



# Malware Analysis Report

---

## WannaCry

Jan 2023 | Alessio Ragazzi



# Table of Contents

<b>Introduction</b>	<b>2</b>
<b>Executive Summary</b>	<b>3</b>
<b>High-Level Technical Summary</b>	<b>5</b>
<b>Execution Process of WannaCry</b>	<b>5</b>
<b>Malware Composition</b>	<b>6</b>
<b>Analysis Environment</b>	<b>7</b>
<b>Basic Static Analysis</b>	<b>8</b>
<b>Basic Dynamic Analysis</b>	<b>11</b>
<b>Advanced Static Analysis</b>	<b>18</b>
<b>Advanced Dynamic Analysis</b>	<b>21</b>
<b>Indicators of Compromise</b>	<b>23</b>
Host-based network Indicators	23
Host-based Indicators	23
Network Indicators	27
<b>YARA rules &amp; Signatures</b>	<b>28</b>
<b>Appendices</b>	<b>29</b>
A. Yara Rules	29
B. Callback URLs	29
C. Decompiled Code Snippets	29



# Introduction

The following report is not meant to be exhaustive. Extensive research has been conducted on WannaCry by teams of experts from all over the world. I've reserved a section at the end of this text to mention some of the best analyses that can be found online today.

My ultimate goal was to demonstrate the methodology acquired upon completion of the TCM Security Practical Malware Analysis & Triage.

Prior to attempting the analysis, I had a very superficial knowledge of the malware. I was well aware of the devastating effects and its crypto-ransom capabilities.

I performed basic and advanced static and dynamic analysis of the sample, including disassembly and debugging limited to the initial dropper. I've collected host-based and network-based IoCs, and I have revealed the malware's major capabilities.

I was able to observe, analyze and report the *KillSwitch* mechanism, the *EternalBlue* exploit, and the role of *tasksche.exe*.

I wasn't able to observe directly some of the components. as well as part of the behavior, such as: Backdoor delivery, Persistence mechanism, and C2 communication.

The following report will only contain the result of my personal analysis of the sample. For further information, please refer to the resources at the end of the text.



## Executive Summary

SHA256 hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
-------------	--

SHA1 hash	3b669778698972c402f7c149fc844d0ddb3a00e8
-----------	--

MD5 hash	d724d8cc6420f06e8a48752f0da11c66
----------	----------------------------------

WannaCry is a crypto-ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computer (32bit/64bit), it encrypts files on the PC's hard drive, making them impossible for users to access, demanding a fee of either \$300 or \$600 worth of bitcoins to an address specified in the instructions displayed after infection.

Utilizing one of the core components of the Microsoft Operating System and a known exploit, it's able to propagate through the network. An estimated of around 230.000 computers being infected have been confirmed up-to-date.

Symptoms of infection include encrypted files, a custom background, a directory containing multiple files dropped in the C:\Windows\ProgramData, and the highly recognizable *Wana Decrypt0r 2.0* program window, containing a timer and information on how to proceed.

Despite security patches and decryption keys having been released, WannaCry is still active. In-depth research and extensive documentation can be found today in this regard.

YARA signature rules are attached in Appendix A, along with the malware's IoCs.



## High-Level Technical Summary

The WannaCry ransomware is composed of multiple components. An initial dropper contains the encrypter, named *tasksche.exe*, as an embedded resource; the encrypter component contains a decryption application called *Wana Decrypt0r 2.0*, a password-protected zip containing a copy of Tor, and several individual files with configuration information and encryption keys.

### First phase - The “KillSwitch”

Once the payload has been delivered, the dropper performs the initial function. The so-called, KillSwitch. The mechanism by which it can terminate its execution if it's able to establish a connection to a hard-coded domain.

The domain requested by the initial dropper is

[http://www\[.\]jiuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\[.\]com](http://www[.]jiuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com).

### Second phase - The EternalBlue exploit

If the connection fails, the dropper attempts to create a service named “mssecsvc2.0” with the DisplayName “Microsoft Security Center (2.0) Service”. WannaCry utilizes windows services to spread, exploiting a vulnerability in the SMB V1.0 protocol via port 445.

### Main phase - *Tasksche.exe*

The dropper then extracts the encrypter binary from its resource R/1831, writes it to the hardcoded filename %WinDir%\tasksche.exe, and then executes it. As shown in the static and dynamic analysis section, *tasksche.exe* is responsible for the encryption of the files in the system, and for launching the *WanaDecrypt0r 2.0* program. The encrypter doesn't encrypt executable files such as .exe and .dll to avoid system interruption.

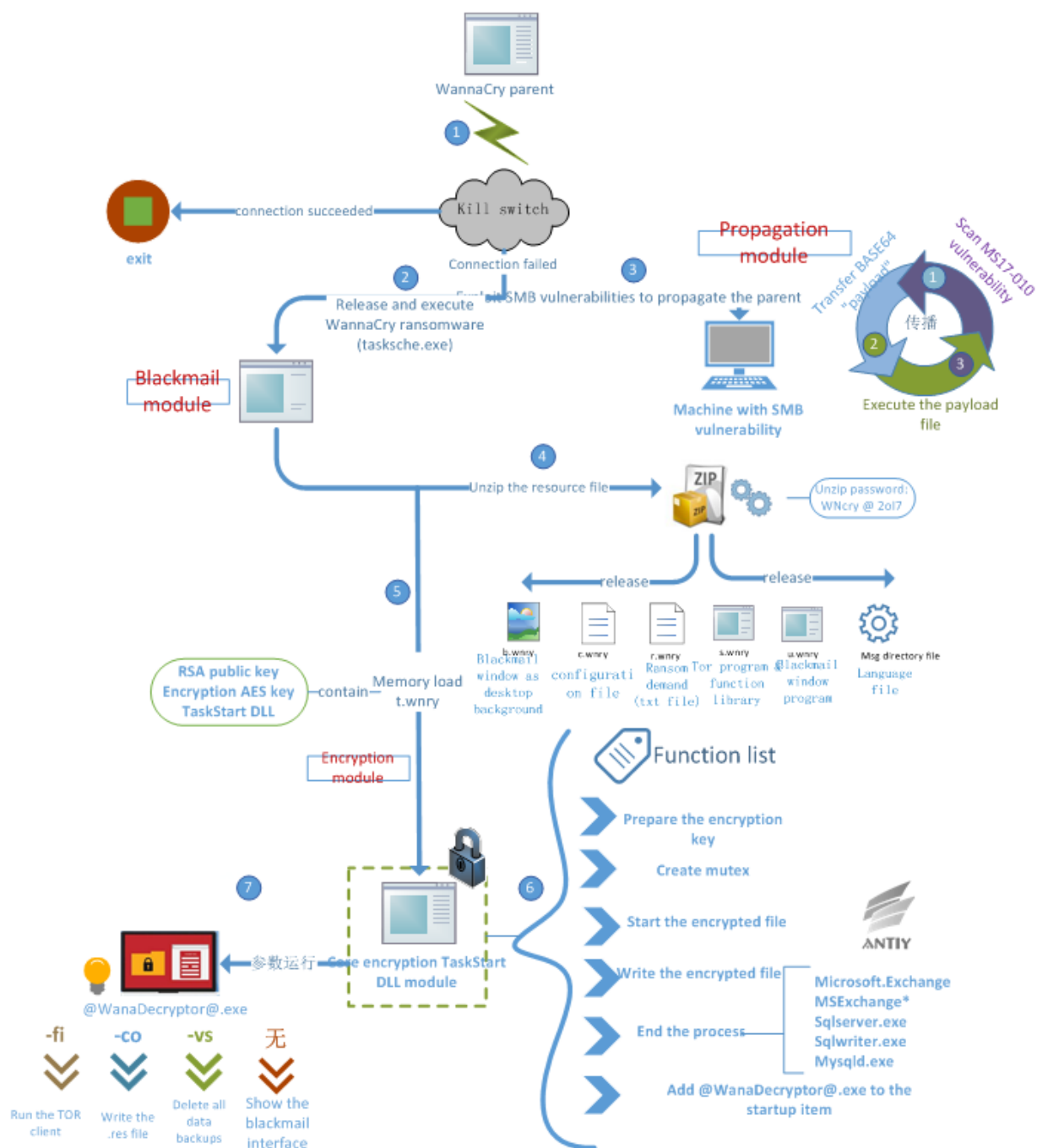
### Double Pulsar, C2 communication and Persistence mechanism

WannaCry performs further actions, such as delivering the *Double Pulsar* backdoor after infecting a new host, establishing persistence by creating a new Registry key, and contacting a C2 server via the TOR service.

Unfortunately, I wasn't able to detect these actions, and therefore I haven't reported the related documentation. Interestingly, the malware's authors have chosen to implement very few Anti-analysis techniques, allowing disassembly and debugging.



## Execution Process of WannaCry





## Malware Composition

The following components were analyzed or observed by me directly:

File Name	SHA256 Hash
<b>mssecsvc.exe</b>	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
<b>tasksche.exe</b>	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
<b>taskse.exe</b>	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
<b>@WanaDecryptor@.exe</b>	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

In addition, the following components can also be observed:

File Name	Description
<b>taskdl.exe</b>	Binary used for deleting temporary files
<b>r.wnry</b>	Shows the ransom message
<b>s.wnry</b>	Contains Tor executable
<b>msg/</b>	Contain Language files
<b>f.wnry</b>	N/A
<b>b.wnry</b>	N/A



## Analysis Environment

Host	Description	IP address	DNS	Use
<b>VM1</b>	Windows 10 - Flare VM distribution	10.0.0.3	10.0.0.4	Main Analysis Environment (Infected Host)
<b>VM2</b>	Linux - Remnux distribution	10.0.0.4	N.A.	Internet simulation and Packet Capture

Host	Tool	Description
<b>VM1</b>	Floss	Uses advanced static analysis techniques to automatically deobfuscate strings from malware binaries.
	Pestudio	Spots artifacts of executable files.
	PEview	Views the structure and content of 32-bit Portable Executable (PE) and Component Object File Format (COFF) files.
	Cutter	Disassemble.r
	Capa	Performs reverse engineering to figure out what a program does. It includes different frameworks, including MITRE ATT&CK.
	X64dbg	An open-source x64/x32 debugger for windows.
	TCPview	Shows detailed listings of all TCP and UDP endpoints on the system.
	Process Hacker	Monitors system resources, debug software, and detect malware.
	Procmon	Advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.
<b>VM2</b>	InetSim	Internet service simulation suite.
	Wireshark	Packet capture.





## Basic Static Analysis

WannaCry binary lab's name: Ransomware.wannacry.exe

Before attempting the detonation, I used floss to try to pull some interesting strings out of the binary. I made use of *floss* for this purpose. It is possible to observe numerous APIs, .exe, a domain, reference to Windows service, and system paths.

