

FickerStealer Teknik Analiz Raporu



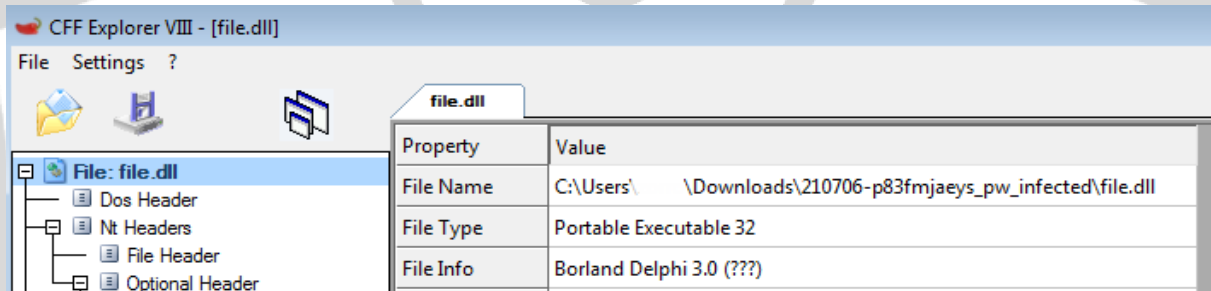
İçindekiler

Giriş	2
Ön İnceleme	2
file.dll ANALİZİ	3
7gfdg5egds.exe ANALİZİ	6
NETWORK ANALİZİ	13
ÇÖZÜM ÖNERİLERİ	14
Yara Kuralları	15

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 .!....J...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	00ø....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	 °.´.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....\$.....

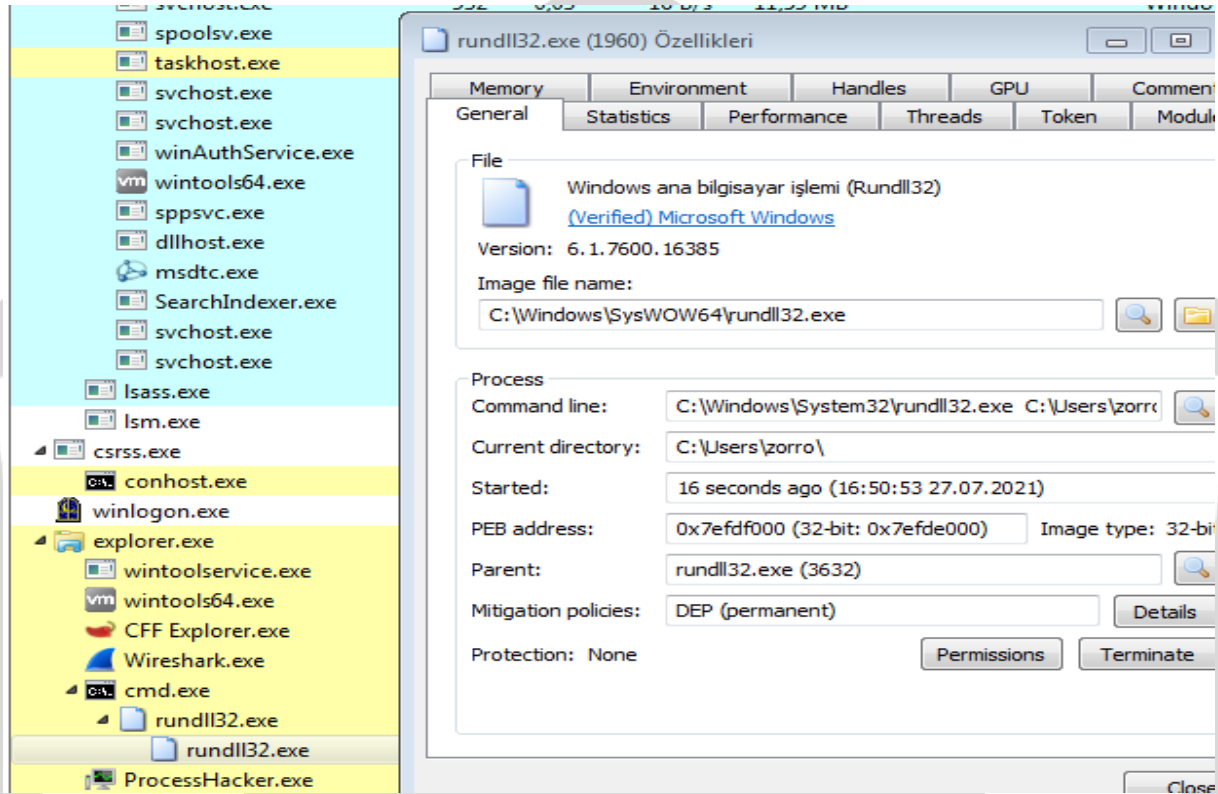


Dinamik olarak yüklenen DLL'ler:

Adres	Hex	ASCII
002F8BA0	C0 65 2D 00 98 82 2E 00 0A 00 00 00 C0 D0 E0 F0 A2/...Adab
002F8BB0	65 D6 FE 7E 5C 00 00 8E 4F 4C 45 33 32 2E 64 6C	eOp-...OLE32.dl
002F8BC0	6C 00 36 00 24 00 5C 00 6A D6 FE 7E 6E 00 00 88	1.6.4.\.jOp-n...
002F8BD0	4F 4C 45 41 55 54 33 32 2E 64 6C 6C 00 00 88	OLEAUT32.d11..e
002F8BE0	6F D6 FE 7E 44 00 00 8D 4D 53 56 43 52 54 2E 64	oOp-D...MSVCRT.d
002F8BF0	6C 6C 00 00 44 00 41 00 6C D6 FE 7E 3D 00 00 8C	11...D.A.Top-...
002F8C00	4D 53 56 43 49 52 54 2E 4E 8E 8C 00 62 00 5C 00	MSVCIRT.d11.s...
002F8C10	51 D6 FE 7E 67 00 00 88 4E 8E 8C 00 62 00 5C 00	QOp-...MSVCRT20
002F8C20	2E 64 6C 6C 00 00 74 00 56 D6 FE 7E 52 00 00 88	.d11..t.vOp-R...
002F8C30	4D 53 56 43 52 54 34 30 2E 64 6C 6C 00 00 6F 00	MSVCRT40.d11..o
002F8C40	58 D6 FE 7E 6F 00 00 8E 4D 46 43 34 30 2E 64 6C	[Op-o...MFC40.d1
002F8C50	6C 00 61 00 6D 00 46 00 58 D6 FE 7E 65 00 00 8E	T.a.m.F.xOp-e...
002F8C60	4D 46 43 34 32 2E 64 6C 6C 00 72 00 6E 00 67 00	MFC42.d11..F.o.g
002F8C70	47 D6 FE 7E 65 00 00 88 4D 46 43 34 30 2E 64 6C	[Op-o...MFC40.d1
002F8C80	64 6C 6C 00 28 00 78 00 42 D6 FE 7E 29 00 00 88	d11..(x.BOp-...
002F8C90	4D 46 43 34 32 2E 64 6C 6C 00 72 00 6E 00 67 00	MFC42ENU.DLL..F
002F8CA0	47 D6 FE 7E 65 00 00 88 4D 46 43 34 30 2E 64 6C	[Op-o...MFC40.d1
002F8CB0	44 4C 4C 00 6E 00 50 00 44 D6 FE 7E 67 00 00 8C	DLL.n.P.DOp-g...
002F8CC0	4D 46 43 34 34 32 2E 64 6C 6C 00 72 00 6E 00 67 00	MFC42D.DLL..S.(
002F8CD0	44 4C 4C 00 6F 00 67 00 4E D6 FE 7E 6D 00 00 8D	DLL.o.g.NOp-m...
002F8CE0	4D 46 43 34 32 2E 64 6C 6C 00 72 00 6E 00 67 00	MFC42D.DLL..(x
002F8CF0	33 D6 FE 7E 65 00 00 88 4B 45 52 4E 45 4C 33 32	3Op-)...KERNEL32
002F8D00	2E 44 4C 4C 00 00 46 00 30 D6 FE 7E 65 00 00 88	.DLL..F.OOp-e...
002F8D10	42 4C 41 43 48 42 4F 58 2E 44 4C 4C 00 00 50 00	BLACKBOX.DLL..P
002F8D20	2E 64 6C 6C 00 00 3D 00 3A D6 FE 7E 5C 00 00 88	.d11..F.OOp-e...
002F8D30	6A 70 69 63 70 6C 33 32 2E 63 70 6C 00 00 46 00	jOp-...cp132.cp1..F
002F8D40	3F D6 FE 7E 65 00 00 88 00 88 2F 00 80 BA 2F 00	7Op-e.../..?/..
002F8D50	A8 38 2D 00 01 00 00 00 3C D6 FE 7E 6C 00 00 88	8-...Op-1...
002F8D60	68 BA 2F 00 98 BA 2F 00 80 29 2D 00 01 00 00 00	h?/..?/..)
002F8D70	21 D6 FE 7E 4E 00 00 88 80 BA 2F 00 80 BA 2F 00	Op-N...9/..?/..
002F8D80	C0 2C 2D 00 01 00 00 00 25 D6 FE 7E 6A 6C 00 88	A-...Op-jü...
002F8D90	98 BA 2F 00 10 88 2F 00 40 FA 2D 00 01 00 00 00	..?/..?/..e...
002F8DA0	28 D6 FE 7E 53 00 00 88 80 BA 2F 00 80 BA 2F 00	Op-S.../..a?/..
002F8DB0	C0 2C 2D 00 01 00 00 00 25 D6 FE 7E 6A 6C 00 88	A-...Op-o...
002F8DC0	C8 BA 2F 00 F8 BA 2F 00 A8 38 2D 00 01 00 00 00	E?/..?/..8-...
002F8DD0	2D D6 FE 7E 5C 00 00 88 E0 BA 2F 00 80 88 2F 00	Op-...a?/..?/..
002F8DE0	80 29 2D 00 01 00 00 00 12 D6 FE 7E 4E 00 00 86	..?/...Op-N...
002F8DF0	80 BA 2F 00 00 88 2F 00 20 88 2F 00 01 00 00 00	..?/...Op-N...
002F8E00	17 D6 FE 7E 48 00 00 8E 4F 4C 45 33 32 2E 64 6C	.Op-k...OLE32.d1
002F8E10	60 00 4D 00 49 00 44 00 14 D6 FE 7E 56 00 00 8E	1.M.E.D...Op-V...
002F8E20	4F 4C 45 41 55 54 33 32 2E 64 6C 6C 00 00 45 00	OLEAUT32.d11..E
002F8E30	19 D6 FE 7E 54 00 00 8D 4D 53 56 43 52 54 2E 64	.Op-T...MSVCRT.d
002F8E40	6C 6C 00 00 72 00 5C 00 1E D6 FE 7E 00 00 00 8C	11..s...Op-r...
002F8E50	4D 53 56 43 49 52 54 2E 64 6C 6C 00 4C 00 41 00	MSVCIRT.d11.L.A
002F8E60	03 D6 FE 7E 44 00 00 88 4D 53 56 43 52 54 32 30	.Op-D...MSVCRT20
002F8E70	2E 64 6C 6C 00 00 73 00 00 D6 FE 7E 73 00 00 88	.d11..s...Op-S...
002F8E80	4D 53 56 43 52 54 34 30 2E 64 6C 6C 00 00 70 00	MSVCRT40.d11..p

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:

