



Practical Malware Analysis & Triage

Malware Analysis Report

Ransomware: WannaCry

by: scruffylord

Executive Summary

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

WannaCry is a widely known ransomware that was initially released in 2017. Basically Wannacry will encrypt a device's files and also tries to traverse the network to encrypt other devices. WannaCry attempts to locate other hosts through the protocol SMB.

I have the WannaCry malware located in a safe and secure lab. Below will be the full analysis of the malware and the results I have discovered.

Enjoy !

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

High-Level Technical Summary

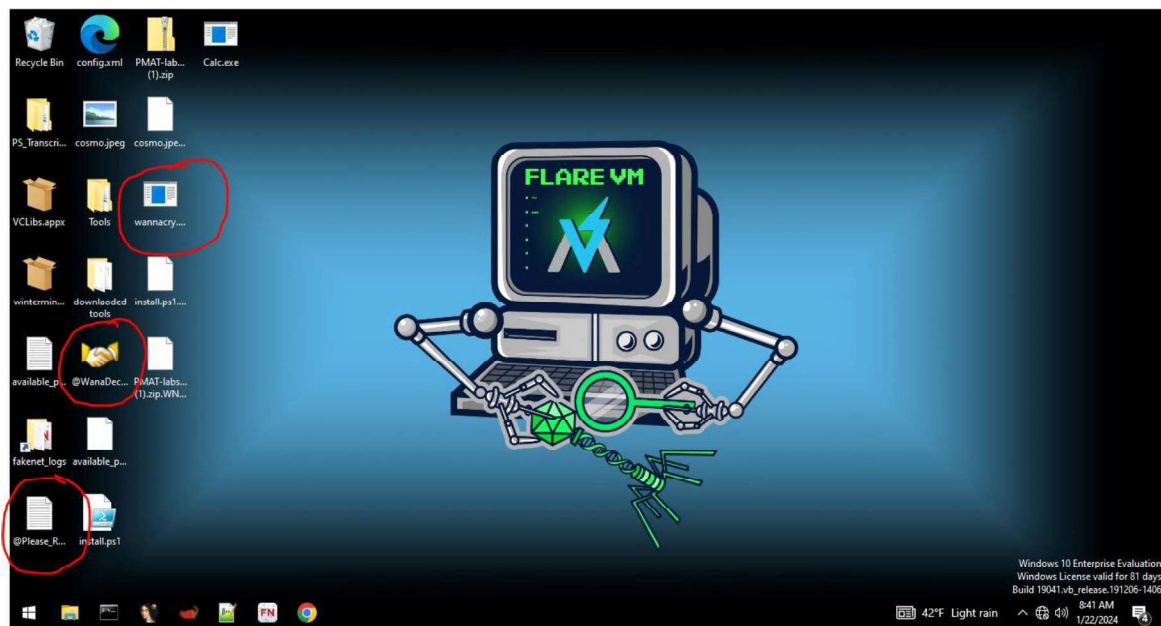
WannaCry is a ransomware cryptoworm, which targets computers running the Microsoft Windows operating system by encrypting (locking) data and demanding ransom

payments in the Bitcoin cryptocurrency. The worm is also known as WannaCrypt, Wana Decrypt0r 2.0, WanaCrypt0r 2.0, and Wanna Decryptor.

Initial Malware detonation

I first wanted to test what exactly happens at the ground level whenever the malware is detonated (without a network connection).

Here are the findings:



After the initial detonation you will see a few icons and files appear on the desktop.



Then only after a few seconds the main message/image appear demanding payment. This payment is demanding \$300 worth of bitcoin. After this point all the files are encrypted. Also tools can longer be accessed.

Static Analysis

The following information was received by a variety of tools. Tools utilized in this part of the analysis are **PView**, **Pestudio**, **CAPA**. The tool **FLOSS** was also used to take a look at the strings.

FileName:

Ransome.WannaCry.exe

SHA25 hash : *24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c*

VirusTotal Results:

<https://www.virustotal.com/gui/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c>

67 security vendors and 5 sandboxes flagged this file as malicious

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

File name: Ransome.WannaCry.exe

Size: 3.55 MB

Last Analysis Date: 13 hours ago

File type: EXE

peexe malware micro-creator runtime-modules detect-debug-environment checks-network-adapters exploit cve-2017-0147 long-shells direct-gpu-clock-access checks-user-input cve-2017-0144

