



# FickerStealer

## Technical Analysis Report



# Contents

<b>Preview .....</b>	<b>2</b>
<b>file.dll ANALYSIS .....</b>	<b>3</b>
<b>7gfdg5egds.exe ANALYSIS .....</b>	<b>6</b>
<b>NETWORK ANALYSIS .....</b>	<b>12</b>
<b>SOLUTION PROPOSALS .....</b>	<b>13</b>
<b>Yara Rules .....</b>	<b>14</b>

# Introduction

FickerStealer is a infostealer threat offered as a MaaS (Malware-as-a-Service) on underground hacker forums. FickerStealer is distributed by various phishing methods. Infected computers of this malware;

- Credentials saved in web browsers,
- Desktop messaging clients,
- To FTP clients,
- Blockchain wallets,
- It provides access to computer documents.

## Preview

The FickerStealer malware in the examined version continued to spread as a DLL with phishing methods. The malicious file was originally named "file.dll". As a result of the analysis, it has been determined that this file acts as a loader to realize Stage 1.

File Name:	file.dll
MD5	9b59d4744ff1de8b338eeb2b85748cf2
SHA1	f3306e866bc9992c2268f204f55e88f89833a25d
SHA256	fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafef6491a404e8ad4

It has been observed that the file.dll malware downloads a file titled MZ when network traffic is monitored.

59 46.513825	8.211.241.0	10.7.0.38	TCP	1514 80 →
60 46.513872	8.211.241.0	10.7.0.38	TCP	1514 80 →
61 46.513874	8.211.241.0	10.7.0.38	TCP	1514 80 →
62 46.513875	8.211.241.0	10.7.0.38	TCP	1514 80 →
63 46.513876	8.211.241.0	10.7.0.38	TCP	1514 80 →
64 46.513917	8.211.241.0	10.7.0.38	TCP	1514 80 →
65 46.513919	8.211.241.0	10.7.0.38	TCP	1514 80 →
66 46.513920	8.211.241.0	10.7.0.38	TCP	1514 80 →
67 46.513922	8.211.241.0	10.7.0.38	TCP	1514 80 →
68 46.513957	8.211.241.0	10.7.0.38	TCP	1514 80 →
69 46.514687	10.7.0.38	8.211.241.0	TCP	60 5370!
70 46.514967	10.7.0.38	8.211.241.0	TCP	60 5370!
71 46.515233	10.7.0.38	8.211.241.0	TCP	60 5370!
72 46.515582	10.7.0.38	8.211.241.0	TCP	60 5370!
73 46.515952	10.7.0.38	8.211.241.0	TCP	60 5370!
74 46.516246	10.7.0.38	8.211.241.0	TCP	60 [TCP
75 46.523788	8.211.241.0	10.7.0.38	TCP	1514 80 →
76 46.523718	8.211.241.0	10.7.0.38	TCP	1514 80 →
77 46.523728	8.211.241.0	10.7.0.38	TCP	1514 80 →
Checksum: 0x95dc [unverified]				
[Checksum Status: Unverified]				
Urgent pointer: 0				
[SEQ/ACK analysis]				
[Timestamp]				
0030 00 ed 20 4f	00 00 48 54	54 50 2f 31	2e 31 20 32	00 00 00 00
0040 30 30 20 4f	4b 0d 0a 53	65 72 76 65	72 3a 20 6e	00 00 00 00
0050 67 69 6e 78	0d 0a 44 61	74 65 3a 20	54 75 65 2c	00 00 00 00
0060 20 30 36 20	4a 75 6c 20	32 30 32 31	20 31 39 3a	00 00 00 00
0070 34 34 3a 30	36 20 47 4d	54 0d 0a 43	6f 6e 74 65	00 00 00 00
0080 6e 74 2d 54	79 70 65 3a	20 61 70 70	6c 69 63 61	00 00 00 00
0090 74 69 6f 6e	2f 6f 63 74	65 74 2d 73	74 72 65 61	00 00 00 00
00a0 6d 0d 0a 43	6f 6e 74 65	6e 74 2d 4c	65 6e 67 74	00 00 00 00
00b0 68 3a 20 32	37 32 39 31	30 0d 0a 43	6f 6e 6e 65	00 00 00 00
00c0 63 74 69 6f	6e 3a 20 69	65 65 70 2d	61 6c 69 76	00 00 00 00
00d0 65 0d 0a 41	73 74 2d	4d 6f 64 69	69 69 65 64	00 00 00 00
00e0 3a 20 57	65 64 2c 20	30 39 20 4a	75 6e 20 32	00 00 00 00
00f0 32 31 20 31	36 3a 30 30	3a 34 30 20	47 4d 54 0d	00 00 00 00
0100 0a 45 54 61	67 3a 20 22	36 30 63 30	65 35 61 38	00 00 00 00
0110 2d 34 32 61	30 65 22 0d	0a 41 63 63	65 70 74 2d	00 00 00 00
0120 52 61 6e 67	65 73 3a 20	62 79 74 65	73 0d 0a 0d	00 00 00 00
0130 0a 4d 5a 90	00 03 00 00	00 04 00 00	00 ff ff 00	00 00 00 00
0140 00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0150 00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0160 00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0170 00 0e 1f ba	0e 00 b4 09	cd 21 b0 01	4c cd 21 54	00 00 00 00
0180 68 69 73 20	70 72 6f 67	72 61 6d 20	63 61 6e 6e	00 00 00 00
0190 6f 74 20 62	65 20 72 75	6e 20 69 6e	20 44 4f 53	00 00 00 00
01a0 20 6d 6f 64	65 2e 0d 0d	0a 24 00 00	00 00 00 00	00 00 00 00
01b0 00 50 45 00	00 4c 01 08	00 00 00 00	00 00 2a 04	00 00 00 00