<pre>*Untitled - Notepad File Edit Format View Help CreateServiceA OpenSCManagerA SetServiceStatus ChangeServiceConfig2A RegisterServiceCtrlHandlerA StartServiceCtrlDispatcherA OpenServiceA InternetCloseHandle InternetOpenUrlA InternetOpenA CloseHandle WriteFile CreateFileA SetCurrentDirectoryA GetCurrentDirectoryA RegCloseKey RegQueryValueExA RegSetValueExA RegCreateKeyW</pre>	<pre>*Untitled - Notepad File Edit Format View Help InitializeCriticalSection LeaveCriticalSection EnterCriticalSection InterlockedDecrement CloseHandle TerminateThread GetCurrentThreadId GetCurrentThread ReadFile CreateFileA MoveFileExA FindResourceA GetProcAddress GetModuleHandleW ExitProcess GetModuleFileNameA CryptAcquireContextA CryptGenRandom</pre>	<pre>*Untitled - Notepad File Edit Format View Help RegCreateKeyW CryptReleaseContext WININET.dll MSVCRT.dll C:\%s\%s !This program cannot be run in DOS mode. /4%D/4%D/4%D4 D,4%D/4%D D.4%DRich/4%D  mssecsvc2.0 Microsoft Security Center (2.0) Service %s -m security C:\%s\qeriuwjhrf C:\%s\%s tasksche.exe cmd.exe /c "%s" taskdl.exe taskse.exe mssecsvc.exe</pre>
--	--	--

```
tasksche.exe
cmd.exe /c "%s"
taskdl.exe
taskse.exe
mssecsvc.exe
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
icaccls . /grant Everyone:F /T /C /Q
attrib +h .
```

From the first two snapshots, we can see some interesting APIs:

- ReadFile, CreateFile, WriteFile (Note that these APIs are common in non-malicious binaries too)
- CryptoGenRandom, CryptReleasContext
- OpenSCManagerA
- OpenServiceA, SetServiceStatus, StartServiceCtrlDispatcherA
- RegSetValueA, RegCreateKeyW
- InternetOpenA, InternetOpenUrlA



We can see the following executable: `tasksche.exe`, `cmd.exe`, `taskdl.exe`, `taskse.exe`, `mssecsvc.exe`

We can also see other strings of interest such as a domain, a system path using token values, more references to windows services, and the string containing *icacils*.

I have run the tool *capa* to see if there's any match in a attempt to understand the malware behavior prior the detonation.

We can start to correlate this output with the strings that we just pulled. We will expect **service execution** (including Persistence), **reconnaissance activity**, **C2 and HTTP communication**, **file creation**, **cryptography** (fig. 3), and **embedded executables** (fig. 2).

```
C:\Users\Gallianico\Desktop
λ capa Ransomware.wannacry.exe
loading : 100% | 485/485 [00:01<00:00, 265.27 rules/s]
matching: 100% | 87/87 [00:08<00:00, 10.71 functions/s]

+-----+-----+
| md5      | db349b97c37d22f5ea1d1841e3c89eb4 |
| sha1     | e889544aff85ffaf8b0d0da705105dee7c97fe26 |
| sha256   | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c |
| path     | Ransomware.wannacry.exe |
+-----+-----+

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

+-----+-----+
| MBC Objective | MBC Behavior |
+-----+-----+
| ANTI-BEHAVIORAL ANALYSIS | Debugger Detection::Timing/Delay Check GetTickCount [B0001.032] |
|                           | Debugger Detection::Timing/Delay Check QueryPerformanceCounter [B0001.033] |
|                           | Execution Guardrails::Runs as Service [E1480.m07] |
| ANTI-STATIC ANALYSIS    | Disassembler Evasion::Argument Obfuscation [B0012.001] |
| COMMAND AND CONTROL     | C2 Communication::Receive Data [B0030.002] |
|                           | C2 Communication::Send Data [B0030.001] |
| COMMUNICATION           | HTTP Communication::Create Request [C0002.012] |
|                           | HTTP Communication::Open URL [C0002.004] |
+-----+-----+
```

Fig. 1 Capa output



contain an embedded PE file	executable/subfile/pe
get file size	host-interaction/file-system/meta
move file	host-interaction/file-system/move
read file	host-interaction/file-system/read
get number of processors	host-interaction/hardware/cpu
get networking interfaces	host-interaction/network/interface
terminate process	host-interaction/process/terminate
run as service	host-interaction/service
create service	host-interaction/service/create
modify service	host-interaction/service/modify
start service	host-interaction/service/start
create thread (4 matches)	host-interaction/thread/create
terminate thread	host-interaction/thread/terminate
link function at runtime	linking/runtime-linking
linked against ZLIB	linking/static/zlib
inspect section memory permissions	load-code/pe
parse PE exports	load-code/pe
parse PE header	load-code/pe
persist via Windows service	persistence/service

Fig.2 Capa output

Socket Communication::Create TCP Socket [C0001.011]	
Socket Communication::Create UDP Socket [C0001.010]	
Socket Communication::Get Socket Status [C0001.012]	
Socket Communication::Initialize Winsock Library [C0001.009]	
Socket Communication::Receive Data [C0001.006]	
Socket Communication::Send Data [C0001.007]	
Socket Communication::Set Socket Config [C0001.001]	
Socket Communication::TCP Client [C0001.008]	
Generate Pseudo-random Sequence::Use API [C0021.003]	
Compression Library [C0060]	
Install Additional Program [B0023]	
Read File [C0051]	
Create Thread [C0038]	
Terminate Process [C0018]	
Terminate Thread [C0039]	

CAPABILITY	NAMESPACE
check for time delay via GetTickCount	anti-analysis/anti-debugging/debugger-detection
check for time delay via QueryPerformanceCounter	anti-analysis/anti-debugging/debugger-detection
contain obfuscated stackstrings	anti-analysis/obfuscation/string/stackstring
receive data (5 matches)	communication
send data (5 matches)	communication
connect to URL	communication/http/client
get socket status	communication/socket
initialize Winsock library	communication/socket
set socket configuration	communication/socket
create UDP socket (4 matches)	communication/socket/udp/send
act as TCP client	communication/tcp/client
generate random numbers via WinAPI	data-manipulation/prng
contain a resource (.rsrc) section	executable/pe/section/rsrc
extract resource via kernel32 functions	executable/resource
contain an embedded PE file	executable/subfile/pe

Fig.3 Capa output



I've opened the file making use of *PEview* and *PEstudio* to try to grab some artifacts, understand the architecture, observe blacklisted strings and imports. *PEstudio* confirms that we are dealing with a **32bit executable** (Fig. 4). We can also see the **original filename** (Fig. 5), and the presence of the **Rich header** (Fig. 4).

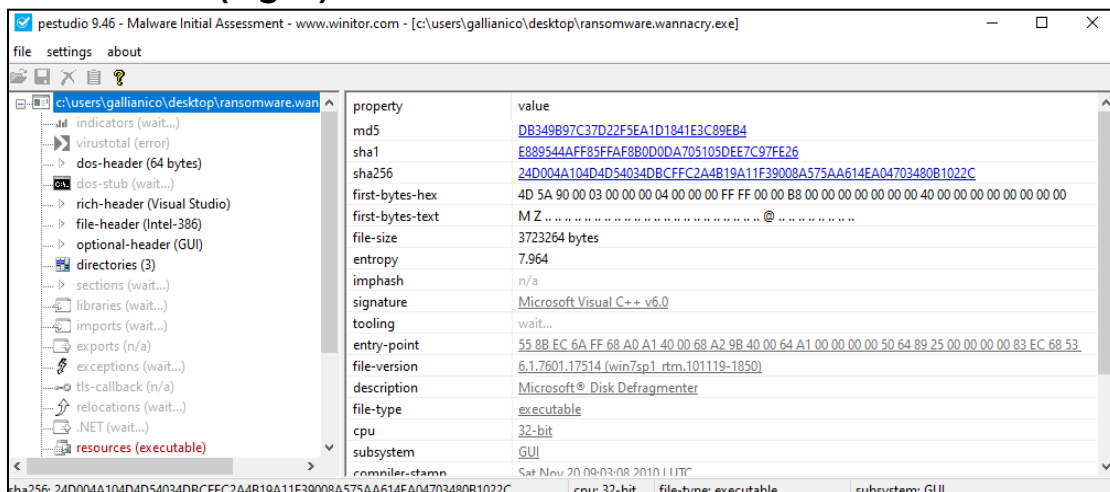


Fig. 4 PEStudio output

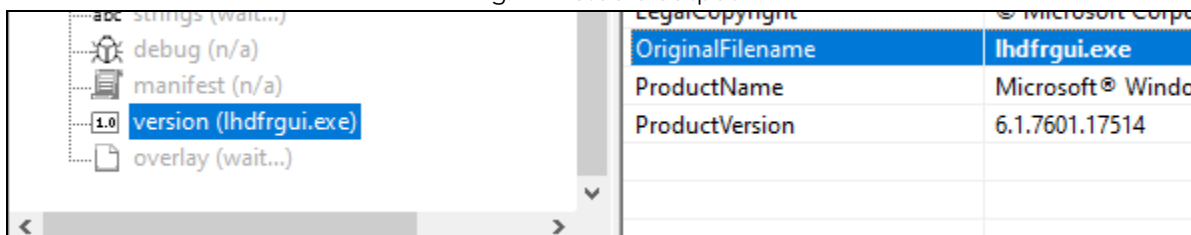


Fig. 5 PEStudio output

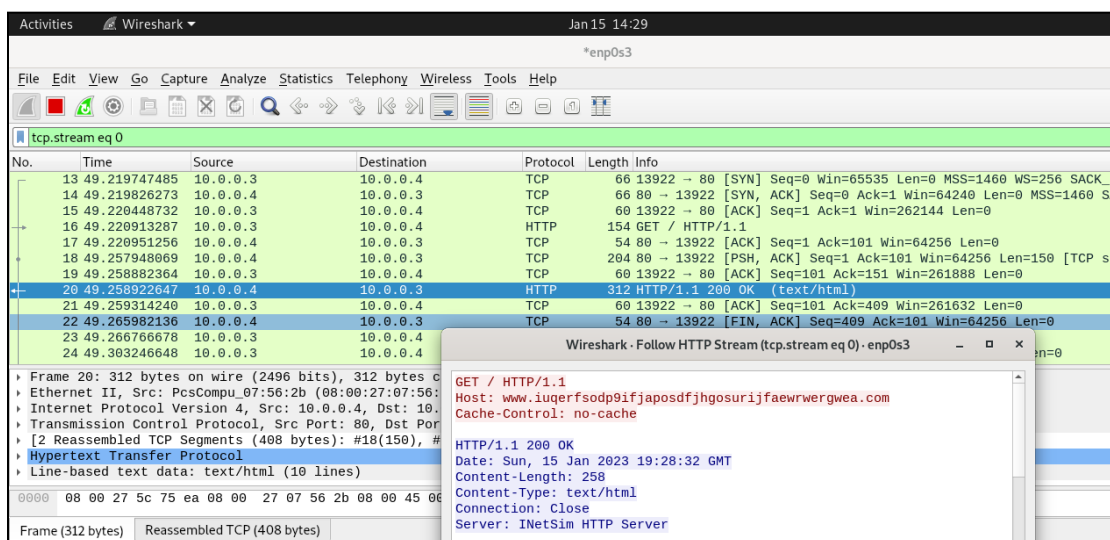
## Basic Dynamic Analysis

### First detonation - Symptoms observation

VM1 : No tools or application running

VM2: Internet Simulation service running - Wireshark running

No symptoms were observed. If we check the packet capture, we can see a DNS request for a type A domain, and the subsequently HTTP/TCP connection established (IoC 1). I'll come back to the *KillSwitch* later during disassembly and debugging.



IoC 1. Wireshark packet capture

## Second detonation - Symptoms observation

**VM1: No tools or application running**

**VM2: Internet Simulation service NOT running**

If we terminate the internet simulation activity on VM2 and we detonate the malware one more time, we can see the first symptoms. The encrypter is deployed and it encrypts the files on the system, appending the .WCRY extension, except the .exe and .dll binaries that will remain unchanged and functional. We can see the @WanaDecrypt0r2.0@ program appearing on the desktop (IoC 2), a custom background image taking the place of our original background, and the notorious window popping up with the instructions to follow if we wish our files to be decrypted.