Community Score: 67/69

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30

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

Popular threat label: trojan.ransome.wanna

Threat categories: trojan ransomware worm

Family labels: wannacry wannacryptor

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan.Win32.WannaCryptor.R200572
Alibaba	Ransom.Win32.WannaCry.398	ALYac	Trojan.Ransom.WannaCryptor
Antiy-AVL	Trojan.Exploit.Win32.CVE-2017-0147	Arcabit	Trojan.Ransom.WannaCryptor.H
Avast	SFWNChyLib-A [Trj]	AvG	SFWNChyLib-A [Trj]
Avira (no cloud)	TR/Ransom.QZ	Baidu	Win32/Worm.Rbot.a
BitDefender	Trojan.Ransom.WannaCryptor.H	BitDefender Theta	Gen:NNLZeuaf.3a680_808aefb0mpl
Blue Pro	W32.RunasMopeal/Trojan	ClamAV	Win.Ransome.Wanna-975998b-0
CrowdStrike Falcon	Win/malicious_confidence_100%_00	Cyberason	Malicious.a988f
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInsect	MALICIOUS	DrWeb	Trojan.Encoder.11432
Elastic	Malicious (high confidence)	emmssoft	Trojan.Ransom.WannaCryptor (A)
eScan	Trojan.Ransom.WannaCryptor.H	ESET-NOD32	Win32/Exploit.CVE-2017-0147.A
Fortinet	W32/RANSOM.Atr	GGData	Win32.Trojan.Ransom.WannaCry.D

67 vendors have identified this to be Ransmoeware. Including Crowdstrike, Bitdefender and Fortinet. Who are very reliable vendors in the cybersecurity space.

Interesting/Suspicious strings:

- `hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com` (defanged url)
- `tasksche.exe`
- `cmd.exe /c %s`
- `%s -m security`
- `WanaCrypt0r`
- `diskpart.exe`
- `W192.168.56.20WIPC$`
- `W172.16.99.5WIPC$`
- `Microsoft Security Center (2.0) Service`
- **This Program cannot be run in DOS Mode**

(This string indicates that there were more executables packed into the binary.)

Here is are snippets from the Floss Results :

```

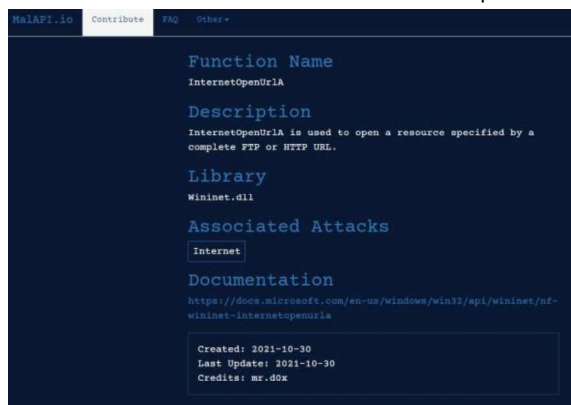
floss.txt - Notepad
File Edit Format View Help
>"u:F
XPVSS
Sleep
GetTickCount
QueryPerformanceCounter
QueryPerformanceFrequency
GlobalFree
GlobalAlloc
InitializeCriticalSection
LeaveCriticalSection
EnterCriticalSection
InterlockedDecrement
CloseHandle
TerminateThread
WaitForSingleObject
InterlockedIncrement
GetCurrentThreadId
GetCurrentThread
ReadFile
GetFileSize
CreateFileA
MoveFileExA
SizeofResource
LockResource
LoadResource
FindResourceA
GetProcAddress
GetModuleHandleW
ExitProcess
GetModuleFileNameA
LocalFree
LocalAlloc
KERNEL32.dll
CryptAcquireContextA
CryptGenRandom
StartServiceA
CloseServiceHandle
CreateServiceA
OpenSCManagerA
SetServiceStatus
ChangeServiceConfig2A
RegisterServiceCtrlHandlerA
StartServiceCtrlDispatcherA
OpenServiceA
ADVAPI32.dll
WS2_32.dll
??1_Lockit@std@@QAE@XZ
??0_Lockit@std@@QAE@XZ
MSVCP60.dll
GetPerAdapterInfo
GetAdaptersInfo
iphlpapi.dll
InternetCloseHandle
InternetOpenUrlA
InternetOpenA
WININET.dll
_ftol
sprintf
_endthreadex
strncpy
rand
GetModuleHandleA
GetStartupInfoA
_stricmp
!This program cannot be run in DOS mode.
Rich9
.text
.rdata
@.data
.rsrc
@.reloc
QVWh
@h80
X[_^Y
PRRrh
RRRrh80
t\tWVS
MWVS
u7WVS
u&WVS
_^[
CloseHandle
WriteFile
CreateFileA
SizeofResource
LockResource
LoadResource
FindResourceA
CreateProcessA
KERNEL32.dll
sprintf
MSVCRT.dll
free
_initterm
malloc
_adjust_fdiv
launcher.dll
PlayGame
C:\%s\%s
WINDOWS
mssecsvc.exe
!This program cannot be run in DOS mode.
/4ND/4ND/4ND4
nl nnnn

```

Suspicious API calls:

- IsDebuggerPresent
- StartService
- CreateService
- RegCreateKey
- RegSetValue
- InternetOpenA
- InternetOpenURL

Some of these API calls were compared on the this website: <https://malapi.io/>



CAPA Results during Static Analysis :

