

Practical Malware Analysis & Triage Malware Analysis Report

WannaCry Malware

SEP 2022 | Rishank Shah | v1.0



Table of Contents

Table of Contents	2
Executive Summary	3
High-Level Technical Summary	4
Malware Composition	5
Ransomware.wannacry.exe	5
tasksche.exe:	5
Basic Static Analysis	6
Strings – Extracted using Floss	6
PEview	7
PEStudio	9
Basic Dynamic Analysis	10
Analysis with inetsim turned on	10
Analysis with inetsim turned off	11
Advanced Static Analysis	16
Advanced Dynamic Analysis	17
Indicators of Compromise	19
Network Indicators	19
Host-based Indicators	20
Rules & Signatures	21



Executive Summary

SHA256 hash 24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C

The WannaCry ransomware attack was a global epidemic that took place in May 2017. This ransomware attack spread through computers operating Microsoft Windows. User's files were held hostage, and a Bitcoin ransom was demanded for their return. Were it not for the continued use of outdated computer systems and poor education around the need to update software, the damage caused by this attack could have been avoided.

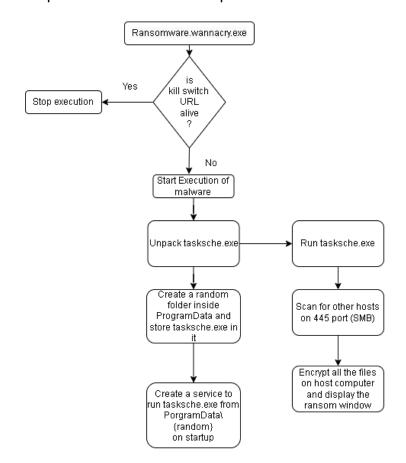
WannaCry is written in C++ language. On executing the malware it checks for a hardcoded URL, if it successfully pings that URL malware does not execute. If the URL was not found then malware execution takes place. Symptoms of the infection include ransomware payment window popup, encryption of the files, new desktop shortcuts and new services created. After executing the malware it creates a file named "C:\Windows\tasksche.exe" which contains the payloads, and then starts encrypting all the files on computer. WannaCry ransomware also tries to spread to other Windows Computers using the EternalBlue vulnerability.

YARA signature rules are attached in Rules & Signatures. Malware sample and hashes have been submitted to VirusTotal for further examination.



High-Level Technical Summary

WannaCry consists of two parts: stage 0 executable and an unpacked stage 2 encryption and worm program. It first attempts to contact its kill switch URL (hxxps://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.local). If the URL is alive it does not execute. If the URL is not found then the malware unpacks tasksche.exe and creates a service to start tasksche.exe on startup. This executable encrypts all the files, shows the popup ransom window and changes the background of Desktop. It creates a random folder inside C:\ProgramData to store all the wannacry files. It exploits the EternalBlue vulnerability on port 445 to spread to other computers.





Malware Composition

WannaCry consists of the following components:

File Name	SHA256 Hash
Ranswomware.wannac	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
ry.exe	
tasksche.exe	ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA

Ransomware.wannacry.exe

The initial executable that runs and checks the kill switch URL. If alive don't run else unpack tasksche.exe.

tasksche.exe:

This is used for persistence. It creates a random folder for wannacry staging area inside ProgramData. After execution of malware on host computer it tries to spread itself on other windows computers using SMB port 445. It starts encrypting all the files and after that it displays the ransomware popup and message.



Basic Static Analysis

Strings - Extracted using Floss

floss -n 6 Ransomware.wannacry.exe.malz > floss.txt

```
59 MSVCP60.dll
60 GetPerAdapterInfo
61 GetAdaptersInfo
62 iphlpapi.dll
63 InternetCloseHandle
64 InternetOpenUrlA
65 InternetOpenA
66 WININET.dll
```

Fig 2: Modules used to open a URL

```
USERID PLACEHOLDER
456 userid
     treeid
       TREEPATH REPLACE
     \\%s\IPC$
     Microsoft Base Cryptographic Provider v1.0
461 %d.%d.%d.%d
     mssecsvc2.0
     Microsoft Security Center (2.0) Service
     %s -m security
     C:\%s\qeriuwjhrf
     C:\%s\%s
     WINDOWS
     tasksche.exe
     CloseHandle
     WriteFile
     CreateFileA
     CreateProcessA
     http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
     !This program cannot be run in DOS mode.
      `.rdata
```

Fig 3: Service names used, Kill Switch URL and random paths



```
cryptacquirecontexta

cmd.exe /c "%s"

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

685 Global\MsWinZonesCacheCounterMutexA

tasksche.exe

TaskStart

688 t.wnry

689 icacls . /grant Everyone:F /T /C /Q

attrib +h .

691 WNcry@2ol7
```

Fig 4: Service names used, random paths icacls used for modifying access controls on files attrib +h . used to hide the file attribute

PEview

pFile	Data	Description	Value
000001F0	2E 74 65 78	Name	.text
000001F4	74 00 00 00		
000001F8	00008BCA	Virtual Size	
000001FC	00001000	RVA	
00000200	00009000	Size of Raw Data	
00000204	00001000	Pointer to Raw Data	
00000208	00000000	Pointer to Relocations	
0000020C	00000000	Pointer to Line Numbers	
00000210	0000	Number of Relocations	
00000212	0000	Number of Line Numbers	
00000214	60000020	Characteristics	
		00000020	IMAGE_SCN_CNT_CODE
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ

Fig 5: IMAGE SECTION HEADER.text



	Data		
0000A004	000000000	Description	Value
	0000A618 H	Est/Name RVA	024A StartServiceCtrlDispatcherA 020C RegisterServiceCtrlHandlerA
800A000	0000A6C0 H	fint/Name RVA	0034 ChangeServiceConfig2A
0000A00C	0000A6AC H	fint/Name RVA	0244 SetServiceStatus
0000A010	0000A6AC H 0000A69A H 0000A688 H	lint/Name RVA	01AD OpenSCManagerA
0000A014	0000A688 H	lint/Name RVA	0064 CreateServiceA
00004018	0000A672 H	Hint/Name RVA	003E CloseServiceHandle
	0000A662 H		0249 StartServiceA
0000A01C	0000A062 F	IIII/IVame RVA	
0000A020	0000A650 F	fint/Name RVA fint/Name RVA fint/Name RVA End of Imports fint/Name RVA	0096 CryptGenRandom
0000A024	0000A638 F	fint/Name RVA	0085 CryptAcquireContextA
0000A028	0000A714 F	lint/Name RVA	01AF OpenServiceA
0000A02C	00000000 E	nd of Imports	ADVAPI32.dll
0000A030	0000A4F6 H	lint/Name RVA	0390 WaitForSingleObject
0000A034	000004500	lint/Name RVA	022C InterlockedIncrement
00007034	000004500 1	lint/Name DVA	
0000A038	0000A5Z4 F	fint/Name RVA fint/Name RVA fint/Name RVA fint/Name RVA fint/Name RVA	0146 GetCurrentThreadId
0000A03C	0000A53A	fint/Name RVA	0145 GetCurrentThread
0000A040	0000A54E F	lint/Name RVA	02B5 ReadFile
0000A044	0000A55A H	lint/Name RVA	0163 GetFileSize
0000A048	0000A568 H	lint/Name RVA	0053 CreateFileA
00000000	0000A576 H	lint/Name DVA	026F MoveFileExA
0000A050	0000A564 F	lint/Name RVA	0355 SizeofResource
0000A054	0000A4E4	fint/Name RVA	035F TerminateThread 0257 LoadResource 00E3 FindResourceA
0000A058	0000A5A6 H	lint/Name RVA	0257 LoadResource
0000A05C	0000A5B6 H	lint/Name RVA	00E3 FindResourceA
00000000	000004506 H	lint/Namo DVA	01A0 GetProcAddress
00000000	0000A3C0 I	E LAL DVA	01A0 Oct 10CAddless
0000AUb4	UUUUA5D8 F	fint/Name RVA fint/Name RVA fint/Name RVA fint/Name RVA fint/Name RVA	0182 GetModuleHandleW
U000A068	UUUUA5EC H	fint/Name RVA fint/Name RVA fint/Name RVA	00B9 ExitProcess
0000A06C	0000A5FA H	lint/Name RVA	017D GetModuleFileNameA
			025C LocalFree
0000A074	0000A61C F	lint/Name RVA	0258 LocalAlloc
0000A078	UUUUAAU IS	IIIII/Name KVA	UUJ4 Cioseriangie
0000MU/C	OUUUM4BE F	microame RVA	0228 InterlockedDecrement
0000A080	U000A4A6 H	fint/Name RVA	0098 EnterCriticalSection
0000A084	0000A48E H	fint/Name RVA	0251 LeaveCriticalSection
880A0000	0000A472 H	lint/Name RVA lint/Name RVA lint/Name RVA lint/Name RVA	0223 InitializeCriticalSection
0000A08C	0000A464 F	Hint/Name RVA	01F8 GlobalAlloc
00000,0000	000001101	lint/Name RVA	01FF GlobalFree
		lint/Name RVA	02A4 QueryPerformanceFrequency
0000A098	0000A420 H	lint/Name RVA	02A3 QueryPerformanceCounter
0000A09C	0000A410 H	lint/Name RVA	01DF GetTickCount
0404000	0000A596 H	lint/Name RVA lint/Name RVA lint/Name RVA	0265 LockResource
000000000	000074330 1	lint/Manne DVA	
0000A0A4	0000A408 F	IInt/Name RVA	0356 Sleep
8A0A0000	0000A97A	fint/Name RVA	01B7 GetStartupInfoA
0000A0AC	0000A966 F	lint/Name RVA	017F GetModuleHandleA
0000A0B0			KERNEL 32 dll
0000A0B4	0000A73E H	lint/Name RVA	010B ??1_Lockit@std@@QAE@XZ
000004000	000004750 1	I I AL DIVA	0040 000 L L'IO LIGODAEOVZ
0000A0B8	0000A758 F	Hint/Name RVA End of Imports	00A2 ??0_Lockit@std@@QAE@XZ
0000A0BC	00000000 E	ind of Imports	MSVCP60.dll
0000A0C0	0000A932 H	Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA	0081set_app_type
00004004	0000A98C F	Hint/Name RVA	01C1 _stricmp
000000000	000000004	lint/Name DVA	OOSE n fmode
000004000	000004044 1	IIIUName RVA	006Fpfmode 006Apcommode
0000A0CC	0000A914 F	fint/Name RVA	006Apcommode
0000A0D0	0000A944 F	lint/Name RVA	00CA _except_handler3
0000A0D4	0000A8F0 H	Hint/Name RVA	0083setusermatherr 010F _initterm
поподоля	0000A8E4 E	Hint/Name RVA	010F initterm
			0000
UUUUAUDC	0000A0D4 F	lint/Name RVA	0058getmainargs
0000A0E0	0000A8CA F	Hint/Name RVA	008F _acmdin
0000A0E4	0000A904 F	Hint/Name RVA	009D _adjust_fdiv
	0000A958 H	Hint/Name RVA	
0000A0E8	UUUUA930 F		00B7 controlfp
0000A0E8 0000A0EC	0000A956 F	lint/Name RVA	008F _acmdln 009D _adjust_fdiv 00B7 _controlfp 0249 exit
0000A0E8 0000A0EC	0000A956 F	lint/Name RVA	00B7 _controlfp 0249 exit
0000A0E8 0000A0EC	0000A956 F	F . 41 B) /4	00B7 _controlfp 0249 exit
0000A0E8 0000A0EC	0000A8C2 F	TIIIIUIVaille KVA	0249 exit
0000A0EC	0000A8C2 F	Hint/Name RVA	0249 exit
0000A0EC 0000A110 0000A114 0000A118	0000A8C2 0000A80A 0000A81A 0000A824	Hint/Name RVA	0249 exit
0000A0EC 0000A110 0000A114 0000A118	0000A8C2 0000A80A 0000A81A 0000A824	Hint/Name RVA Hint/Name RVA Hint/Name RVA	0249 exit 0000enumeratex 02C1 strncpy 02A6 rand
0000A0EC 0000A110 0000A114 0000A118 0000A11C	0000A8C2 H 0000A00A 0000A81A 0000A824 0000A82C	Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA	0000enotineadex 02C1 strncpy 02A6 rand 00A6 beginthreadex
