



# Practical Malware Analysis & Triage

## Malware Analysis Report

Ransomware.wannacry.exe

Jan 2022 | Lanzo | v1.0



# Table of Contents

Table of Contents .....	2
Executive Summary .....	3
High-Level Technical Summary .....	4
Malware Composition.....	5
Ransomware.wannacry.exe .....	Errore. Il segnalibro non è definito.
Basic Static Analysis.....	6
Basic Dynamic Analysis .....	7
Advanced Static Analysis.....	11
Advanced Dynamic Analysis.....	12
Indicators of Compromise .....	13
Network Indicators .....	13
Host-based Indicators .....	14
Rules & Signatures.....	16
Appendices.....	17
A. Yara Rules .....	17
B. Callback URLs .....	17
C. Decompiled Code Snippets .....	18

## Executive Summary

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

Wannacry is a ransomware malware compiled in C++ that runs on x64 and x86 Windows OS.

The sample consist of a main payload that unpacks an additional payload, the malware then encrypts your files then demand ransom payments to unlock those files.

It also have worm capability and try to propagate itself using EternalBlue SMB Exploit.

Symptoms of infection include :

- Files are encrypted using the .WNRy extension
- Changed wallpaper on the infected host
- A Program windows explicitly telling the host is infected and the files encrypted and asking for a ransom with a countdown times and a payment link
- @WanaDecryptor@ executable and a @Please\_Read\_Me@ files on the desktop
- A hidden directory C:\ProgramData\ and a new service with the same name used for persistence
- A service listening on port 9050 taskche.exe

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.

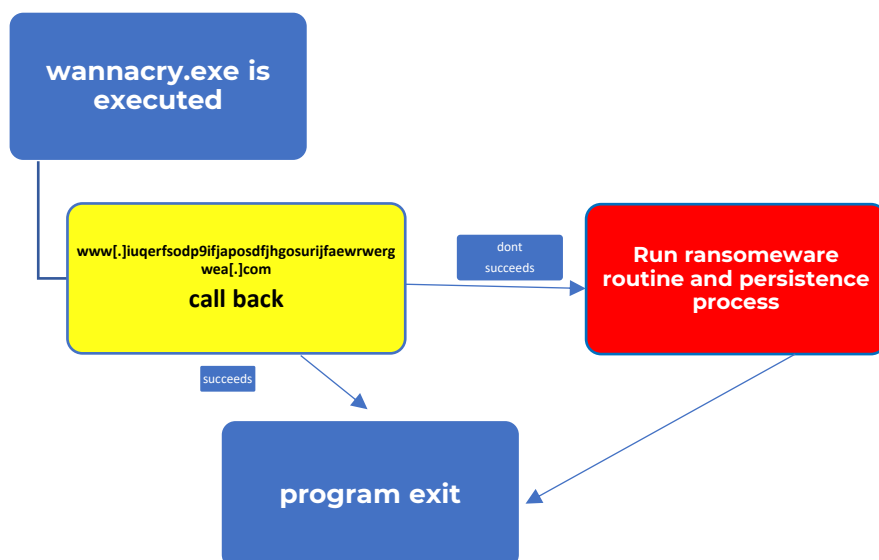


## High-Level Technical Summary

Wannacry consists of two parts: an encrypted stage 0 dropper and an unpacked and decoded stage 2 command execution program. It first attempts to contact its callback URL

(hxxp[:]//]www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com ) as a kill switch if it succeeds the program just terminate otherwise it unpack the next stage, copy the files in the hidden directory, create the persistence process and run the crypto routine.