# file.dll ANALYSIS

When file.dll is examined statically, it is seen that it is a 32-bit executable file.

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...vY..
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	.....@...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	º º . ' ! , L í ! 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....\$.....

CFF Explorer VIII - [file.dll]

File Settings ?

file.dll

Property	Value
File Name	C:\Users\ \Downloads\210706-p83fmjaeys_pw_infected\file.dll
File Type	Portable Executable 32
File Info	Borland Delphi 3.0 (???)

File: file.dll

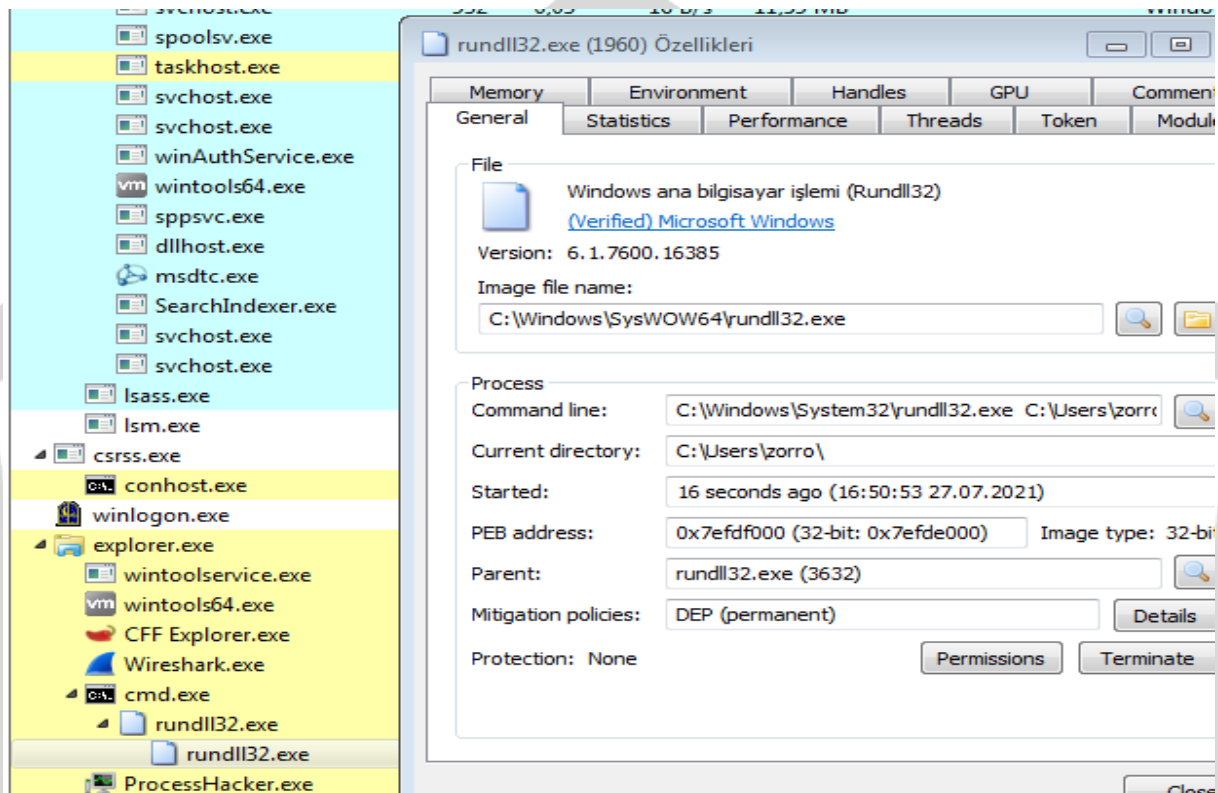
- Dos Header
- Nt Headers
- File Header
- Optional Header