0000A0EC 0000A110 0000A114 0000A118 0000A11C 0000A120	0000A8C2 F 0000A80A 0000A81A 0000A824 0000A82C 0000A83E	Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA	0000enotineadex 02C1 strncpy 02A6 rand 00A6 beginthreadex
0000A0EC 0000A110 0000A114 0000A118 0000A11C 0000A120 0000A124	0000A8C2 F 0000A80A 0000A81A 0000A824 0000A82C 0000A83E 0000A852	Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA	0249 exit 02C1 stringpy 02A6 rand 00A6 _beginthreadex 0049 _CxxFrameHandler 02E4 stand
0000A0EC 0000A110 0000A114 0000A118 0000A11C 0000A120	0000A8C2 F 0000A80A 0000A81A 0000A824 0000A82C 0000A83E 0000A852	Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA	0000enotineadex 02C1 strncpy 02A6 rand 00A6 beginthreadex
0000A110 0000A114 0000A114 0000A116 0000A120 0000A124 0000A124	0000A8C2 H 0000A80A 0000A81A 0000A824 0000A82C 0000A83E 0000A852 0000A85A	Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA Hint/Name RVA	02C1 strncpy 02C6 rand 02C6 beginthreadex 049Cxx5rameHandler 02B4 srand 0200 time
0000A0EC 0000A110 0000A114 0000A118 0000A11C 0000A120 0000A124 0000A124 0000A128	0000A8C2 F 0000A80A 0000A81A 0000A824 0000A82C 0000A83E 0000A852 0000A85A 0000A862	Hint/Name RVA	021 strncpy 0221 strncpy 0246 rand 0046 _beginthreadex 0049 _CxxFrameHandler 0284 srand 0200 time 0062 _p_argc
0000A0EC 0000A110 0000A114 0000A118 0000A120 0000A120 0000A124 0000A128 0000A12C 0000A130	0000A8C2 0000A8DA	Hint/Name RVA End of Imports	02C1 strncpy 02A6 rand 00A6 _beginthreadex 049 _CxoframeHandler 02B4 strand 02D0 time 00B2 _p_argc MSVCRT.dll
0000A0EC 0000A110 0000A114 0000A118 0000A120 0000A120 0000A124 0000A128 0000A126 0000A130 0000A134	0000A8C2 0000A8DA	Hint/Name RVA End of Imports	02C1 structy 02A6 rand 00A6 _beginthreadex 0049 _C.coFrameHandler 02B4 srand 0200 time 0062 _p_ argc MSVORT.dll 0092 [InternetOpenA
0000A0EC 0000A110 0000A114 0000A118 0000A120 0000A120 0000A124 0000A128 0000A12C 0000A130	0000A8C2 0000A80A	Hint/Name RVA End of Imports	02C1 strncpy 02A6 rand 00A6 _beginthreadex 049 _CxoframeHandler 02B4 strand 02D0 time 00B2 _p_argc MSVCRT.dll
0000A0EC 0000A110 0000A114 0000A118 0000A120 0000A124 0000A124 0000A12C 0000A134 0000A134	0000A8C2 0000A8C4 0000A8C4 0000A82C 0000A82C 0000A85A 0000A85A 0000A7DC 0000A7C8	Hint/Name RVA	0219 exit 02C1 strncpy 02A6 reanthreadex 04A6 _beginthreadex 04A9 _CxxFrameHandler 02B4 srand 02D0 time 0062 _p_argc MSVCRT.dll 0092 InternetOpenA 0030 InternetOpenA 0030 InternetOpenUrlA
0000A0EC 0000A110 0000A114 0000A118 0000A120 0000A124 0000A124 0000A12C 0000A134 0000A134	0000A8C2 0000A8C4 0000A8C4 0000A82C 0000A82C 0000A85A 0000A85A 0000A7DC 0000A7C8	Hint/Name RVA	0249 ext 02C1 strincpy 02A6 rand 00A6 _beginthreadex 0049 _CxxFrameHandler 02B4 srand 0200 time 0062 _p_ argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenHufA 0099 InternetClopenHufA 0099 InternetClopenHufA
0000A0EC 0000A114 0000A114 0000A112 0000A120 0000A124 0000A124 0000A126 0000A130 0000A134 0000A136 0000A136 0000A136	0000A8C2 0000A8C2 0000A81A 0000A824 0000A826 0000A85A 0000A85A 0000A7DC	Hint/Name RVA	021 strncpy 026 rainesee 021 strncpy 026 rainesee 026 beginthreadex 029 cxoFrameHandler 0284 srand 0200 time 0062 p_argc MSVCRT.dll 0092 internetOpenA 0093 internetOpenUrlA 0099 internetCoseHandle VMNINET.dll
0000A0E5 0000A0E5 0000A110 0000A114 0000A120 0000A120 0000A120 0000A120 0000A120 0000A130 0000A130 0000A130 0000A130 0000A140	0000A8C2 0000A8TA	Hint/Name RVA Codinal	0249 exit 02C1 strncpy 02A6 rand 00A6 _ beginthreadex 0049 _ CxxFrameHandler 02E4 srand 02D0 time 0062 argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenUrIA 0099 InternetCloseHandle WININET.dll 0003
0000A0EC 0000A114 0000A114 0000A112 0000A120 0000A124 0000A124 0000A126 0000A130 0000A134 0000A136 0000A136 0000A136	0000A8C2 0000A8C2 0000A81A 0000A824 0000A826 0000A85A 0000A85A 0000A7DC	Hint/Name RVA	021 strncpy 026 rainesee 021 strncpy 026 rainesee 026 beginthreadex 029 cxoFrameHandler 0284 srand 0200 time 0062 p_argc MSVCRT.dll 0092 internetOpenA 0093 internetOpenUrlA 0099 internetCoseHandle VMNINET.dll
0000A0E5 0000A0E5 0000A114 0000A118 0000A118 0000A120 0000A128 0000A128 0000A130 0000A138 0000A134 0000A144	0000A8C2 F 0000A81A 0000A824 0000A826 0000A83E 0000A852 0000A852 0000A7C8 0000A7C8 0000A7C8 0000A7C8 0000A7C8	Hint/Name RVA Codinal Ordinal	020 sminiscrept 02C1 strincyy 02A6 rand 00A6 _beginthreadex 0049 _C.coFrameHandler 02B4 srand 0200 time 0062 _p_ argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenUrlA 0099 InternetCloseHandle WININET.dll 0003
