

# WANNACRY RANSOMWARE ANALİZİ

## ZAYOTEM

---

## ***İÇİNDEKİLER***

---

### ***1.GİRİŞ***

---

### ***2.ANALİZ***

---

## 1- GİRİŞ

WannaCry bir çeşit ransomware(fidye yazılımı)dir. Bu zararlı yazılım kendi kendine bilgisayar ağları üzerinden yayılabilir. Kullanıcının bilgisayarına bulaştıktan sonra bütün dosyalarını şifreleyer ve okunamaz hale getirir. Dosyalarını kurtarmak isteyen kullanıcıdan belirtilen adrese kripto para yatırmasını ister. Zamanında yatırmazsa 3 gün içerisinde dosyaların şifresini açmaya yarayan “decryption key”in silineceğini ve bütün dosyaların kullanılamaz hale geleceğini belirtir.

Dosyayla ilgili temel bilgiler

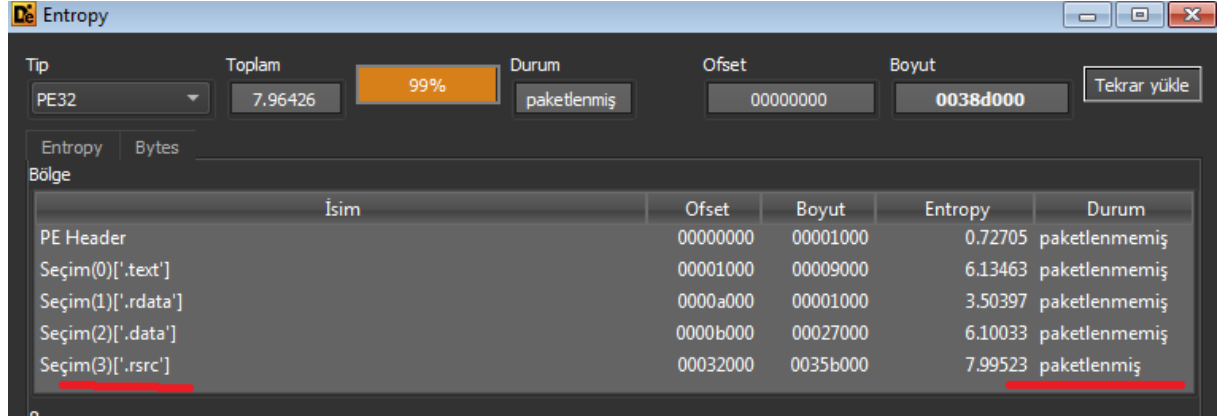
WannaCry.exe	
Property	Value
File Name	C:\Users\zorro\Desktop\s\WannaCry\WannaCry.exe
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	3.55 MB (3723264 bytes)
MD5	DB349B97C37D22F5EA1D1841E3C89EB4
SHA-1	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26

Uygulamada kullanılan kütüphaneler

WannaCry.exe				
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain
0000A62A	N/A	0000A1E0	0000A1E4	0000A1E8
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.dll	32	0000A2B0	00000000	00000000
ADVAPI32.dll	11	0000A280	00000000	00000000
WS2_32.dll	13	0000A3C4	00000000	00000000
MSVCP60.dll	2	0000A334	00000000	00000000
iphlpapi.dll	2	0000A3FC	00000000	00000000
WININET.dll	3	0000A3B4	00000000	00000000
MSVCRT.dll	28	0000A340	00000000	00000000

## 2. Analiz

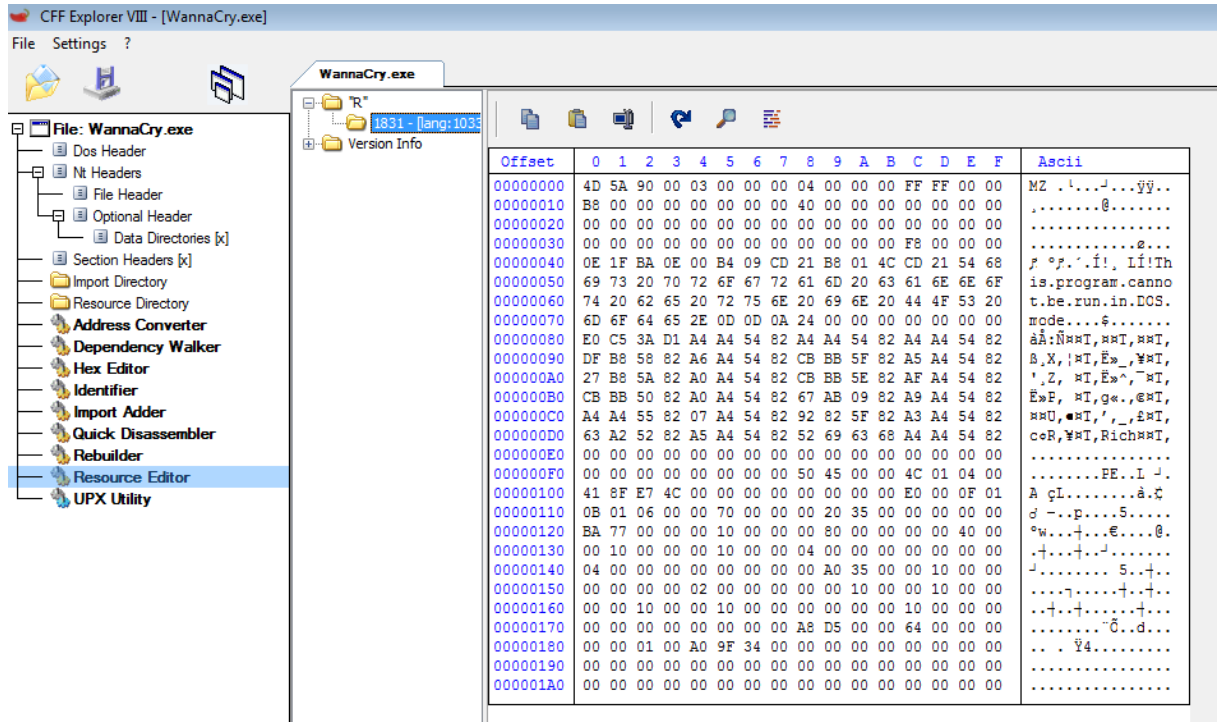
Programı Detect It Easy adlı analiz programına attığımda .rsrc sectionunda paketlenmiş bir veri olduğu gözükmemektedir.