IoC 2. WanaDecrypt0r window appearing on desktop



Lucky for us, we won't have to pay any ransom at this time! At this point I've brought back the virtual machines to a clean state for another detonation, deploying more tool for basic dynamic analysis.

### Third detonation - Analysis

VM1 : Procmon, Process Hacker, TCPview

VM2: Internet Simulation service not running

As shown in the picture below, we can see that the first indicators that take our attention are the attempted TCP connections on remote port **445** (Bottom-left - IoC 3), and the new process called **tasksche.exe** (Right - IoC 3) taking the place of our original binary's name (Ransomware.wannacry.exe) in the live process tree.

As we'll see later during the disassembly phase, the malware is searching available hosts on the network via open **SMB port 445**. We'll also see in what moment the dropper will release **tasksche.exe**

The screenshot displays three windows from Sysinternals:

- Process Monitor:** Shows a list of events. The 'Process Name' column lists 'Ransomware.wannacry.exe'. The 'Operation' column shows 'ReadFile' and 'RegOpenKey'. The 'Path' column shows 'C:\Windows\System32\thumbcache.dll' and 'HKLM\SOFTWARE\Microsoft\Internet...'. The 'Result' column shows 'SUCCESS' and 'NAME NOT FOUND Length: 90'.
- Process Hacker:** Shows a list of processes. The 'Name' column lists 'VBoxTray.exe', 'msedge.exe', 'notepad.exe', 'Procmon.exe', 'ProcessHacker.exe', 'tcpview.exe', and 'tasksche.exe'. The 'PID' column shows values like 3780, 3808, 4004, 3608, 3744, 3772, 3676, 2144, 1392, 3164, 1464, 2368, and 3160. The 'CPU' column shows values like 0.05, 0.07, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, 41.20, 3.24, 0.74, and 22.87. The 'I/O total' column shows values like 28 B/s, 27.64 MB, 1.98 MB, 16.52 MB, 9.82 MB, 7.5 MB, 3.7 MB, 2.53 MB, 6.11 MB, 106.04 MB, 14.39 MB, 6.93 MB, and 110.77 kB/s. The 'Private b...' column shows values like 2.46 MB, 27.64 MB, 1.98 MB, 16.52 MB, 9.82 MB, 7.5 MB, 3.7 MB, 2.53 MB, 6.11 MB, 106.04 MB, 14.39 MB, 6.93 MB, and 15.96 MB. The 'User name' column shows 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', 'DESKTOP-V...', and 'NT AUTHOF'.
- TCPView:** Shows a list of connections. The 'Process Name' column lists 'Ransomware.wannacry.exe'. The 'Process ID' column shows values like 4716. The 'Protocol' column shows 'TCP'. The 'State' column shows 'Syn Sent'. The 'Local Address' column shows '169.254.72.102'. The 'Local Port' column shows values like 44300, 44301, 44302, 44303, 44304, 44302, 44168, and 44169. The 'Remote Address' column shows '169.254.84.10', '169.254.85.10', '169.254.86.10', '169.254.87.10', '169.254.88.10', '169.254.89.10', '169.254.80.10', and '169.254.81.10'. The 'Remote Port' column shows values like 445, 445, 445, 445, 445, 445, 445, and 445.

IoC 3. A snapshot at the initial detonation. From Top-left to right: Procmon, Process Hacker, TCPview





If we take a look at **procmon** (IoC 4), we can see the file creation of **tasksche.exe**, by our original dropper, **Ransomware.wannacry.exe**. For this view, I've applied 3 sets of filters:

- Process name is **Ransomware.wannacry.exe**
- Operation is **Create file**
- Path contains **.exe**

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\Prefetch\RANSOMWARE...	NAME NOT FOUND	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	NAME NOT FOUND	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	2812	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: G...

IoC 4. A snapshot of procmon after initial detonation

If we change our set of filters, we can see further activity coming from **tasksche.exe**. The new set of filters is:

- Process name is **tasksche.exe**
- Operation is **Create file**
- Path contains **.exe**

Two new files have been created: **@WanaDecryptor2.0@.exe** and **taskdl.exe** (IoC 5). We can also see another executable been spawned, **cmd.exe** (IoC 6), and a new directory with an obfuscated name under the **/ProgramData** directory (IoC 7).



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:33:...	tasksche.exe	3688	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-348996749...	NAME NOT FOUND	Length: 40
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe.lnk	NAME NOT FOUND	Desired Access: G...
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe.lnk	NAME NOT FOUND	Desired Access: G...
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe.lnk	NAME NOT FOUND	Desired Access: G...
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe.lnk	NAME NOT FOUND	Desired Access: G...
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	Desired Access: G...
11:33:...	tasksche.exe	2220	QueryAttributeT...	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	Attributes: ANCI, R...
11:33:...	tasksche.exe	2220	QueryStandardI...	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	AllocationSize: 245...
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	CreationTime: 16/0...
11:33:...	tasksche.exe	2220	QueryStreamInfor...	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	0:::\$DATA
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	CreationTime: 16/0...
11:33:...	tasksche.exe	2220	QueryEaInfor...	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	EaSize: 0
11:33:...	tasksche.exe	2220	CreateFile	C:\@WanaDecryptor@.exe	SUCCESS	Desired Access: G...
11:33:...	tasksche.exe	2220	QueryAttribute...	C:\@WanaDecryptor@.exe	SUCCESS	FileSystemAttribute...
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\@WanaDecryptor@.exe	SUCCESS	CreationTime: 16/0...
11:33:...	tasksche.exe	2220	QueryAttribute...	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	FileSystemAttribute...
11:33:...	tasksche.exe	2220	QueryRemotePr...	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	INVALID PARAM...	
11:33:...	tasksche.exe	2220	QuerySecurityFile	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	Information: Attribute
11:33:...	tasksche.exe	2220	SetEndOfFileIn...	C:\@WanaDecryptor@.exe	SUCCESS	EndOfFile: 245,760
11:33:...	tasksche.exe	2220	ReadFile	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	Offset: 0, Length: 1...
11:33:...	tasksche.exe	2220	WriteFile	C:\@WanaDecryptor@.exe	SUCCESS	Offset: 0, Length: 1...
11:33:...	tasksche.exe	2220	ReadFile	C:\ProgramData\vmtdddzngmrqq135\@WanaDecryptor@.exe	SUCCESS	Offset: 131,072, Le...
11:33:...	tasksche.exe	2220	WriteFile	C:\@WanaDecryptor@.exe	SUCCESS	Offset: 131,072, Le...
11:33:...	tasksche.exe	2220	SetBasicInfor...	C:\@WanaDecryptor@.exe	SUCCESS	CreationTime: 01/0...
11:33:...	tasksche.exe	2220	QueryRemotePr...	C:\@WanaDecryptor@.exe	INVALID PARAM...	
11:33:...	tasksche.exe	2220	CloseFile	C:\@WanaDecryptor@.exe	SUCCESS	

IoC 5. A snapshot of procmon after initial detonation

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:33:...	tasksche.exe	2220	ReadFile	C:\Windows\SysWOW64\cmd.exe	SUCCESS	Offset: 192,512, Le...
11:33:...	tasksche.exe	2220	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\Device\H...	NAME NOT FOUND	Length: 40
11:33:...	tasksche.exe	2220	Process Create	C:\Windows\SysWOW64\cmd.exe	SUCCESS	PID: 4252, Comma...
11:33:...	tasksche.exe	2220	QuerySecurityFile	C:\Windows\SysWOW64\cmd.exe	SUCCESS	Information: Owner...
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\Windows\SysWOW64\cmd.exe	SUCCESS	CreationTime: 06/1...
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\Windows\SysWOW64\cmd.exe	SUCCESS	CreationTime: 06/1...
11:33:...	tasksche.exe	2220	QueryNameInfo...	C:\Windows\SysWOW64\cmd.exe	SUCCESS	Name: \Windows\...
11:33:...	tasksche.exe	2220	CloseFile	C:\Windows\SysWOW64\cmd.exe	SUCCESS	
11:33:...	tasksche.exe	3688	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-348996749...	NAME NOT FOUND	Length: 40
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\taskidl.exe	SUCCESS	Desired Access: R...
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\ProgramData\vmtdddzngmrqq135\taskidl.exe	SUCCESS	CreationTime: 12/0...
11:33:...	tasksche.exe	2220	CloseFile	C:\ProgramData\vmtdddzngmrqq135\taskidl.exe	SUCCESS	
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\taskidl.exe	SUCCESS	Desired Access: R...
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\ProgramData\vmtdddzngmrqq135\taskidl.exe	SUCCESS	CreationTime: 12/0...
11:33:...	tasksche.exe	2220	CloseFile	C:\ProgramData\vmtdddzngmrqq135\taskidl.exe	SUCCESS	
11:33:...	tasksche.exe	2220	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Option...	NAME NOT FOUND	Desired Access: Q...

IoC 6. A snapshot of procmon after initial detonation

File Explorer - C:\ProgramData

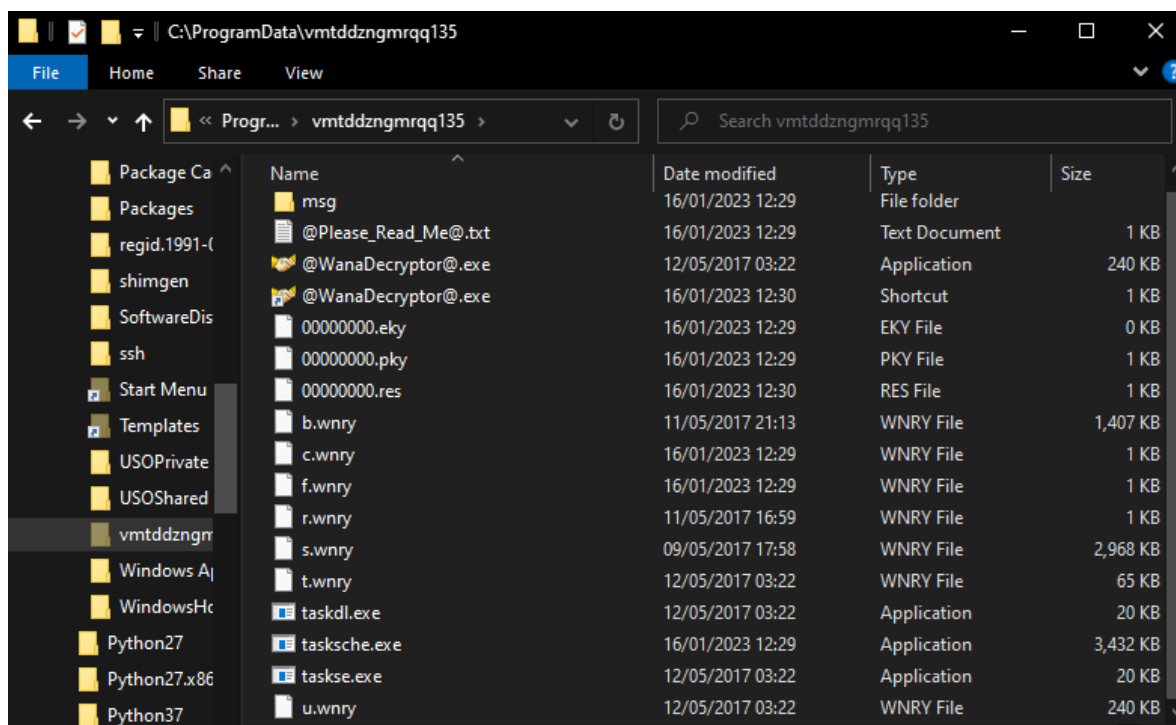
File Home Share View

Local Disk (C:) > ProgramData

Name	Date modified	Type	Size
Packages	21/09/2022 10:51	File folder	
regid.1991-06.com.microsoft	07/01/2023 10:58	File folder	
shimgen	22/09/2022 07:50	File folder	
SoftwareDistribution	07/12/2019 09:14	File folder	
ssh	06/10/2021 14:58	File folder	
Start Menu	20/09/2022 13:55	File folder	
Templates	20/09/2022 13:55	File folder	
USOPrivate	20/09/2022 14:01	File folder	
USOShared	07/12/2019 09:14	File folder	
vmtdddzngmrqq135	16/01/2023 12:29	File folder	
Windows App Certification Kit	22/09/2022 06:45	File folder	