0000A1E0 0000A0E0 0000A114 0000A114 0000A116 0000A120 0000A120 0000A120 0000A130 0000A130 0000A130 0000A140 0000A140 0000A140	0000A8C2 F 0000A81A 0000A81A 0000A824 0000A826 0000A85A 0000A85A 0000A75B 0000A7C8	Hint/Name RVA End of Imports Ordinal Ordinal	0249 exit 02C1 strncpy 02A6 reanthreadex 00A6 _beginthreadex 0049CxxFrameHandler 02B4 srand 02D0 time 0062 _p_argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenHold 0099 InternetCloseHandle WMINIET.dll 0003 0010 0013
0000A0E0 0000A0E0 0000A114 0000A114 0000A114 0000A120 0000A124 0000A130 0000A130 0000A130 0000A140 0000A140 0000A140 0000A140 0000A140 0000A140 0000A140	0000A8C2 1000A8C2 1000A8C2 1000A8C3 1000A8C3 1000A8C3 1000A8C3 1000A8C3 1000A8C3 1000A8C3 1000A8C3 1000A7C3	Hint/Name RVA Ordinal Ordinal Ordinal	020 strictly 021 strictly 026 rand 0046 _beginthreadex 0049 _C.cof-rameHandler 0284 strand 0200 time 0662 _p_ argc MSVCRT.dll 0092 internetOpenUnd 0093 InternetOpenUnd 0093 InternetCloseHandle WININET.dll 0003 0010 0013
0000A1E0 0000A0E0 0000A114 0000A114 0000A116 0000A120 0000A120 0000A120 0000A130 0000A130 0000A130 0000A140 0000A140 0000A140	0000A8C2 F 0000A81A 0000A81A 0000A824 0000A826 0000A85A 0000A85A 0000A75B 0000A7C8	Hint/Name RVA End of Imports Ordinal Ordinal	0249 exit 02C1 strncpy 02A6 reanthreadex 00A6 _beginthreadex 0049CxxFrameHandler 02B4 srand 02D0 time 0062 _p_argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenHold 0099 InternetCloseHandle WMINIET.dll 0003 0010 0013
0000A1E3 0000A1E4 0000A114 0000A114 0000A114 0000A120 0000A124 0000A126 0000A130 0000A130 0000A134 0000A134 0000A134 0000A136 0000A136 0000A136	0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C2 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 00000AC7DC 0000A7C8 00000A7C8 00000A7C8 0000A7C8 0000A7C	Hint/Name RVA End of Imports Hint/Name RVA End of Imports Ordinal Ordinal Ordinal Ordinal	021 strncpy 02A6 rameback 02C1 strncpy 02A6 rameback 00A6 _beginthreadex 00A9 _CxoFrameHandler 02B4 srand 02D0 time 0062 _p_ argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenAl 0003 0010
0000A1E3 0000A1E4 0000A114 0000A114 0000A115 0000A120 0000A120 0000A130 0000A130 0000A130 0000A140 0000A140 0000A140 0000A140 0000A140 0000A140 0000A150	0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C4 0000A8C2 0000A8C5 0000A8C5 0000A7C6	Hint/Name RVA Ordinal Ordinal Ordinal Ordinal Ordinal	021 strincpy 0216 rand 0045 _beginthreadex 0049 _CxxFrameHandler 0284 srand 0200 time 0062 _p_ argc MSVCRT.dill 0093 InternetOpenD/IA 0093 InternetCloseHandle WNINET.dill 0003 0010 0013 0008 000E
0000A1E3 0000A1E4 0000A114 0000A114 0000A116 0000A120 0000A120 0000A120 0000A130 0000A130 0000A140 0000A140 0000A140 0000A150 0000A150	0000A8C2 0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A7DC	Hint/Name RVA End of Imports Hint/Name RVA End of Imports Ordinal Ordinal Ordinal Ordinal Ordinal Ordinal Ordinal	0249 exit 02C1 strncpy 02A6 rand 00A6 _beginthreadex 0049 _CxoFrameHandler 02B4 srand 02D0 time 0062 _p _argc MSVCRT.dll 0093 InternetOpenA 0093 InternetOpenUrlA 0099 InternetCloseHandle WININET.dll 0003 0010 0011 0011 0011 0010 0013 00006 00006 000073 0000C
0000A1E3 0000A1E4 0000A114 0000A114 0000A115 0000A120 0000A120 0000A130 0000A130 0000A130 0000A140 0000A140 0000A140 0000A140 0000A140 0000A140 0000A150	0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000C6 00000C6 0000C6 0000C6 0000C6 0000C6 0000C6 0000C6 000	Hint/Name RVA Codinal Ordinal	021 strincpy 0216 rand 0045 _beginthreadex 0049 _CxxFrameHandler 0284 srand 0200 time 0062 _p_ argc MSVCRT.dill 0093 InternetOpenD/IA 0093 InternetCloseHandle WNINET.dill 0003 0010 0013 0008 000E
00000A1E3 00000A1E4 00000A114 0000A114 0000A120 0000A120 0000A130 0000A130 0000A130 0000A130 0000A130 0000A136 0000A156 0000A156 0000A156 0000A156 0000A156	0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000A7C6 0000C6 00000C6 0000C6 0000C6 0000C6 0000C6 0000C6 0000C6 000	Hint/Name RVA Codinal Ordinal	0219 exit 021 strncpy 0246 ramepalex 020 beginthreadex 040CxyFrameHandler 0284 srand 0200 time 0062P_argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenAl 0099 InternetCloseHandle VMINIET.dll 0001 0010 0010 0011 0013 0000 0000 00
0000A1ES 0000A0ES 0000A1E 0000A114 0000A12 0000A12 0000A12 0000A12 0000A13 0000A13 0000A13 0000A14 0000A14 0000A15 0000A15 0000A15 0000A15 0000A15 0000A15	0000A8C2 0000A00A8C2 0000A8C2 0000A8C4 0000A8C4 0000A8C5 0000A8C6 0000A8C6	Hint/Name RVA Ordinal	020 strictly 021 strictly 0226 rand 0046 _beginthreadex 0049 _C.coFrameHandler 0284 srand 0200 time 0062 _p_ argc MSVCRT.dll 0093 InternetOpenIA 0093 InternetOpenIUIA 0099 InternetCloseHandle WININET.dll 0003 0010 0013 0000 00013 00000 00000 00000 00000000
