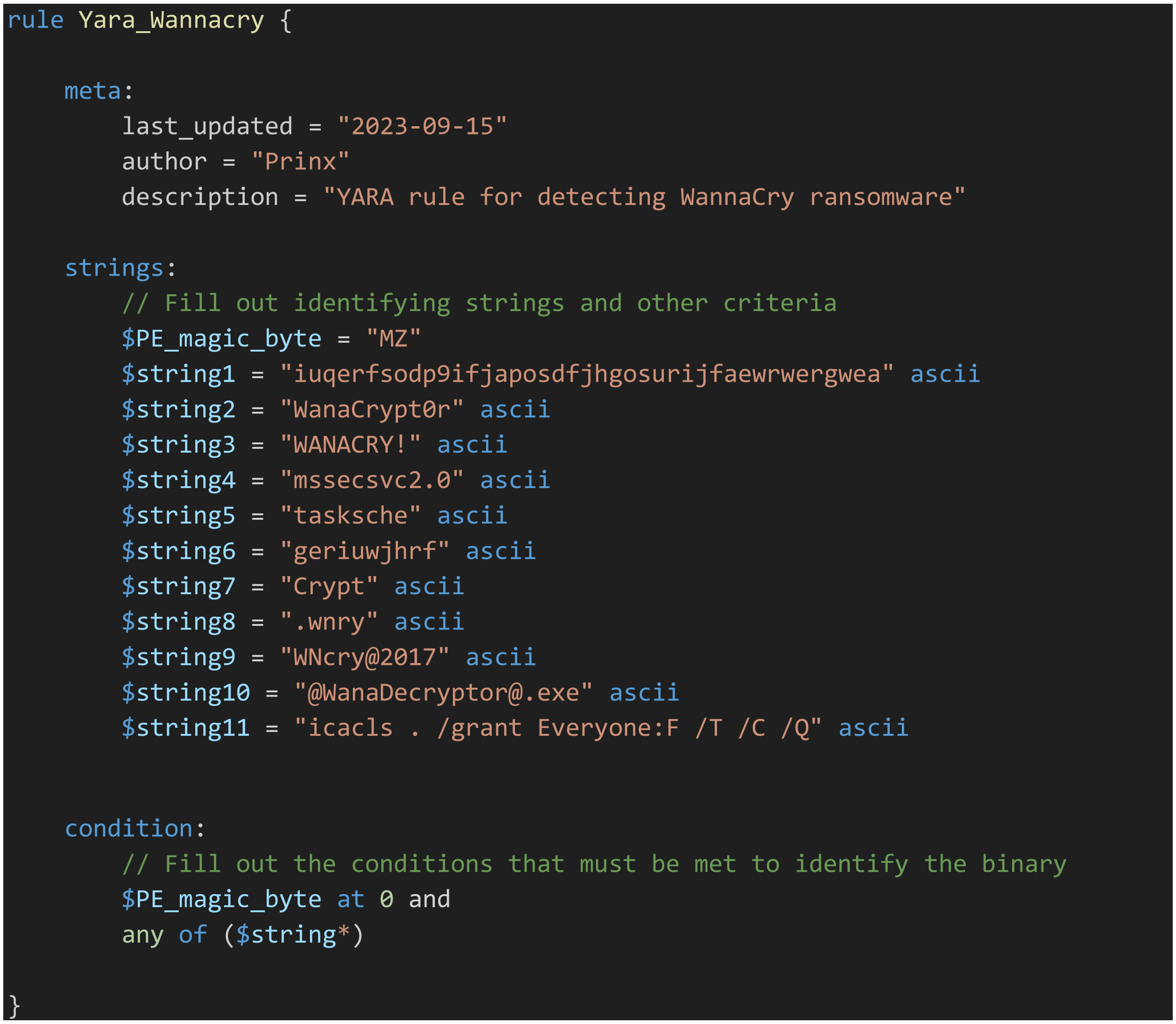
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Appendices

