FickerStealer

Teknik Analiz Raporu

İçindekiler

Giriş

FickerStealer hacker forumlarında MaaS (Malware-as-a-Service) olarak sunulan bir bilgi hırsızı tehdidir. FickerStealer çeşitli oltalama yöntemleriyle dağıtılır.
Bu kötü amaçlı yazılımın virüs bulaşmış bilgisayarları;

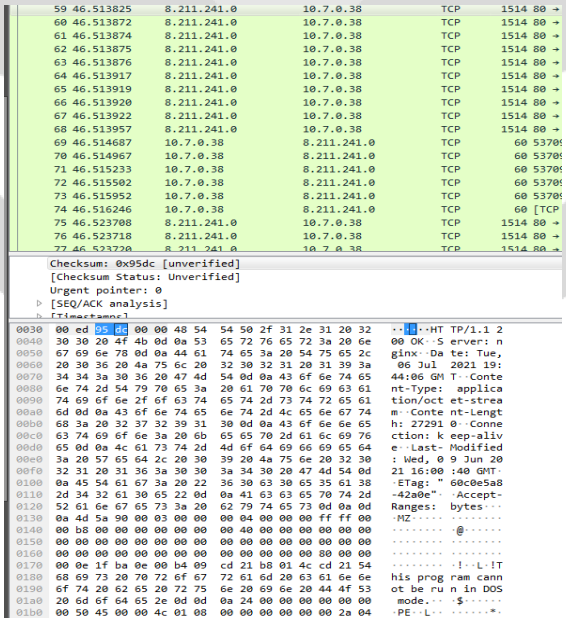
- Web tarayıcılarına kaydedilen kimlik bilgilerine,
- Masaüstü mesajlaşma istemcilerine,
- FTP istemcilerine,
- Blockchain cüzdanlarına,
- Bilgisayar belgelerine erişim sağlamasına olanak sağlamaktadır.

Ön İnceleme

İncelenen versiyondaki FickerStealer zararlısı bir DLL olarak, phishing yöntemleriyle yayılmayı sürdürmüştür. Zararlı dosya ilk "file.dll" olarak adlandırılmıştır. Yapılan analizler sonucunda bu dosyanın Stage 1'i gerçekleştirmek için loader görevi gördüğü tespit edilmiştir.

Dosya Adı:	file.dll
MD5	9b59d4744ff1de8b338eeb2b85748cf2
SHA1	f3306e866bc9992c2268f204f55e88f89833a25d
SHA256	fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4

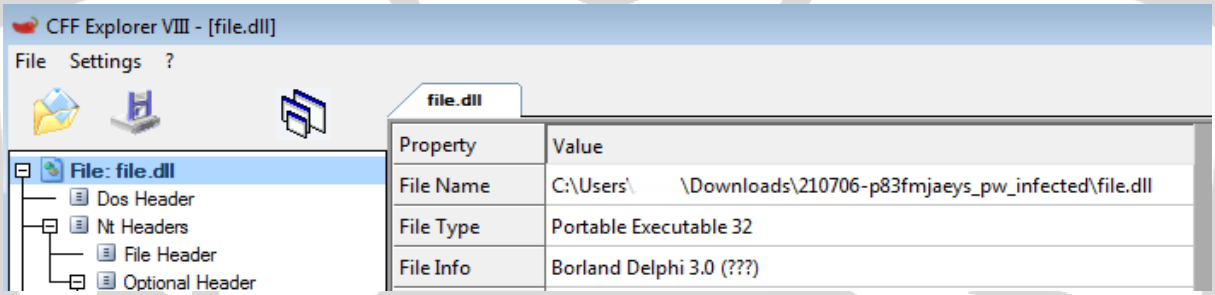
file.dll zararlısının network trafiği izlendiğinde MZ başlıklı bir dosya indirdiği gözlenmiştir.



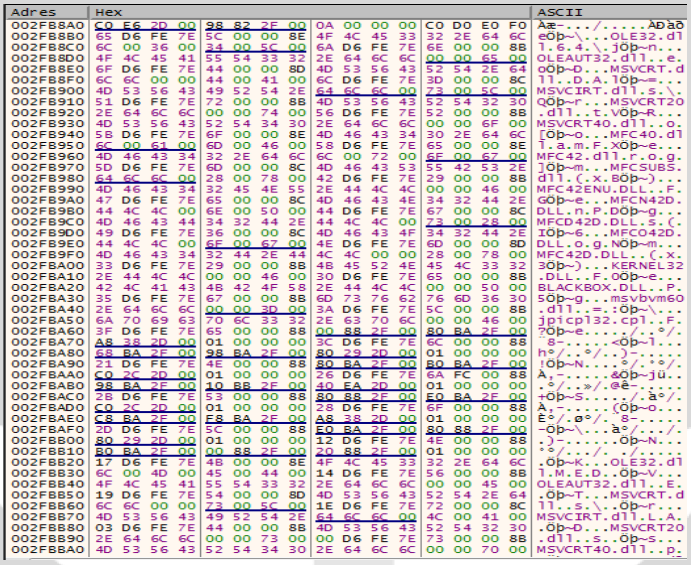
file.dll ANALİZİ

file.dll statik olarak incelendiğinde kendisinin 32 bit yürütülebilir bir dosya olduğu görülmektedir.

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 .ˡ...ˡ...ÿÿ..
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	....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F8	00	00	00	............ø...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	ƒ °ƒ.´.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....$.......