IoC 7. A snapshot of the new directory under /ProgramData



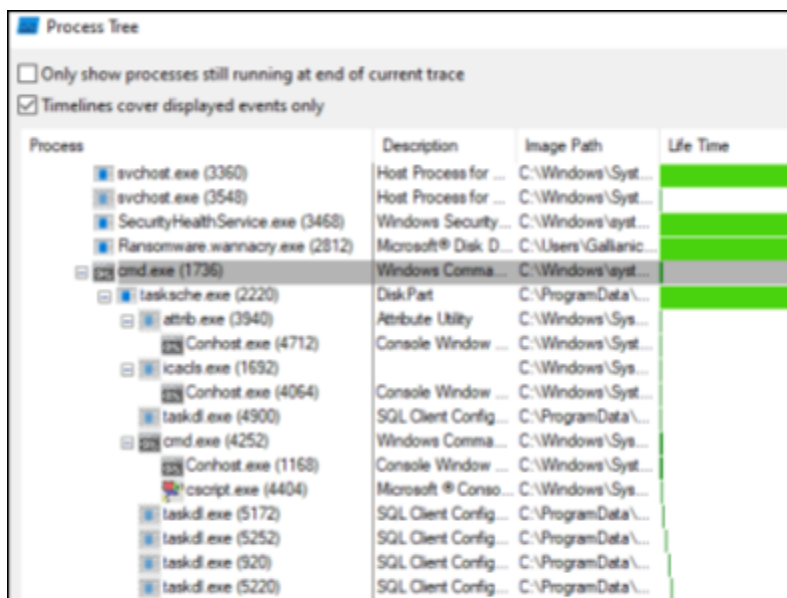


IoC 8. A snapshot of the content of the new directory

It is useful to utilize the **Process tree** utility in **procmon** (IoC 9). We can confirm that **cmd.exe** has been run to then execute **tasksche.exe**. From there, we can see the other executables run: **attrib.exe**, **conhost.exe**, **icacfs.exe**, and **taskdl.exe**.

**icacfs** is a command-line utility that can be used to modify NTFS file system permissions.

**attrib.exe** Displays sets, or removes attributes assigned to files or directories. If we recall the strings that we pulled previously, we can start putting all the pieces together.

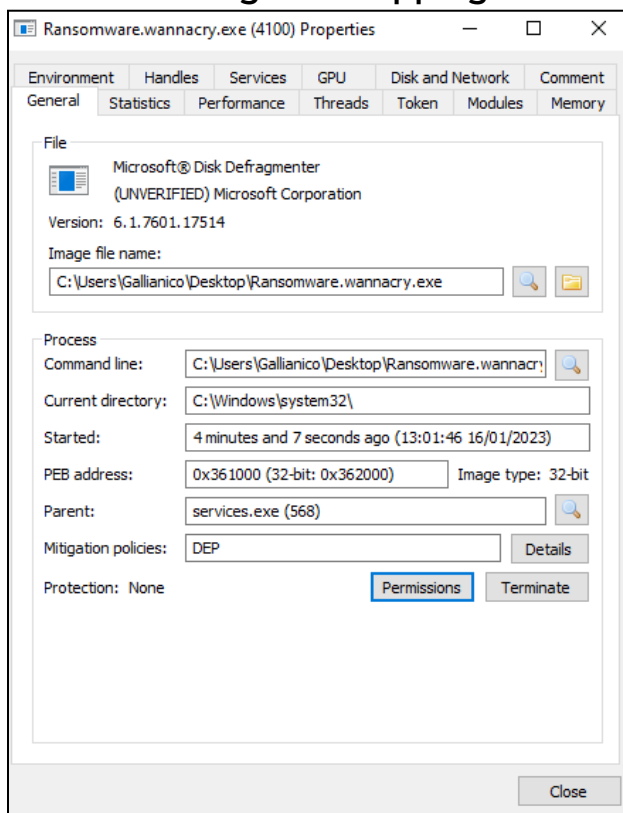


IoC 9. A view of Process Tree in Procmon



Another confirmation comes from analyzing the result of **Process Hacker** (IoC 10). We can see that the original dropper it's been executed as a child process of **services.exe**.

**services.exe** is a part of the Microsoft Windows Operating System and manages the operation of starting and stopping services.



IoC 10. Detailed view of the Ransomware.wannacry.exe process

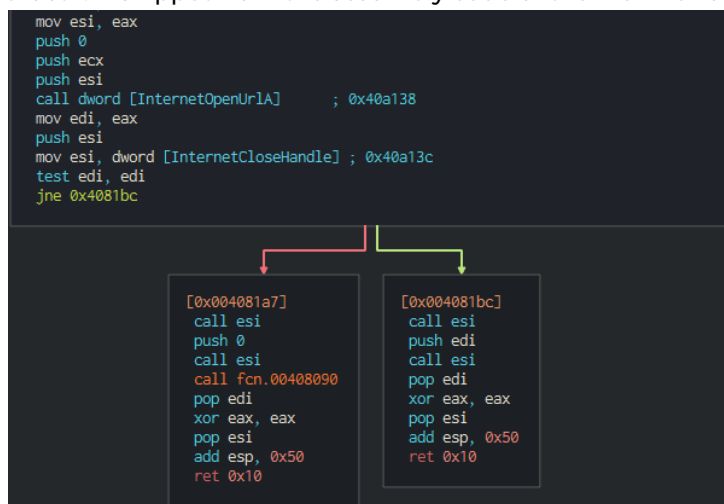


## Advanced Static Analysis

I've made use of **cutter** to perform the disassembly of the binary. If we analyze the **main** function we can recognize the **KillSwitch**. From the graph view, we can see the hard-coded domain being passed to the **esi register** (Art. 1). The domain is then used during the APIs calls: **InternetOpenA**, **InternetOpenUrlA** (Art. 2). After attempting the connection, the program performs a test on the **edi registers**. If the connection is successful, the program terminates, if not, it proceeds with the rest of the program (**fcn.00408090** - Art. 2).

```
[0x00408140]
139: int main (int argc, char **argv, char **envp);
; var int32_t var_14h @ esp+0x28
; var int32_t var_8h @ esp+0x3c
; var int32_t var_41h @ esp+0x75
; var int32_t var_45h @ esp+0x79
; var int32_t var_49h @ esp+0x7d
; var int32_t var_4dh @ esp+0x81
; var int32_t var_51h @ esp+0x85
; var int32_t var_55h @ esp+0x89
; var int32_t var_6bh @ esp+0x8b
sub esp, 0x50
push esi
push edi
mov ecx, 0xe ; 14
mov esi, str.http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com ; 0x4313d0
lea edi, [var_8h]
xor eax, eax
rep movsd dword es:[edi], dword ptr [esi]
movsb byte es:[edi], byte ptr [esi]
mov dword [var_41h], eax
mov dword [var_45h], eax
mov dword [var_49h], eax
mov dword [var_4dh], eax
mov dword [var_51h], eax
mov word [var_55h], ax
push eax
push eax
push eax
```

Artifact 1. A snippet from the assembly code of the main function



Artifact 2. A snippet from the assembly code of the main function



If we jump inside this function, we can see the binary performing a conditional execution by using the comparison (*cmp*). If the program takes the jump, we can see it making a call to the **OpenSCmanagerA** function (Art. 3). This function establishes a connection to the **service control manager** on the specified computer and opens the specified service control manager database.

The binary has now installed itself as a service.

```
Graph (fcn.00408090)
fcn.00408090 ();
;
; 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 1...
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, L...
```

Artifact 3. A snippet from the assembly code. On the right branch, the binary executes **OpenSCManagerA**

If it doesn't take the jump, it'll call **fcn. 00407f20**. If we follow the function call, we can see that it'll execute 2 additional function calls: **fcn. 00407c40** and **fcn. 00407ce0** (Art. 4).

The first one will perform the same function as the previous one. It'll install the binary as a service (Art 5).

The second function will drop the remaining executables that will handle encryption, file creation, and all the rest.

It is possible to dig deeper into the assembly code. It is also possible to perform disassembly on the

```
[0x00407f20]
13: fcn.00407f20 ();
call    fcn.00407c40
call    fcn.00407ce0
xor     eax, eax
ret
```

Artifact 4

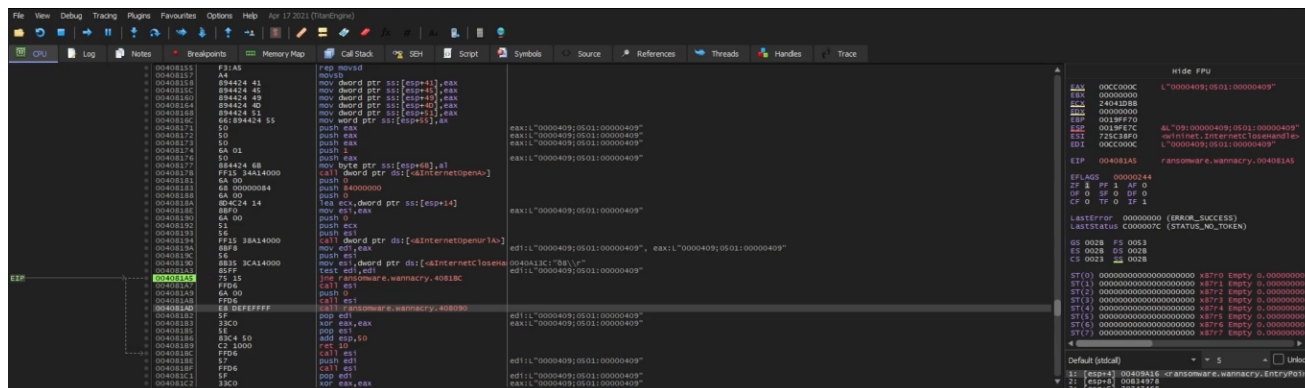


other files too, but this would fall outside the scope of this report, and it would go beyond my capacity to analyze assembly.

```
[0x00407c40]
148: fcn.00407c40 ();
; var int32_t var_1ch @ esp+0x54
sub     esp, 0x104
lea     eax, [esp]
push    edi
push    0x70f760
push    str.s__m_security      ; 0x431330 ; const char *format
push    eax                   ; char *s
call    dword [sprintf]       ; 0x40a10c ; int sprintf(char *s, const char *format, ...)
add     esp, 0xc
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      0x407cca
```

Artifact 5. A snippet from the assembly code. The binary calls again the OpenSCManagerA function





Artifact 7. A snippet from the debugger. On the left we can see the registers being tested, and on the right box we can see the value of the zero flag.