Adres	Hex	ASCII	Adres	Hex	ASCII
002F7370	02 00 00 00üüüü	00667464	00 00 00 00
002F7380	00 00 00 008...	00667474	00 00 00 00F1 CB B3 08
002F7390	00 00 00 00göüü.e.n..U	00667484	30 49 00 00	0I..Ä.c.,@f.,C.
002F73A0	8F 67 F3 75	20 FC 00 08	00667494	4F 00 4C 00	4C 00 41 00
002F73B0	53 00 00 00	61 00 72 00	006674A4	75 00 72 00	68 00 69 00
002F73C0	70 00 74 00	20 00 42 00	006674B4	75 00 72 00	68 00 65 00
002F73D0	20 00 54 00	57 00 00 00	006674C4	35 00 34 00	38 00 4C 00
002F73E0	4E 00 00 00	7A 00 68 00	006674D4	59 00 50 00	45 00 3D 00
002F73F0	63 00 73 00	20 00 43 00	006674E4	69 00 73 00	68 00 5F 00
002F7400	20 00 44 00	48 00 00 00	006674F4	65 00 79 00	2E 00 31 00
002F7410	52 00 00 00	65 00 73 00	00667504	4C 00 43 00	5F 00 4D 00
002F7420	66 00 69 00	20 00 46 00	00667514	41 00 52 00	59 00 3D 00
002F7430	20 00 46 00	52 00 00 00	00667524	69 00 73 00	68 00 5F 00
002F7440	45 00 00 00	68 00 65 00	00667534	65 00 79 00	2E 00 31 00
002F7450	68 00 75 00	20 00 48 00	00667544	4C 00 43 00	5F 00 4E 00
002F7460	20 00 49 00	54 00 00 00	00667554	49 00 43 00	3D 00 54 00
002F7470	50 00 00 00	68 00 6F 00	00667564	73 00 68 00	5F 00 54 00
002F7480	6E 00 6C 00	20 00 4E 00	00667574	79 00 2E 00	31 00 32 00
002F7490	20 00 4E 00	4F 00 00 00	00667584	43 00 5F 00	54 00 49 00
002F74A0	4C 00 00 00	70 00 74 00	00667594	75 00 72 00	68 00 69 00
002F74B0	72 00 75 00	20 00 52 00	006675A4	75 00 72 00	68 00 65 00
002F74C0	20 00 53 00	45 00 00 00	006675B4	35 00 34 00	00 00 00 00
002F74D0	52 00 00 00	62 00 67 00	006675C4	00 00 00 00	00 00 00 00
002F74E0	68 00 72 00	20 00 48 00	006675D4	00 00 00 00	00 00 00 00
002F74F0	20 00 45 00	45 00 00 00	006675E4	00 00 00 00	00 00 00 00
002F7500	56 00 00 00	6C 00 74 00	006675F4	00 00 00 00	00 00 00 00
002F7510	72 00 6F 00	20 00 52 00	00667604	00 00 00 00	00 00 00 00
002F7520	20 00 4C 00	61 00 74 00	00667614	00 00 00 00	00 00 00 00
002F7530	00 00 73 00	68 00 2D 00	00667624	00 00 00 00	00 00 00 00
002F7540	6C 00 2D 00	53 00 49 00	00667634	00 00 00 00	00 00 00 00
002F7550	54 00 48 00	00 00 75 00	00667644	00 00 00 00	00 00 00 00
002F7560	00 00 66 00	79 00 2D 00	00667654	00 00 00 00	00 00 00 00
002F7570	70 00 73 00	20 00 70 00	00667664	00 00 00 00	00 00 00 00
002F7580	71 00 70 00	73 00 2D 00	00667674	00 00 00 00	00 00 00 00
002F7590	6C 00 00 00	00 00 00 00	00667684	00 00 00 00	00 00 00 00

cmd.exe yolu:

edi:L"=::~:\\\"	EBX 00000001
edi:L"=::~:\\\"	ECX 00000000
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	EDX 00000002
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe", edi:L"=::~:\\\"	EBP 0013F264
edi:L"=::~:\\\"	ESP 0013F258
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	ESI 0030342E L"ComSpec=C:\\Windows\\system32\\cmd.exe"
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	EDI 00303210 L"=::~:\\\"
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	EIP 6F199802 fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199802
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	EFLAGS 00000206
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	ZE 0 PE 1 AE 0
	OE 0 SE 0 DF 0
	CE 0 TF 0 IF 1
	LastError 0000007F (ERROR_PROC_NOT_FOUND)

username:

6F1997E1 FF15 20411A6F call dword ptr ds:[<&GetEnvironmentStringsW>]	edi:L"=::~:\\\"
6F1997E7 8BF8 mov edi,eax	edi:L"=::~:\\\"
6F1997E9 33C0 xor eax,eax	esi:L"USERNAME="
6F1997EB 85FF test edi,edi	esi:L"USERNAME="
6F1997ED 74 75 je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199802	edi:L"=::~:\\\"
6F1997EF 56 push esi	esi:L"USERNAME="
6F1997F0 8BF7 mov esi,edi	esi:L"USERNAME="
6F1997F2 66:3907 cmp word ptr ds:[edi],ax	esi:L"USERNAME="
6F1997F5 74 10 je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199802	esi:L"USERNAME="
6F1997F7 83C6 02 add esi,2	esi:L"USERNAME="
6F1997FA 66:3906 cmp word ptr ds:[esi],ax	esi:L"USERNAME="
6F1997FC 75 F8 jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F1997F7	esi:L"USERNAME="
6F1997FE 83C6 02 add esi,2	esi:L"USERNAME="
6F199802 66:3906 cmp word ptr ds:[esi],ax	esi:L"USERNAME="
6F199805 75 F0 jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F1997F7	
6F199807 53 push ebx	

LOGONSERVER:

edi:L"=::~:\\\"	EBX 00000001
edi:L"=::~:\\\"	ECX 00000000
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"	EDX 00000002
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J", edi:L"=::~:\\\"	EBP 0013F264
edi:L"=::~:\\\"	ESP 0013F258
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"	ESI 00303538 L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"	EDI 00303210 L"=::~:\\\"
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"	EIP 6F199802 fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199802
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"	EFLAGS 00000202
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"	ZE 0 PE 0 AE 0
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"	OE 0 SE 0 DF 0
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"	CE 0 TF 0 IF 1

NUMBER_OF_PROCESSOR:

call dword ptr ds:[<&GetEnvironmentStringsW>]	edi:L"=::~:\\\"
mov edi,eax	edi:L"=::~:\\\"
xor eax,eax	esi:L"NUMBER_OF_PROCESSORS=1"
test edi,edi	esi:L"NUMBER_OF_PROCESSORS=1", edi:L"=::~:\\\"
je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199864	edi:L"=::~:\\\"
push esi	esi:L"NUMBER_OF_PROCESSORS=1"
mov esi,edi	esi:L"NUMBER_OF_PROCESSORS=1"
cmp word ptr ds:[edi],ax	esi:L"NUMBER_OF_PROCESSORS=1"
je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199807	esi:L"NUMBER_OF_PROCESSORS=1"
add esi,2	esi:L"NUMBER_OF_PROCESSORS=1"
cmp word ptr ds:[esi],ax	esi:L"NUMBER_OF_PROCESSORS=1"
jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F1997F7	esi:L"NUMBER_OF_PROCESSORS=1"
add esi,2	esi:L"NUMBER_OF_PROCESSORS=1"
cmp word ptr ds:[esi],ax	
jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F1997F7	