Dynamically loaded DLLs:

Adres	Hex	ASCII
002F8BA0	C0 65 2D 00 98 82 2E 00 0A 00 00 00 C0 D0 E0 F0 A2 ..../.....Ada5	
002F8BB0	65 D6 FE 7E 5C 00 00 8E 4F 4C 45 33 32 2E 64 6C e0p-...OLE32.d1	
002F8BC0	6C 00 36 00 24 00 5C 00 6A D6 FE 7E 6E 00 00 88 1.6.4.\.j0p-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 o0p-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 4B 5E 5C 00 62 00 5C 00 MSVCIRT.d11.s...	
002F8C10	51 D6 FE 7E 67 00 00 88 4D 53 56 43 62 00 5C 00 Q0p-...MSVCRT20	
002F8C20	2E 64 6C 6C 00 00 74 00 56 D6 FE 7E 52 00 00 88 .d11..t.v0p-R...	
002F8C30	002F8920 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 [0p-o...MFC40.d1	
002F8C50	6C 00 61 00 6D 00 46 00 58 D6 FE 7E 65 00 00 8E 1.a.m.F.x0p-e...	
002F8C60	4D 46 43 34 32 2E 64 6C 6C 00 72 00 6E 00 67 00 MFC42.d11..f.o.g	
002F8C70	50 D6 FE 7E 65 00 00 88 4D 46 43 34 30 2E 64 6C [0p-o...MFC40.d1	
002F8C80	64 6C 6C 00 28 00 78 00 42 D6 FE 7E 29 00 00 88 d11..(x.B0p-)	
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 [0p-e...MFC42D.	
002F8CB0	44 4C 4C 00 6E 00 50 00 44 D6 FE 7E 67 00 00 8C DLL.n.P.D0p-g...	
002F8CC0	4D 46 43 34 34 32 44 2E 44 4C 4C 00 72 00 28 00 MFC42D.DLL..S.(	
002F8CD0	4D 4C 4C 00 6F 00 67 00 4E D6 FE 7E 6D 00 00 8D DLL.o.g.N0p-m...	
002F8CE0	4D 46 43 34 32 44 2E 44 4C 4C 00 28 00 78 00 MFC42D.DLL..(x.	
002F8CF0	33 D6 FE 7E 29 00 00 88 4B 45 52 4E 45 4C 33 32 30p-)...KERNEL32	
002F8D00	2E 44 4C 4C 00 00 46 00 3D D6 FE 7E 65 00 00 88 .DLL..F.O0p-e...	
002F8D10	42 4C 41 43 4B 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.O0p-...	
002F8D30	6A 70 69 63 70 6C 33 32 2E 63 70 6C 00 00 46 00 j0p1cp132.cp1..F	
002F8D40	3F D6 FE 7E 65 00 00 88 00 88 2F 00 80 BA 2F 00 70p-e....../.º/..	
002F8D50	A8 38 2D 00 01 00 00 00 3C D6 FE 7E 6C 00 00 88 8-...o0p-1...	
002F8D60	68 BA 2F 00 98 BA 2F 00 80 29 2D 00 01 00 00 00 hº/º/º/..)	
002F8D70	21 D6 FE 7E 4E 00 00 88 80 BA 2F 00 80 BA 2F 00 10p-N...º/..º/..	
002F8D80	C0 2C 2D 00 01 00 00 00 25 D6 FE 7E 6A 6C 00 88 A-...o0p-ju...	
