



Malware Analysis Report

<https://github.com/j3rmcyber/MalwareAnalysis>

WannaCry Ransomware Malware

Feb 2024 | j3rmcyber | v1.0



Table of Contents	
Table of Contents	2
Executive Summary	3
High-Level Technical Summary	5
Malware Composition.....	6
WannaCry.exe:	6
TaskSche.exe:	6
Taskse.exe:	6
Taskdl.exe:	6
Tasksvc.exe:	6
Basic Static Analysis.....	7
Basic Dynamic Analysis.....	11
Advanced Static Analysis.....	12
Indicators of Compromise	18
Network Indicators	18
Host-based Indicators:	19
Appendices.....	21
A. Yara Rules	21
B. Callback URLs	21



Executive Summary

SHA256 hash	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
-------------	--

WannaCry is a ransomware malware introduced in 2017 that targets Windows computers. The program demands ransom in cryptocurrency (Bitcoin) and encrypts all data on the hard drive. The program will execute, then looks for remote systems to propagate to (worm capabilities). The program is also known as: WannaCrypt, Wana Decryptor 2.0, WanaCrypt0r 2.0, and Wana Decryptor. The program contains packed executables which are dropped upon execution.

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

Dropped files on the desktop after execution:





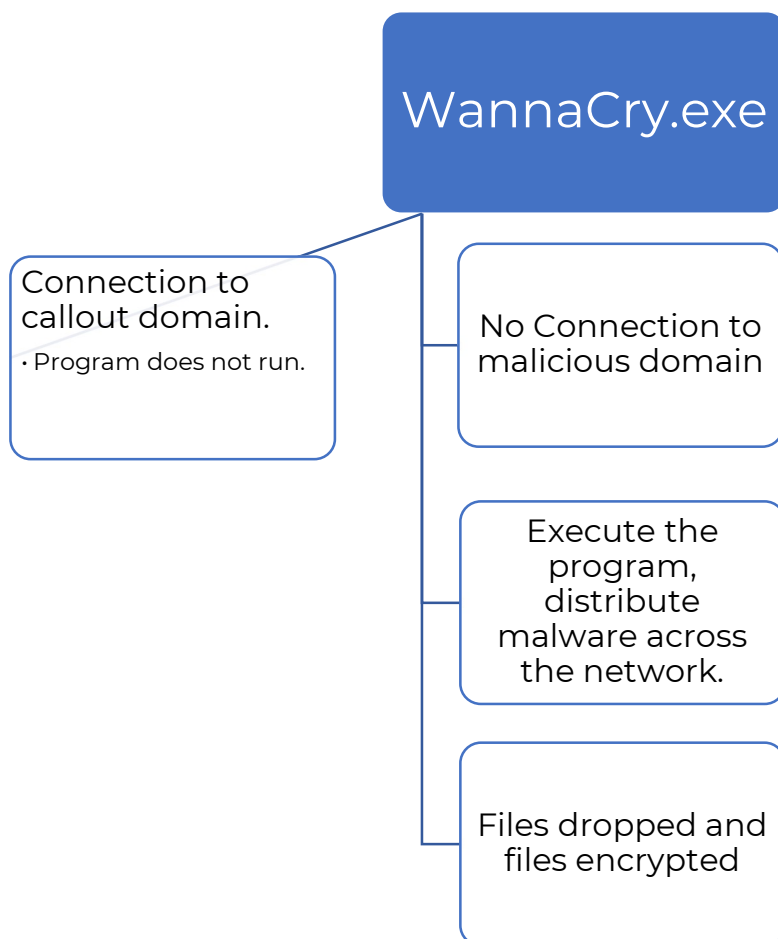
The encryptor windows and wallpaper on the desktop:





High-Level Technical Summary

WannaCry consists of one executable that then drops several more files once the conditions are met:





Malware Composition

WannaCry consists of the following components:

File Name	SHA256 Hash
wannacry.exe	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
Tasksche.exe	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Taskse.exe	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
Taskdl.exe	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79

WannaCry.exe:

The initial executable that runs after successful conditions are met.