COMPUTERNAME:

edi:L"=::~:\\\"	EBX 00000001
edi:L"=::~:\\\"	ECX 00000000
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"	EDX 00000002
esi:L"COMPUTERNAME=WIN-L1KDN79P80J", edi:L"=::~:\\\"	EBP 0013F264
edi:L"=::~:\\\"	ESP 0013F258
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"	ESI 00303F4 L"COMPUTERNAME=WIN-L1KDN79P80J"
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"	EDI 00303210 L"=::~:\\\"
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"	EIP 6F199802 fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199802
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"	EFLAGS 00000202
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"	ZE 0 PE 0 AE 0
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"	OE 0 SE 0 DF 0
esi:L"COMPUTERNAME=WIN-L1KDN79P80J"	CE 0 TF 0 IF 1

PROCESSOR:

<&GetEnvironmentStringsW>	edi:L"=::~:\\\"
edi:L"=::~:\\\"	edi:L"=::~:\\\"
esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"	esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"	esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
edi:L"=::~:\\\"	esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"	esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"	esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"	esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"	esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"
esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"	esi:L"PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel"

7gfdg5egds.exe ANALİZİ

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

File pos	Mem pos	ID	Text
A 000000041C62	000000445662	0	malloc
A 000000041C6C	00000044566C	0	memcpy
A 000000041C76	000000445676	0	memcpy
A 000000041C80	000000445680	0	memmove
A 000000041C8A	00000044568A	0	memset
A 000000041C94	000000445694	0	signal
A 000000041C9E	00000044569E	0	strlen
A 000000041CA8	0000004456A8	0	strcmp
A 000000041CB2	0000004456B2	0	vfprintf
A 000000041CBE	0000004456BE	0	WSACleanup
A 000000041CCC	0000004456CC	0	WSAGetLastError
A 000000041CDE	0000004456DE	0	WSASocketW
A 000000041CEC	0000004456EC	0	WSAStartup
A 000000041CFA	0000004456FA	0	closesocket
A 000000041D08	000000445708	0	connect
A 000000041D12	000000445712	0	freeaddrinfo
A 000000041D22	000000445722	0	getaddrinfo
A 000000041D30	000000445730	0	ioctlsocket
A 000000041D4E	00000044574E	0	setsockopt
A 000000041D5C	00000044575C	0	shutdown
A 000000041D68	000000445768	0	RegCloseKey
A 000000041D76	000000445776	0	RegEnumKeyExW
A 000000041D86	000000445786	0	RegOpenKeyExW
A 000000041D96	000000445796	0	RegQueryInfoKeyW
A 000000041DA4	0000004457AA	0	RegQueryValueExW
A 000000041DBE	0000004457BE	0	CryptUnprotectData
A 000000041DD4	0000004457D4	0	BitBlt
A 000000042300	000000445D00	0	msvcrt.dll
A 000000042340	000000445D40	0	WS2_32.dll
A 000000042360	000000445D60	0	ADVAPI32.dll
A 000000042374	000000445D74	0	CRYPT32.dll
A 00000004239C	000000445D9C	0	GDI32.dll
A 000000042470	000000445E70	0	KERNEL32.dll
A 000000042498	000000445E98	0	USER32.dll

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

Zararlıının içindeki önemli DLL ve fonksiyonları incelediğimizde;

- CreateToolhelp32Snapshot
- WriteFile
- GetSystemInfo
- CreateMutexA

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

Address	Disassembly	Comment	Module Name
00415833	0303	add esp, dword ptr [esi], ebx	EDI:"C:\Program Files\...
00415837	74 00	je esp, esi	
00415839	51	pop esi	
0041583B	51	pop esi	
0041583D	51	pop esi	
0041583F	51	pop esi	
00415841	51	pop esi	
00415843	51	pop esi	
00415845	51	pop esi	
00415847	51	pop esi	
00415849	51	pop esi	
0041584B	51	pop esi	
0041584D	51	pop esi	
0041584F	51	pop esi	
00415851	51	pop esi	
00415853	51	pop esi	
00415855	51	pop esi	
00415857	51	pop esi	
00415859	51	pop esi	
0041585B	51	pop esi	
0041585D	51	pop esi	
0041585F	51	pop esi	
00415861	51	pop esi	
00415863	51	pop esi	
00415865	51	pop esi	
00415867	51	pop esi	
00415869	51	pop esi	
0041586B	51	pop esi	
0041586D	51	pop esi	
0041586F	51	pop esi	
00415871	51	pop esi	
00415873	51	pop esi	
00415875	51	pop esi	
00415877	51	pop esi	
00415879	51	pop esi	
0041587B	51	pop esi	
0041587D	51	pop esi	
0041587F	51	pop esi	
00415881	51	pop esi	
00415883	51	pop esi	
00415885	51	pop esi	
00415887	51	pop esi	
00415889	51	pop esi	
0041588B	51	pop esi	
0041588D	51	pop esi	
0041588F	51	pop esi	
00415891	51	pop esi	
00415893	51	pop esi	
00415895	51	pop esi	
00415897	51	pop esi	
00415899	51	pop esi	
0041589B	51	pop esi	
0041589D	51	pop esi	
0041589F	51	pop esi	
004158A1	51	pop esi	
004158A3	51	pop esi	
004158A5	51	pop esi	
004158A7	51	pop esi	
004158A9	51	pop esi	
004158AB	51	pop esi	
004158AD	51	pop esi	
004158AF	51	pop esi	
004158B1	51	pop esi	
004158B3	51	pop esi	
004158B5	51	pop esi	
004158B7	51	pop esi	
004158B9	51	pop esi	
004158BB	51	pop esi	
004158BD	51	pop esi	
004158BF	51	pop esi	
004158C1	51	pop esi	
004158C3	51	pop esi	
004158C5	51	pop esi	
004158C7	51	pop esi	
004158C9	51	pop esi	
004158CB	51	pop esi	
004158CD	51	pop esi	
004158CF	51	pop esi	
004158D1	51	pop esi	
004158D3	51	pop esi	
004158D5	51	pop esi	
004158D7	51	pop esi	
004158D9	51	pop esi	
004158DB	51	pop esi	
004158DD	51	pop esi	
004158DF	51	pop esi	
004158E1	51	pop esi	
004158E3	51	pop esi	
004158E5	51	pop esi	
004158E7	51	pop esi	
004158E9	51	pop esi	
004158EB	51	pop esi	
004158ED	51	pop esi	
004158EF	51	pop esi	
004158F1	51	pop esi	
004158F3	51	pop esi	

[illegible]