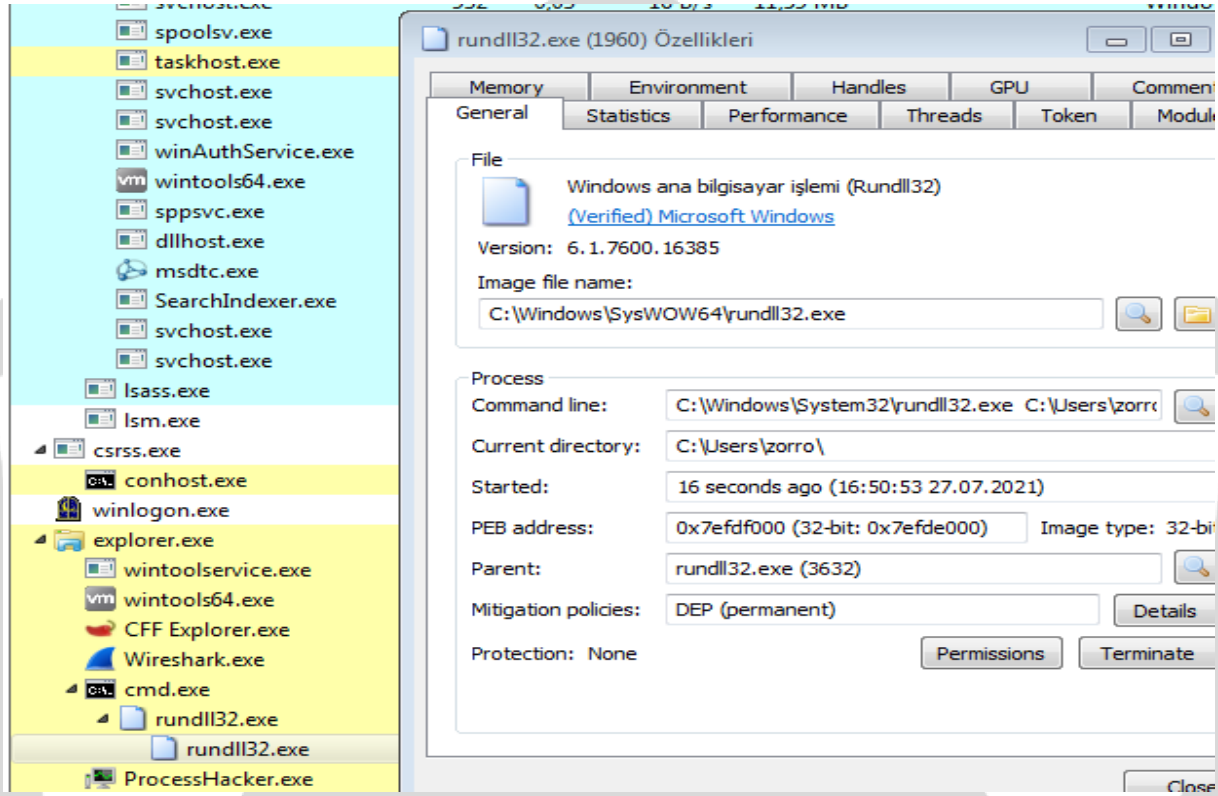


Dinamik olarak yüklenen DLL'ler:



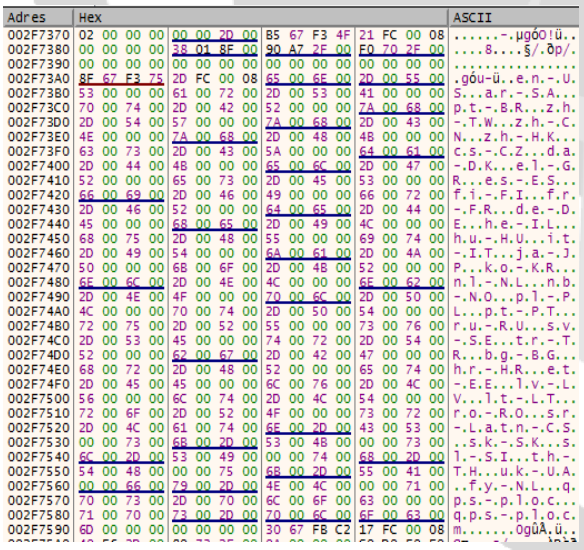
GDI32.dll	USP10.dll
MFC42.dll	msvcrt.dll
VERSION.dll	ADVAPI32.dll
MSCTF.dll	SHLWAPI.dll
OLEAUT32.dll	IMM32.dll

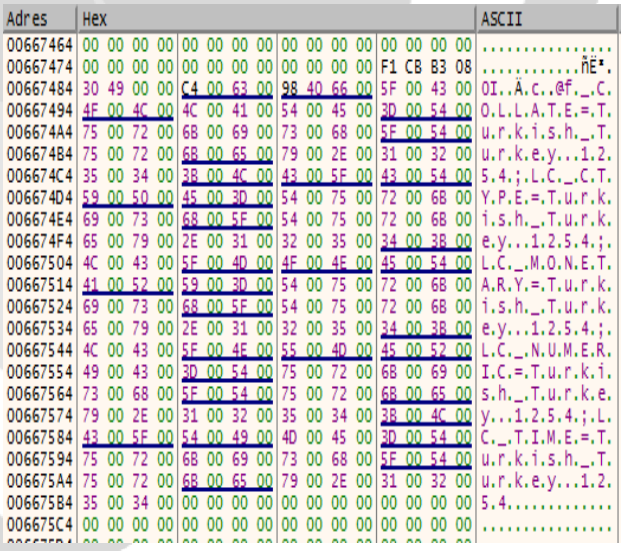
Genel olarak file.dll'in davranışları incelendiğinde, Process Hollowing tekniğini kullanarak kendini suspend olarak tekrardan çalıştırmaktadır.



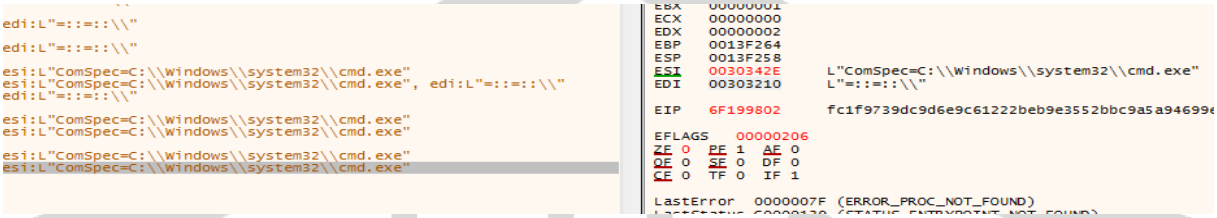
Topladığı Bilgiler:

Hedeflediği dil ve ülkeler:

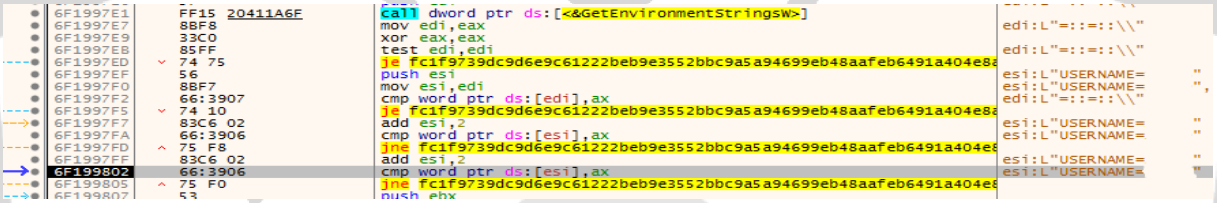




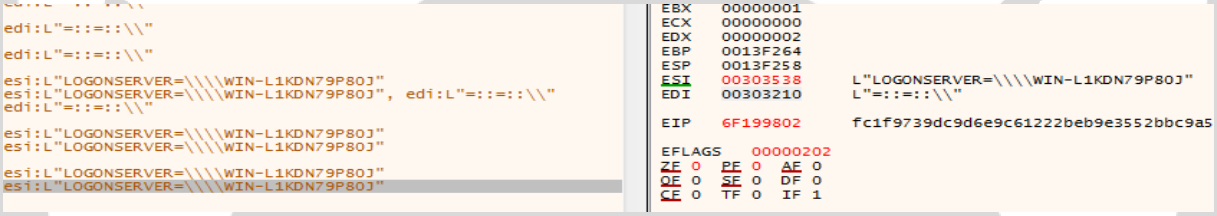
cmd.exe yolu:



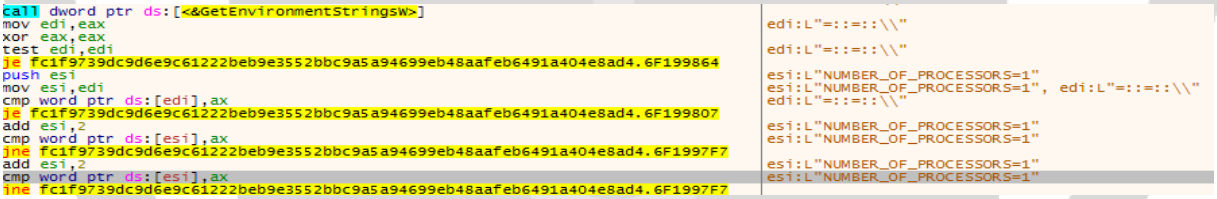
username:



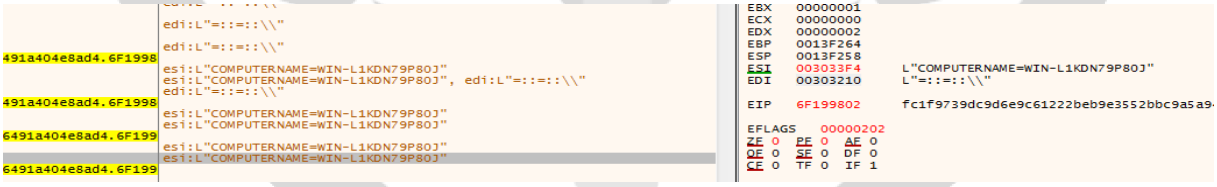
LOGONSERVER:



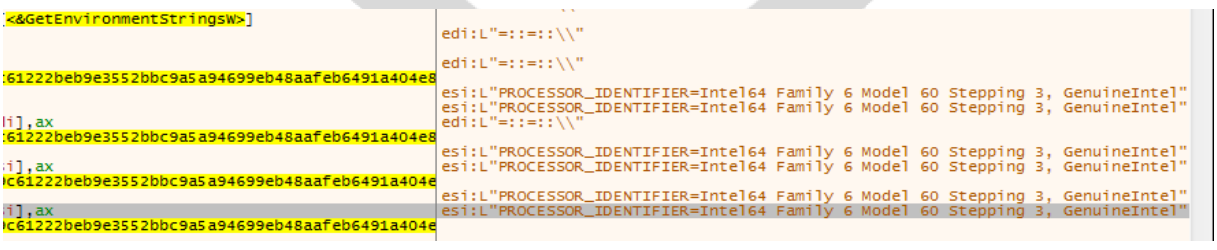
NUMBER_OF_PROCESSOR:



COMPUTERNAME:

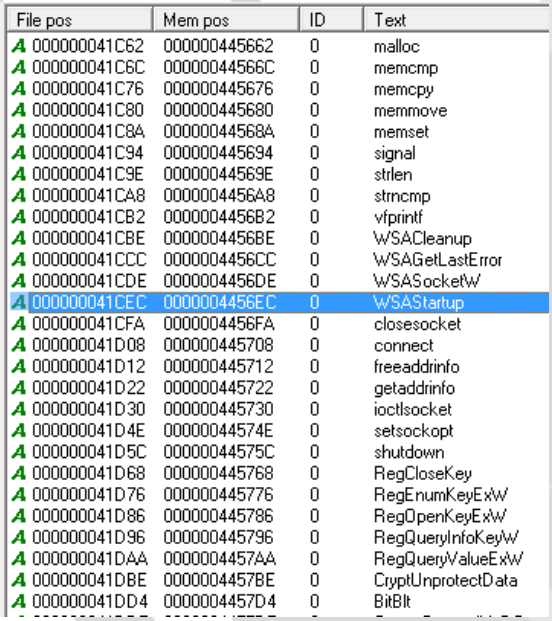


PROCESSOR:



7gfdg5egds.exe ANALİZİ

Dosya Adı:	7gfdg5egds.exe
MD5	270C3859591599642BD15167765246E3
SHA1	E227A8A338166DC97E360CA9CDDDA5E007079C58
SHA256	DEE4BB7D46BBBEC6C01DC41349CB8826B27BE9A0DCF39816CA8BD6E0A39C2019



File pos	Mem pos	ID	Text
000000041C62	000000445662	0	malloc
000000041C6C	00000044566C	0	memcmp
000000041C76	000000445676	0	memcpy
000000041C80	000000445680	0	memmove
000000041C8A	00000044568A	0	memset
000000041C94	000000445694	0	signal
000000041C9E	00000044569E	0	strlen
000000041CA8	0000004456A8	0	strncmp
000000041CB2	0000004456B2	0	vfprintf
000000041CBE	0000004456BE	0	WSACleanup
000000041CCC	0000004456CC	0	WSAGetLastError
000000041CDE	0000004456DE	0	WSASocketW
000000041CEC	0000004456EC	0	WSAStartup
000000041CFA	0000004456FA	0	closesocket
000000041D08	000000445708	0	connect
000000041D12	000000445712	0	freeaddrinfo
000000041D22	000000445722	0	getaddrinfo
000000041D30	000000445730	0	ioctlsocket
000000041D4E	00000044574E	0	setsockopt
000000041D5C	00000044575C	0	shutdown
000000041D68	000000445768	0	RegCloseKey
000000041D76	000000445776	0	RegEnumKeyExW
000000041D86	000000445786	0	RegOpenKeyExW
000000041D96	000000445796	0	RegQueryInfoKeyW
000000041DAA	0000004457AA	0	RegQueryValueExW
000000041DBE	0000004457BE	0	CryptUnprotectData
000000041DD4	0000004457D4	0	BitBlt

000000042300	000000445D00	0	msvcrt.dll
000000042340	000000445D40	0	WS2_32.dll
000000042360	000000445D60	0	ADVAPI32.dll
000000042374	000000445D74	0	CRYPT32.dll
00000004239C	000000445D9C	0	GDI32.dll
000000042470	000000445E70	0	KERNEL32.dll
000000042498	000000445E98	0	USER32.dll

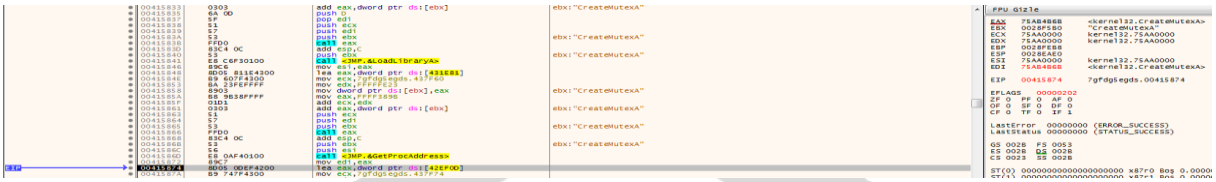
Zararlının import ettiklerine baktığımızda, USER32 ve WS2_32 gibi önemli kütüphaneleri kullanıyor. WS2_32 kütüphanesine baktığımızda içinde kullandığı fonksiyonlardan da anlaşılabileceği üzere network işlemleri gerçekleştirme kapasitesine sahip olduğu anlaşılmaktadır.