TaskSche.exe:

File drops after execution and sets a scheduled task. This also sets a startup program to persist when rebooted.

Taskse.exe:

This file performs the Wanna Decryptor pop-up window

Taskdl.exe:

This file performs the Wanna Decryptor pop-up window

Tasksvc.exe:

This opens a listening port on 9050



Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

Function calls of interest:

0000A134	0000A7DC	Hint/Name RVA	0092 InternetOpenA
0000A138	0000A7C8	Hint/Name RVA	0093 InternetOpenUrlA
0000A13C	0000A7B2	Hint/Name RVA	0069 InternetCloseHandle
0000A140	00000000	End of Imports	WININET.dll
0000A00C	0000A6AC	Hint/Name RVA	0244 SetServiceStatus
0000A010	0000A69A	Hint/Name RVA	01AD OpenSCManagerA
0000A014	0000A688	Hint/Name RVA	0064 CreateServiceA
0000A018	0000A672	Hint/Name RVA	003E CloseServiceHandle
0000A01C	0000A662	Hint/Name RVA	0249 StartServiceA
0000A020	0000A650	Hint/Name RVA	0096 CryptGenRandom
0000A024	0000A638	Hint/Name RVA	0085 CryptAcquireContextA
0000A028	0000A714	Hint/Name RVA	01AF OpenServiceA
0000A02C	00000000	End of Imports	ADVAPI32.dll

RegQueryValueExA
RegSetValueExA
RegCreateKeyW
CryptReleaseContext
CreateServiceA
CloseServiceHandle
StartServiceA
OpenServiceA
OpenSCManagerA



Strings of interest:

```
\%s\IPC$
Microsoft Base Cryptographic Provider v1.0
%d.%d.%d.%d
mssecsvc2.0
Microsoft Security Center (2.0) Service
%s -m security
C:\%s\qeriuwjhrf
C:\%s\%s
tasksche.exe
CloseHandle
WriteFile
CreateFileA
CreateProcessA
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwa.com
!This program cannot be run in DOS mode.
```

```
WANACRY!|
CloseHandle
DeleteFileW
MoveFileExW
MoveFileW
ReadFile
WriteFile
CreateFileW
kernel32.dll
2/0-_.X8w.+
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
115p7UMMngoj1pMvkhHjcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Global\MSWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
icacls . /grant Everyone:F /T /C /Q
attrib +h .
WNCry@2017
```




```
USER32.DLL
Windows 2000 2195
Windows 2000 5.0
\172.16.99.5\IPC$
Windows 2000 2195
Windows 2000 5.0
\192.168.56.20\IPC$
kernel32.dll
WanaCrypt0r
```

CAPA output:

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



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



Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

TCP Connection:

22	5.668017369	10.0.0.3	10.0.0.2	TCP	66 49677 → 80	[SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
23	5.668047663	10.0.0.2	10.0.0.3	TCP	66 80 → 49677	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
24	5.668233979	10.0.0.3	10.0.0.2	TCP	60 49677 → 80	[ACK] Seq=1 Ack=1 Win=262144 Len=0
25	5.668386497	10.0.0.3	10.0.0.2	HTTP	154 GET / HTTP/1.1	
26	5.668393381	10.0.0.2	10.0.0.3	TCP	54 80 → 49677	[ACK] Seq=1 Ack=101 Win=64256 Len=0
27	5.711181014	10.0.0.2	10.0.0.3	TCP	204 80 → 49677	[PSH, ACK] Seq=1 Ack=101 Win=64256 Len=150 [TCP segment of a reassembled PDU]
28	5.711334564	10.0.0.3	10.0.0.2	TCP	60 49677 → 80	[ACK] Seq=101 Ack=151 Win=261888 Len=0
29	5.711345980	10.0.0.2	10.0.0.3	HTTP	312 HTTP/1.1 200 OK	(text/html)
30	5.711442324	10.0.0.3	10.0.0.2	TCP	60 49677 → 80	[ACK] Seq=101 Ack=409 Win=261632 Len=0
31	5.711583900	10.0.0.3	10.0.0.2	TCP	60 49677 → 80	[FIN, ACK] Seq=101 Ack=409 Win=261632 Len=0