\\Sessions\\1\\BaseNamedObjects\\serhershershsfesrf

00415879	51	push ecx	
0041587A	6A 0B	push B	
0041587C	56	push esi	esi:"Urlmon.dll"
0041587D	FFD0	call eax	
0041587F	83C4 0C	add esp,C	
00415882	56	push esi	esi:"Urlmon.dll"
00415883	EB 84F00100	call <JMP.&LoadLibraryA>	
00415885	89C3	mov ebx,eax	ebx:"ru-RU"
0041588A	8D05 75A64200	lea eax,dword ptr ds:[42A675]	
00415890	8D00 597D4300	lea ecx,dword ptr ds:[37D59]	
00415896	8907	mov dword ptr ds:[edi],eax	edi:"Urlmon.dll"
00415898	B8 A780FFFF	mov eax,FFFF80A7	
0041589D	0307	add eax,dword ptr ds:[edi]	edi:"Urlmon.dll"
0041589F	51	push	

00415BA0	56	push esp	
00415BA2	56	push esi	esi:"URLDownloadToFileA"
00415BA3	FFD0	call eax	
00415BA5	83C4 0C	add esp,C	
00415BA8	56	push esi	esi:"URLDownloadToFileA"
00415BA9	53	push ebx	
00415BAE	CD F00100	jmp .GetProcAddress	
00415BAF	894424 04	mov dword ptr ss:[esp+4],eax	
00415BB3	8D05 B9BD4200	lea eax,dword ptr ds:[42B0B9]	
00415BB9	8D00 2A7E4300	lea ecx,dword ptr ds:[437E2A]	
00415BBF	8907	mov dword ptr ds:[edi],eax	edi:"URLDownloadToFileA"
00415BC1	8B 6399FFFF	mov eax,FFFF9963	
00415BC6	0307	add dword ptr ds:[edi]	edi:"URLDownloadToFileA"

The screenshot shows a Windows XP desktop. The 'Bilgisayar' (Computer) icon is on the desktop. The 'ProgramData' folder is open, displaying a list of files and folders. The 'kaosdma.txt' file is selected. The taskbar at the bottom shows the 'Not Defteri' (Notepad) application open with the file 'kaosdma.txt'.

Navigation: Bilgisayar > Yerel Disk (C:) > ProgramData

Buttons: Düzenle, Aç, Yazdır, Yaz, Yeni klasör

Left Panel (Sık Kullanılanlar):

- ★ Sık Kullanılanlar
- 📁 Karşından Yüklemeler
- 📁 Masaüstü
- 📁 Son Yerler
- 📁 Kitaplıklar
- 📄 Belgeler
- 🎵 Müzik

Right Panel (Ad):

- 📁 Microsoft
- 📁 Microsoft Help
- 📁 Oracle
- 📁 Package Cache
- 📁 VMware
- 📄 kaosdma.txt (Selected)

Taskbar:

kaosdma.txt - Not Defteri

Buttons: Dosya, Düzen, Biçim, Görünüm, Yardım

Address Bar: 78.175.61.217

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

```

0040D955 898C24 00000000 mov dword ptr ss:[esp+D0],ecx
0040D956 808C24 00020000 lea edi,dword ptr ss:[esp+200],0
0040D957 888424 88000000 mov eax,dword ptr ss:[esp+88],0
0040D958 888C24 8C000000 mov ecx,dword ptr ss:[esp+8C],0
0040D959 83A424 88000000 and dword ptr ss:[esp+88],0
0040D95A 85C0 test eax,ecx
0040D95B 70FD95E8S.400B88 je 70FD95E8S.400B88
0040D95C 808C24 86000000 cmp byte ptr ss:[esp+86],0
0040D95D 898424 40010000 mov dword ptr ss:[esp+140],ecx
0040D95E 898424 44010000 mov dword ptr ss:[esp+144],ecx
0040D95F 899424 48010000 mov dword ptr ss:[esp+148],edx
0040D960 0F84 20010000 je 70FD95E8S.400AC8
0040D961 83A424 04020000 and dword ptr ss:[esp+204],0
0040D962 83A424 0C020000 and dword ptr ss:[esp+20C],0
0040D963 C78424 10020000 0700 mov dword ptr ss:[esp+210],7
0040D964 8367 18 00 and dword ptr ds:[edi+18],0
0040D965 8367 14 00 and dword ptr ds:[edi+14],0
0040D966 8367 1E 00 and dword ptr ds:[edi+1E],0
0040D967 8367 1A 00 and dword ptr ds:[edi+1A],0
0040D968 808C24 40010000 lea ecx,dword ptr ss:[esp+140],0
0040D969 C68424 1C020000 01 mov byte ptr ss:[esp+21C],1
0040D96A C78424 00020000 0000 mov dword ptr ss:[esp+200],20000000
0040D96B E8 908F0100 call 70FD95E8S.4269F5
0040D96C 8906 mov esi,edx
0040D96D 8D8C24 C0040000 lea ecx,dword ptr ss:[esp+4C0],0
0040D96E
0040D96F

```

dword ptr [esp+144]=[0028E224 &"recent_common1"]=00719799 "recent_common1"
ecx=8
.text:0040D997 70FD95E8S.exe:5D997 #CD97

Adres	Hex	ASCII
00719769	91 89 44 00 00 00 80 FF 00	00 5C 55 73 65 72 73 5C
00719770	7A 6F 72 72 6F 5C 41 70 70	44 61 74 61 5C 52 6F
00719771	61 6D 69 6E 67 5C 57 69 72	65 73 68 61 72 68 5C
00719772	60 6D 6E 74 5F 60 6D 6E 6E	69 00 6E 6E 6E 6E 6E 6E
00719773	00 67 00 5C 00 53 00 75 00	6E 00 5C 00 2A 00 00 00
00719774	00 75 70 33 2F 37 65 74 91	68 44 00 00 80 36 00 00

0028C700	00 00 00 00	00 00 00 00	90 CB 28 00	00 00 00 00É(.....
0028C710	08 00 00 00	E0 C9 28 00	4C 00 00 00	08 00 0A 00ðÉ(.L.....
0028C720	80 A1 38 77	00 00 00 00	9C C9 28 00	43 00 3A 00	..i;w.....É(.C.:.
0028C730	5C 00 55 00	73 00 65 00	72 00 73 00	5C 00 7A 00	..U.s.e.r.s.\.
0028C740	6F 00 72 00	72 00 6F 00	7C 00 41 00	70 00 70 00	..A.p.p.\.
0028C750	44 00 61 00	74 00 61 00	5C 00 52 00	6F 00 61 00	D.a.t.a.\.R.o.a.
0028C760	6D 00 69 00	6E 00 67 00	5C 00 41 00	64 00 6F 00	m.i.n.g.\.A.d.o.
0028C770	62 00 65 00	5C 00 2A 00	00 00 00 00	00 00 00 00	b.e.\.º.....
0028C780	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0028C790	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0028C7A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00