Tip	Toplam	Durum	Ofset	Boyut
PE32	7.96426	99%	00000000	0038d000

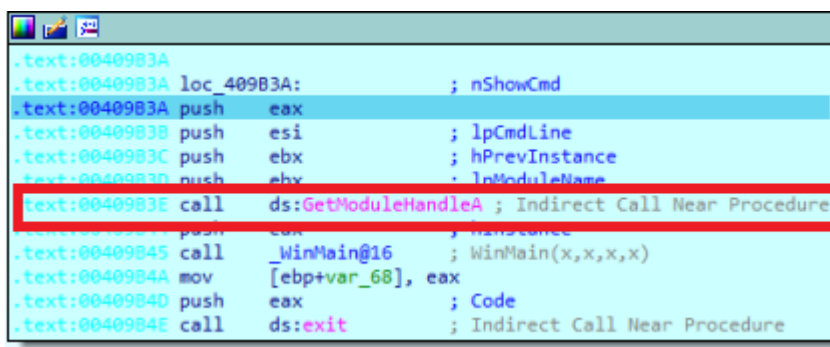
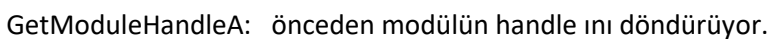
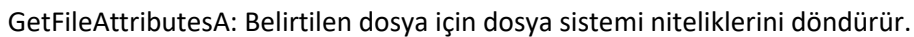
Bölge	İsim	Ofset	Boyut	Entropy	Durum
PE Header		00000000	00001000	0.72705	paketlenmemiş
Seçim(0)['.text']		00001000	00009000	6.13463	paketlenmemiş
Seçim(1)['.rdata']		0000a000	00001000	3.50397	paketlenmemiş
Seçim(2)['.data']		0000b000	00027000	6.10033	paketlenmemiş
Seçim(3)['.rsrc']		00032000	0035b000	7.99523	paketlenmiş



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ .i...j...yÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	,.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....e.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F8	00	00	00	.....e.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	p °p. .í! , Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is.program.canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t.be.run.in.DOS.
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode.....s.....
00000080	E0	C5	3A	D1	A4	A4	54	82	A4	A4	54	82	A4	A4	54	82	ââ:ÑÑÑI,ÑÑI,ÑÑI,
00000090	DF	B8	58	82	A6	A4	54	82	CB	BB	5F	82	A5	A4	54	82	ß,X, !ÑI,È»,¥ÑI,
000000A0	27	B8	5A	82	A0	A4	54	82	CB	BB	5E	82	AF	A4	54	82	' ,Z, ÑI,È»^, ÑI,
000000B0	CB	BB	50	82	A0	A4	54	82	67	AB	09	82	A9	A4	54	82	È»F, ÑI,g«,«ÑI,
000000C0	A4	A4	55	82	07	A4	54	82	92	82	5F	82	A3	A4	54	82	ÑÑU,«ÑI,' ,_ÑÑI,
000000D0	63	A2	52	82	A5	A4	54	82	52	69	63	68	A4	A4	54	82	ceR,¥ÑI,RichÑÑI,
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000F0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00	.....FE..L .
00000100	41	8F	E7	4C	00	00	00	00	00	00	00	00	E0	00	0F	01	A çL.....â.ç
00000110	0B	01	06	00	00	70	00	00	00	20	35	00	00	00	00	00	d -..p.....S.....
00000120	BA	77	00	00	00	10	00	00	00	80	00	00	00	00	40	00	°w...+...€.....@.
00000130	00	10	00	00	00	10	00	00	00	04	00	00	00	00	00	00	.+...+...J.....
00000140	04	00	00	00	00	00	00	00	00	A0	35	00	00	10	00	00	J..... S...+..
00000150	00	00	00	00	02	00	00	00	00	00	10	00	00	10	00	00	.....+...+...+...
00000160	00	00	10	00	00	10	00	00	00	00	00	00	00	10	00	00	.....+...+...+...
00000170	00	00	00	00	00	00	00	00	A8	D5	00	00	64	00	00	00	.....ç.....d...
00000180	00	00	01	00	A0	9F	34	00	00	00	00	00	00	00	00	00	... ÿ4.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Cff explorerde resource editör sekmesinde MZ başlıklı hex kodları görüyoruz. MZ Windows çalıştırılabilir dosyası demek. Dosyanın içerisine başka bir exe dosyası gömülmüş. Bunun dumpını alıp .exe dosyası olarak kaydediyoruz.