Domain callout:

```
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/]
    [HTTP request 1/1]
    [Response in frame: 29]
```



Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}

The main function that contains the kill switch:

```
[0x00408140]
int main(int argc, char **argv, char **envp);
; var int32_t var_64h @ stack - 0x64
; var int32_t var_50h @ stack - 0x50
; var int32_t var_17h @ stack - 0x17
; var int32_t var_13h @ stack - 0x13
; var int32_t var_fh @ stack - 0xf
; var int32_t var_bh @ stack - 0xb
; var int32_t var_7h @ stack - 0x7
; var int32_t var_3h @ stack - 0x3
; var int32_t var_1h @ stack - 0x1
0x00408140 sub esp, 0x50
0x00408143 push esi
0x00408144 push edi
0x00408145 mov ecx, 0xe ; 14
0x0040814a esi, str.http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com ; 0x4313d0
0x0040814f lea edi, [var_50h]
0x00408153 xor eax, eax
0x00408155 rep movsd dword es:[edi], dword ptr [esi]
0x00408157 movsb byte es:[edi], byte ptr [esi]
0x00408158 mov dword [var_17h], eax
0x0040815c mov dword [var_13h], eax
0x00408160 mov dword [var_fh], eax
0x00408164 mov dword [var_bh], eax
0x00408168 mov dword [var_7h], eax
0x0040816c mov word [var_3h], ax
0x00408171 push eax
0x00408172 push eax
0x00408173 push eax
0x00408174 push 1 ; 1
0x00408176 push eax
0x00408177 mov byte [var_1h], al
0x0040817b call dword [InternetOpenA] ; 0x40a134
0x00408181 push 0
0x00408183 push 0x84000000
0x00408188 push 0
0x0040818a lea ecx, [var_64h]
0x0040818e mov esi, eax
0x00408190 push 0
0x00408192 push ecx
0x00408193 push esi
0x00408194 call dword [InternetOpenUrlA] ; 0x40a138
0x0040819a mov edi, eax
0x0040819c push esi
0x0040819d mov esi, dword [InternetCloseHandle] ; 0x40a13c
0x004081a3 test edi, edi
0x004081a5 jne 0x4081bc

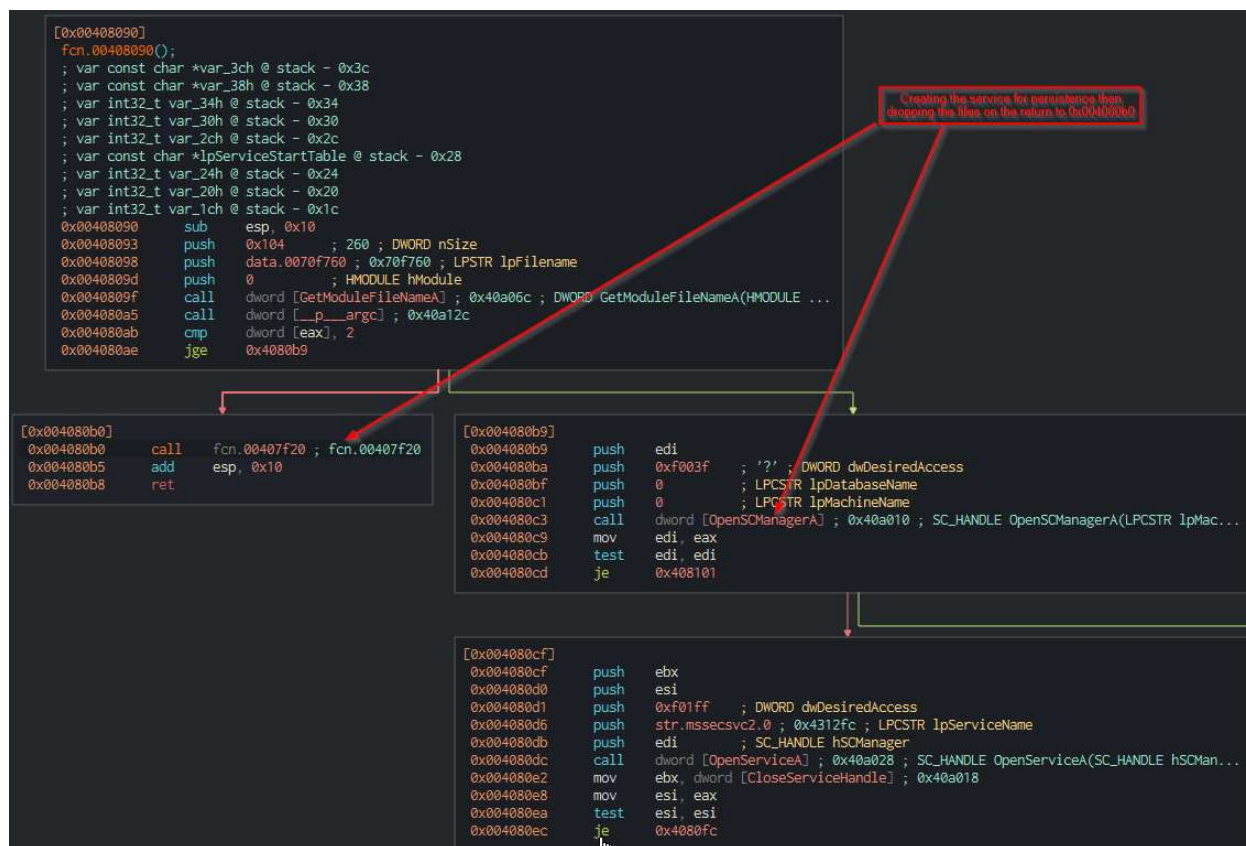
[0x004081a7]
0x004081a7 call esi
0x004081a9 push 0
0x004081ab call esi
0x004081ad call fcn.00408090 ; fcn.00408090
0x004081b2 pop edi
0x004081b3 xor eax, eax
0x004081b5 pop esi
0x004081b6 add esp, 0x50
0x004081b9 ret 0x10

[0x004081bc]
0x004081bc call esi
0x004081be push edi
0x004081bf call esi
0x004081c1 pop edi
0x004081c2 xor eax, eax
0x004081c4 pop esi
0x004081c5 add esp, 0x50
0x004081c8 ret 0x10
```