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

Google Chrome:

```

836424 58 00 and dword ptr ss:[esp+58],0
83F6 test esi,esi
83F7 lea edi,edx
83F8 mov ebx,esi
808C24 58010000 lea ecx,dword ptr ss:[esp+158],0
83F2 mov edx,esi
83F3 push edi
83F4 call 70FD95E8S.429008
83F5 pop eax
8005 88174300 lea ecx,dword ptr ds:[4317B8]
83F6 mov ecx,FFFF3F64
83F7 mov dword ptr ss:[esp+AD0],eax
83F8 mov eax,dword ptr ss:[esp+AD0],0
01C8 add eax,ecx
800D 25714300 lea ecx,dword ptr ds:[437128]
83F1 push ecx
83F2 push 7
80B424 B0010000 lea esi,dword ptr ss:[esp+180],0
83F3 push esi
83F4 add esp,C
83F5 lea ecx,dword ptr ss:[esp+AD0],0
83F6 mov edx,esi
83F7 call 70FD95E8S.40289A
83F8 lea esi,dword ptr ss:[esp+158],0
808424 58010000 lea edx,dword ptr ss:[esp+AD0],0
83F1 mov ecx,esi
83F2 call 70FD95E8S.402374
83F3 mov eax,edi

```

esi:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Login Data\\RecentClosed_out.db-journal"
esi:&"P\rn"

esi:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
ebx:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Login Data\\RecentClosed_out.db-journal"
[esp+158]:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
esi:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
esi:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
esi:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
[esp+158]:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
esi:&"C:\\Users\\...\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"

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

[illegible]

Address	Hex		ASCII	
00EEEDA0	22 64 73 00	00 00 00 46	8F CD A6 44 00 00 0C 8C	rds...F.iD...
00EEEDA8	73 65 72 76	65 72 7F 63	81 72 64 5F 60 65 74 61	server_card_meta
00EEEDB0	64 61 74 61	00 00 00 46	83 CD A6 44 00 00 89	data..F.iD...
00EEEDD0	61 75 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEEDD8	73 65 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEEDF0	61 75 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEEEE0	73 63 75 6D	65 6E 74 73	F8 CD A6 44 00 00 89	saccounts01.D...
00EEEE10	61 75 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEEE20	5F 6D 6D 61	69 6C 73 63	F3 CD A6 44 00 00 89	_emailcy01.D...
00EEEE30	73 65 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	sqlc_indexindex
00EEEE40	61 75 74 6F	66 69 6C 6C	F3 CD A6 44 00 00 89	meta_01.D...
00EEEE50	30 14 71 00	FF FF FF FF	00 00 00 00 00 00 00	0.q.yyyy...
00EEEE60	00 00 00 00	00 00 00 00	F7 CD A6 44 00 00 8E	...i.D...
00EEEE70	65 00 70 00	6D 00 61 00	70 00 70 00 65 00 72 00	e.p.m.a.p.p.e.r.
00EEEE80	00 00 00 00	00 00 00 00	E8 CD A6 44 00 00 8E	...e.i.D...
00EEEE90	65 00 70 00	6D 00 61 00	70 00 70 00 65 00 72 00	e.p.m.a.p.p.e.r.
00EEEEA0	00 00 00 00	00 00 00 00	EF CD A6 44 00 00 8A	...i.D...
00EEEEB0	70 61 79 6D	65 6E 74 73	5F 63 75 73 74 6F 6D 65	payments_customer
00EEEEC0	72 5F 64 61	74 61 00 00	E3 CD A6 44 00 00 8C	r_data.ai.D...
00EEEEDD	05 00 00 00	A7 00 00 00	00 00 00 00 60 01 00 00	...S...
00EEEEEE	68 00 00 00	00 00 00 00	DE CD A6 44 00 00 88	h.q.i.d...
00EEEEF0	00 00 00 00	F4 FE 6E 00	24 FE 6E 00 00 00 00	...g.in.D...
00EEEF00	01 00 00 00	2C 89 44 06	D8 CD A6 44 00 00 88	...D.O1.D...
00EEEF10	01 00 00 00	04 02 00 00	00 00 00 00 80 69 71 00	...
00EEEF20	88 21 70 00	01 01 01 00	DF CD A6 44 00 00 8C	...ip...i.D...
00EEEF30	00 00 00 00	F0 64 68 75	00 00 00 00 00 00 00	...o.ku...
00EEEF40	00 00 00 00	00 00 00 00	D3 CD A6 44 00 00 8C	...oi.D...
00EEEF50	01 00 00 00	00 00 00 00	00 00 00 00 00 00 00	...
00EEEF60	0A 00 00 00	00 00 00 00	D7 CD A6 44 00 00 8A	...xi.D...
00EEEF70	61 75 74 6F	66 69 6C 6C	5F 73 79 6E 63 5F 6D 65	autofill_sync_me
00EEEF80	74 61 64 61	74 61 71 00	C8 CD A6 44 00 00 88	tadata.ei.D...
00EEEF90	00 00 00 00	94 EF 6E 00	24 EF 6E 00 00 00 00	...in.in...
00EEFE00	01 00 00 00	00 00 00 06	CD A6 44 00 00 8C	...tadai.D...
00EEFE10	61 75 74 6F	66 69 6C 6C	5F 73 6F 66 6C 6C 65	autofill_profile
00EEFE20	73 00 00 00	65 6E 74 73	C3 CD A6 44 00 00 89	s...entsAi.D...
00EEFE30	61 75 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEFE40	5F 70 68 6F	65 6E 73 00	C7 CD A6 44 90 00 8D	_phones.Ci.D...
00EEFE50	6D 61 73 68	65 64 5F 83	72 65 64 69 74 5F 63 61	masked_credit_ca
00EEFE60	73 64 73 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEFE70	61 75 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEFE80	5F 6D 6D 61	69 6C 73 63	3F CE A6 44 00 00 89	_emails.Ti.D...
00EEFE90	61 75 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEFEA0	73 5F 74 72	61 73 68 00	C3 CE A6 44 00 00 89	s_trash.3i.D...
00EEFEB0	61 75 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEFEC0	AF 70 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEFED0	61 75 74 6F	66 69 6C 6C	5F 70 72 6F 66 6C 6C	autofill_profile
00EEFEE0	73 00 00 00	01 01 01 0E	28 CE A6 44 00 00 88	s...i.D...
00EEFEF0	A0 58 72 00	FF FF FF FF	00 00 00 00 00 00 00	[r.yyyy...
00EEFF00	00 00 00 00	00 00 00 00	2F CE A6 44 00 00 88	...i.D...
00EEFF10	68 00 00 00	00 00 00 00	2F CE A6 44	[r.yyyy...
00EEFF20	00 00 00 00	00 00 00 00	23 CE A6 44	...i.D...
00EEFF30	61 75 74 6F	66 69 6C 6C	5F 73 79 6E 63 5F 6D 65	autofill_sync_me
00EEFF40	74 61 64 61	74 61 23 06	27 CE A6 44 00 00 8C	tadata.i.D...
00EEFF50	73 65 72 76	65 72 5F 63	61 72 64 5F 60 65 74 61	server_card_meta
00EEFF60	64 61 74 61	AF 6E 72 F4	1B CE A6 44 00 00 8B	data.nro.i.D...
00EEFF70	75 6D 6D 61	69 6C 73 63	3F CE A6 44 00 00 88	masked_credit_ca
00EEFF80	61 75 74 6F	66 69 6C 6C	5F 73 6F 66 6C 6C 65	autofill_profile
00EEFF90	73 65 72 76	65 72 5F 61	64 64 72 65 73 73 5F 6D	server_address_m
00EEFFA0	65 74 61 64	61 74 61 46	13 CE A6 44 00 00 8B	etadata.f.i.D...
00EEFFB0	75 6E 6D 61	73 68 65 64	5F 63 72 65 64 69 74 5F	unmasked_credit_
00EEFFC0	61 73 72 64	73 00 00 00	17 CE A6 44 00 00 8A	cards...i.D...