0000A150 0000A150	0000A8C2 0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C2 0000A8C3 0000A8C3 0000A8C3 0000A8C3 0000A8C3 0000A8C3 0000A8C3 0000A8C3 0000A8C3 00000C3 0000A7C3 0000A7C3 0000A7C3 0000C3	Hint/Name RVA Cordinal Ordinal	021 strncpy 02A6 rameback 02C1 strncpy 02A6 rameback 00A6 _beginthreadex 00A9 _CxoFrameHandler 02B4 srand 02D0 time 0062 _p_argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenAl 0093 InternetOpenAl 0093 InternetOpenAl 0003 0010 0013 0000 0013 0000 0073 0000C 0000A 0012 0009
00000A1EC 00000A1EC 00000A1EC 00000A1EC 00000A1EC 00000A120 0000A120 0000A130 0000A130 0000A130 0000A140 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150	0000A8C2 0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A7C8	Hint/Name RVA Ordinal	0201 strincpy 0204 rand 0202 strincpy 0204 rand 00046 _beginthreadex 0009 _C.oxf-rameHandler 0202 time 0002 _p_ argc MSVCRT.dll 0003 InternetOpenUrlA 0003 InternetCloseHandle VMNINET.dll 0003 0010 0013 0000 0000 0000 0000
00000A1EC 00000A1EC 00000A1EC 00000A1EC 00000A1EC 00000A120 0000A120 0000A130 0000A130 0000A130 0000A140 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150	0000A8C2 0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A7C8	Hint/Name RVA Ordinal	021 strncpy 02A6 rameback 02C1 strncpy 02A6 rameback 00A6 _beginthreadex 00A9 _CxoFrameHandler 02B4 srand 02D0 time 0062 _p_argc MSVCRT.dll 0092 InternetOpenA 0093 InternetOpenAl 0093 InternetOpenAl 0093 InternetOpenAl 0003 0010 0013 0000 0013 0000 0073 0000C 0000A 0012 0009
0000A1E8 0000A1E8 0000A114 0000A114 0000A116 0000A120 0000A120 0000A130 0000A130 0000A130 0000A130 0000A130 0000A130 0000A130 0000A130 0000A130 0000A140 0000A140 0000A140 0000A150 0000A160 0000A160 0000A160	0000A8C2 0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C4 0000A8C5 0000A8C6 0000A8C6 0000A8C6 0000A7C8 0000A7C8 0000A7C8 0000A7C8 0000A7C8 00000000 0000A7C8 00000000 0000A7C8 00000000 0000A7C8 00000000 000000000000000000000000	Hint/Name RVA End of Imports Hint/Name RVA End of Imports Ordinal	0201 strincpy 0204 rand 0202 strincpy 0204 rand 00046 _beginthreadex 0009 _C.oxf-rameHandler 0202 time 0002 _p_ argc MSVCRT.dll 0003 InternetOpenUrlA 0003 InternetCloseHandle VMNINET.dll 0003 0010 0013 0000 0000 0000 0000
0000A1E3 0000A1E4 0000A114 0000A116 0000A116 0000A120 0000A120 0000A130 0000A130 0000A130 0000A140 0000A140 0000A140 0000A140 0000A140 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150 0000A150	0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C4 0000A8C5 00000000 0000A8C5 00000000 0000A8C5 00000000 0000A8C5 00000000 00000000 00000000 000000	Hint/Name RVA Condinal Ordinal	020 sammerous 021 sammerous 022 sammerous 022 string 0246 rand 0046 _beginthreadex 0049 _CxoFrameHandler 0284 srand 0200 time 0062 _p_argc MSVCRT.dill 0093 InternetOpenUrlA 0093 InternetCloseHandle VININET.dil 0003 0010 0010 0013 0000 0000 0000 0000 0000 0001 0017 0004 0009
0000A1E8 0000A1E8 0000A114 0000A118 0000A118 0000A120 0000A124 0000A124 0000A130 0000A130 0000A130 0000A130 0000A150 000	0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C6 0000A8C6 0000A8C6 0000A8C6 0000A7C8 0000A7C8 0000A7C8 0000A7C8 0000A7C8 0000A7C8 0000A7C8 00000C1 00000C1 00000C1 00000C1 00000C1 00000C1 00000C1 0000C1 00	Hint/Name RVA End of Imports Ordinal	0249 exit 02C1 strncpy 02A6 rand 00A6 _beginthreadex 0049 _CxoFrameHandler 02B4 srand 02D0 time 0062 _p _argc MSVCRT.dll 0093 InternetOpenA 0093 InternetOpenUrlA 0093 InternetCloseHandle WININET.dll 0003 0010 0011 0013 0000 0000 0000 00
0000A1E6 0000A1E7 0000A114 0000A114 0000A116 0000A120 0000A120 0000A120 0000A120 0000A130 0000A130 0000A130 0000A140 0000A140 0000A140 0000A160 0000A160 0000A160 0000A160 0000A160 0000A160 0000A170 0000A170	0000A8C2 0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A7C5 00000C5 00000C5 0000C5 0000C	Hint/Name RVA Cordinal Ordinal	021 strincpy 0216 rand 0016beginthreadex 0019Cx5rrameHandler 0284 srand 0200 time 0062p_ argc MSVCRT.dill 0093 InternetOpenDrIA 0093 InternetOpenDrIA 0093 InternetCloseHandle VININET.dill 0003 0010 0010 0013 0006 0010 0017 0000 0001 0017 0000 0017 0000 0017 0000 0001
0000A1E8 0000A1E8 0000A114 0000A118 0000A118 0000A120 0000A124 0000A124 0000A130 0000A130 0000A130 0000A130 0000A150 000	0000A8C2 0000A8C2 0000A8C2 0000A8C3 0000A8C4 0000A8C4 0000A8C4 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A8C5 0000A7C5 00000C5 00000C5 0000C5 0000C	Hint/Name RVA End of Imports Ordinal	0249 exit 02C1 strncpy 02A6 rand 00A6 _beginthreadex 0049 _CxoFrameHandler 02B4 srand 02D0 time 0062 _p _argc MSVCRT.dll 0093 InternetOpenA 0093 InternetOpenUrlA 0093 InternetCloseHandle WININET.dll 0003 0010 0011 0013 0000 0000 0000 00