CAPA C:\Users\scruffy\Desktop\Ransomware.WannaCry.exe.malz	
md5	db349b97c37d22f5ea1d1841e3c89eb4
sha1	e889544aff85ffaf8b0d0da705105dee7c97fe26
sha256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
os	windows
format	pe
arch	i386
path	C:/Users/scruffy/Desktop/Ransomware.wannacry.exe.malz
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	Conditional Execution::Runs as Service [B0025.007] Debugger Detection::Timing/Delay Check QueryPerformanceCounter [B0001.033]
ANTI-STATIC ANALYSIS	Executable Code Obfuscation::Argument Obfuscation [B0032.020] Executable Code Obfuscation::Stack Strings [B0032.017]
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] Socket Communication::Connect Socket [C0001.004] Socket Communication::Create TCP Socket [C0001.011] Socket Communication::Create UDP Socket [C0001.010] Socket Communication::Get Socket Status [C0001.012] Socket Communication::Initialize Winsock Library [C0001.009] Socket Communication::Receive Data [C0001.006] Socket Communication::Send Data [C0001.007] Socket Communication::Set Socket Config [C0001.001] Socket Communication::TCP Client [C0001.008]
CRYPTOGRAPHY	Generate Pseudo-random Sequence::Use API [C0021.003]
DATA	Compression Library [C0060]
DISCOVERY	Analysis Tool Discovery::Process detection [B0013.001] Code Discovery::Inspect Section Memory Permissions [B0046.002] File and Directory Discovery [E1083]
EXECUTION	Install Additional Program [B0023]
FILE SYSTEM	Move File [C0063] Read File [C0051]
PROCESS	Create Thread [C0038] Terminate Process [C0018] Terminate Thread [C0039]

Capability	Namespace
reference analysis tools strings	anti-analysis
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
extract resource via kernel32 functions	executable/resource
contain an embedded PE file	executable/subfile/pe
get file size	host-interaction/file-system/meta
move file	host-interaction/file-system/move
read file on Windows	host-interaction/file-system/read
get number of processors	host-interaction/hardware/cpu
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 on Windows	linking/runtime-linking
linked against ZLIB	linking/static/zlib
inspect section memory permissions	load-code/pe
persist via Windows service	persistence/service

CAPA provided tons of information on the capability of this malware. If you take a look at the "namespace" section you will see very suspicious items, just to name a few :