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

Address	Disassembly	Comment
0040FF0E	89DA	mov edx,ebx
0040FF10	F2:0F18C24 80000000	movsd qword ptr ss:[esp+80],xmm1
0040FF19	F2:0F18424 A8000000	movsd qword ptr ss:[esp+A8],xmm0
0040FF22	E8 6F4A0000	call 70f9d5egds.414996
0040FF27	8B4C24 F0010000	mov eax,dword ptr ss:[esp+1F0]
0040FF2E	85C0	test eax,eax
0040FF30	74 60	jz 70f9d5egds.40FF92
0040FF32	8B4C24 40	mov ecx,dword ptr ss:[esp+40]
0040FF36	85C9	test ecx,ecx
0040FF38	74 58	jz 70f9d5egds.40FF92
0040FF3A	98BC24 AC000000	mov dword ptr ss:[esp+AC],ecx
0040FF41	8B4C24 48	mov ecx,dword ptr ss:[esp+48]
0040FF45	8B4C24 F8010000	mov dword ptr ss:[esp+1F8],ecx
0040FF4C	98BC24 B4000000	mov dword ptr ss:[esp+B4],ecx
0040FF53	8B4C24 44	mov ecx,dword ptr ss:[esp+44]

```
ax=006EEE30 "jigiw47411@dmsdmg.com_1"  
word ptr [esp+1F0]=[0028E988 &"jigiw47411@dmsdmg.com_1"]=006EEE30 "jigiw47411@dmsdmg.com_1"
```

```
text:0040FF27 7qfdq5eqds.exe:$FF27 #F327
```

Dokü1	Dokü2	Dokü3	Dokü4	Dokü5	İzle 1	[x=] Yerel Değişkenler	Yapı
İres	Hex					ASCII	
06EEEE30	6A 69 67 69 77 34 37 34	31 31 40 64	6D 73 64 6D				igigw4741@dmsdm
06EEEE40	67 2E 63 6F 6D 5F 31 00	F3 CD A6 44	00 00 00 88				g.com_1.6i'D....
06EEEE50	30 14 71 00	FF FF FF FF	00 00 00 00				0.q.yyyy.....
06EEEE60	00 00 00 00	00 00 00 00	F7 CD A6 44			i'D....
06EEEE70	00 00 00 00	6D 00 61 00	70 00 72 00				e.p.m.a.p.p.e.r.
06EEEE80	00 00 00 00	00 00 00 00	EB CD A6 44			ei'D....
06EEEE90	65 00 70 00	6D 00 61 00	70 00 70 00				e.p.m.a.p.p.e.r.
06EEEEA0	00 00 00 00	00 00 00 00	EF CD A6 44			i'D....
06EEEEB0	70 61 79 6D	65 6E 74 73	5F 63 75 73				payments_custome
06EEEC00	72 5F 64 00	74 1D A6 44	00 00 00 8C				_data..ai'D....
06EEEC10	05 99 00 00	A7 00 00 00	09 00 00 00			s.....

Bitcoin cüzdan:

00419244	8D0D 13794300	lea ecx,dword ptr ds:[437913]	
0041924A	8906	mov dword ptr ds:[esi],eax	
0041924C	B8 7ADAF0FF	mov eax,FFFFFFA7A	
00419251	0306	add eax,dword ptr ds:[esi]	
00419253	51	push ecx	
00419254	6A 19	push 19	
00419256	8D9C24 38070000	lea ebx,dword ptr ss:[esp+738]	ebx: "%appdata%\Bitcoin\wallets"
0041925D	53	push ebx	
0041925E	FFD0	call eax	
00419260	83C4 0C	add esp,C	
00419263	31D2	xor edx,edx	
00419265	8D8C24 40030000	lea ecx,dword ptr ss:[esp+340]	
0041926C	8D8424 B0040000	lea eax,dword ptr ss:[esp+480]	

Exodus cüzdan:

0041955D	83C4 0C	add esp,C	
00419560	8D8C24 40030000	lea ecx,dword ptr ss:[esp+340]	[esp+340]: "%appdata%\Exodus\exodus.walletA"
00419567	89FA	mov edx,edi	
00419569	E8 5098FEFF	call 79fdg5egds.40208E	
0041956E	8D05 33364300	lea eax,dword ptr ds:[433633]	
00419574	89 5C7D4300	mov ecx,79fdg5egds.437D5C	ecx: "%appdata%\Exodus\exodus.walletA"
00419579	8903	mov dword ptr ds:[ebx],eax	[ebx]: "Jaxxp"
0041957B	B8 E920FFFF	mov eax,FFFFFF0E9	[ebx]: "Jaxxp"
00419580	0303	add eax,dword ptr ds:[ebx]	
00419582	6A 95	push FFFFFFF95	
00419584	5A	pop edx	
00419585	01D1	add ecx,edx	ecx: "%appdata%\Exodus\exodus.walletA"
00419587	51	push ecx	ecx: "%appdata%\Exodus\exodus.walletA"