Reaches to domain, then decides to continue or kill upon connection.

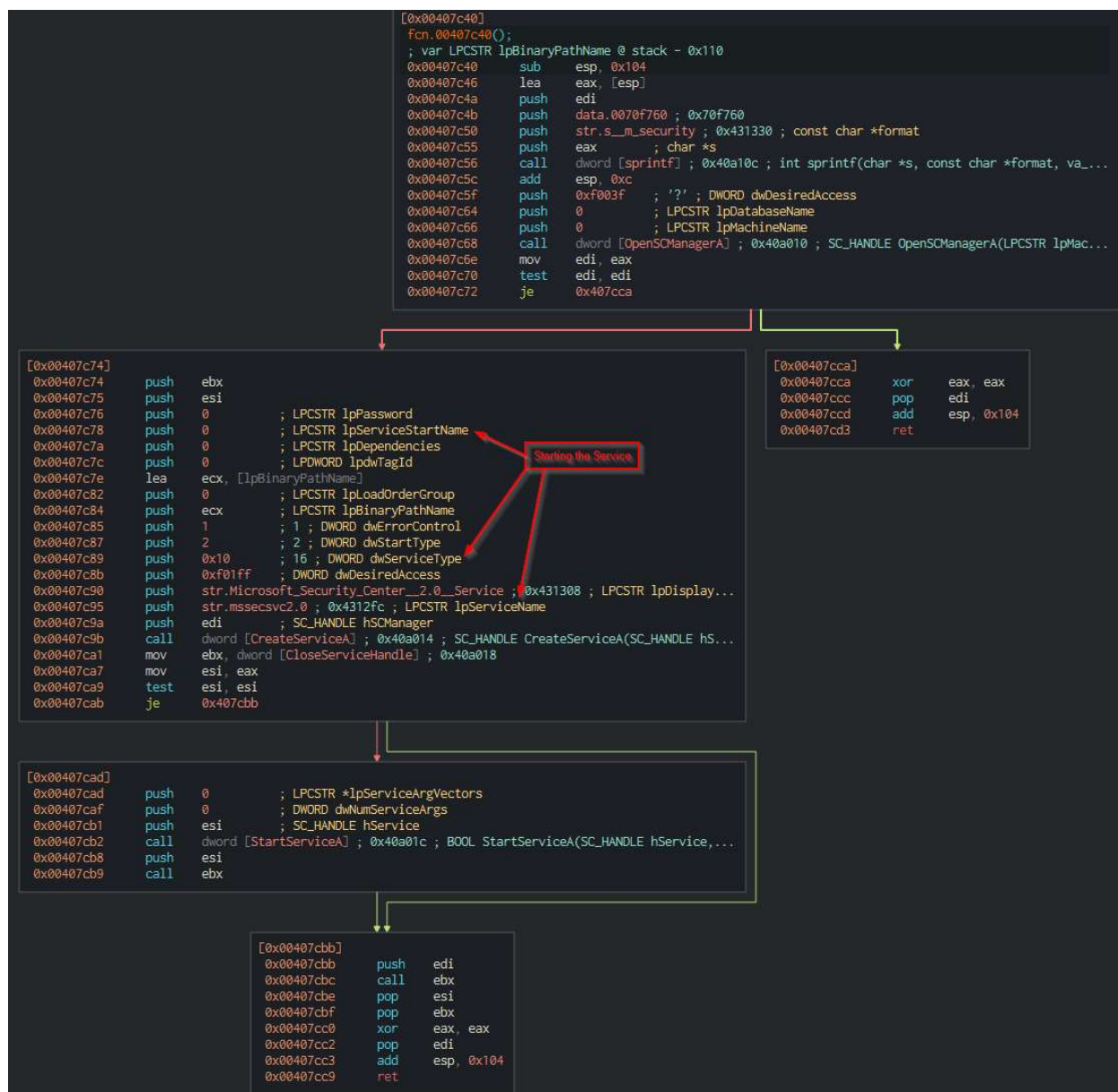


The file then checks for a service, if not found it creates one:





Service creation:





The program then creates the staging directory:

```
[0x00407db9]
0x00407db9  mov     ecx, 0x40 ; '@' ; 64
0x00407dbe  xor     eax, eax
0x00407dc0  lea     edi, [lpExistingFileName + 0x1]
0x00407dc4  mov     byte [lpExistingFileName], bl
0x00407dc8  rep     stosd dword es:[edi], eax
0x00407dca  stosw   word es:[edi], ax
0x00407dcc  stosb   byte es:[edi], al
0x00407dcd  mov     ecx, 0x40 ; '@' ; 64
0x00407dd2  xor     eax, eax
0x00407dd4  lea     edi, [lpNewFileName + 0x1]
0x00407ddb  mov     byte [lpNewFileName], bl
0x00407de2  rep     stosd dword es:[edi], eax
0x00407de4  mov     esi, dword [sprintf] ; 0x40a10c
0x00407dea  push    str.tasksche.exe ; 0x43136c
0x00407def  stosw   word es:[edi], ax
0x00407df1  stosb   byte es:[edi], al
0x00407df2  push    str.WINDOWS ; 0x431364
0x00407df7  lea     eax, [lpExistingFileName]