r





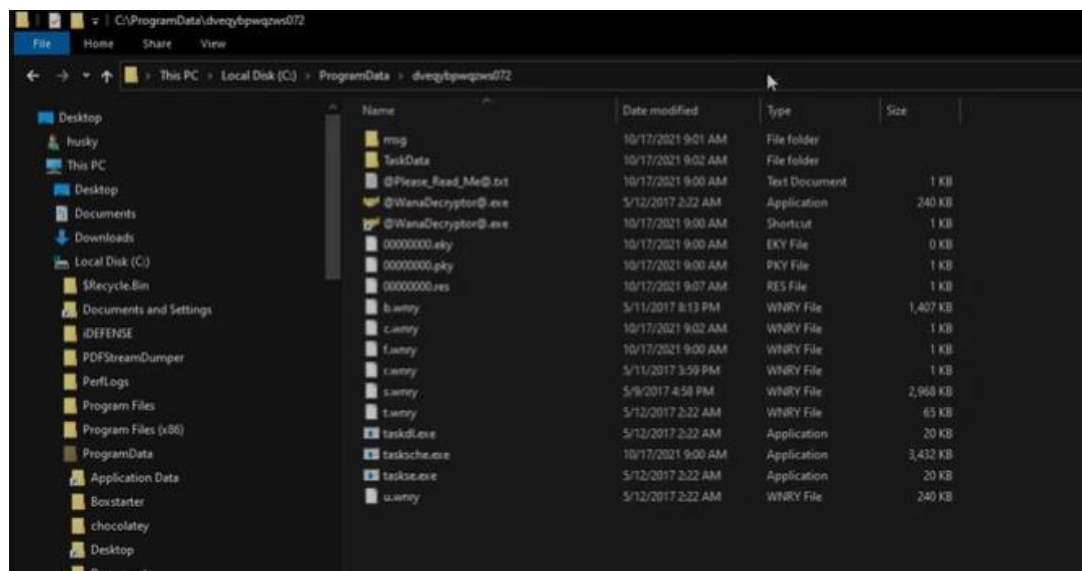
# Malware Composition

DemoWare consists of the following components:

File Name	SHA256 Hash
Ransomware.wannacry.exe	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

**Ransomware.wannacry.exe** The initial executable that runs if the callback URL fails.

Hidden files created by the second stage in C:\ProgramData\ with random name.





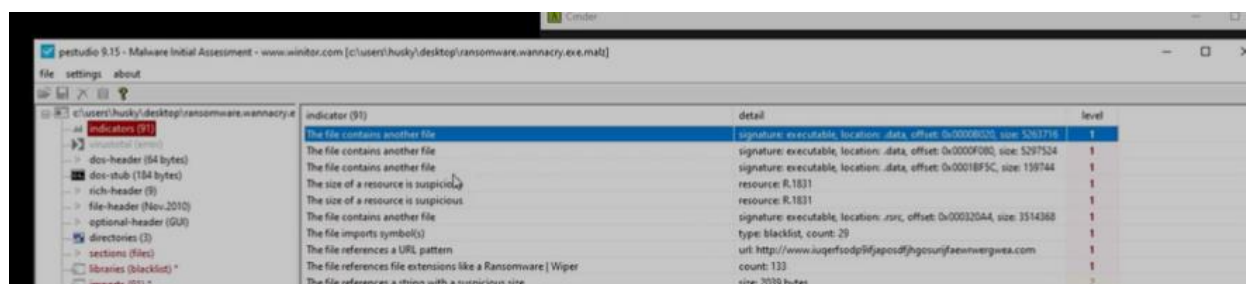
## Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

```
%d.%d.%d.%d
mssecsvc2.0
Microsoft Security Center (2.0) Service
%$ -m security
C:\%$%geriuwjhrf.
C:\%$%$
tasksche.exe
CloseHandle
WriteFile
CreateFileA
CreateProcessA
http://www.luqerfsodp9ifjaposdfjhgosurijfaewrgwea.com
!This program cannot be run in DOS mode.
+j8&LZ661A??~
f""D~**f
V22dN::t

CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
115p7UMNgoj1pHvkpH1jcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AABisjr65Mw
13AM4VW2dhxYgXeQepoHkH5Quy6NGaEb94
GlobalVMsWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
icaccls . /grant Everyone:F /T /C /Q
attrib +h .
Wicry@2017
```

We can see the URL, a path with %s string replacement, cmd command execution , directory attribute permission modifier and +h hidden attribute , some crypto API call and the suspicious 'look alike' windows process tasksche.exe.



This sample contain another file packed, many encryption API call and as indicator we have “ The file references file extensions like a Ransomware | Wiper.

One of the API call is InternetOpenA, probably the API used to reach the killswitch URL.