Fig 6: Import Address Table



PEStudio

property	value
	10.00
md5	<u>DB349B97C37D22F5EA1D1841E3C89EB4</u>
sha1	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26
sha256	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 07 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00
first-bytes-text	MZ
file-size	3723264 bytes
entropy	7.964
imphash	n/a
signature	Microsoft Visual C++ v5.0/v6.0 (MFC)
tooling	wait
entry-point	55 8B EC 6A FF 68 A0 A1 40 00 68 A2 9B 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53
file-version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
description	Microsoft® Disk Defragmenter
file-type	<u>executable</u>
cpu	<u>32-bit</u>
subsystem	<u>GUI</u>
compiler-stamp	Sat Nov 20 09:03:08 2010 UTC
debugger-stamp	n/a
resources-stamp	Thu Jan 01 00:00:00 1970 UTC
import-stamp	Thu Jan 01 00:00:00 1970 UTC
exports-stamp	n/a

Fig 7: Basic Information about the executable



Basic Dynamic Analysis

Analysis with inetsim turned on

When the malware is executed with inetsim turned on, the malware does not execute. It tries to connect to "hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com". On successful connection it does not infect the system.

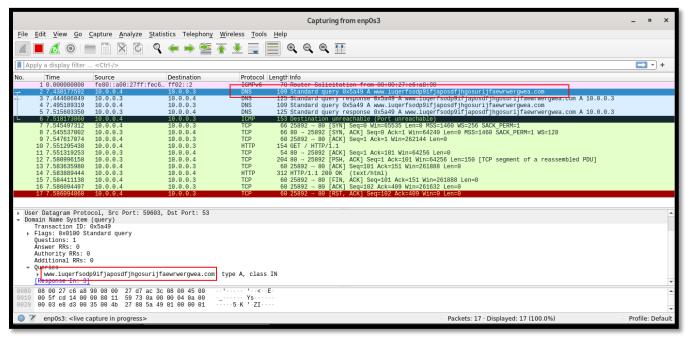


Fig 8: Network traffic when malware is executed



Analysis with inetsim turned off

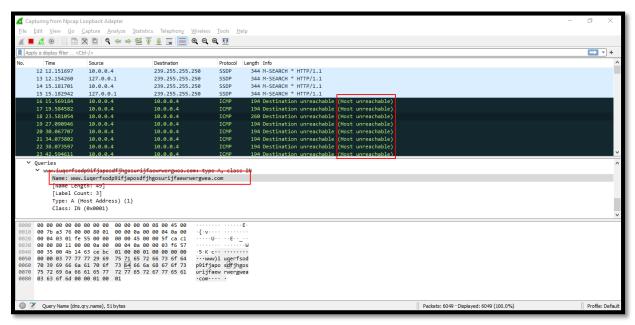


Fig 9: Network traffic when malware is executed. The requests are unreachable because inetsim is turned off

10:26: Ransomware.w	4784 TreateFileMappC:\Windows\SysWOW64\cryptsp.dl	II SUCCESS SyncType: SyncTy
10:26: 📧 Ransomware.w	4784 CreateFile C:\Windows\SysWOW64\rsaenh.dl	I SUCCESS Desired Access: R
10:26: 📧 Ransomware.w	4784 TreateFile C:\Windows\SysWOW64\rsaenh.dl	I SUCCESS Desired Access: R
10:26: 📧 Ransomware.w	4784 CreateFileMappC:\Windows\SysWOW64\rsaenh.dl	FILE LOCKED WI SyncType: SyncTy
10:26: • Ransomware.w	4784 CreateFileMapp C:\Windows\SysWOW64\rsaenh.dl	L SUCCESS SyncType: SyncTy
10:26: 📧 Ransomware.w	1248 CreateFile C:\Windows\tasksche.exe	SUCCESS Desired Access: R
10:26: 📧 Ransomware.w	1248 CreateFile C:\Windows\tasksche.exe	SUCCESS Desired Access: R
10:26: 📧 Ransomware.w	1248 CreateFile C:\Windows\tasksche.exe	SUCCESS Desired Access: R
10:26: 📧 Ransomware.w	1248 TreateFileMappC:\Windows\tasksche.exe	SUCCESS SyncType: SyncTy
10:26: • Ransomware.w	1248 TreateFileMappC:\Windows\tasksche.exe	FILE LOCKED WI SyncType: SyncTy
10:26: 📧 Ransomware.w	1248 TreateFileMappC:\Windows\tasksche.exe	SUCCESS SyncType: SyncTy
10:26: 📧 Ransomware.w	1248 CreateFile C:\Windows\apppatch\sysmain.sdb	SUCCESS Desired Access: G
10:26: • Ransomware.w	1248 CreateFile C:\Windows\apppatch\sysmain.sdb	SUCCESS Desired Access: G
10:26: 📭 Ransomware w	1248 CreateFileMappC:\Windows\apppatch\svsmain.sdb	FILE LOCKED WI SyncType: SyncTy

Fig 10: Procmon analysis. Creation of tasksche.exe file

TU.Z6 III taskscrie.exe	420 MICIOSEFIIE	C. Vriogrami Data Wobrogerzoo Vaskserie	3UCCE33	
10:26: ■ tasksche.exe	3428 ➪ Load Image	C:\ProgramData\xdbrugci209\tasksche	SUCCESS	Image Base: 0x400
10:26: ■ tasksche.exe	3428 🦮 CreateFile	C:\ProgramData\xdbrugci209	SUCCESS	Desired Access: E
10:26: ■ tasksche.exe	3428 🧱 Create File	C:\ProgramData\xdbrugci209	SUCCESS	Desired Access: R
10:26: Intaksche.exe	3428 🙀 Query Basic Infor	C:\ProgramData\xdbrugci209	SUCCESS	CreationTime: 9/25
10:26: ■ tasksche.exe	3428 🙀 Close File	C:\ProgramData\xdbrugci209	SUCCESS	
10:26: ■ tasksche.exe	3428 🙀 Create File	C:\ProgramData\xdbrugci209\b.wnry	SUCCESS	Desired Access: G
10.00	2420 - Wa El	CVD D.L.V.II :200VL	CHECECO	011 1 1 1