Zararlının içindeki önemli DLL ve fonksiyonları incelediğimizde;

- CreateToolhelp32Snapshot
- WriteFile
- GetSystemInfo
- CreateMutexA

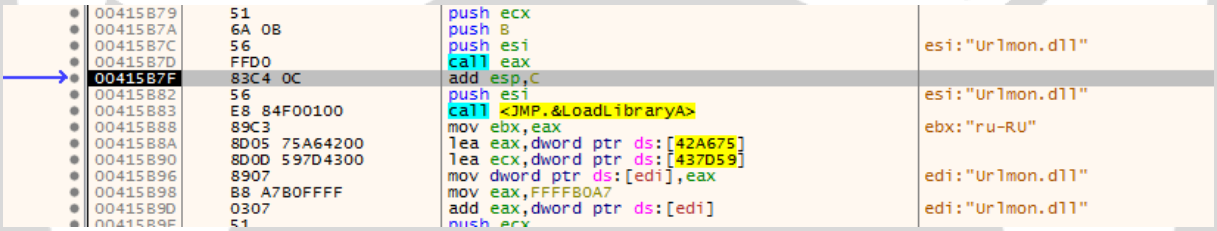
Zararlının, sistem bilgilerine ulaşabildiğini, mutex nesnesi oluşturduğunu, sistem ve dosyalar hakkında bilgi alabildiğini, dosya yazabildiğini, yapılan işlemin anlık görüntüsünü alabildiği görülmektedir.

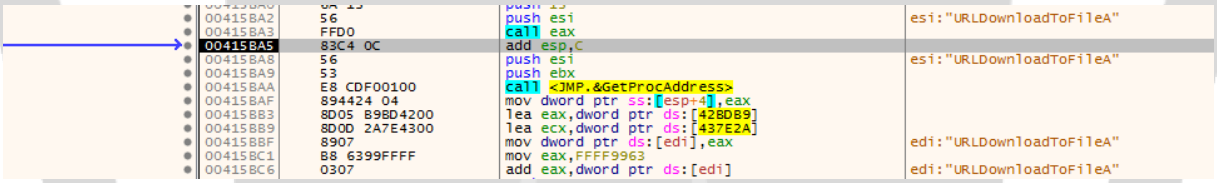
Zararlı ilk olarak dinamik olarak yüklediği “CreateMutexA” API ile mutex nesnesini oluşturuyor.



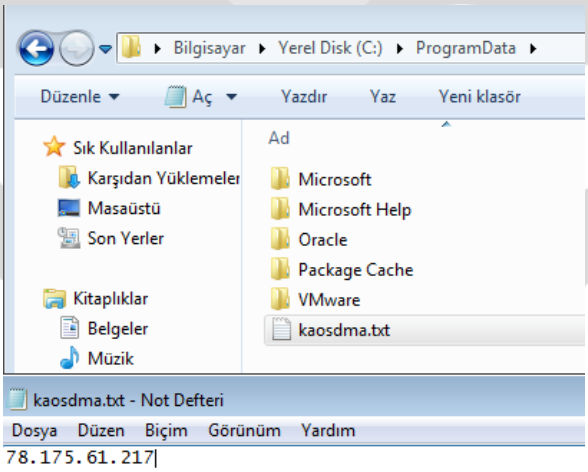
Mutex nesnesinin adı:

Dinamik olarak yüklediği diğer bazı DLL ve API’lar:

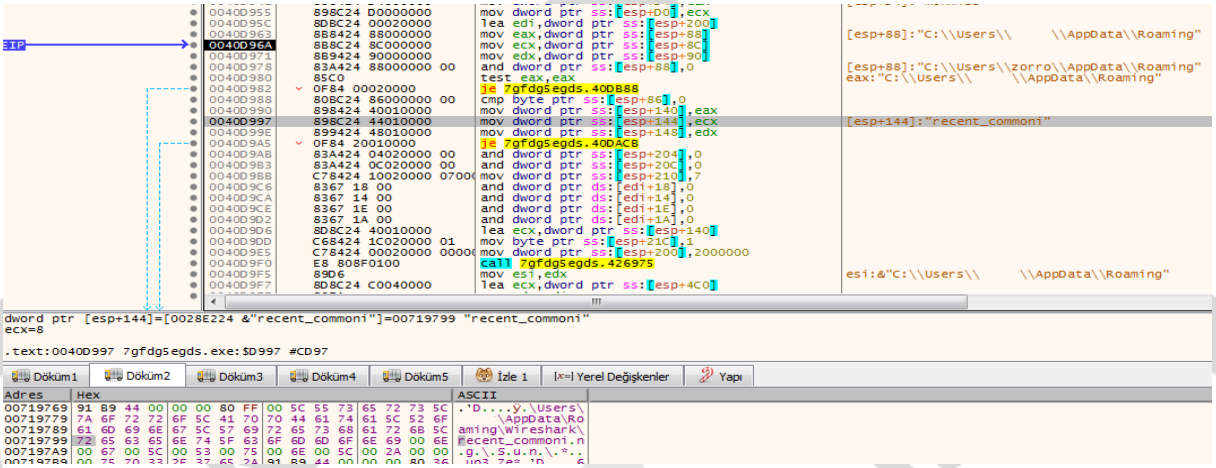




Zararlı daha sonra içinde bir ip adresi bulunan .txt uzantılı dosyayı ProgramData içine drop etmekte.



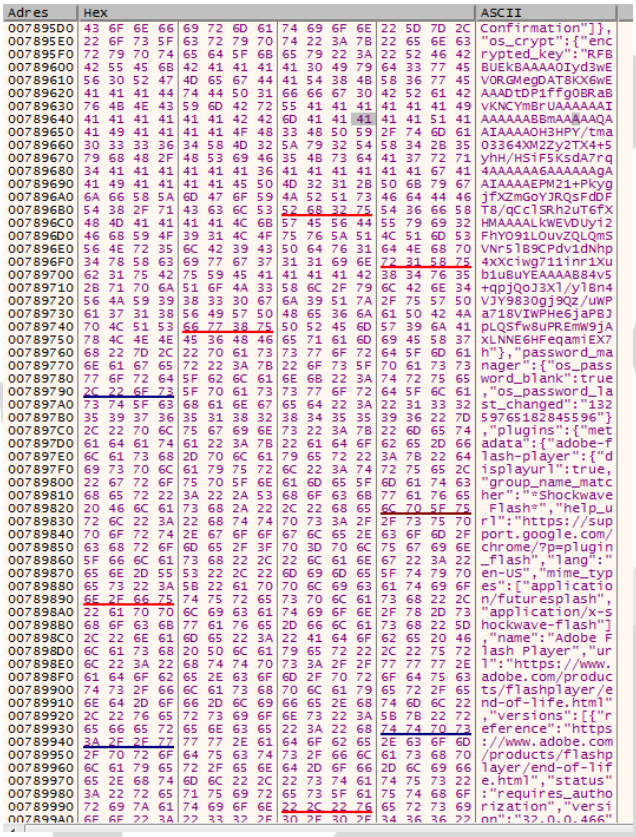
Genel olarak bakıldığında zararlı yazılımın 2 temel davranışı olduğu görülmektedir. İlk olarak sistemde yüklü olan yazılımları taramaktadır.