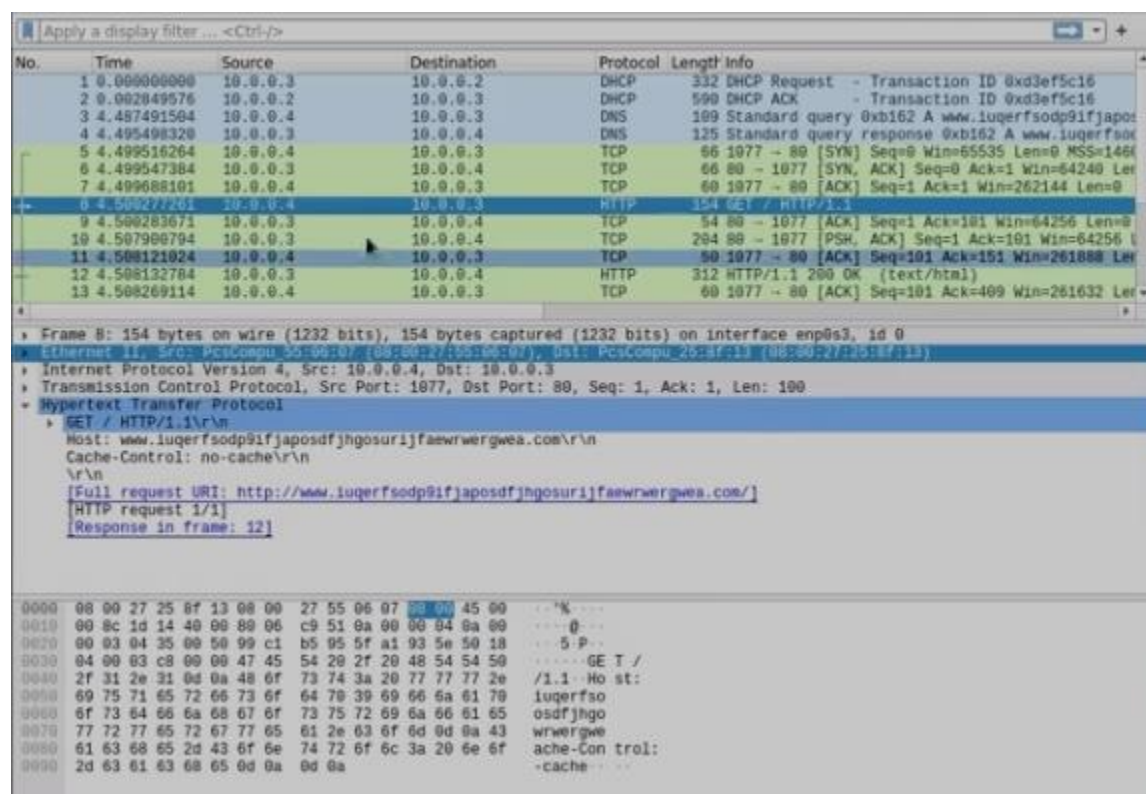


## Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

### Detonation with Remnux as Internet simulator

Running the sample with Administrator Privilege with Remnux as internet service emulator using Wireshark and Procmon as soon as the URL respond the sample just terminated execution.





Detonating the sample without an internet simulator we can see the DNS request fail and the malware continue the execution.

Many call on SMB port 445 to different local host addresses ( EternalBlue exploit )