0x00407dfb  push    str.C:___s___s ; 0x431358
0x00407e00  push    eax
0x00407e01  call    esi
0x00407e03  add     esp, 0x10
0x00407e06  lea     ecx, [lpNewFileName]
0x00407e0d  push    str.WINDOWS ; 0x431364
0x00407e12  push    str.C:___s___qeriujhrf ; 0x431344
0x00407e17  push    ecx
0x00407e18  call    esi
0x00407e1a  add     esp, 0xc
0x00407e1d  lea     edx, [lpNewFileName]
0x00407e24  lea     eax, [lpExistingFileName]
0x00407e28  push    1 ; 1 ; DWORD dwFlags
0x00407e2a  push    edx ; LPCSTR lpNewFileName
0x00407e2b  push    eax ; LPCSTR lpExistingFileName
0x00407e2c  call    dword [MoveFileExA] ; 0x40a04c ; BOOL MoveFileExA(LPCSTR lpExistingFileNa...
0x00407e32  push    ebx
0x00407e33  push    4 ; 4
0x00407e35  push    2 ; 2
0x00407e37  push    ebx
0x00407e38  push    ebx
0x00407e39  lea     ecx, [var_258h]
0x00407e3d  push    0x40000000
0x00407e42  push    ecx
0x00407e43  call    dword [data.00431458] ; 0x431458
0x00407e49  mov     esi, eax
0x00407e4b  cmp     esi, 0xffffffff
0x00407e4e  je      0x407f08
```