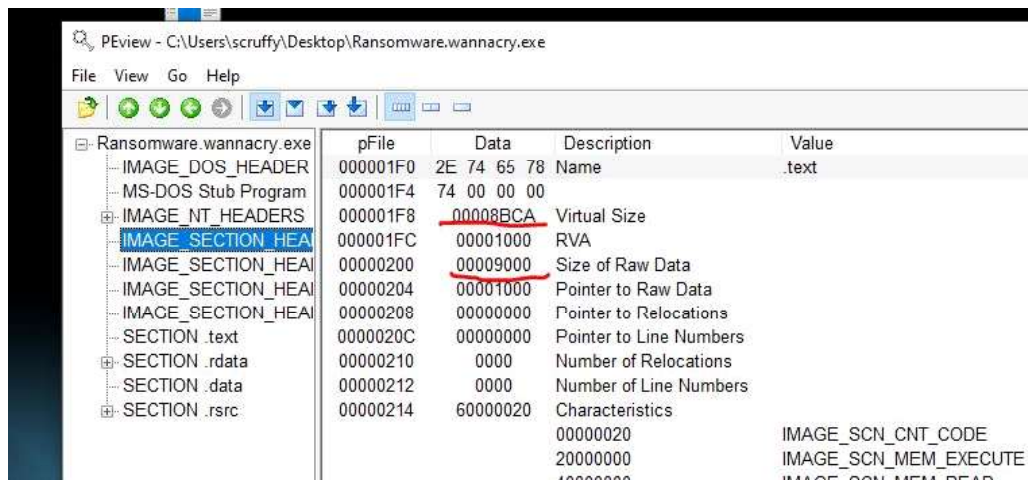
Anti-analysis

Anti-debugging

Persistence

Data-manipulation

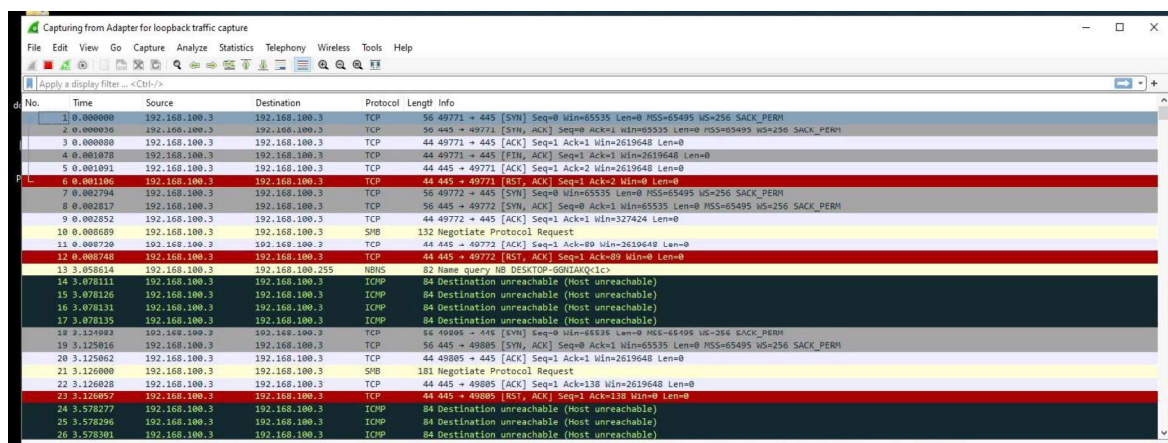
After review of PEView I was able to ascertain that this looks to be Packed Malware, In order to do this you need to compare the Virtual Size to the Size of Raw Data. Packed malware is used by threat actors in order to obfuscate programs so they cannot be analyzed by anti-virus softwares.



Dynamic Analysis

Now I wanted to detonate the malware with TCPview and Wireshark (Without Internet).

We can see the malware trying to reach out here:



The screenshot shows the TCPView application window with the following data:

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	820	TCP	Listen	0.0.0.0	135	0.0.0.0	0	1/20/2024 1:36:08 PM	RpcSs
System	4	TCP	Listen	192.168.100.3	139	0.0.0.0	0	1/22/2024 10:28:49 AM	System
svchost.exe	684	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	1/20/2024 1:36:15 PM	CDPSvc
lsass.exe	620	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	1/20/2024 1:36:08 PM	lsass.exe
wininit.exe	532	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	1/20/2024 1:36:08 PM	wininit.exe
svchost.exe	52	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	1/20/2024 1:36:08 PM	EventLog
svchost.exe	996	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	1/20/2024 1:36:09 PM	Schedule
spoolsv.exe	1804	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	1/20/2024 1:36:10 PM	Spooler
services.exe	612	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	1/20/2024 1:36:10 PM	services.exe
svchost.exe	2036	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	1/20/2024 1:36:11 PM	PolicyAgent
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49746	192.168.100.36	445	1/22/2024 10:40:27 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49747	192.168.100.57	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49748	192.168.100.58	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49749	192.168.100.59	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49750	192.168.100.60	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49751	192.168.100.61	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49752	192.168.100.62	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49753	192.168.100.63	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49754	192.168.100.64	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49755	192.168.100.65	445	1/22/2024 10:40:28 AM	mssecvcs2.0
Ransomware.wannacry.exe	5864	TCP	Syn Sent	192.168.100.3	49756	192.168.100.66	445	1/22/2024 10:40:28 AM	mssecvcs2.0
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	1/20/2024 1:36:10 PM	System
svchost.exe	1632	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	1/20/2024 1:36:10 PM	DfsSvc
svchost.exe	620	TCPv6	Listen	::	135	::	0	1/20/2024 1:36:08 PM	RpcSs
System	4	TCPv6	Listen	::	445	::	0	1/20/2024 1:36:10 PM	System
svchost.exe	1632	TCPv6	Listen	::	7680	::	0	1/20/2024 1:36:10 PM	DfsSvc
lsass.exe	620	TCPv6	Listen	::	49664	::	0	1/20/2024 1:36:08 PM	lsass.exe
wininit.exe	532	TCPv6	Listen	::	49665	::	0	1/20/2024 1:36:08 PM	wininit.exe
svchost.exe	52	TCPv6	Listen	::	49666	::	0	1/20/2024 1:36:08 PM	EventLog
svchost.exe	996	TCPv6	Listen	::	49667	::	0	1/20/2024 1:36:09 PM	Schedule
spoolsv.exe	1804	TCPv6	Listen	::	49668	::	0	1/20/2024 1:36:10 PM	Spooler
services.exe	612	TCPv6	Listen	::	49669	::	0	1/20/2024 1:36:10 PM	services.exe
svchost.exe	2036	TCPv6	Listen	::	49670	::	0	1/20/2024 1:36:11 PM	PolicyAgent
svchost.exe	1968	UDP	0.0.0.0	*	123	*	0	1/22/2024 10:36:56 AM	W32Time
System	4	UDP	192.168.100.3	*	137	*	0	1/22/2024 10:28:49 AM	System
System	4	UDP	192.168.100.3	*	138	*	0	1/22/2024 10:28:49 AM	System
svchost.exe	996	UDP	0.0.0.0	*	500	*	0	1/20/2024 1:36:10 PM	KEEEXT
svchost.exe	2536	UDP	127.0.0.1	*	1900	*	0	1/22/2024 10:28:47 AM	SSDPsrv
svchost.exe	2536	UDP	192.168.100.3	*	1900	*	0	1/22/2024 10:28:47 AM	SSDPsrv
svchost.exe	1968	UDP	0.0.0.0	*	4011	*	0	1/20/2024 1:36:10 PM	KEEEXT