This process listening on port 9050

Ransomware.wannacry.exe  
Jan 2022  
v1.0

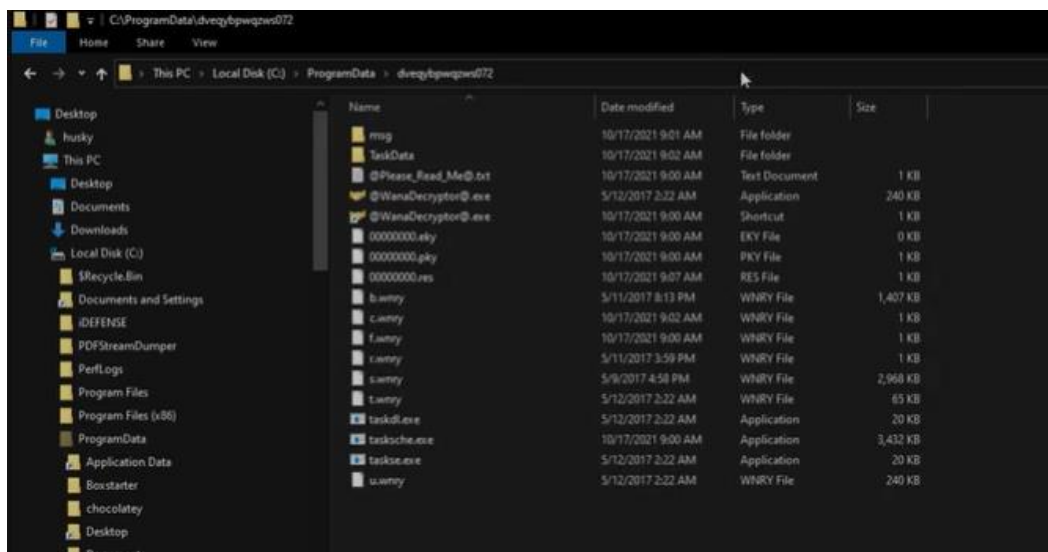


[illegible][illegible]

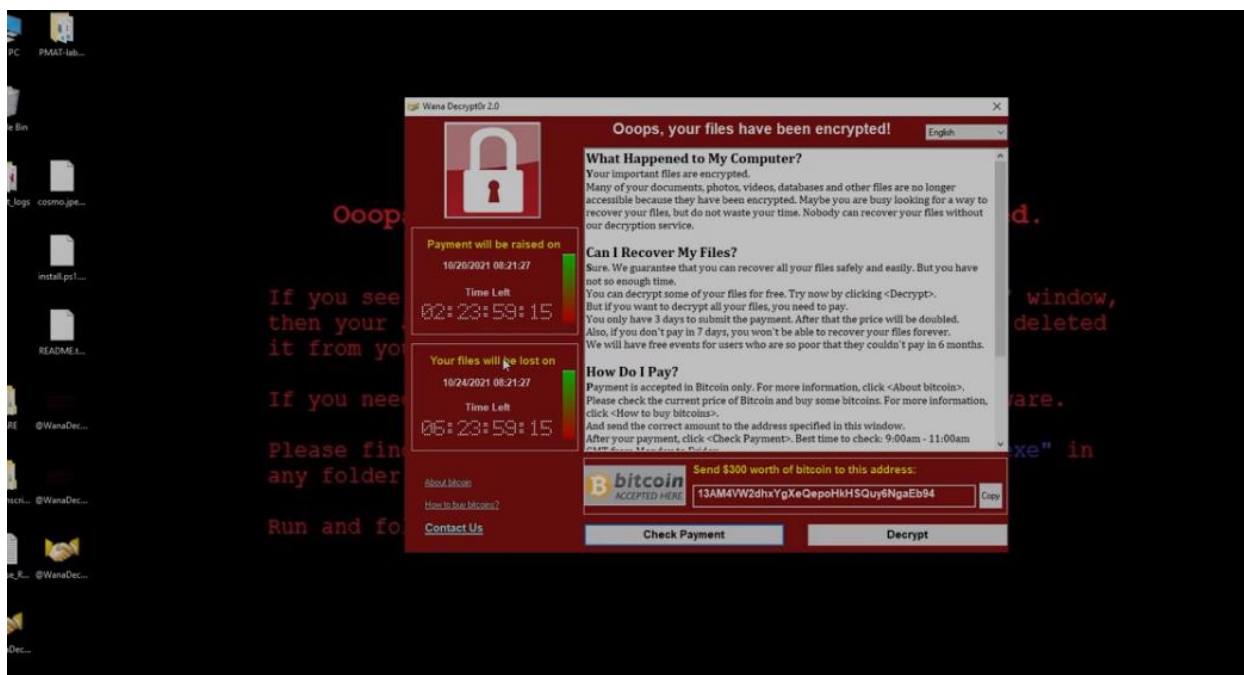
Ransomware.wannacry.exe  
Jan 2022  
v1.0



Following the process Tree we can see it create a folder with a random name with all the unpacked files.



At the end we can see that our wallpaper changed and a program start saying that all our files are being encrypted and we have a limited time to pay the ransom to get them back.