Function to drop files



Then begins to drop files:

```
0x00407ce0    sub    esp, 0x260
0x00407ce6    push   ebx
0x00407ce7    push   ebp
0x00407ce8    push   esi
0x00407ce9    push   edi
0x00407cea    push   str.kernel32.dll ; 0x4313b4 ; LPCWSTR lpModuleName
0x00407cef    call   dword [GetModuleHandleW] ; 0x40a064 ; HMODULE GetModuleHandleW(LPCWSTR lp...
0x00407cf5    mov     esi, eax
0x00407cf7    xor     ebx, ebx
0x00407cf9    cmp     esi, ebx
0x00407cfb    je      0x407f08

[0x00407d01]
0x00407d01    mov     edi, dword [GetProcAddress] ; 0x40a060
0x00407d07    push   str.CreateProcessA ; 0x4313a4 ; LPOVERLAPPED lpOverlapped
0x00407d0c    push   esi ; LPDWORD lpNumberOfBytesWritten
0x00407d0d    call   edi
0x00407d0f    push   str.CreateFileA ; 0x431398 ; DWORD nNumberOfBytesToWrite
0x00407d14    push   esi ; LPCVOID lpBuffer
0x00407d15    mov     dword data.00431478, eax ; 0x431478
0x00407d1a    call   edi
0x00407d1c    push   str.WriteFile ; 0x43138c ; HANDLE hFile
0x00407d21    push   esi
0x00407d22    mov     dword data.00431458, eax ; 0x431458
0x00407d27    call   edi
0x00407d29    push   str.CloseHandle ; 0x431380 ; HANDLE hObject
0x00407d2e    push   esi
0x00407d2f    mov     dword data.00431460, eax ; 0x431460
0x00407d34    call   edi
0x00407d36    mov     ecx, dword data.00431478 ; 0x431478
0x00407d3c    mov     dword data.0043144c, eax ; 0x43144c
0x00407d41    cmp     ecx, ebx
0x00407d43    je      0x407f08
```

Writing bytes to...



Final file drop:

```
[0x00407d69]
0x00407d69    push    data.0043137c ; 0x43137c ; LPCSTR lpType
0x00407d6e    push    0x727          ; 1831 ; LPCSTR lpName
0x00407d73    push    ebx            ; HMODULE hModule
0x00407d74    call    dword [FindResourceA] ; 0x40a05c ; HRSRC FindResourceA(HMODULE hModule, L...
0x00407d7a    mov     esi, eax
0x00407d7c    cmp     esi, ebx
0x00407d7e    je      0x407f08

[0x00407d84]
0x00407d84    push    esi            ; HRSRC hResInfo
0x00407d85    push    ebx            ; HMODULE hModule
0x00407d86    call    dword [LoadResource] ; 0x40a058 ; HGLOBAL LoadResource(HMODULE hModule, H...
0x00407d8c    cmp     eax, ebx
0x00407d8e    je      0x407f08

[0x00407d94]
0x00407d94    push    eax            ; HGLOBAL hResData
0x00407d95    call    dword [LockResource] ; 0x40a0a0 ; LPVOID LockResource(HGLOBAL hResData)
0x00407d9b    cmp     eax, ebx
0x00407d9d    mov     dword [var_29ch], eax
0x00407da1    je      0x407f08

[0x00407da7]
0x00407da7    push    esi            ; HRSRC hResInfo
0x00407da8    push    ebx            ; HMODULE hModule
0x00407da9    call    dword [SizeofResource] ; 0x40a050 ; DWORD SizeofResource(HMODULE hModule, ...
0x00407daf    mov     ebp, eax
0x00407db1    cmp     ebp, ebx
0x00407db3    je      0x407f08
```