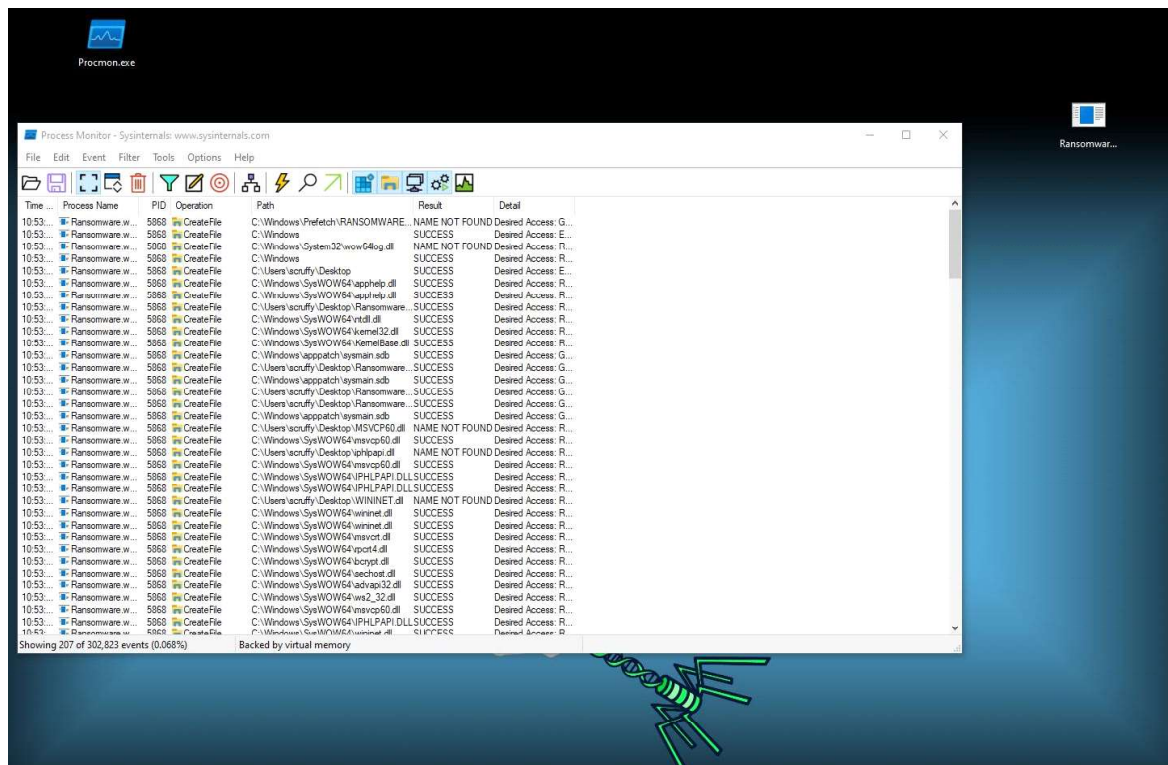
Endpoints: 64 Established: Listening: 22 Time Wait: Close Wait: Update: 2 sec States: (All)

As soon as the malware was detonated it tried to reach out on port 445. The Server Message Block Protocol. This is a network file sharing protocol, and as implemented in Microsoft Windows.

Also in this tool we see a new task created called tasksvc.exe on listening port 9050:

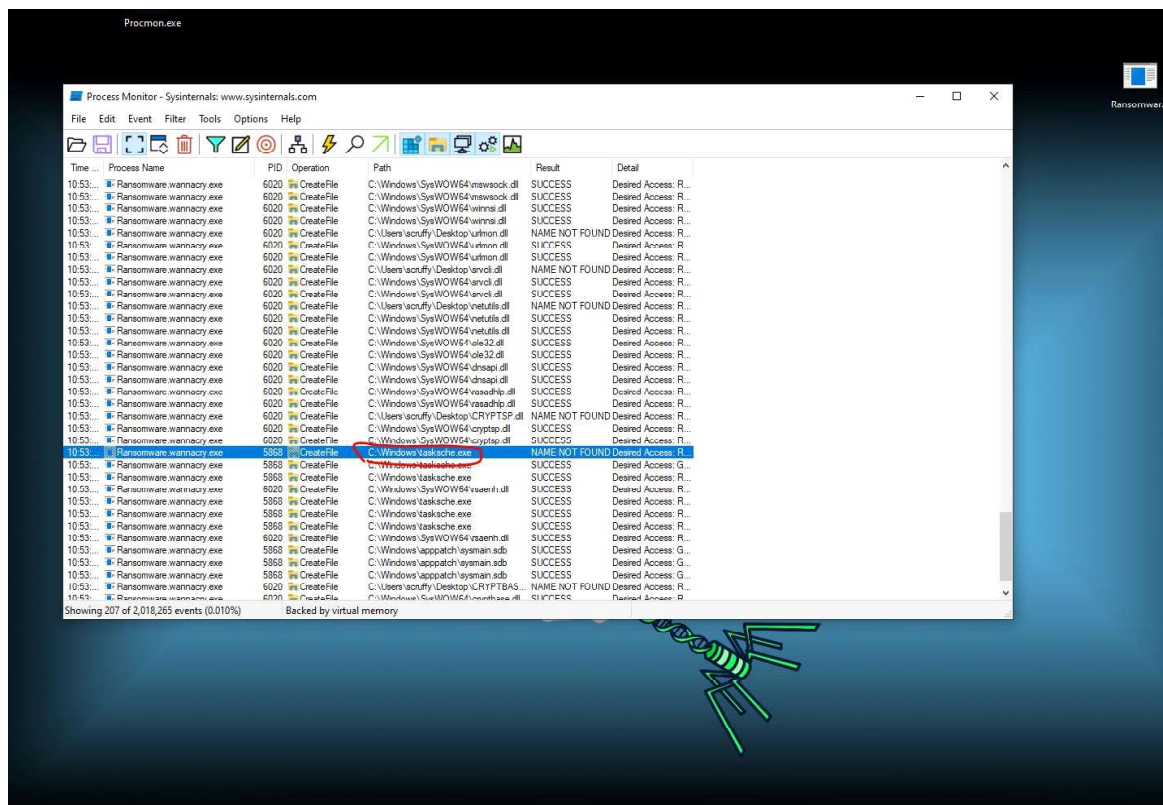
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
tasksvc.exe	1028	TCP	Listen	127.0.0.1	9050	0.0.0.0	0	10/17/2021 8:57:23 AM	tasksvc.exe

Results and findings from Procmon:



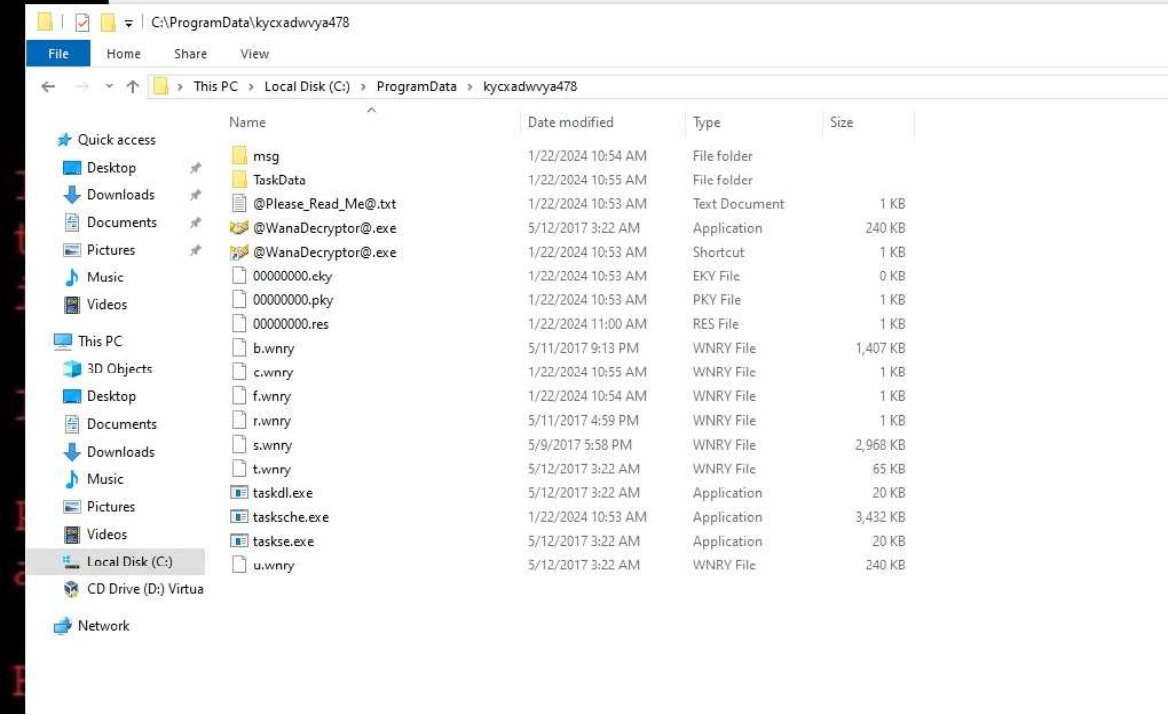
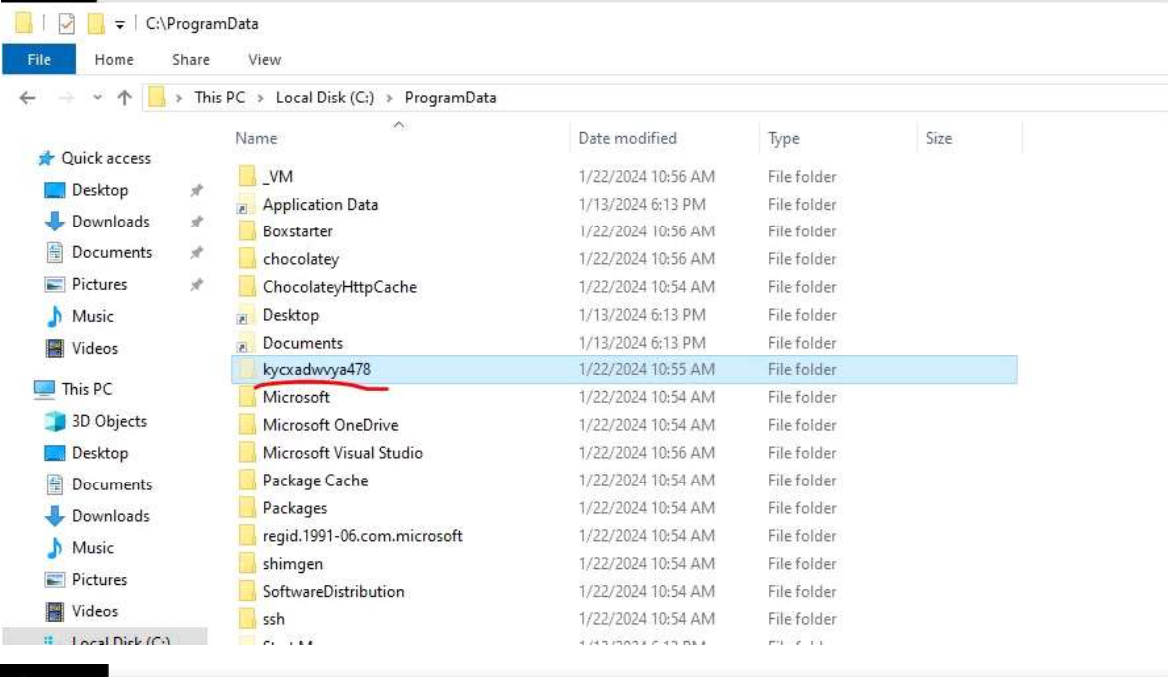
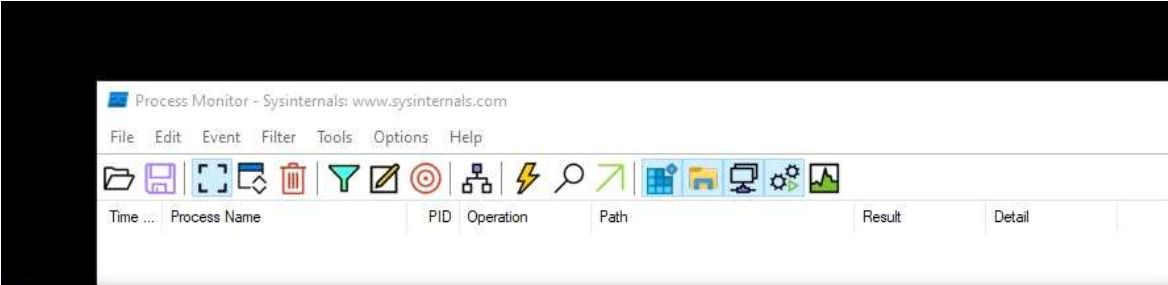
When the malware is detonated we see tons of processes being created and starting to run.

One process that really stands out is C:\Windows\Wtasksche.exe . Most likely this is a second stage payload.



I was able to locate the staging area by finding a strange name directory in procmon:

This is the hidden directory found in the ProgramData directory.



Now I wanted to take a look at the program itself using the tool Tool [~] IDA _~

Here are the results:

```
; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
_WinMain@16 proc near

szUrl= byte ptr -50h
var_17= dword ptr -17h
var_13= dword ptr -13h
var_F= dword ptr -0Fh
var_8= dword ptr -08h
var_7= dword ptr -7
var_3= word ptr -3
var_1= byte ptr -1
hInstance= dword ptr 4
hPrevInstance= dword ptr 8
lpCmdLine= dword ptr 0Ch
nShowCmd= dword ptr 10h

sub     esp, 50h
push    esi
push    edi
mov     ecx, 0Eh
mov     esi, offset aHttpWwwIuqerfs ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
lea     edi, [esp+58h+szUrl]
xor     eax, eax
rep movsd
movsb
mov     [esp+58h+var_17], eax
mov     [esp+58h+var_13], eax
mov     [esp+58h+var_F], eax
mov     [esp+58h+var_8], eax
mov     [esp+58h+var_7], eax
mov     [esp+58h+var_3], ax
push    eax                ; dwFlags
push    eax                ; lpszProxyBypass
push    eax                ; lpszProxy
push    1                  ; dwAccessType
push    eax                ; lpszAgent
mov     [esp+6Ch+var_1], al
call    ds:InternetOpenA ←
push    0                  ; dwContext
push    84000000h          ; dwFlags
push    0                  ; dwHeadersLength
lea     ecx, [esp+64h+szUrl]
mov     esi, eax
push    0                  ; lpszHeaders
push    ecx                ; lpszUrl
push    esi                ; hInternet
call    ds:InternetOpenUrlA ←
mov     edi, eax
push    esi                ; hInternet
mov     esi, ds:InternetCloseHandle ←
test    edi, edi
jnz     short loc_4081BC

call    esi ; InternetCloseHandle
push    0                ; hInternet
call    esi ; InternetCloseHandle
call    sub_408090
pop     edi
xor     eax, eax
pop     esi
add     esp, 50h
retn    10h

loc_4081BC:
call    esi ; InternetCloseHandle
push    edi                ; hInternet
call    esi ; InternetCloseHandle
pop     edi
xor     eax, eax
pop     esi
add     esp, 50h
retn    10h
_WinMain@16 endp
```