Ransomware.wannacry.exe  
Jan 2022  
v1.0



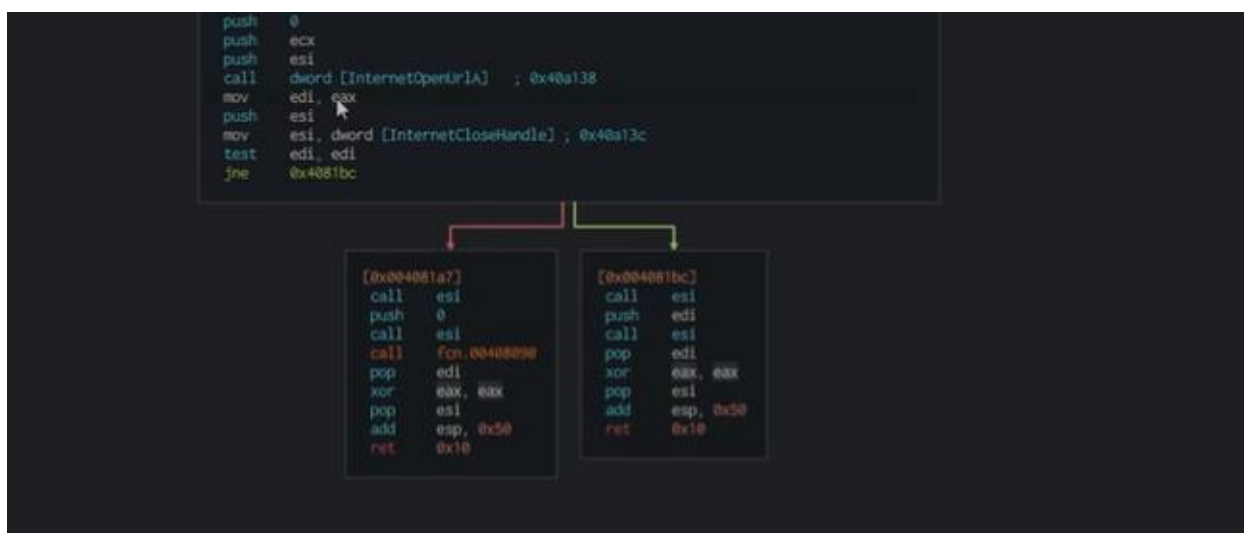
# Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}

In Cutter we can see the string with the URL being loaded in ESI register and then used in InternetOpenA API call.

```
[0x00408140]  
139: int main (int argc, char **argv, char **envp);  
; var int32_t var_14h @ esp+0x28  
; var int32_t var_18h @ esp+0x3c  
; var int32_t var_1ch @ esp+0x50  
; var int32_t var_20h @ esp+0x64  
; var int32_t var_24h @ esp+0x78  
; var int32_t var_28h @ esp+0x8c  
; var int32_t var_2ch @ esp+0xa0  
; var int32_t var_30h @ esp+0xb4  
; var int32_t var_34h @ esp+0xc8  
; var int32_t var_38h @ esp+0xdc  
sub esp, 0x50  
push esi  
push edi  
mov ecx, 0x0  
mov esi, str:http://www.lugersodp01fjapodfjg0sur1jfanwvewgwa.com ; 0x4313db  
lea edi, [var_8h]  
xor eax, eax  
rep movsd dword es:[edi], dword ptr [esi]  
mov 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  
mov byte [var_66h], al  
call dword [InternetOpenA] ; 0x40a134  
push 0  
push 0x00000000
```

The result of the API Call is tested before taking the JNE in “test edi, edi” before the killer switch, if it is true the program terminate ( 0x004081bc) otherwise the program before quit call the function 00408090 and run the rest of the program ( 0x004081a7)





# Advanced Dynamic Analysis

{Screenshots and description about advanced dynamic artifacts and methods}

Using x32dbg we can change the execution modifying the ZF zero flag set before the JNE, this way even if the URL is reached and ZF is not set we can change this right before the JNE e execute the rest of the program.