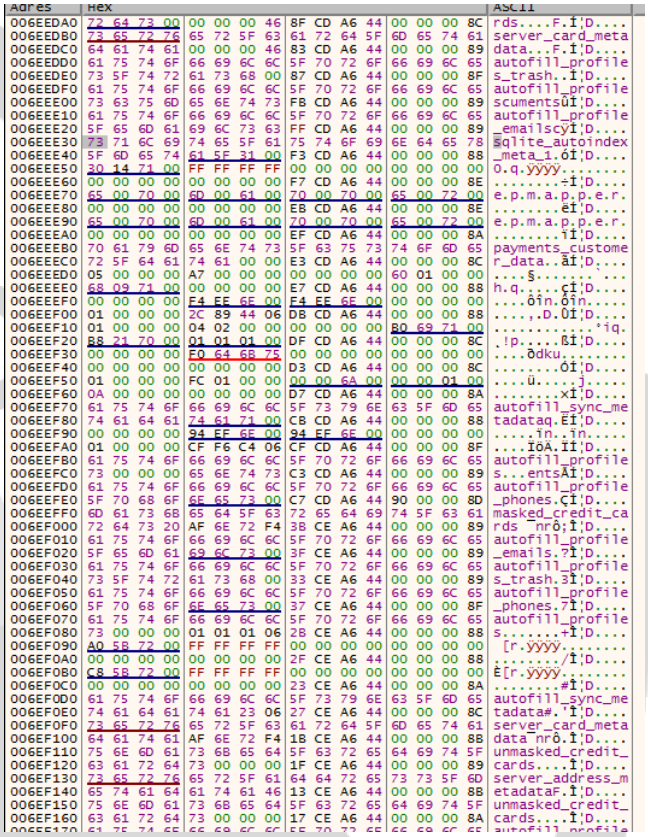


Diğer bir davranışı ise kişisel veri ve web tarayıcılarından kimlik bilgileri çalmasıdır. Çoğu uygulama yüklü olmadığından dolayı sadece kontrol ettiği görülmektedir.

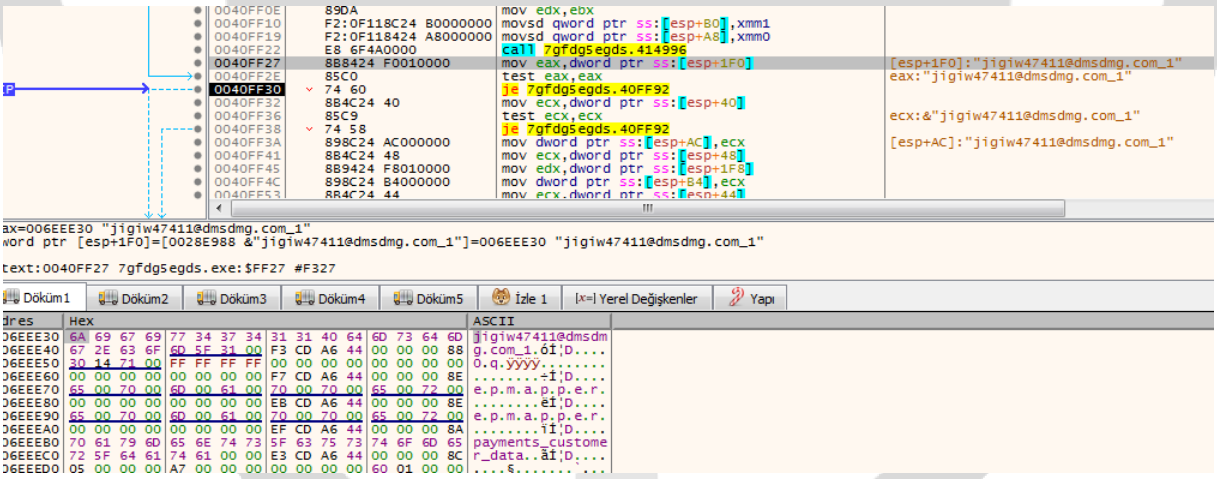
Google Chrome:

Google Chrome'da tutulan telefon numarası, kredi kartı bilgileri:

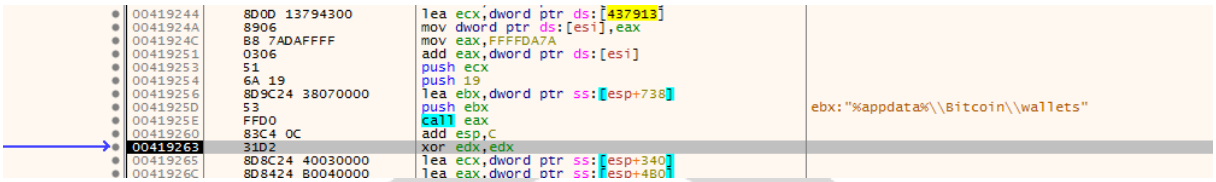




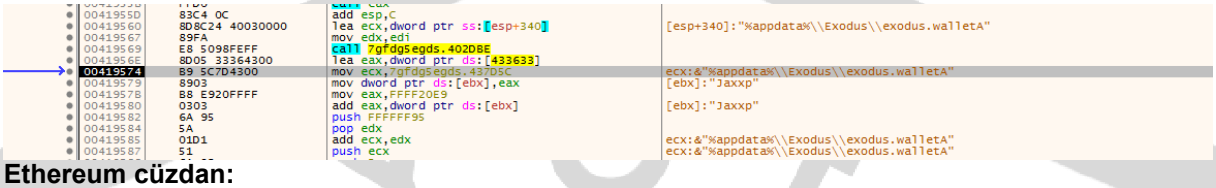
Giriş yaptıktan sonra Google Chrome'un tuttuğu e-posta adresi:



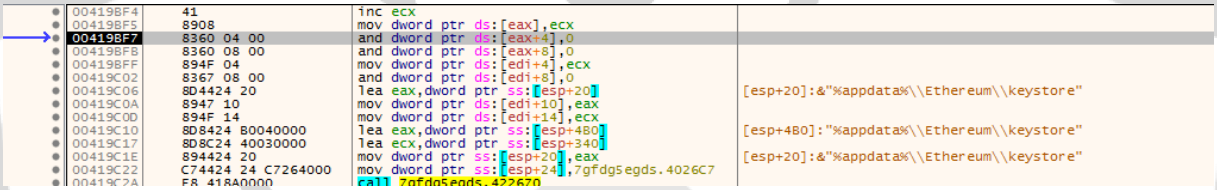
Bitcoin cüzdan:



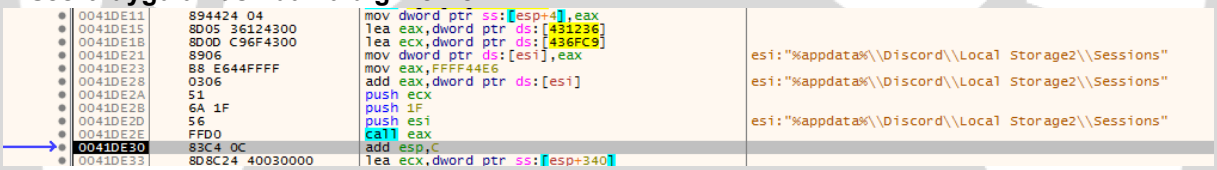
Exodus cüzdan:



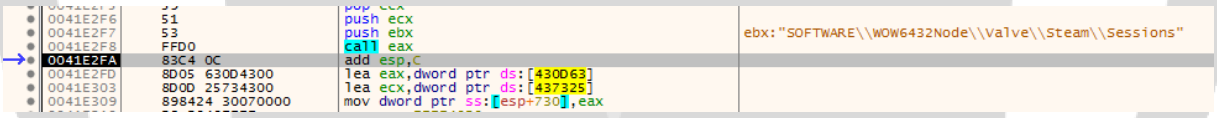
Ethereum cüzdan:



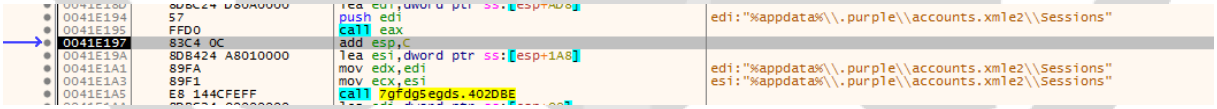
Discord uygulamasından aldığı veriler:



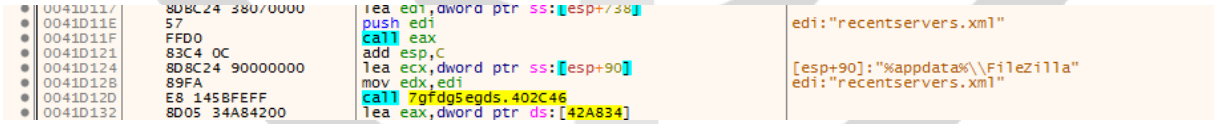
Steam:



.purple: Windowstaki yapılandırma dizinidir. Burada sohbet günlükleri, diğer kullanıcılardan gelen resimler, şifreler dahil olmak üzere hesapla ilgili bilgiler bulunabilir.

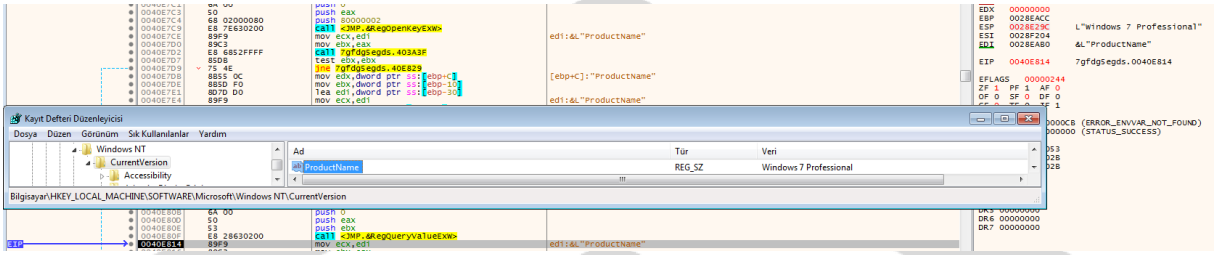


FileZilla:

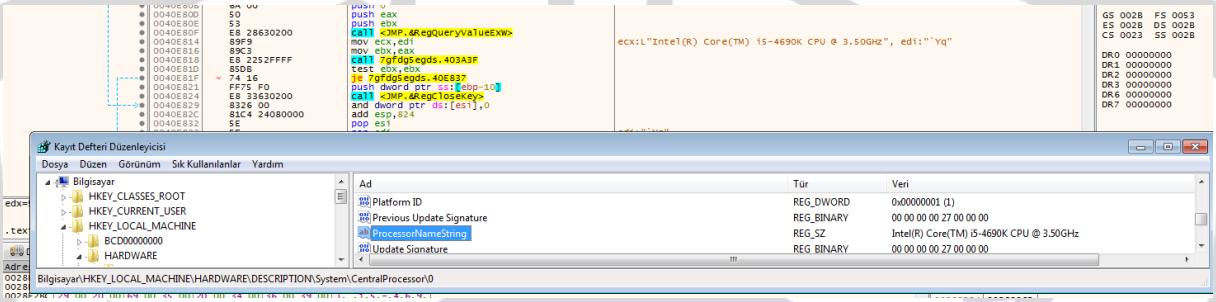


Burada zararlı yazılımın aldığı sistem bilgileri görülmektedir.

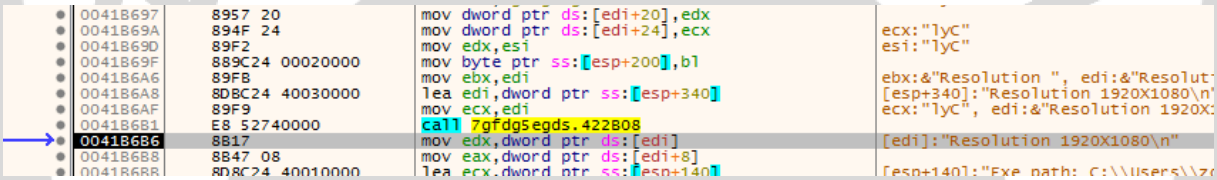
OS:



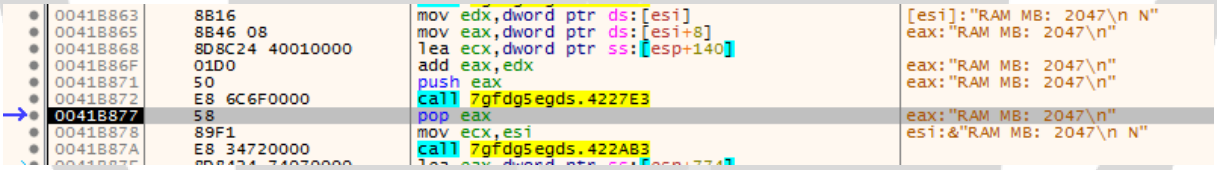
İşlemci:



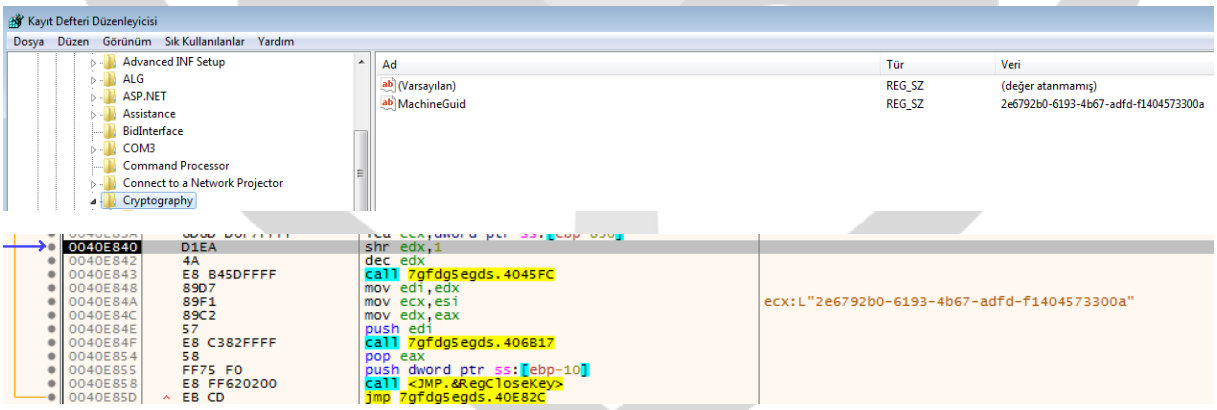
Çözünürlük:

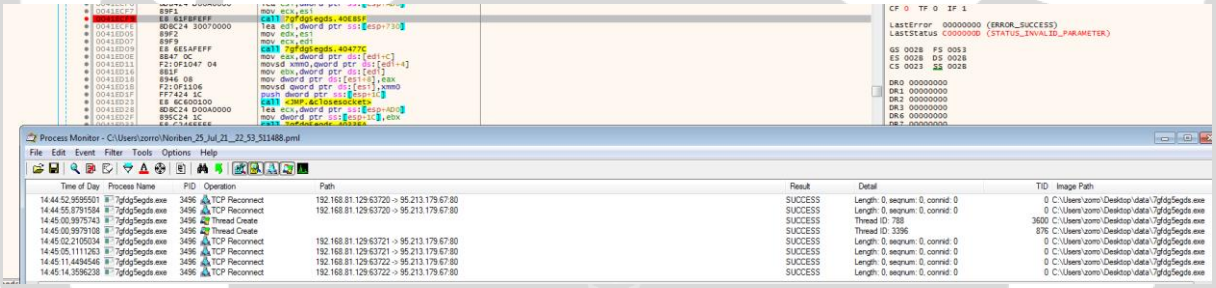


Ram:



Machine-Guid:





Zararlı yazılımın yapılan işlemin anlık görüntüsünü aldığını görmekteyiz.

```
0041C081   E8 6E8B0100           call <JMP.&Process32Next>
0041C086   83F8 01               cmp eax,1
0041C089   0F85 A9000000         jne 7gfdg5egds.41C138
0041C08F   8D8C24 64030000       lea ecx,dword ptr ss:[esp+364]
0041C096   E8 27CF0000           call 7gfdg5egds.428FC2
0041C09B   C78424 B0040000 9C7A4 mov dword ptr ss:[esp+4B0],7gfdg5egds.437A9C   [esp+4B0]:&"\"SomeNone", 437
0041C0A6   C78424 B4040000 03000 mov dword ptr ss:[esp+4B4],3
0041C0B1   83A424 B8040000 00    and dword ptr ss:[esp+4B8],0
0041C0B9   894424 20             mov dword ptr ss:[esp+20],eax                  [esp+20]:"x32dbg.exe"
0041C0BD   8D4424 20             lea eax,dword ptr ss:[esp+20]                  [esp+20]:"x32dbg.exe"
0041C0C1   8D7424 30             lea esi,dword ptr ss:[esp+30]
0041C0C5   895424 24             mov dword ptr ss:[esp+24],edx
0041C0C9   8D9424 B0040000       lea edx,dword ptr ss:[esp+4B0]                 [esp+4B0]:&"\"SomeNone"
0041C0D0   898424 08010000       mov dword ptr ss:[esp+108],eax                 [esp+108]:&"x32dbg.exe"
0041C0D7   8D8424 08010000       lea eax,dword ptr ss:[esp+108]                 [esp+108]:&"x32dbg.exe"
0041C0DE   89F1                  mov ecx,esi
0041C0E0   C78424 0C010000 39244 mov dword ptr ss:[esp+10C],7gfdg5egds.402439
```

Zararlının anti virüslerden kaçmak için kayıt defterinden değiştirdiği değerler:

```
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\cval  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiVirusOverride  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiSpywareOverride  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\FirewallOverride  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiVirusOverride  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiSpywareOverride  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\FirewallOverride  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiVirusOverride  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\AntiSpywareOverride  =  0
[RegSetValue] svchost.exe:744 > HKLM\SOFTWARE\MICROSOFT\Security Center\Svc\FirewallOverride  =  0
```

NETWORK ANALİZİ

```
0041ECF7   89F1                  mov ecx,esi
0041ECF9   E8 61FBFEFF           call 7gfdg5egds.40E85F
0041ECFE   8DBC24 30070000       lea edi,dword ptr ss:[esp+730]
0041ED05   89F2                  mov edx,esi
0041ED07   89F9                  mov ecx,edi
0041ED09   E8 6E5AFEFF           call 7gfdg5egds.40477C
0041ED0E   8B47 0C               mov eax,dword ptr ds:[edi+C]
0041ED11   F2:0F1047 04          movsd xmm0,qword ptr ds:[edi+4]
0041ED16   8B1F                  mov ebx,dword ptr ds:[edi]
0041ED18   8946 08               mov dword ptr ds:[esi+8],eax
0041ED1B   F2:0F1106             movsd qword ptr ds:[esi],xmm0
0041ED1F   FF7424 1C             push dword ptr ss:[esp+1C]
0041ED23   E8 6C600100           call <JMP.&closesocket>
0041ED28   8DBC24 D00A0000       lea ecx,dword ptr ss:[esp+AD0]
0041ED2F   895C24 1C             mov dword ptr ss:[esp+1C],ebx
```

```
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C000000D (STATUS_INVALID_PARAMETER)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

DR0 00000000
DR1 00000000
DR2 00000000
DR3 00000000
DR6 00000000
```