finding and loading the files



Indicators of Compromise

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

Network Indicators

Opens listening port:

taskshvc.exe (6032)		DESKTOP-L88K1DR	9050		TCP	Listen			
taskshvc.exe (6032)		DESKTOP-L88K1DR	50471	DESKTOP-L88K1DR	50472	TCP	Establish...		
taskshvc.exe (6032)		DESKTOP-L88K1DR	50472	DESKTOP-L88K1DR	50471	TCP	Establish...		
taskshvc.exe (6032)		DESKTOP-L88K1DR	9050	DESKTOP-L88K1DR	8643	TCP	Establish...		
taskshvc.exe	4664	TCP	Listen	127.0.0.1	9050	0.0.0.0	0	3/2/2024 3:07:33 PM	taskshvc.exe
taskshvc.exe	4664	TCP	Established	127.0.0.1	9050	127.0.0.1	50925	3/2/2024 3:08:07 PM	taskshvc.exe
taskshvc.exe	4664	TCP	Established	127.0.0.1	50165	127.0.0.1	50166	3/2/2024 3:07:33 PM	taskshvc.exe
taskshvc.exe	4664	TCP	Established	127.0.0.1	50166	127.0.0.1	50165	3/2/2024 3:07:33 PM	taskshvc.exe

Scans the network for worm capabilities:

80	16.291492	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.4? Tell 10.0.0.3			
81	16.715662	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.12? Tell 10.0.0.3			
82	16.782115	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.13? Tell 10.0.0.3			
83	16.788257	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.5? Tell 10.0.0.3			
84	16.788311	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.6? Tell 10.0.0.3			
85	16.788339	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.7? Tell 10.0.0.3			
86	16.788375	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.8? Tell 10.0.0.3			
87	16.788411	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.9? Tell 10.0.0.3			
88	16.788431	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.10? Tell 10.0.0.3			
89	16.788448	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.11? Tell 10.0.0.3			
90	16.838749	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.14? Tell 10.0.0.3			
91	16.908368	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.15? Tell 10.0.0.3			
92	16.960695	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.16? Tell 10.0.0.3			
93	17.013477	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.17? Tell 10.0.0.3			
94	17.076332	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.18? Tell 10.0.0.3			
95	17.132366	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.19? Tell 10.0.0.3			
96	17.194917	VMware_d8:06:c1	Broadcast	ARP	42	Who has 10.0.0.20? Tell 10.0.0.3			
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49713	10.0.0.30	445	3/2/2024 3:07:05 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49716	10.0.0.31	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49717	10.0.0.32	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49719	10.0.0.33	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49720	10.0.0.34	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49721	10.0.0.35	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49722	10.0.0.36	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49723	10.0.0.37	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49724	10.0.0.38	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49725	10.0.0.39	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49726	10.0.0.40	445	3/2/2024 3:07:06 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49692	10.0.0.12	445	3/2/2024 3:07:04 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49700	10.0.0.20	445	3/2/2024 3:07:04 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49693	10.0.0.13	445	3/2/2024 3:07:04 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49694	10.0.0.14	445	3/2/2024 3:07:04 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49695	10.0.0.15	445	3/2/2024 3:07:04 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49696	10.0.0.16	445	3/2/2024 3:07:04 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49697	10.0.0.17	445	3/2/2024 3:07:04 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49698	10.0.0.18	445	3/2/2024 3:07:04 PM	mssecsvc2.0
Ransomware.wannacr...	1224	TCP	Syn Sent	10.0.0.3	49699	10.0.0.19	445	3/2/2024 3:07:04 PM	mssecsvc2.0