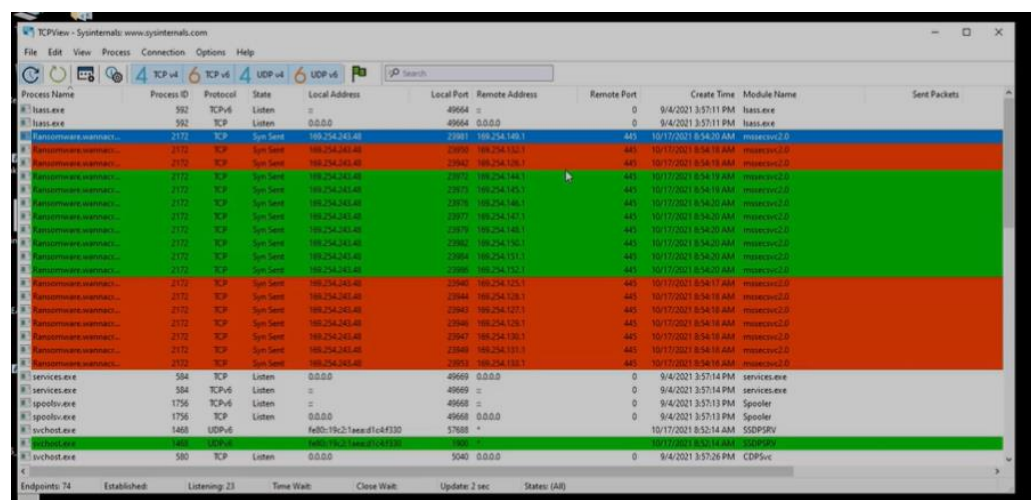
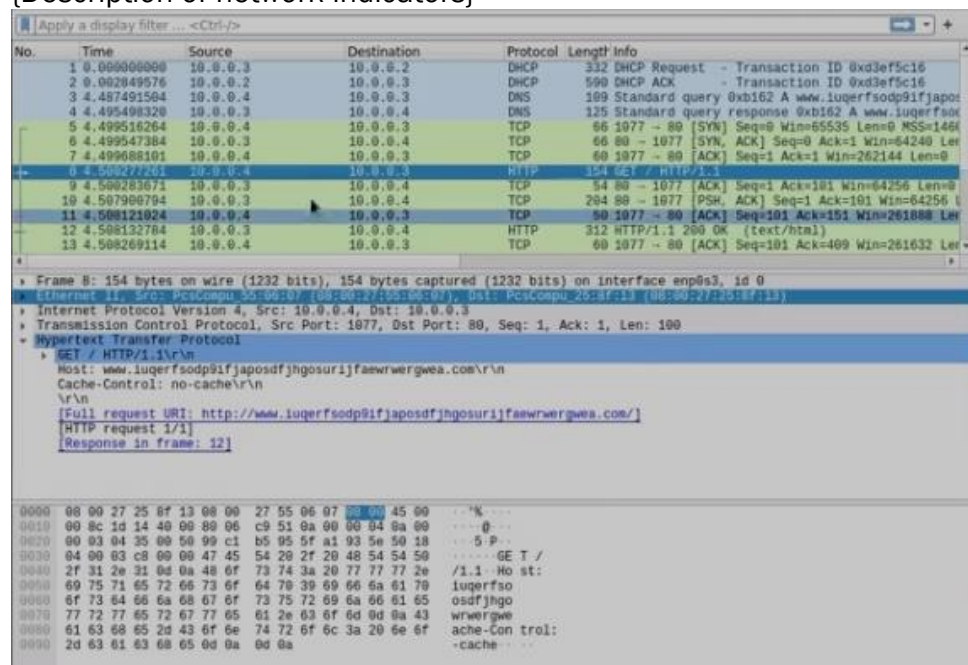


# Indicators of Compromise

The full list of IOCs can be found in the Appendices.

## Network Indicators

{Description of network indicators}



Ransomware.wannacry.exe  
Jan 2022  
v1.0



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent #
wininit.exe	492	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	9/4/2021 3:57:11 PM	wininit.exe	
wininit.exe	492	TCPv6	Listen	::	49665	::	0	9/4/2021 3:57:11 PM	wininit.exe	
taskhsvc.exe	1028	TCP	Listen	127.0.0.1	9050	0.0.0.0	0	10/17/2021 8:57:23 AM	taskhsvc.exe	
taskhsvc.exe	1028	TCP	Established	127.0.0.1	30305	127.0.0.1	30306	10/17/2021 8:57:23 AM	taskhsvc.exe	
taskhsvc.exe	1028	TCP	Established	127.0.0.1	30306	127.0.0.1	30305	10/17/2021 8:57:23 AM	taskhsvc.exe	
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0	9/4/2021 3:57:13 PM	System	