As we can see from Fig 6, the program completed its execution, and the symptoms described in the previous section have appeared again.

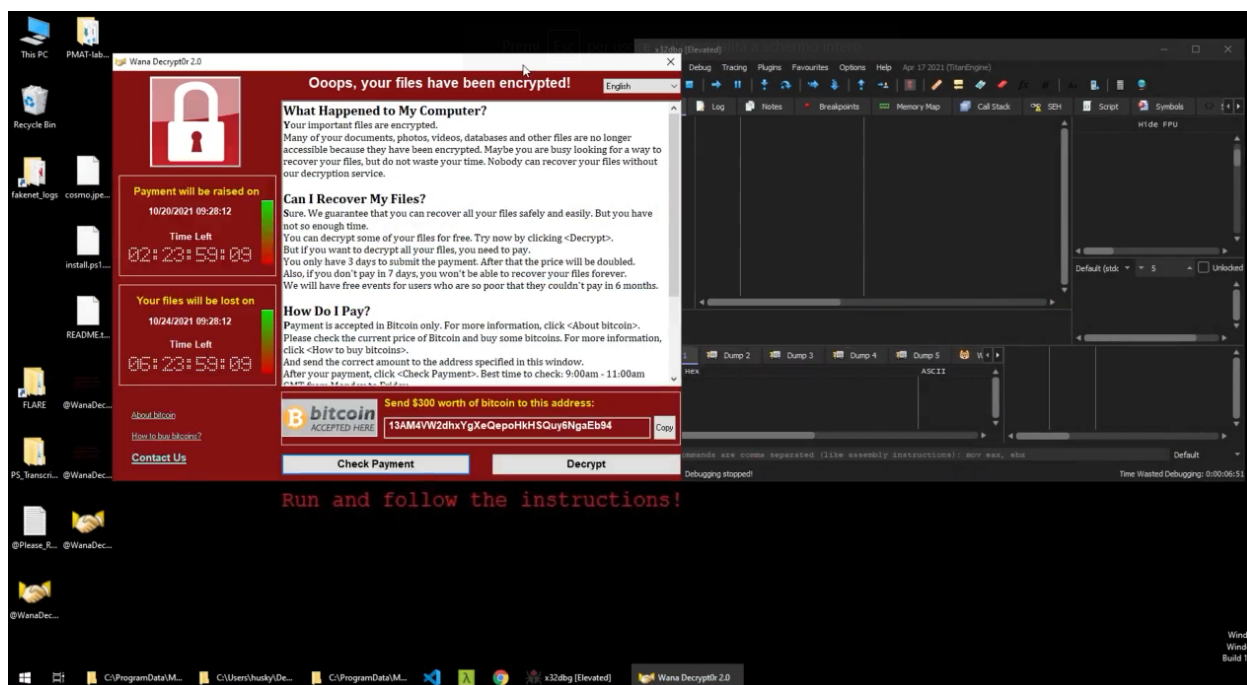


Fig. 6. A snapshot showing the successful execution of the binary





# Indicators of Compromise

## Host-based Network Indicators

IoC 11. A snapshot of TCPview showing the binary scanning available hosts one the network via SMB port 445

The screenshot shows the TCPView application window with the search filter set to 'Ransomware.wannacr.exe'. The table displays several TCP connections in a 'Syn Sent' state, all originating from the local address 169.254.72.102 and targeting various remote addresses on port 445.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port
Ransomware.wannacr...	4716	TCP	Syn Sent	169.254.72.102	63910	169.254.5.14	445
Ransomware.wannacr...	4716	TCP	Syn Sent	169.254.72.102	63911	169.254.6.14	445
Ransomware.wannacr...	4716	TCP	Syn Sent	169.254.72.102	63912	169.254.7.14	445
Ransomware.wannacr...	4716	TCP	Syn Sent	169.254.72.102	63913	169.254.8.14	445
Ransomware.wannacr...	4716	TCP	Syn Sent	169.254.72.102	63914	169.254.9.14	445
Ransomware.wannacr...	4716	TCP	Syn Sent	169.254.72.102	63915	169.254.10.14	445
Ransomware.wannacr...	4716	TCP	Syn Sent	169.254.72.102	63916	169.254.11.14	445
Ransomware.wannacr...	4716	TCP	Syn Sent	169.254.72.102	63917	169.254.12.14	445

Endpoints: 311    Established:    Listening: 23    Time Wait:    Close Wait:    Update: 2 sec    States: (All)

## Host-based indicators

IoC 3. A snapshot showing the combined output from Procmon, Process Hacker and TCPView

The screenshot displays three windows: Process Monitor, Process Hacker, and TCPView. Process Monitor shows a list of system events, including file reads and registry operations. Process Hacker shows a list of running processes with their PIDs, CPU usage, and memory. TCPView shows a list of network connections, including those from Ransomware.wannacr.exe.

Name	Process ID	CPU	I/O total	Private b...	User name
VBoxTray.exe	3780	0.05	28 B/s	2.46 MB	DESKTOP-V...
msedge.exe	3808	0.07		27.64 MB	DESKTOP-V...
msedge.exe	4004			1.98 MB	DESKTOP-V...
msedge.exe	3608			16.52 MB	DESKTOP-V...
msedge.exe	3744			9.82 MB	DESKTOP-V...
msedge.exe	3772			7.5 MB	DESKTOP-V...
notepad.exe	3676			3.7 MB	DESKTOP-V...
notepad.exe	2144			2.53 MB	DESKTOP-V...
Procmon.exe	1392			6.11 MB	DESKTOP-V...
Procmon64.exe	3164	41.20	12.42 MB/s	106.04 MB	DESKTOP-V...
ProcessHacker.exe	1464	3.24		14.39 MB	DESKTOP-V...
tcpview.exe	2368	0.74		6.93 MB	DESKTOP-V...
tasksche.exe	3160	22.87	110.77 kB...	15.96 MB	NT AUTHO...





#### IoC 4. A snapshot from Procmon showing the creation of *tasksche.exe*

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\Prefetch\RANSOMWARE...	NAME NOT FOUND	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	NAME NOT FOUND	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: G...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	4300	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
11:32:...	Ransomware.w...	2812	CreateFile	C:\Users\Gallianico\Desktop\Ransomw...	SUCCESS	Desired Access: G...

#### IoC 5. A snapshot from Procmon showing the creation of additional file on the system

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
11:33:...	tasksche.exe	3688	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-348996749...	NAME NOT FOUND	Length: 40
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe.lnk	NAME NOT FOUND	Desired Access: G...
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe.lnk	NAME NOT FOUND	Desired Access: G...
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe.lnk	NAME NOT FOUND	Desired Access: G...
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe.lnk	NAME NOT FOUND	Desired Access: G...
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	Desired Access: G...
11:33:...	tasksche.exe	2220	QueryAttributeT...	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	Attributes: ANCI, R...
11:33:...	tasksche.exe	2220	QueryStandardI...	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	AllocationSize: 245...
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	CreationTime: 16/0...
11:33:...	tasksche.exe	2220	QueryStreamInf...	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	0:::\$DATA
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	CreationTime: 16/0...
11:33:...	tasksche.exe	2220	QueryEaInfor...	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	EaSize: 0
11:33:...	tasksche.exe	2220	CreateFile	C:\@WanaDecryptor@.exe	SUCCESS	Desired Access: G...
11:33:...	tasksche.exe	2220	QueryAttributeI...	C:\@WanaDecryptor@.exe	SUCCESS	FileSystemAttribute...
11:33:...	tasksche.exe	2220	QueryBasicInfor...	C:\@WanaDecryptor@.exe	SUCCESS	CreationTime: 16/0...
11:33:...	tasksche.exe	2220	QueryAttributeI...	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	FileSystemAttribute...
11:33:...	tasksche.exe	2220	QueryRemotePr...	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	INVALID PARAM...	
11:33:...	tasksche.exe	2220	QuerySecurityFile	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	Information: Attribute
11:33:...	tasksche.exe	2220	SetEndOfFileInf...	C:\@WanaDecryptor@.exe	SUCCESS	EndOfFile: 245,760
11:33:...	tasksche.exe	2220	ReadFile	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	Offset: 0, Length: 1...
11:33:...	tasksche.exe	2220	WriteFile	C:\@WanaDecryptor@.exe	SUCCESS	Offset: 0, Length: 1...
11:33:...	tasksche.exe	2220	ReadFile	C:\ProgramData\vmtdddzngmrq135\@WanaDecryptor@.exe	SUCCESS	Offset: 131,072, Le...
11:33:...	tasksche.exe	2220	WriteFile	C:\@WanaDecryptor@.exe	SUCCESS	Offset: 131,072, Le...
11:33:...	tasksche.exe	2220	SetBasicInfor...	C:\@WanaDecryptor@.exe	SUCCESS	CreationTime: 01/0...
11:33:...	tasksche.exe	2220	QueryRemotePr...	C:\@WanaDecryptor@.exe	INVALID PARAM...	
11:33:...	tasksche.exe	2220	CloseFile	C:\@WanaDecryptor@.exe	SUCCESS	



IoC 6. A snapshot from Procmon showing the creation of additional file on the system

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
11:33:...	tasksche.exe	2220	ReadFile	C:\Windows\SysWOW64\cmd.exe	SUCCESS	Offset: 192,512, Le...
11:33:...	tasksche.exe	2220	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\Device\H...	NAME NOT FOUND	Length: 40
11:33:...	tasksche.exe	2220	Process Create	C:\Windows\SysWOW64\cmd.exe	SUCCESS	PID: 4252, Comma...
11:33:...	tasksche.exe	2220	QuerySecurityFile	C:\Windows\SysWOW64\cmd.exe	SUCCESS	Information: Owner...
11:33:...	tasksche.exe	2220	QueryBasicInfo...	C:\Windows\SysWOW64\cmd.exe	SUCCESS	CreationTime: 06/1...
11:33:...	tasksche.exe	2220	QueryNameInfo...	C:\Windows\SysWOW64\cmd.exe	SUCCESS	CreationTime: 06/1...
11:33:...	tasksche.exe	2220	CloseFile	C:\Windows\SysWOW64\cmd.exe	SUCCESS	Name: \Windows\...
11:33:...	tasksche.exe	3688	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-348996749...	NAME NOT FOUND	Length: 40
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\taskdl.exe	SUCCESS	Desired Access: R...
11:33:...	tasksche.exe	2220	QueryBasicInfo...	C:\ProgramData\vmtdddzngmrqq135\taskdl.exe	SUCCESS	CreationTime: 12/0...
11:33:...	tasksche.exe	2220	CloseFile	C:\ProgramData\vmtdddzngmrqq135\taskdl.exe	SUCCESS	
11:33:...	tasksche.exe	2220	CreateFile	C:\ProgramData\vmtdddzngmrqq135\taskdl.exe	SUCCESS	Desired Access: R...
11:33:...	tasksche.exe	2220	QueryBasicInfo...	C:\ProgramData\vmtdddzngmrqq135\taskdl.exe	SUCCESS	CreationTime: 12/0...
11:33:...	tasksche.exe	2220	CloseFile	C:\ProgramData\vmtdddzngmrqq135\taskdl.exe	SUCCESS	
11:33:...	tasksche.exe	2220	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Option...	NAME NOT FOUND	Desired Access: Q...