A. Yara Rules

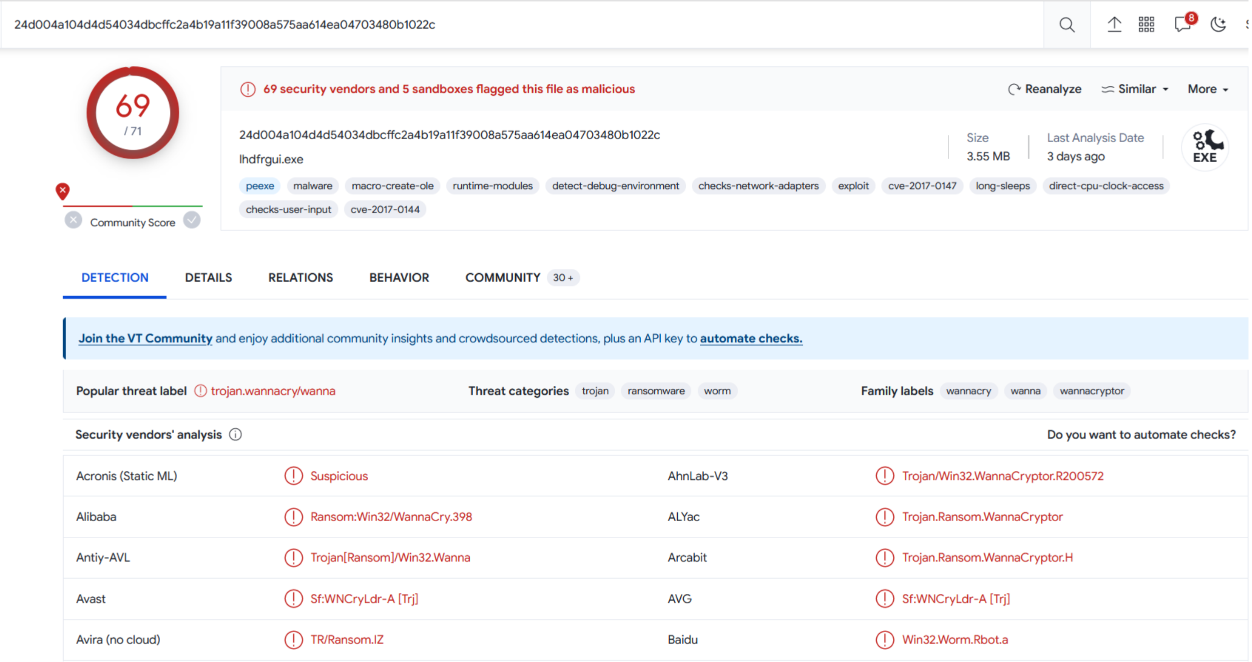


```
rule Yara_Wannacry {

    meta:
        last_updated = "2023-09-15"
        author = "Prinx"
        description = "YARA rule for detecting WannaCry ransomware"

    strings:
        // Fill out identifying strings and other criteria
        $PE_magic_byte = "MZ"
        $string1 = "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea" ascii
        $string2 = "WanaCrypt0r" ascii
        $string3 = "WANACRY!" ascii
        $string4 = "mssecsvc2.0" ascii
        $string5 = "tasksche" ascii
        $string6 = "geriuwjhrf" ascii
        $string7 = "Crypt" ascii
        $string8 = ".wnry" ascii
        $string9 = "WNcry@2017" ascii
        $string10 = "@WanaDecryptor@.exe" ascii
        $string11 = "icacls . /grant Everyone:F /T /C /Q" ascii


    condition:
        // Fill out the conditions that must be met to identify the binary
        $PE_magic_byte at 0 and
        any of ($string*)

}
```

B. Callback URLs

Domain	Port
hxxp[://]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[dot]com	80

C. VirusTotal



24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

69 security vendors and 5 sandboxes flagged this file as malicious

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

lhdfrgui.exe

Size 3.55 MB

Last Analysis Date 3 days ago

EXE

peexe malware macro-create-ole runtime-modules detect-debug-environment checks-network-adapters exploit cve-2017-0147 long-sleeps direct-cpu-clock-access checks-user-input cve-2017-0144

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.wannacry/wanna

Threat categories trojan ransomware worm

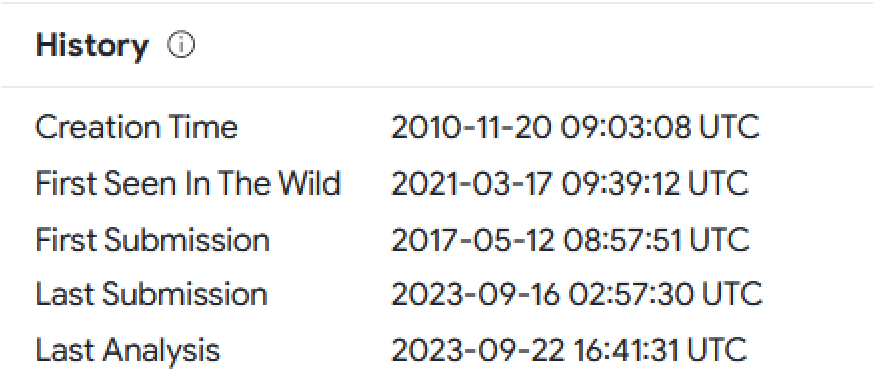
Family labels wannacry wanna wannacryptor

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.WannaCryptor.R200572
Alibaba	Ransom:Win32/WannaCry.398	ALYac	Trojan.Ransom.WannaCryptor
Antiy-AVL	Trojan[Ransom]/Win32.Wanna	Arcabit	Trojan.Ransom.WannaCryptor.H
Avast	Sf:WNCryLdr-A [Trj]	AVG	Sf:WNCryLdr-A [Trj]
Avira (no cloud)	TR/Ransom.IZ	Baidu	Win32.Worm.Rbot.a

VirusTotal



History

Creation Time	2010-11-20 09:03:08 UTC
First Seen In The Wild	2021-03-17 09:39:12 UTC
First Submission	2017-05-12 08:57:51 UTC
Last Submission	2023-09-16 02:57:30 UTC
Last Analysis	2023-09-22 16:41:31 UTC

History of WannaCry virus