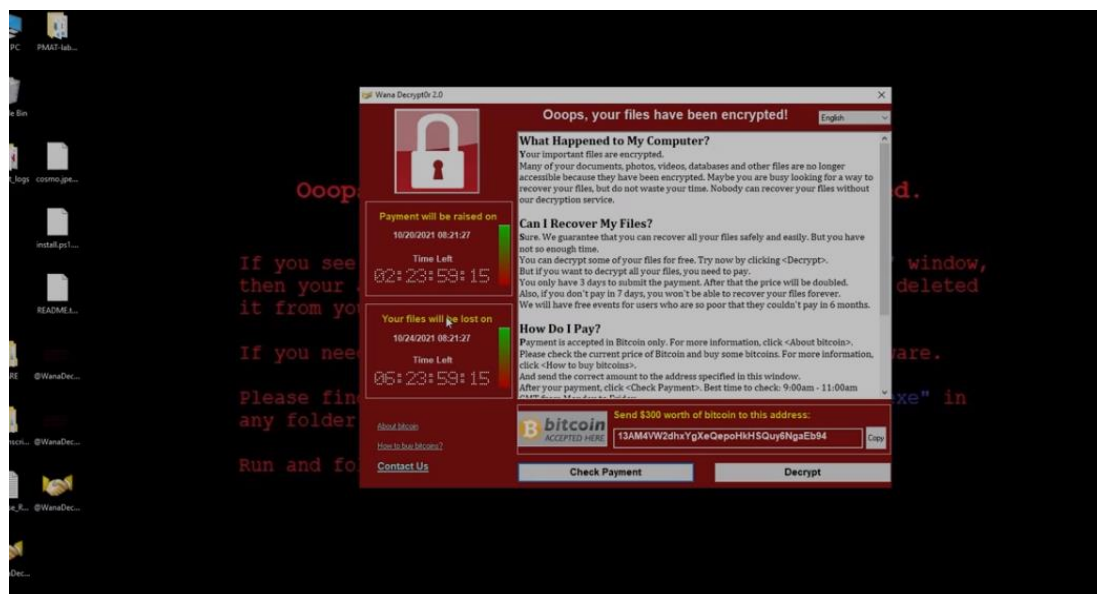
## Host-based Indicators

{Description of host-based indicators}

Name	Date modified	Type	Size
TaskData	10/17/2021 9:01 AM	File folder	
@Please_Read_Me.txt	10/17/2021 9:00 AM	Text Document	1 KB
@WanaDecryptor.exe	5/12/2017 2:22 AM	Application	240 KB
@WanaDecryptor.exe	10/17/2021 9:00 AM	Shortcut	1 KB
00000000.wky	10/17/2021 9:00 AM	WKY File	0 KB
00000000.pky	10/17/2021 9:00 AM	PKY File	1 KB
00000000.res	10/17/2021 9:07 AM	RES File	1 KB
b.wmy	5/11/2017 8:13 PM	WMRY File	1,407 KB
c.wmy	10/17/2021 9:02 AM	WMRY File	1 KB
f.wmy	10/17/2021 9:00 AM	WMRY File	1 KB
g.wmy	5/11/2017 3:59 PM	WMRY File	1 KB
h.wmy	5/9/2017 4:58 PM	WMRY File	2,968 KB
i.wmy	5/12/2017 2:22 AM	WMRY File	65 KB
taskdl.exe	5/12/2017 2:22 AM	Application	20 KB
taskdsch.exe	10/17/2021 9:00 AM	Application	3,432 KB
taskse.exe	5/12/2017 2:22 AM	Application	20 KB
u.wmy	5/12/2017 2:22 AM	WMRY File	240 KB

Time	Process Name	PID	Operation	Path	Result	Detail	Start Time
10/17/2021 9:00:43 AM	Ransomware.wannacry.exe	3336	Start	C:\Users\hukky\Desktop\Ransomware.wannacry.exe	Success	Process Name: R	10/17/2021 9:00:43 AM
10/17/2021 9:00:43 AM	Taskhsvc.exe	1028	Start	C:\ProgramData\dwegbpgwqnd072\Taskhsvc.exe	Success	Process Name: R	10/17/2021 9:00:43 AM