Fig 11: Wannacry creates tasksche.exe and executes it. Tasksche.exe creates a file with a random name in C:\ProgramData\{random name}. This folder is a staging area for wannacry ransomware



ile Edit View Process	Connection TCP v4	TCP v6	1 UDP v4 /	5 UDP v6	ran					
rocess Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packe
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2256	169.254.224.1	445	9/25/2022 9:48:02 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2257	169.254.225.1	445	9/25/2022 9:48:02 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2263	169.254.226.1	445	9/25/2022 9:48:02 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2264	169.254.227.1	445	9/25/2022 9:48:02 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2270	169.254.228.1	445	9/25/2022 9:48:02 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2209	169.254.207.1	445	9/25/2022 9:48:00 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2217	169.254.210.1	445	9/25/2022 9:48:00 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2207	169.254.205.1	445	9/25/2022 9:48:00 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2215	169.254.208.1	445	9/25/2022 9:48:00 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2208	169.254.206.1	445	9/25/2022 9:48:00 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2216	169.254.209.1	445	9/25/2022 9:48:00 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2224	169.254.211.1	445	9/25/2022 9:48:00 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2226	169.254.212.1	445	9/25/2022 9:48:01 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2227	169.254.213.1	445	9/25/2022 9:48:01 PM	mssecsvc2.0	
Ransomware.wannacr	3028	TCP	Syn Sent	169.254.208.169	2228	169.254.214.1	445	9/25/2022 9:48:01 PM	mssecsvc2.0	

Fig 12: Tasksche.exe tries to locate and infect computers using port 445 (SMB)

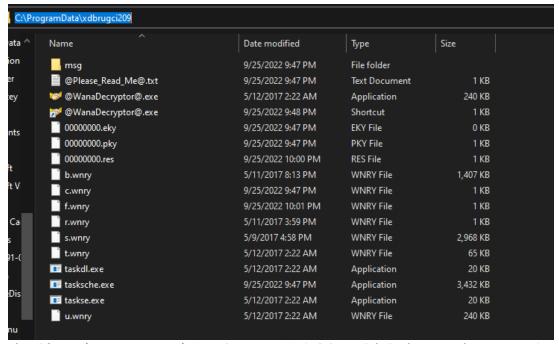


Fig 13: C:\ProgramData\{random name} folder which is staging area for wannacry



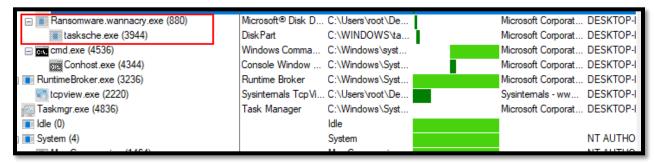


Fig 14: Procmon process tree

ME MACANC	4550	occurity center	Kummy	EOCOIDCIVICCIV
WSearch WSearch	3464	Windows Search	Running	
wuauserv		Windows Update	Stopped	netsvcs
		WWAN AutoConfig	Stopped	LocalSystemN
XbIAuthManager		Xbox Live Auth Manager	Stopped	netsvcs
XblGameSave		Xbox Live Game Save	Stopped	netsvcs
XboxGipSvc		Xbox Accessory Management Service	Stopped	netsvcs
XboxNetApiSvc		Xbox Live Networking Service	Stopped	netsvcs
🔍 xdbrugci209		xdbrugci209	Stopped	

Fig 15: Task Manager. Service name is same as the random file name created by tasksche.exe

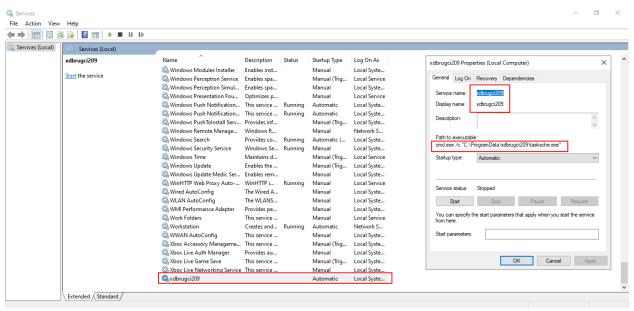


Fig 16: Service. Service name is same as the random file name created by tasksche.exe. This service just invokes the tasksche.exe command on startup.



netcat-win32-1.12	9/25/2022 10:09 PM	File folder	
nestudio pestudio	9/25/2022 10:09 PM	File folder	
PMAT-labs-main	9/25/2022 10:09 PM	File folder	
SysinternalsSuite	9/25/2022 10:10 PM	File folder	
@Please_Read_Me@.txt	9/25/2022 9:47 PM	Text Document	1 KB
🌠 @WanaDecryptor@.exe	9/25/2022 9:48 PM	Shortcut	1 KB
📶 fakenet_logs	8/16/2022 12:01 PM	Shortcut	1 KB
📊 FLARE	8/16/2022 11:26 AM	Shortcut	2 KB
👩 Google Chrome	8/17/2022 2:01 AM	Shortcut	3 KB
install.ps1.WNCRY	8/16/2022 5:54 AM	WNCRY File	16 KB
netcat-win32-1.12.zip WNC	RY 8/31/2022 7:14 AM	WNCRY File	110 KB
pestudio.zip WNCRY	8/17/2022 8:53 PM	WNCRY File	1,106 KB
PMAT-labs-main.zip.WNCR	Y 8/17/2022 2:35 AM	WNCRY File	14,528 KB
README.tx: .WNCRY	8/16/2022 12:02 PM	WNCRY File	2 KB
SysinternalsSuite.zip.WNCR	Y 8/30/2022 6:29 AM	WNCRY File	45,403 KB

Fig 17: New files added and old files are encrypted.



Fig 18: After Infection. New desktop icons and ransom payment popup





Fig 19: After Infection. Ransom message



Advanced Static Analysis

Cutter

```
[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_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
            esp, 0x50
    sub
    push
            esi
            edi
    push
    mov
            ecx.
            esi, str.http:__www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com ; 0x4313d0
    mov
            edi, [var_8n]
    lea
            movsd dword es:[edi], dword ptr [esi]
    rep
    movsb
            byte es:[edi], byte ptr [esi]
                                                                  Kill Switch URL
            dword [var_41h], eax
            dword [var_45h], eax
dword [var_49h], eax
dword [var_4dh], eax
            dword [var_51h], eax
word [var_55h], ax
    push
            eax
            eax
    push
    push
    push
            eax
            byte [var_6bh], al
    mov
            dword [InternetOpenA]
                                        ; 0x40a134
    push
            0x84000000
    push
            ecx, [var_14h]
    lea
           dword [InternetOpenUrlA] ; 0x40a138
   test edi, edi
            0x4081bc
                                                                               If url
If url
                      [0x004081a7]
                                                   [0x004081bc]
                                                                                exists
doesnot
                                                                               malware is
exists this
                                                            edi
                                                                               not
block gets
                                                                               executed
                              fcn.004080
                      call
                                                            edi
executed
                                                            eax, eax
                                                                               and it
                              eaı
which has a
                               eax, eax
                                                            esi
                                                                               exits out
function
                              esi
                                                    add
                                                                               of the
call
                      add
                                                            0x10
                                                                               program
```