Here we can see the main function and the APIs being called. We can see the URL `hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com` loaded into the beginning of the program as well.

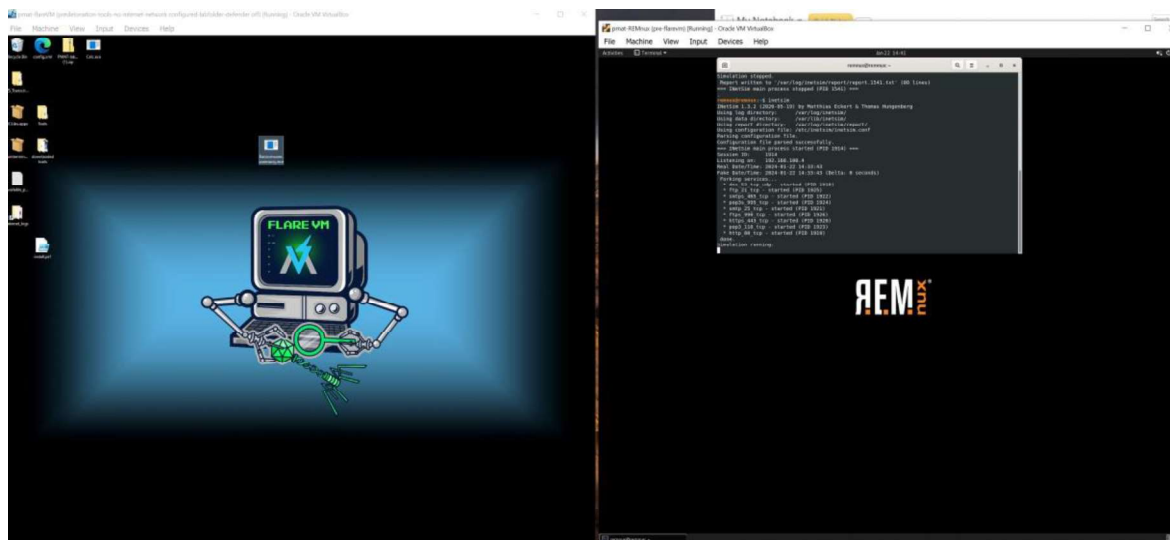
The outcome of the malware being executed depends on two things:

If the result of the API call from `InternetOpenURL` is successful then the malware will go to a specific location in the Memory.

If the result of the API call from `InternetOpenURL` is unsuccessful then the malware will go to a different location. This Function call will detonate the payload and still carry out every other part of the encryption. We have seen this side of the payload already.

Now I wanted to test the results of running the payload with an internet connection.

When the malware executable is run there are no changes to our host desktop. Unlike our first attempt we see files being created and the ransomware note pops up. Please review the screenshot below:



There are no created messages or files after detonation that we can see. Wanna cry will wait to access the URL `hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com` (this is the url defanged) before it begins the encryption payload.

Like discussed before, If the payload **cannot** reach that URL the malware will detonate and encrypt the device. Now after researching WannaCry it is not known for sure why the payload does not detonate after connecting to that URL. Though it is expected that the malware authors did this in order to hide the hide from analyst.

Appendices

- Yara Rules

```
rule RansomWare_WannaCry{
  meta:
    last_update = "2024-01-22"
    author = "scruffylord"
    description = "Yara rule for WannaCry"

  strings:
    $string1 = "%s -m security" ascii
    $string2 = "WNCry@2017" ascii
    $string3 = "wnry" ascii
    $string4 = "WanaCrypt0r" ascii
    $string5 = "%s -m security" ascii
    $PE_magic_byte = "MZ"
    $url = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergrgwea.com" ascii
    $exe = "tasksche" ascii
    $exe = "diskpart"
    $address = "\\192.168.56.20\\IPC$" fullword wide

  condition:
    $MZ_magic_byte at 0 and
    any of them
}
```