Process Monitor - C:\Users\zorro\Noriben_25_Jul_21__22_53_511488.pml

```
Time of Day       Process Name    PID   Operation      Path                                        Result   Detail                            TID   Image Path
14:44:52,9595501  7gfdg5egds.exe  3496  TCP Reconnect  192.168.81.129:63720 -> 95.213.179.67:80    SUCCESS  Length: 0, seqnum: 0, connid: 0     0   C:\Users\zorro\Desktop\data\7gfdg5egds.exe
14:44:55,8791584  7gfdg5egds.exe  3496  TCP Reconnect  192.168.81.129:63720 -> 95.213.179.67:80    SUCCESS  Length: 0, seqnum: 0, connid: 0     0   C:\Users\zorro\Desktop\data\7gfdg5egds.exe
14:45:00,9975743  7gfdg5egds.exe  3496  Thread Create                                              SUCCESS  Thread ID: 788                   3600  C:\Users\zorro\Desktop\data\7gfdg5egds.exe
14:45:00,9979108  7gfdg5egds.exe  3496  Thread Create                                              SUCCESS  Thread ID: 3396                   876  C:\Users\zorro\Desktop\data\7gfdg5egds.exe
14:45:02,2105034  7gfdg5egds.exe  3496  TCP Reconnect  192.168.81.129:63721 -> 95.213.179.67:80    SUCCESS  Length: 0, seqnum: 0, connid: 0     0   C:\Users\zorro\Desktop\data\7gfdg5egds.exe
14:45:05,1111263  7gfdg5egds.exe  3496  TCP Reconnect  192.168.81.129:63721 -> 95.213.179.67:80    SUCCESS  Length: 0, seqnum: 0, connid: 0     0   C:\Users\zorro\Desktop\data\7gfdg5egds.exe
14:45:11,4494546  7gfdg5egds.exe  3496  TCP Reconnect  192.168.81.129:63722 -> 95.213.179.67:80    SUCCESS  Length: 0, seqnum: 0, connid: 0     0   C:\Users\zorro\Desktop\data\7gfdg5egds.exe
14:45:14,3596238  7gfdg5egds.exe  3496  TCP Reconnect  192.168.81.129:63722 -> 95.213.179.67:80    SUCCESS  Length: 0, seqnum: 0, connid: 0     0   C:\Users\zorro\Desktop\data\7gfdg5egds.exe
```

Zararlı çaldığı verilerden sonra 95[.]213[.]179[.]67[:]80 adresine bağlanmaya çalıştığı görülmüştür. Fakat sunucu aktif olmadığı için bağlantı sağlayamamıştır.

```
Network Traffic:
==================
[UDP] svchost.exe:988 > 192.168.81.2:53
[UDP] 192.168.81.2:53 > svchost.exe:988
[UDP] svchost.exe:744 > 255.255.255.255:67
[UDP] 192.168.81.254:67 > svchost.exe:744
[TCP] 7gfdg5egds.exe:2536 > 50.16.239.65:80
[TCP] 50.16.239.65:80 > 7gfdg5egds.exe:2536
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:50805 > svchost.exe:988
[UDP] svchost.exe:988 > 224.0.0.252:5355
[UDP] System:4 > 192.168.81.2:137
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:57681 > svchost.exe:988
[UDP] System:4 > 192.168.81.255:137
[UDP] 192.168.81.129:137 > System:4
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:62065 > svchost.exe:988
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:54482 > svchost.exe:988
[TCP] jucheck.exe:1776 > 184.24.22.47:443
[TCP] 184.24.22.47:443 > jucheck.exe:1776
[TCP] jucheck.exe:1776 > 23.55.161.133:80
[TCP] 23.55.161.133:80 > jucheck.exe:1776
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:50409 > svchost.exe:988
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:52542 > svchost.exe:988
[TCP] jp2launcher.exe:1160 > b818:162f:0:0:0:0:0:0:443
[TCP] b818:162f:0:0:0:0:0:0:443 > jp2launcher.exe:1160
[TCP] jp2launcher.exe:1160 > 5db8:dc1d:0:0:0:0:0:0:80
[TCP] 5db8:dc1d:0:0:0:0:0:0:80 > jp2launcher.exe:1160
[UDP] fe80:0:0:0:a0e5:93f0:a5d4:a0f8:50460 > svchost.exe:988
[TCP] svchost.exe:988 > 23.55.161.165:80
[TCP] 23.55.161.165:80 > svchost.exe:988
```

```
0040E8A5   B9 E096FFFF           mov ecx,FFFF96E0                      ecx:&"pospvisis.com:803"
0040E8AA   894424 10             mov dword ptr ss:[esp+10],eax
0040E8AE   8B4424 10             mov eax,dword ptr ss:[esp+10]
0040E8B2   01C8                  add eax,ecx                           ecx:&"pospvisis.com:803"
0040E8B4   8D0D 58794300         lea ecx,dword ptr ds:[437958]         ecx:&"pospvisis.com:803"
0040E8BA   51                    push ecx                              ecx:&"pospvisis.com:803"
0040E8BB   6A 10                 push 10
0040E8BD   8DB424 F8000000       lea esi,dword ptr ss:[esp+F8]
0040E8C4   56                    push esi
0040E8C5   FFD0                  call eax
0040E8C7   83C4 0C               add esp,C
0040E8CA   8D8C24 04010000       lea ecx,dword ptr ss:[esp+104]        [esp+104]:"pospvisis.com:803"
0040E8D1   89F2                  mov edx,esi
0040E8D3   E8 F641FFFF           call 7gfdg5egds.402ACE
0040E8D8   F2:0F108424 04010000  movsd xmm0,qword ptr ss:[esp+104]
0040E8E1   8B9C24 0C010000       mov ebx,dword ptr ss:[esp+10C]
```

ÇÖZÜM ÖNERİLERİ

- Sistemlerde güncel, güvenilir bir anti virüs yazılımı kullanılmalı.
- Gelen mailler dikkatle okunmalı veya bilinmeyen kaynaklardan gelen maillere ve URL'ler ile ilgili şüpheli davranmalı ve eklerde tam tarama yapmadan dosya açılmamalı.
- Tüm yüklü olan yazılımlar ve işletim sistemi güncel tutulmalı.
- Kullanıcıların, kimlik avı şemalarından haberdar olmaları ve bu saldırıları nasıl yönetebilecekleri konusunda eğitimler verilmeli.
- Sistem üzerinde çalışan processlerin ağ hareketleri incelenmeli.

Yara Kuralları

```
import "hash"
rule FickerStealer
{
meta:
author = "Hakan Soysal - ZAYOTEM"
description ="file.dll"
strings:
 $export0 = "Closewhether"
 $export1 = "Meantduck"
 $export2 = "My"
 $export3 = "Ropemay"

 condition:
 hash.md5(0,filesize) == "9b59d4744ff1de8b338eeb2b85748cf2" or all of them
 }
```

```
import "hash"
rule FickerStealer
{
meta:
author ="Hakan Soysal - ZAYOTEM"
description ="7gfdg5egds.exe"
strings:
 $a =
"0x000102030405060708091011121314151617181920212223242526272829303132
333435363738394041424344454647484950515253545556575859606162636465666
768697071727374757677787980818283848586878889909192939495969798 99[]"
 $b = "_matherr(): %s in %s(%g, %g)  (retval=%g)\\n"
 $c = {48 09 0A 46 45 1B 48 08 53 1D 39 81 07 46 0A 1D}
 $d = {22 53 6F 6D 65 4E 6F 6E 65 00 00 00 BC 94 43 00}

 condition:
 hash.md5(0,filesize) == "270c3859591599642bd15167765246e3" or all of them
 }
```

Hakan Soysal

https://www.linkedin.com/in/hakansoysal/