Ransomware.wannacry.exe  
Jan 2022  
v1.0



9:00.4	Ransomware.w	2396	Create File	C:\Users\hasky\Desktop\CRYPTBASE.dll	NAME NOT FOUND	Desired Access: R...
9:00.4	Ransomware.w	2396	Create File	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Desired Access: R...
9:00.4	Ransomware.w	2396	Create File	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Desired Access: R...
9:00.4	Ransomware.w	2396	Create File	C:\Users\hasky\Desktop\Ransomware.wannacry.exe	SUCCESS	Desired Access: G...
9:00.4	Ransomware.w	3336	Create File	C:\Windows\TaskSch.exe	NAME NOT FOUND	Desired Access: R...
9:00.4	Ransomware.w	3336	Create File	C:\Windows\TaskSch.exe	SUCCESS	Desired Access: G...
9:00.4	Ransomware.w	3336	Create File	C:\Windows\TaskSch.exe	SUCCESS	Desired Access: R...
9:00.4	Ransomware.w	3336	Create File	C:\Windows\TaskSch.exe	SUCCESS	Desired Access: R...

Ransomware.wannacry.exe  
Jan 2022  
v1.0



## Rules & Signatures

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

{Information on specific signatures, i.e. strings, URLs, etc}

%s -m security

C:\%s\qeriuwjhrf

tasksche.exe

icaccls . /grant Everyone:F /T /C /Q

WNCry@2ol7

` .WNCRY`

- **www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com**
- - CryptGetRandom
- - CryptAcquireContextA
- - InternetOpenA
- - InternetOpenUrl
- - CreateServiceA
- - ChangeServiceConfig2A





# Appendices

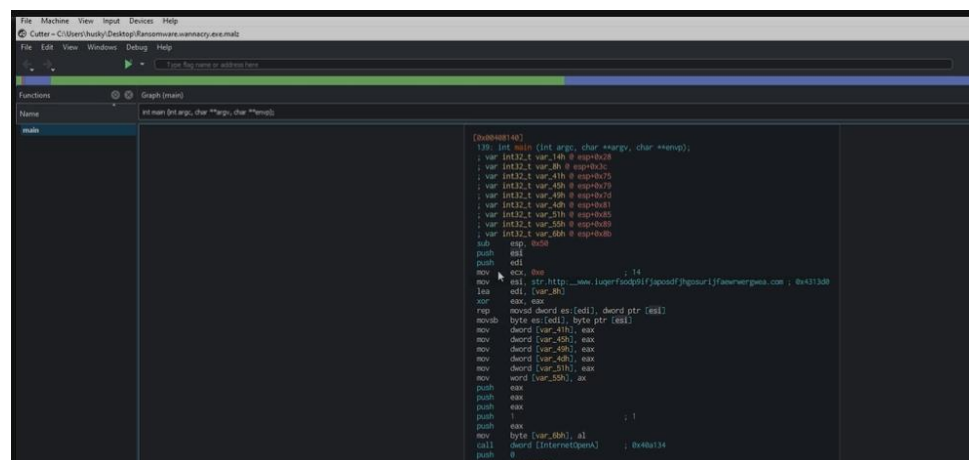
## A. Yara Rules

```
rule Wannacry_rules {  
  
    meta:  
        last_updated = "2022-01-30"  
        author = "Lanzo"  
        description = "Wannacry rules"  
  
    strings:  
        // rules  
        $string1 = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwea.com" ascii  
        $string2 = "tasksche.exe" ascii  
        $PE_magic_byte = "MZ"  
  
    condition:  
        // Conditions  
        $PE_magic_byte at 0 and  
        ($string1 and $string2)  
}
```

```
C:\Users\lanzo\Desktop  
λ yara32 wannacry_rule.yara Ransomware.wannacry.exe.malz -s -w -p 32  
Wannacry_rules Ransomware.wannacry.exe.malz  
0x313d7:$string1: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwea.com  
0x3136c:$string2: tasksche.exe  
0x4157c:$string2: tasksche.exe  
0x0:$PE_magic_byte: MZ
```

## B. Callback URLs

Domain	Port
www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwea[.]com	80

[illegible]

Ransomware.wannacry.exe  
Jan 2022  
v1.0