IoC 7. A snapshot of the file system showing the newly created directory

C:\ProgramData				
File Home Share View				
Search ProgramData				
Name	Date modified	Type	Size	
Packages	21/09/2022 10:51	File folder		
regid.1991-06.com.microsoft	07/01/2023 10:58	File folder		
shimgen	22/09/2022 07:50	File folder		
SoftwareDistribution	07/12/2019 09:14	File folder		
ssh	06/10/2021 14:58	File folder		
Start Menu	20/09/2022 13:55	File folder		
Templates	20/09/2022 13:55	File folder		
USOPrivate	20/09/2022 14:01	File folder		
USOShared	07/12/2019 09:14	File folder		
vmtdddzngmrqq135	16/01/2023 12:29	File folder		
Windows App Certification Kit	22/09/2022 06:45	File folder		

IoC 8. A snapshot of the file system showing the content of the newly created directory

C:\ProgramData\vmtdddzngmrqq135				
File Home Share View				
Search vmtdddzngmrqq135				
Name	Date modified	Type	Size	
Package Ca				
Packages				
regid.1991-06.com.microsoft				
shimgen				
SoftwareDis				
ssh				
Start Menu				
Templates				
USOPrivate				
USOShared				
vmtdddzngmr				
Windows App				
WindowsHc				
Python27				
Python27x86				
Python37				
msg	16/01/2023 12:29	File folder		
@Please_Read_Me@.txt	16/01/2023 12:29	Text Document		
@WanaDecryptor@.exe	12/05/2017 03:22	Application		
@WanaDecryptor@.exe	16/01/2023 12:30	Shortcut		
00000000.eky	16/01/2023 12:29	EKY File		
00000000.pkty	16/01/2023 12:29	PKY File		
00000000.res	16/01/2023 12:30	RES File		
b.wnry	11/05/2017 21:13	WNRY File		
c.wnry	16/01/2023 12:29	WNRY File		
f.wnry	16/01/2023 12:29	WNRY File		
r.wnry	11/05/2017 16:59	WNRY File		
s.wnry	09/05/2017 17:58	WNRY File		
t.wnry	12/05/2017 03:22	WNRY File		
taskdl.exe	12/05/2017 03:22	Application		
tasksche.exe	16/01/2023 12:29	Application		
taskse.exe	12/05/2017 03:22	Application		
u.wnry	12/05/2017 03:22	WNRY File		



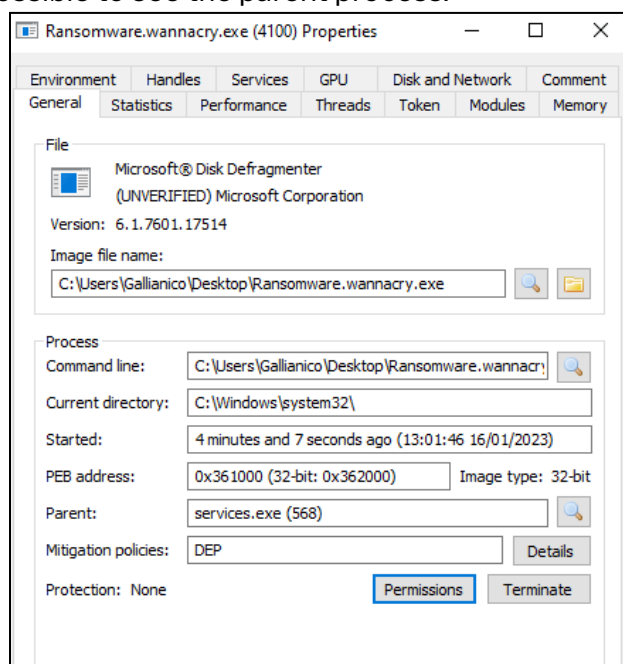
IoC 9. A snapshot from the Process Tree utility showing the processes initiated by the binary

Process Tree

☐ Only show processes still running at end of current trace  
☒ Timelines cover displayed events only

Process	Description	Image Path	Life Time
svchost.exe (3360)	Host Process for ...	C:\Windows\Syst...	
svchost.exe (3548)	Host Process for ...	C:\Windows\Syst...	
SecurityHealthService.exe (3468)	Windows Security...	C:\Windows\seyst...	
Ransomware.wannacry.exe (2812)	Microsoft® Disk D...	C:\Users\Gallianic...	
cmd.exe (1736)	Windows Comma...	C:\Windows\seyst...	
taskche.exe (2220)	DiskPart	C:\ProgramData\...	
attrib.exe (3940)	Attribute Utility	C:\Windows\Sys...	
conhost.exe (4712)	Console Window ...	C:\Windows\Syst...	
icacds.exe (1692)		C:\Windows\Sys...	
conhost.exe (4064)	Console Window ...	C:\Windows\Syst...	
taskcl.exe (4900)	SQL Client Config...	C:\ProgramData\...	
cmd.exe (4252)	Windows Comma...	C:\Windows\Sys...	
conhost.exe (1168)	Console Window ...	C:\Windows\Syst...	
cmdscript.exe (4404)	Microsoft® Conso...	C:\Windows\Sys...	
taskcl.exe (5172)	SQL Client Config...	C:\ProgramData\...	
taskcl.exe (5252)	SQL Client Config...	C:\ProgramData\...	
taskcl.exe (520)	SQL Client Config...	C:\ProgramData\...	
taskcl.exe (5220)	SQL Client Config...	C:\ProgramData\...	

IoC 10. A snapshot from the Process Tree utility showing the Ransomware.wannacry.exe process in detail. It's possible to see the parent process.





IoC 12. A snapshot from Process hacker showing the *tasksche.exe* running process

Name	PID	CPU	I/O total ...	Private b...	User name	Descr
VBoxTray.exe	3780	0.12	36 B/s	2.46 MB	DESKTOP-V...\Gallianico	Virtua
msedge.exe	3808			27.75 MB	DESKTOP-V...\Gallianico	Micro
msedge.exe	4004			1.98 MB	DESKTOP-V...\Gallianico	Micro
msedge.exe	3608			16.52 MB	DESKTOP-V...\Gallianico	Micro
msedge.exe	3744			9.75 MB	DESKTOP-V...\Gallianico	Micro
msedge.exe	3772			7.5 MB	DESKTOP-V...\Gallianico	Micro
notepad.exe	3676			3.7 MB	DESKTOP-V...\Gallianico	Note
notepad.exe	2144			2.53 MB	DESKTOP-V...\Gallianico	Note
Procmon.exe	1392			6.11 MB	DESKTOP-V...\Gallianico	Proce
Procmon64.exe	3164	24.40	3.36 MB/s	108.15 MB	DESKTOP-V...\Gallianico	Proce
ProcessHacker.exe	1464	8.15		14.39 MB	DESKTOP-V...\Gallianico	Proce
tcpview.exe	2368	0.34		8.71 MB	DESKTOP-V...\Gallianico	Sysin
tasksche.exe	3160	24.80	28.96 kB/s	18.2 MB	NT AUTHORITY\SYSTEM	DiskP

## Network-based Indicators

IoC 1. A snapshot from Wireshark showing the attempted communication between the binary and the hard-coded domain

No.	Time	Source	Destination	Protocol	Length	Info
13	49.219747485	10.0.0.3	10.0.0.4	TCP	66	13922 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_P
14	49.219826273	10.0.0.3	10.0.0.4	TCP	66	80 → 13922 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA
15	49.220448732	10.0.0.3	10.0.0.4	TCP	60	13922 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16	49.220913287	10.0.0.3	10.0.0.4	HTTP	154	GET / HTTP/1.1
17	49.220951256	10.0.0.4	10.0.0.3	TCP	54	80 → 13922 [ACK] Seq=1 Ack=101 Win=64256 Len=0
18	49.257948069	10.0.0.4	10.0.0.3	TCP	204	80 → 13922 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=150 [TCP seq
19	49.258882364	10.0.0.3	10.0.0.4	TCP	60	13922 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
20	49.258922647	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (text/html)
21	49.259314240	10.0.0.3	10.0.0.4	TCP	60	13922 → 80 [ACK] Seq=101 Ack=409 Win=261632 Len=0
22	49.265982136	10.0.0.4	10.0.0.3	TCP	54	80 → 13922 [FIN, ACK] Seq=409 Ack=101 Win=64256 Len=0
23	49.266766678	10.0.0.3	10.0.0.4			
24	49.303246648	10.0.0.3	10.0.0.4			

Frame 20: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bytes) on interface 0
Ethernet II, Src: PcsCompu, 08:00:07:56:2b:08, Dst: 10.0.0.4
Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
Transmission Control Protocol, Src Port: 80, Dst Port: 13922
[2 Reassembled TCP Segments (408 bytes): #18(150), #20(258)]
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)

GET / HTTP/1.1
Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com
Cache-Control: no-cache
HTTP/1.1 200 OK
Date: Sun, 15 Jan 2023 19:28:32 GMT
Content-Length: 258
Content-Type: text/html
Connection: Close
Server: InetSim HTTP Server



## YARA Rules & Signatures

```
rule wannacry_detector

    meta:
        author = "Alessio Ragazzi"
        date = "18/01/2023"
        version = "18/01/2023"
        comment = "Basic yara rules to detect the ransomware WannaCry. Rules are based on the strings that I was able to pull during basic static analysis of the binary"

    strings:
        $executable1 = "tasksche.exe"
        $executable2 = "taskdl.exe"
        $string1 = "mssecsvc2.0"
        $string2 = "wannacry"
        $string3 = "wanadecryptor"
        $url1= "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"

    condition:
        $executable1 and $executable2 and $string1 or
        $string2 and $executable1 or
        $string3 and $executable1 or
        $url1 and $executable1 or $executable1 or $string1 or $string2 or
        $string3
```



## Appendices

### A. Yara Rules

Full Yara repository located at: <https://github.com/ale17ragazzi>

### B. Further reading

<https://www.mandiant.com/resources/blog/wannacry-malware-profile>

### C. URLs of interest

Domain	Port
<a href="http://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com">http://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com</a>	80