Ethereum cüzdan:

004198F4	41	inc ecx	
004198F7	8360 04 00	and dword ptr ds:[eax],ecx	
004198F8	8360 08 00	and dword ptr ds:[eax+8],0	
004198FF	894F 04	mov dword ptr ds:[edi+4],ecx	
00419C02	8367 08 00	and dword ptr ds:[edi+8],0	
00419C06	8D424 20	lea eax,dword ptr ss:[esp+20]	[esp+20]: "%appdata%\Ethereum\keystore"
00419C0A	8947 10	mov dword ptr ds:[edi+10],eax	
00419C0D	894F 14	mov dword ptr ds:[edi+14],ecx	
00419C10	8D8424 B0040000	lea eax,dword ptr ss:[esp+480]	[esp+480]: "%appdata%\Ethereum\keystore"
00419C17	8D8C24 40030000	lea ecx,dword ptr ss:[esp+340]	
00419C1E	894424 20	mov dword ptr ss:[esp+20],eax	[esp+20]: "%appdata%\Ethereum\keystore"
00419C22	C74424 24 C7264000	mov dword ptr ss:[esp+24],79fdg5egds.4026C7	
00419C2A	FA 41A00000	call 79fdg5egds.4026C7	

Discord uygulamasından aldığı veriler:

0041DE11	894424 04	mov dword ptr ss:[esp+4],eax	
0041DE15	8D05 36124300	lea eax,dword ptr ds:[431236]	
0041DE18	8D0D C96F4300	lea ecx,dword ptr ds:[436FC9]	
0041DE21	8906	mov dword ptr ds:[esi],ecx	esi: "%appdata%\Discord\Local Storage2\Sessions"
0041DE23	B8 E44FFFFF	mov eax,FFFFFF4E6	esi: "%appdata%\Discord\Local Storage2\Sessions"
0041DE28	0306	add eax,dword ptr ds:[esi]	
0041DE2A	51	push ecx	
0041DE2B	6A 1F	push 1F	
0041DE2D	56	push esi	esi: "%appdata%\Discord\Local Storage2\Sessions"
0041DE2E	FFD0	call eax	
0041DE30	83C4 0C	add esp,C	
0041DE33	8D8C24 40030000	lea ecx,dword ptr ss:[esp+340]	

Steam:

0041E2F5	51	push ecx	
0041E2F6	53	push ecx	
0041E2F7	53	push ebx	
0041E2F8	FFD0	call eax	ebx: "SOFTWARE\WOW6432Node\Valve\Steam\Sessions"
0041E2FA	83C4 0C	add esp,C	
0041E2FD	8D05 630D4300	lea eax,dword ptr ds:[430D63]	
0041E303	8D0D 25734300	lea ecx,dword ptr ds:[437325]	
0041E309	898424 30070000	mov dword ptr ss:[esp+730],eax	

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

0041E180	8D8C24 B0040000	lea edi,dword ptr ss:[esp+480]	
0041E184	57	push edi	
0041E195	FFD0	call eax	edi: "%appdata%\purple\accounts.xml2\Sessions"
0041E197	83C4 0C	add esp,C	
0041E19A	8D8424 A8010000	lea esi,dword ptr ss:[esp+1A8]	
0041E1A1	89FA	mov edx,edi	edi: "%appdata%\purple\accounts.xml2\Sessions"
0041E1A3	89F1	mov ecx,esi	esi: "%appdata%\purple\accounts.xml2\Sessions"
0041E1A5	E8 144CFF	call 79fdg5egds.40208E	

FileZilla:

0041D117	8D8C24 38070000	lea edi,dword ptr ss:[esp+738]	
0041D11E	57	push edi	
0041D11F	FFD0	call eax	edi: "recentServers.xml"
0041D121	83C4 0C	add esp,C	
0041D124	8D8C24 90000000	lea ecx,dword ptr ss:[esp+90]	[esp+90]: "%appdata%\FileZilla"
0041D128	89FA	mov edx,edi	edi: "recentServers.xml"
0041D12D	E8 145BFEFF	call 79fdg5egds.402C46	
0041D132	8D05 34A84200	lea eax,dword ptr ds:[42A834]	

Zararlı yazılımın yapılan işlemin anlık görüntüsünü aldığını görmekteyiz.

0041C087	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	
0041C098	C78424 B0040000 9C7A	mov dword ptr ss:[esp+480],7gfdg5egds.437A9C	[esp+480]:&"\"SomeNone", 437
0041C0A6	C78424 B4040000 0300	mov dword ptr ss:[esp+484],3	
0041C0B1	83A424 B8040000 00	and dword ptr ss:[esp+488],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+480]	[esp+480]:&"\"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 3924	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

0041C087	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	
0041C098	C78424 B0040000 9C7A	mov dword ptr ss:[esp+480],7gfdg5egds.437A9C	
0041C0A6	C78424 B4040000 0300	mov dword ptr ss:[esp+484],3	
0041C0B1	83A424 B8040000 00	and dword ptr ss:[esp+488],0	
0041C0B9	894424 20	mov dword ptr ss:[esp+20],eax	
0041C0BD	8D4424 20	lea eax,dword ptr ss:[esp+20]	
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+480]	
0041C0D0	898424 08010000	mov dword ptr ss:[esp+108],eax	
0041C0D7	8D8424 08010000	lea eax,dword ptr ss:[esp+108]	
0041C0DE	89F1	mov ecx,esi	
0041C0E0	C78424 0C010000 3924	mov dword ptr ss:[esp+10C],7gfdg5egds.402439	

Zararlı çaldığı verilerden sonra 95[.213[.179[.167[.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
[UDP] 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	8E4424 10	mov eax,dword ptr ss:[esp+10]	
0040E8B2	01C9	add ecx,ecx	ecx:&"pospvisis.com:803"
0040E8B4	800D 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	8D8424 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
76869707172737475767778798081828384858687888990919293949596979899[]"
$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/>