**STARTF\_USESHOWWINDOW** adlı değişkeni aradığını anlıyoruz.



http://www[.]juqerfsodp9ifjaposdfjhgosurijfaewrrergwea[.]com

sitesi stringler içerisinde görünüyor.

Hemen arkasından

InternetOpenA: wininet kütüphanesini kullanmak için bir nevi başlangıç fonksiyonu

InternetOpenUrlA: yukarıda belirtilen siteye bağlanmak için gerekli metod.

InternetCloseHandle: internet handle'ını kapatmaya yarıyor.

Metodlarıyla siteyle bağlantı kurmaya çalışıyor.

```
.text:00408174 push 1 ; dwAccessType
.text:00408176 push eax ; lpzAgent
.text:00408178 call ds:InternetOpenA ; Indirect Call Near Procedure
.text:00408181 push 0 ; dwContext
.text:00408183 push 8400000h ; dwFlags
.text:00408188 push 0 ; dwHeadersLength
.text:0040818A lea ecx, [esp+64h+szUrl] ; Load Effective Address
.text:0040818E mov esi, eax
.text:00408190 push 0 ; lpzheaders
.text:00408192 push ecx ; lpzUrl
.text:00408193 push esi ; hInternet
.text:00408194 call ds:InternetOpenUrlA ; Indirect Call Near Procedure
.text:00408196 mov esi, esi ; hInternet
.text:00408198 push esi ; hInternet
.text:0040819D mov esi, ds:InternetCloseHandle
.text:004081A3 test edi, edi ; Logical Compare
.text:004081A5 jnz short loc_4081BC ; Jump if Not Zero (ZF=0)

x:004081A7 call esi ; InternetCloseHandle ; Indirect Call Near Procedure
x:004081A9 push 0 ; hInternet
x:004081AB call esi ; InternetCloseHandle ; Indirect Call Near Procedure
x:004081AD call sub_408090 ; Call Procedure
x:004081B3 xor eax, eax ; Logical Exclusive OR
x:004081BE nop

loc_4081BC:
x:004081BC call esi ; InternetCloseHandle ; Indirect Call Near
x:004081BE push edi ; hInternet
x:004081BF call esi ; InternetCloseHandle ; Indirect Call Near
x:004081C1 pop edi

80.00% (24,562) (6,170) 00008140 00408140: WinMain(x,x,x,x) (Synchronized with Hex View-1)
```

GetModuleFileNameA: lpfilename degiskeninde tutulan modülün tam konumunu alıyor.

```
.text:00408090 sub esp, 10h ; Integer Subtraction
.text:00408093 push 104h ; nSize
.text:00408098 push offset FileName ; lpFilename
.text:0040809D push 0 ; hModule
.text:0040809F call ds:GetModuleFileNameA ; Indirect Call Near Procedure
.text:004080A5 call ds:p_argc ; Indirect Call Near Procedure
.text:004080AB cmp dword ptr [eax], 2 ; Compare Two Operands
.text:004080AE jge short loc_4080B9 ; Jump if Greater or Equal (SF=OF)
```

OpenSCManagerA: Servis kontrol yöneticisiyle bağlantı kurup veritabanını açar

```

ure
.text:004080B9 loc_4080B9:
.text:004080B9 push     edi
.text:004080BA push     0F003Fh      ; dwDesiredAccess
.text:004080BE push     0          ; lpDatabaseName
.text:004080C1 push     0          ; lpMachineName
.text:004080C3 call     ds:OpenSCManagerA ; Indirect Call Near Procedure
.text:004080C9 mov     edi, eax
.text:004080CB test     edi, edi      ; Logical Compare
.text:004080CD jz      short loc_408101 ; Jump if Zero (ZF=1)

```

OpenServiceA: mssecsvc2.0 isimli servisi baslatıyor

CloseServiceHandle: servisin handle'ını kapatıyor

```

.text:004080D0 push     esi
.text:004080D1 push     0F01FFh      ; dwDesiredAccess
.text:004080D6 push     offset ServiceName ; "mssecsvc2.0"
.text:004080DB push     0          ; dwOpenMode
.text:004080DC call     ds:OpenServiceA ; Indirect Call Near Procedure
.text:004080E2 mov     ebx, ds:CloseServiceHandle
.text:004080E8 mov     esi, eax

```

HAZIRLAYAN TARIK YILDIZ