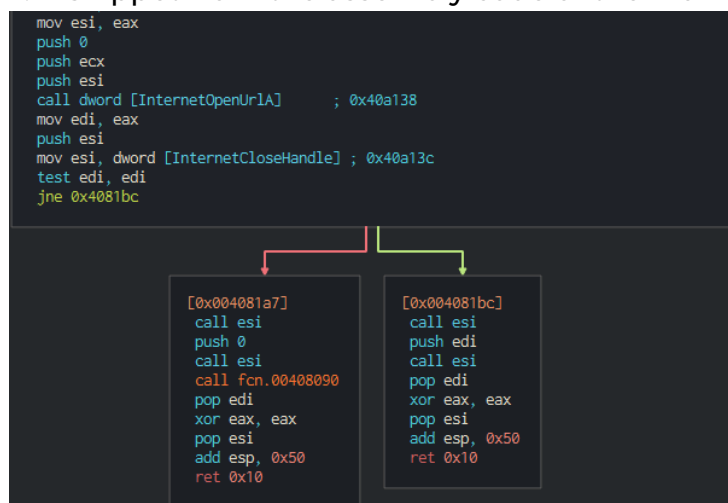
### D. Disassembled Code Snippets

Artifact 1. A snippet from the assembly code of the main function

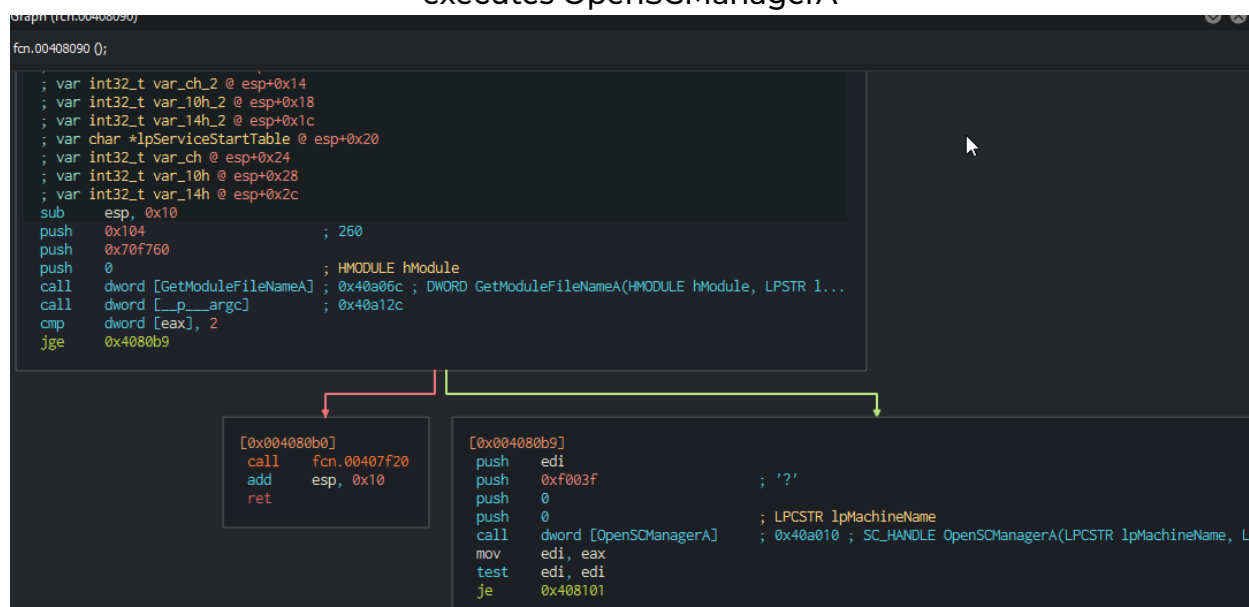
```
[0x00408140]
139: int main (int argc, char **argv, char **envp);
; var int32_t var_14h @ esp+0x28
; var int32_t var_8h @ esp+0x3c
; var int32_t var_41h @ esp+0x75
; var int32_t var_45h @ esp+0x79
; var int32_t var_49h @ esp+0x7d
; var int32_t var_4dh @ esp+0x81
; var int32_t var_51h @ esp+0x85
; var int32_t var_55h @ esp+0x89
; var int32_t var_6bh @ esp+0x8b
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
```



Artifact 2. A snippet from the assembly code of the main function



Artifact 3. A snippet from the assembly code. On the right branch, the binary executes OpenSCManagerA





#### Artifact 4

```
[0x00407f20]
13: fcn.00407f20 ();
call    fcn.00407c40
call    fcn.00407ce0
xor     eax, eax
ret
```

#### Artifact 5

```
[0x00407c40]
148: fcn.00407c40 ();
; var int32_t var_1ch @ esp+0x54
sub     esp, 0x104
lea     eax, [esp]
push    edi
push    0x70f760
push    str.s__m_security      ; 0x431330 ; const char *format
push    eax                    ; char *s
call    dword [sprintf]       ; 0x40a10c ; int sprintf(char *s, const char *format, ...)
add     esp, 0xc
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      0x407cca
```

Artifact 6. A snippet from the debugger. On the top-left corner we can see the domain being called