Host-based Indicators:

Service created:

Service Name	Service Description	Driver	Status	Start Type
NdisWan	Remote Access NDIS WAN Driver	Driver	Stopped	Demand start
ndiswanlegacy	Remote Access LEGACY NDIS WAN D...	Driver	Stopped	Demand start
NDKPing	NDKPing Driver	Driver	Stopped	Demand start
ndproxy	NDIS Proxy Driver	Driver	Stopped	Demand start
Ndu	Windows Network Data Usage Monit...	Driver	Running	Auto start
NetAdapterCx	Network Adapter Wdf Class Extension...	Driver	Stopped	Demand start
NetBIOS	NetBIOS Interface	FS driver	Running	System start
NetBT	NetBT	Driver	Running	System start
Netlogon	Netlogon	Share process	Stopped	Demand start
Netman	Network Connections	Unknown	Running	Demand start
netprofm	Network List Service	Unknown	Running	Demand start
NetSetupSvc	Network Setup Service	Unknown	Stopped	Demand start (tr
NetTcpPortSharing	Net.Tcp Port Sharing Service	Share process	Stopped	Disabled
netvsc	netvsc	Driver	Stopped	Demand start
NgcCtnrSvc	Microsoft Passport Container	Unknown	Stopped	Demand start (tr
NgcSvc	Microsoft Passport	Unknown	Stopped	Demand start (tr
ngftvtcrceboovl131	ngftvtcrceboovl131	Own process	Stopped	Auto start
NlaSvc	Network Location Awareness	Unknown	Running	Auto start
npcap	Npcap Packet Driver (NPCAP)	Driver	Running	System start

ngftvtcrceboovl131 Properties

Triggers: General, Security, Recovery, Dependencies, Comment

General: ngftvtcrceboovl131

Type: Own process Start type: Auto start

Error control: Normal Group:

Binary path: E:\ProgramData\ngftvtcrceboovl131\tasksche.exe Browse...

User account: LocalSystem Password: Password: Service DLL: N/A

☐ Delayed start

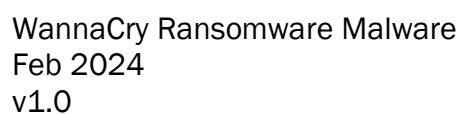
Dropped / created files:

tasksche.e...	C:\\$Extend\\$\UsnJrnl:\$J	56 B/s	73.48 kB/s	73.54 kB/s	Normal	8
Unknown ...	C:\Windows\tasksche.exe		59.17 kB/s	59.17 kB/s	Normal	1
No process	C:\ProgramData\ngftvtcrceboovl131\tasksche.exe		59.17 kB/s	59.17 kB/s	Normal	1

2:42:3...	Ransomware.w...	168	CreateFile	C:\Windows\tasksche.exe	NAME NOT FOUND	Desired Access: R...
2:42:3...	Ransomware.w...	168	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: G...
2:42:3...	Ransomware.w...	168	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
2:42:3...	Ransomware.w...	168	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
2:42:3...	Ransomware.w...	168	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
2:42:3...	Ransomware.w...	168	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...



Startup file:





Appendices

A. Yara Rules

Full Yara repository located at: <https://github.com/j3rmcyber/MalwareAnalysis>

```
rule WannaCry_Ransomware {  
  
    meta:  
        last_updated = "2024-3-11"  
        author = "j3rmcyber"  
        description = "YARA Rule for Detecting WannaCry"  
  
    strings:  
        // Fill out identifying strings and other criteria  
        $string1 = "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"  
        $string2 = "qeriuwjhrf"  
        $string3 = "WANACRY!" ascii  
        $string4 = "WNCry@2017" ascii  
        $string5 = "tasksche.exe"  
        $PE_magic_byte = "MZ"  
  
    condition:  
        // Fill out the conditions that must be met to identify the binary  
        $PE_magic_byte at 0 and  
        4 of them  
}
```

B. Callback URLs

Domain	Port
hxxp[://]www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com	80
127.0.0.1	9050