Fig 20: Main function viewed inside cutter graph mode



Advanced Dynamic Analysis

X32dbg

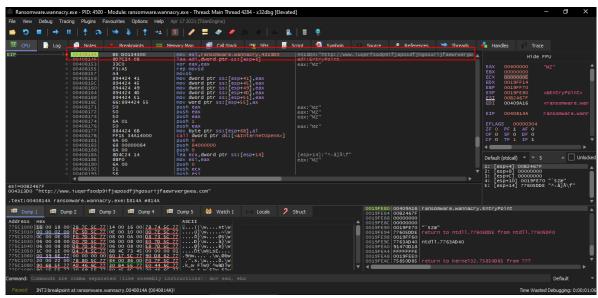


Fig 21: Set a breakpoint on kill switch URL

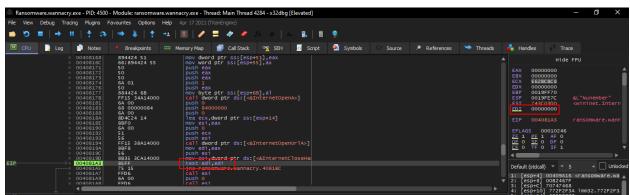


Fig 22: The kill switch URL was not found therefore the EDI has value 0



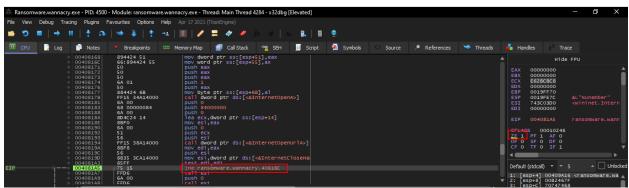


Fig 23: The zero flag is evaluated to 1 but we change it to 0

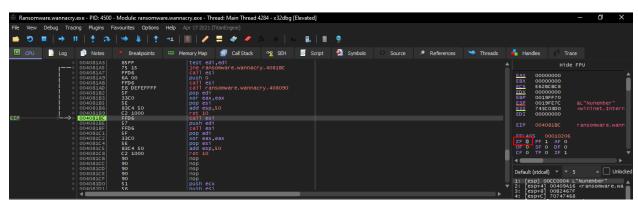


Fig 24: Changing the zero flag to 0. This makes the program to take the jump call and the malware is not executed.



Indicators of Compromise

Network Indicators

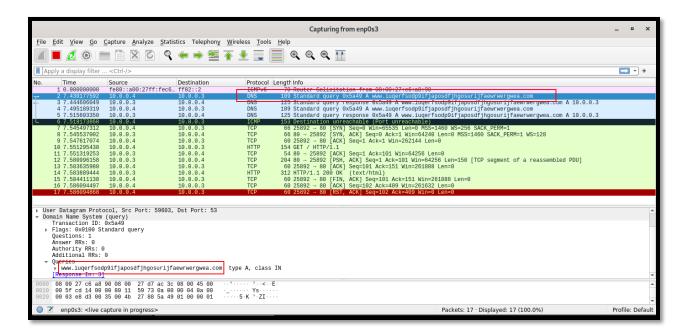


Fig 25: Initial connection to kill switch URL.

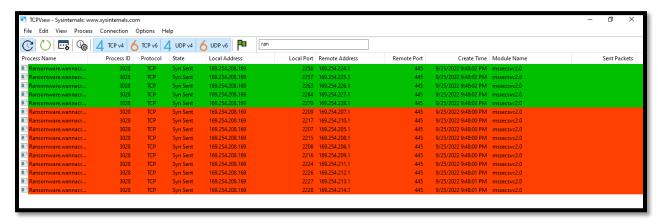


Fig 26: Locating other machines and exploiting them using 445 port (SMB)



Host-based Indicators

C:\Pr	ogramData\xdbrugci209			
ata ^	Name	Date modified	Туре	Size
ion	msg	9/25/2022 9:47 PM	File folder	
er	@Please_Read_Me@.txt	9/25/2022 9:47 PM	Text Document	1 KB
ey	🚧 @WanaDecryptor@.exe	5/12/2017 2:22 AM	Application	240 KB
	🌠 @WanaDecryptor@.exe	9/25/2022 9:48 PM	Shortcut	1 KB
nts	00000000.eky	9/25/2022 9:47 PM	EKY File	0 KB
	00000000.pky	9/25/2022 9:47 PM	PKY File	1 KB
	00000000.res	9/25/2022 10:00 PM	RES File	1 KB
τ	b.wnry	5/11/2017 8:13 PM	WNRY File	1,407 KB
t V	c.wnry	9/25/2022 9:47 PM	WNRY File	1 KB
	f.wnry	9/25/2022 10:01 PM	WNRY File	1 KB
Ca	r.wnry	5/11/2017 3:59 PM	WNRY File	1 KB
s	s.wnry	5/9/2017 4:58 PM	WNRY File	2,968 KB
91-(t.wnry	5/12/2017 2:22 AM	WNRY File	65 KB
	■ taskdl.exe	5/12/2017 2:22 AM	Application	20 KB
р.	tasksche.exe	9/25/2022 9:47 PM	Application	3,432 KB
:Dis	■ taskse.exe	5/12/2017 2:22 AM	Application	20 KB
	u.wnry	5/12/2017 2:22 AM	WNRY File	240 KB
nu				

Fig 27: random folder present inside C:\ProgramData which contains tasksche.exe. This exe is executed on startup.



Fig 28: @WanaDecryptor@.bpm, @WanaDecryptor@.exe present on User's desktop



Rules & Signatures

YARA Rule

```
rule Ransomware WannaCry {
 meta:
    last updated = "2022-09-26"
    author = "rishank-shah"
    description = "Yara rule for WannaCry Ransomware"
  strings:
   $string1 = "attrib +h ." fullword ascii
   $string2 = "icacls . /grant Everyone:F /T /C /Q" fullword ascii
    $string3 = "C:\\%s\\qeriuwjhrf" fullword ascii
    $string4 = "WNcry@2o17" fullword ascii
    $string5 = "wnry" ascii
    $url = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" ascii
   $payload = "tasksche.exe" ascii
    $PE magic byte = "MZ"
  condition:
    $PE magic byte at 0 and
    ($url or 1 of ($string*) or $payload)
```