File Machine View Input Devices Help  
Ransomware.wannacry.exe - PID: 4860 - Module ransomware.wannacry.exe - Thread: Main Thread 4720 - x32dbg [Elevated]  
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (x86\_64)  
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace  
00401141 16 push esi  
00401142 17 push edi  
00401143 18 mov ecx, 1  
00401144 19 xor eax, eax  
00401145 1A rep movsb  
00401146 1B  
00401147 1C mov dword ptr esi:[esp+4],eax  
00401148 1D mov dword ptr esi:[esp+4],eax  
00401149 1E mov dword ptr esi:[esp+4],eax  
0040114A 1F mov dword ptr esi:[esp+4],eax  
0040114B 20 mov word ptr esi:[esp+4],eax  
0040114C 21  
0040114D 22 push eax  
0040114E 23 push ecx  
0040114F 24 push 1  
00401150 25  
00401151 26 mov byte ptr esi:[esp+8],al  
00401152 27 call dword ptr ds:[4InternetOpenA]  
00401153 28 push 0  
00401154 29 push 80000000  
00401155 2A test ecx, dword ptr esi:[esp+14]  
00401156 2B jnz 0040115C  
00401157 2C mov ecx, dword ptr esi:[esp+14]  
00401158 2D push 0  
00401159 2E call dword ptr ds:[4InternetOpenA]  
0040115A 2F mov edi, eax  
0040115B 30  
0040115C 31 mov esi, dword ptr ds:[4InternetOpenA]  
0040115D 32 test esi, esi  
0040115E 33 jnz 0040115C  
0040115F 34 call esi  
00401160 35  
00401161 36 call esi  
00401162 37  
00401163 38 pop edi  
00401164 39 mov eax, eax  
00401165 3A pop esi  
00401166 3B  
00401167 3C  
00401168 3D  
00401169 3E  
0040116A 3F  
0040116B 40  
0040116C 41  
0040116D 42  
0040116E 43  
0040116F 44  
00401170 45  
00401171 46  
00401172 47  
00401173 48  
00401174 49  
00401175 4A  
00401176 4B  
00401177 4C  
00401178 4D  
00401179 4E  
0040117A 4F  
0040117B 50  
0040117C 51  
0040117D 52  
0040117E 53  
0040117F 54  
00401180 55  
00401181 56  
00401182 57  
00401183 58  
00401184 59  
00401185 5A  
00401186 5B  
00401187 5C  
00401188 5D  
00401189 5E  
0040118A 5F  
0040118B 60  
0040118C 61  
0040118D 62  
0040118E 63  
0040118F 64  
00401190 65  
00401191 66  
00401192 67  
00401193 68  
00401194 69  
00401195 6A  
00401196 6B  
00401197 6C  
00401198 6D  
00401199 6E  
0040119A 6F  
0040119B 70  
0040119C 71  
0040119D 72  
0040119E 73  
0040119F 74  
004011A0 75  
004011A1 76  
004011A2 77  
004011A3 78  
004011A4 79  
004011A5 7A  
004011A6 7B  
004011A7 7C  
004011A8 7D  
004011A9 7E  
004011AA 7F  
004011AB 80  
004011AC 81  
004011AD 82  
004011AE 83  
004011AF 84  
004011B0 85  
004011B1 86  
004011B2 87  
004011B3 88  
004011B4 89  
004011B5 8A  
004011B6 8B  
004011B7 8C  
004011B8 8D  
004011B9 8E  
004011BA 8F  
004011BB 90  
004011BC 91  
004011BD 92  
004011BE 93  
004011BF 94  
004011C0 95  
004011C1 96  
004011C2 97  
004011C3 98  
004011C4 99  
004011C5 9A  
004011C6 9B  
004011C7 9C  
004011C8 9D  
004011C9 9E  
004011CA 9F  
004011CB 100  
004011CC 101  
004011CD 102  
004011CE 103  
004011CF 104  
004011D0 105  
004011D1 106  
004011D2 107  
004011D3 108  
004011D4 109  
004011D5 10A  
004011D6 10B  
004011D7 10C  
004011D8 10D  
004011D9 10E  
004011DA 10F  
004011DB 110  
004011DC 111  
004011DD 112  
004011DE 113  
004011DF 114  
004011E0 115  
004011E1 116  
004011E2 117  
004011E3 118  
004011E4 119  
004011E5 11A  
004011E6 11B  
004011E7 11C  
004011E8 11D  
004011E9 11E  
004011EA 11F  
004011EB 120  
004011EC 121  
004011ED 122  
004011EE 123  
004011EF 124  
004011F0 125  
004011F1 126  
004011F2 127  
004011F3 128  
004011F4 129  
004011F5 12A  
004011F6 12B  
004011F7 12C  
004011F8 12D  
004011F9 12E  
004011FA 12F  
004011FB 130  
004011FC 131  
004011FD 132  
004011FE 133  
004011FF 134  
00401200 135  
00401201 136  
00401202 137  
00401203 138  
00401204 139  
00401205 13A  
00401206 13B  
00401207 13C  
00401208 13D  
00401209 13E  
0040120A 13F  
0040120B 140  
0040120C 141  
0040120D 142  
0040120E 143  
0040120F 144  
00401210 145  
00401211 146  
00401212 147  
00401213 148  
00401214 149  
00401215 14A  
00401216 14B  
00401217 14C  
00401218 14D  
00401219 14E  
0040121A 14F  
0040121B 150  
0040121C 151  
0040121D 152  
0040121E 153  
0040121F 154  
00401220 155  
00401221 156  
00401222 157  
00401223 158  
00401224 159  
00401225 15A  
00401226 15B  
00401227 15C  
00401228 15D  
00401229 15E  
0040122A 15F  
0040122B 160  
0040122C 161  
0040122D 162  
0040122E 163  
0040122F 164  
00401230 165  
00401231 166  
00401232 167  
00401233 168  
00401234 169  
00401235 16A  
00401236 16B  
00401237 16C  
00401238 16D  
00401239 16E  
0040123A 16F  
0040123B 170  
0040123C 171  
0040123D 172  
0040123E 173  
0040123F 174  
00401240 175  
00401241 176  
00401242 177  
00401243 178  
00401244 179  
00401245 17A  
00401246 17B  
00401247 17C  
00401248 17D  
00401249 17E  
0040124A 17F  
0040124B 180  
0040124C 181  
0040124D 182  
0040124E 183  
0040124F 184  
00401250 185  
00401251 186  
00401252 187  
00401253 188  
00401254 189  
00401255 18A  
00401256 18B  
00401257 18C  
00401258 18D  
00401259 18E  
0040125A 18F  
0040125B 190  
0040125C 191  
0040125D 192  
0040125E 193  
0040125F 194  
00401260 195  
00401261 196  
00401262 197  
00401263 198  
00401264 199  
00401265 19A  
00401266 19B  
00401267 19C  
00401268 19D  
00401269 19E  
0040126A 19F  
0040126B 1A0  
0040126C 1A1  
0040126D 1A2  
0040126E 1A3  
0040126F 1A4  
00401270 1A5  
00401271 1A6  
00401272 1A7  
00401273 1A8  
00401274 1A9  
00401275 1AA  
00401276 1AB  
00401277 1AC  
00401278 1AD  
00401279 1AE  
0040127A 1AF  
0040127B 1B0  
0040127C 1B1  
0040127D 1B2  
0040127E 1B3  
0040127F 1B4  
00401280 1B5  
00401281 1B6  
00401282 1B7  
00401283 1B8  
00401284 1B9  
00401285 1BA  
00401286 1BB  
00401287 1BC  
00401288 1BD  
00401289 1BE  
0040128A 1BF  
0040128B 1C0  
0040128C 1C1  
0040128D 1C2  
0040128E 1C3  
0040128F 1C4  
00401290 1C5  
00401291 1C6  
00401292 1C7  
00401293 1C8  
00401294 1C9  
00401295 1CA  
00401296 1CB  
00401297 1CC  
00401298 1CD  
00401299 1CE  
0040129A 1CF  
0040129B 1D0  
0040129C 1D1  
0040129D 1D2  
0040129E 1D3  
0040129F 1D4  
004012A0 1D5  
004012A1 1D6  
004012A2 1D7  
004012A3 1D8  
004012A4 1D9  
004012A5 1DA  
004012A6 1DB  
004012A7 1DC  
004012A8 1DD  
004012A9 1DE  
004012AA 1DF  
004012AB 1E0  
004012AC 1E1  
004012AD 1E2  
004012AE 1E3  
004012AF 1E4  
004012B0 1E5  
004012B1 1E6  
004012B2 1E7  
004012B3 1E8  
004012B4 1E9  
004012B5 1EA  
004012B6 1EB  
004012B7 1EC  
004012B8 1ED  
004012B9 1EE  
004012BA 1EF  
004012BB 1F0  
004012BC 1F1  
004012BD 1F2  
004012BE 1F3  
004012BF 1F4  
004012C0 1F5  
004012C1 1F6  
004012C2 1F7  
004012C3 1F8  
004012C4 1F9  
004012C5 1FA  
004012C6 1FB  
004012C7 1FC  
004012C8 1FD  
004012C9 1FE  
004012CA 1FF  
004012CB 200  
004012CC 201  
004012CD 202  
004012CE 203  
004012CF 204  
004012D0 205  
004012D1 206  
004012D2 207  
004012D3 208  
004012D4 209  
004012D5 20A  
004012D6 20B  
004012D7 20C  
004012D8 20D  
004012D9 20E  
004012DA 20F  
004012DB 210  
004012DC 211  
004012DD 212  
004012DE 213  
004012DF 214  
004012E0 215  
004012E1 216  
004012E2 217  
004012E3 218  
004012E4 219  
004012E5 21A  
004012E6 21B  
004012E7 21C  
004012E8 21D  
004012E9 21E  
004012EA 21F  
004012EB 220  
004012EC 221  
004012ED 222  
004012EE 223  
004012EF 224  
004012F0 225  
004012F1 226  
004012F2 227  
004012F3 228  
004012F4 229  
004012F5 22A  
004012F6 22B  
004012F7 22C  
004012F8 22D  
004012F9 22E  
004012FA 22F  
004012FB 230  
004012FC 231  
004012FD 232  
004012FE 233  
004012FF 234  
00401300 235  
00401301 236  
00401302 237  
00401303 238  
00401304 239  
00401305 23A  
00401306 23B  
00401307 23C  
00401308 23D  
00401309 23E  
0040130A 23F  
0040130B 240  
0040130C 241  
0040130D 242  
0040130E 243  
0040130F 244  
00401310 245  
00401311 246  
00401312 247  
00401313 248  
00401314 249  
00401315 24A  
00401316 24B  
00401317 24C  
00401318 24D  
00401319 24E  
0040131A 24F  
0040131B 250  
0040131C 251  
0040131D 252  
0040131E 253  
0040131F 254  
00401320 255  
00401321 256  
00401322 257  
00401323 258  
00401324 259  
00401325 25A  
00401326 25B  
00401327 25C  
00401328 25D  
00401329 25E  
0040132A 25F  
0040132B 260  
0040132C 261  
0040132D 262  
0040132E 263  
0040132F 264  
00401330 265  
00401331 266  
00401332 267  
00401333 268  
00401334 269  
00401335 26A  
00401336 26B  
00401337 26C  
00401338 26D  
00401339 26E  
0040133A 26F  
0040133B 270  
0040133C 271  
0040133D 272  
0040133E 273  
0040133F 274  
00401340 275  
00401341 276  
00401342 277  
00401343 278  
00401344 279  
00401345 27A  
00401346 27B  
00401347 27C  
00401348 27D  
00401349 27E  
0040134A 27F  
0040134B 280  
0040134C 281  
0040134D 282  
0040134E 283  
0040134F 284  
00401350 285  
00401351 286  
00401352 287  
00401353 288  
00401354 289  
00401355 28A  
00401356 28B  
00401357 28C  
00401358 28D  
00401359 28E  
0040135A 28F  
0040135B 290  
0040135C 291  
0040135D 292  
0040135E 293  
0040135F 294  
00401360 295  
00401361 296  
00401362 297  
00401363 298  
00401364 299  
00401365 29A  
00401366 29B  
00401367 29C  
00401368 29D  
00401369 29E  
0040136A 29F  
0040136B 2A0  
0040136C 2A1  
0040136D 2A2  
0040136E 2A3  
0040136F 2A4  
00401370 2A5  
00401371 2A6  
00401372 2A7  
00401373 2A8  
00401374 2A9  
00401375 2AA  
00401376 2AB  
00401377 2AC  
00401378 2AD  
00401379 2AE  
0040137A 2AF  
0040137B 2B0  
0040137C 2B1  
0040137D 2B2  
0040137E 2B3  
0040137F 2B4  
00401380 2B5  
00401381 2B6  
00401382 2B7  
00401383 2B8  
00401384 2B9  
00401385 2BA  
00401386 2BB  
00401387 2BC  
00401388 2BD  
00401389 2BE  
0040138A 2BF  
0040138B 2C0  
0040138C 2C1  
0040138D 2C2  
0040138E 2C3  
0040138F 2C4  
00401390 2C5  
00401391 2C6  
00401392 2C7  
00401393 2C8  
00401394 2C9  
00401395 2CA  
00401396 2CB  
00401397 2CC  
00401398 2CD  
00401399 2CE  
0040139A 2CF  
0040139B 2D0  
0040139C 2D1  
0040139D 2D2  
0040139E 2D3  
0040139F 2D4  
004013A0 2D5  
004013A1 2D6  
004013A2 2D7  
004013A3 2D8  
004013A4 2D9  
004013A5 2DA  
004013A6 2DB  
004013A7 2DC  
004013A8 2DD  
004013A9 2DE  
004013AA 2DF  
004013AB 2E0  
004013AC 2E1  
004013AD 2E2  
004013AE 2E3  
004013AF 2E4  
004013B0 2E5  
004013B1 2E6  
004013B2 2E7  
004013B3 2E8  
004013B4 2E9  
004013B5 2EA  
004013B6 2EB  
004013B7 2EC  
004013B8 2ED  
004013B9 2EE  
004013BA 2EF  
004013BB 2F0  
004013BC 2F1  
004013BD 2F2  
004013BE 2F3  
004013BF 2F4  
004013C0 2F5  
004013C1 2F6  
004013C2 2F7  
004013C3 2F8  
004013C4 2F9  
004013C5 2FA  
004013C6 2FB  
004013C7 2FC  
004013C8 2FD  
004013C9 2FE  
004013CA 2FF  
004013CB 300  
004013CC 301  
004013CD 302  
004013CE 303  
004013CF 304  
004013D0 305  
004013D1 306  
004013D2 307  
004013D3 308  
004013D4 309  
004013D5 30A  
004013D6 30B  
004013D7 30C  
004013D8 30D  
004013D9 30E  
004013DA 30F  
004013DB 310  
004013DC 311  
004013DD 312  
004013DE 313  
004013DF 314  
004013E0 315  
004013E1 316  
004013E2 317  
004013E3 318  
004013E4 319  
004013E5 31A  
004013E6 31B  
004013E7 31C  
004013E8 31D  
004013E9 31E  
004013EA 31F  
004013EB 320  
004013EC 321  
004013ED 322  
004013EE 323  
004013EF 324  
004013F0 325  
004013F1 326  
004013F2 327  
004013F3 328  
004013F4 329  
004013F5 32A  
004013F6 32B  
004013F7 32C  
004013F8 32D  
004013F9 32E  
004013FA 32F  
004013FB 330  
004013FC 331  
004013FD 332  
004013FE 333  
004013FF 334  
00401400 335  
00401401 336  
00401402 337  
00401403 338  
00401404 339  
00401405 33A  
00401406 33B  
00401407 33C  
00401408 33D  
00401409 33E  
0040140A 33F  
0040140B 340  
0040140C 341  
0040140D 342  
0040140E 343  
0040140F 344  
00401410 345  
00401411 346  
00401412 347  
00401413 348  
00401414 349  
00401415 34A  
00401416 34B  
00401417 34C  
00401418 34D  
00401419 34E  
0040141A 34F  
0040141B 350  
0040141C 351  
0040141D 352  
0040141E 353  
0040141F 354  
00401420 355  
00401421 356  
00401422 357  
00401423 358  
00401424 359  
00401425 35A  
00401426 35B  
00401427 35C  
00401428 35D  
00401429 35E  
0040142A 35F  
0040142B 360  
0040142C 361  
0040142D 362  
0040142E 363  
0040142F 364  
00401430 365  
00401431 366  
00401432 367  
00401433 368  
00401434 369  
00401435 36A  
00401436 36B  
00401437 36C  
00401438 36D  
00401439 36E  
0040143A 36F  
0040143B 370  
0040143C 371  
0040143D 372  
0040143E 373  
0040143F 374  
00401440 375  
00401441 376  
00401442 377  
00401443 378  
00401444 379  
00401445 37A  
00401446 37B  
00401447 37C  
00401448 37D  
00401449 37E  
0040144A 37F  
0040144B 380  
0040144C 381  
0040144D 382  
0040144E 383  
0040144F 384  
00401450 385  
00401451 386  
00401452 387  
00401453 388  
00401454 389  
00401455 38A  
00401456 38B  
00401457 38C  
00401458 38D  
00401459 38E  
0040145A 38F  
0040145B 390  
0040145C 391  
0040145D 392  
0040145E 393  
0040145F 394  
00401460 395  
00401461 396  
00401462 397  
00401463 398  
00401464 399  
00401465 39A  
00401466 39B  
00401467 39C  
00401468 39D  
00401469 39E  
0040146A 39F  
0040146B 3A0  
0040146C 3A1  
0040146D 3A2  
0040146E 3A3  
0040146F 3A4  
00401470 3A5  
00401471 3A6  
00401472 3A7  
00401473 3A8  
00401474 3A9  
00401475 3AA  
00401476 3AB  
00401477 3AC  
00401478 3AD  
00401479 3AE  
0040147A 3AF  
0040147B 3B0  
0040147C 3B1  
0040147D 3B2  
0040147E 3B3  
0040147F 3B4  
00401480 3B5  
00401481 3B6  
00401482 3B7  
00401483 3B8  
00401484 3B9  
00401485 3BA  
00401486 3BB  
00401487 3BC  
00401488 3BD  
00401489 3BE  
0040148A 3BF  
0040148B 3C0  
0040148C 3C1  
0040148D 3C2  
0040148E 3C3  
0040148F 3C4  
00401490 3C5  
00401491 3C6  
00401492 3C7  
00401493 3C8  
00401494 3C9  
00401495 3CA  
00401496 3CB  
00401497 3CC  
00401498 3CD  
00401499 3CE  
0040149A 3CF  
0040149B 3D0  
0040149C 3D1  
0040149D 3D2  
0040149E 3D3  
0040149F 3D4  
004014A0 3D5  
004014A1 3D6  
004014A2 3D7  
004014A3 3D8  
004014A4 3D9  
004014A5 3DA  
004014A6 3DB