002F8D90	98 BA 2F 00 10 88 2F 00 40 FA 2D 00 01 00 00 00 º/..º/..º/..e...	
002F8DA0	28 D6 FE 7E 53 00 00 88 80 BA 2F 00 E0 BA 2F 00 10p-S...º/..º/..	
002F8DB0	C0 2C 2D 00 01 00 00 00 25 D6 FE 7E 6A 6C 00 88 A-...o0p-ju...	
002F8DC0	C8 BA 2F 00 E8 BA 2F 00 A8 38 2D 00 01 00 00 00 Eº/º/º/..º/..	
002F8DD0	2D D6 FE 7E 5C 00 00 88 E0 BA 2F 00 80 88 2F 00 10p-...º/..º/..	
002F8DE0	80 29 2D 00 01 00 00 00 12 D6 FE 7E 4E 00 00 86 º/...º/..º/..	
002F8DF0	80 BA 2F 00 00 88 2F 00 20 88 2F 00 01 00 00 00 º/...º/..º/..	
002F8E00	17 D6 FE 7E 48 00 00 8E 4F 4C 45 33 32 2E 64 6C .0p-k...OLE32.d1	
002F8E10	60 00 4D 00 49 00 44 00 14 D6 FE 7E 56 00 00 88 1.m.E.D...0p-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 .0p-T...MSVCRT.d	
002F8E40	6C 6C 00 00 72 00 5C 00 1E D6 FE 7E 00 00 00 8C 11..s...0p-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 .0p-D...MSVCRT20	
002F8E70	2E 64 6C 6C 00 00 73 00 00 D6 FE 7E 73 00 00 88 .d11..s...0p-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

In general, when the behavior of file.dll is examined, it re-runs itself as suspend using the Process Hollowing technique.



### Information Collected:

Targeted languages and countries:

Adres	Hex	ASCII	Adres	Hex	ASCII
002F7370	02 00 00 00	.....µgöü..	00667464	00 00 00 00	.....
002F7380	00 00 00 00	....8....\$/..	00667474	00 00 00 00	.....F1 CB B3 08
002F7390	00 00 00 00	.....	00667484	30 49 00 00	0I..Ä.c.,@f.,C.
002F73A0	8F 67 F3 75	..göü..e.n..U.	00667494	4F 00 4C 00	0.L.L.A.T.E.=T.
002F73B0	53 00 00 00	S...a.r..S.A..	006674A4	75 00 72 00	u.r.k.i.s.h..T.
002F73C0	70 00 74 00	p.t..B.R..z.h.	006674B4	75 00 72 00	u.r.k.e.y...1.2.
002F73D0	20 00 54 00	..T.W...z.h..C.	006674C4	35 00 34 00	5.4.;L.C..C.T.
002F73E0	4E 00 00 00	N...z.h..H.K..	006674D4	59 00 50 00	Y.P.E.=T.u.r.k.
002F73F0	63 00 73 00	C..S..C.Z...d.a.	006674E4	69 00 73 00	i.s.h..T.u.r.k.
002F7400	20 00 44 00	..D.K...e.l..G.	006674F4	65 00 79 00	e.y...1.2.5.4.;
002F7410	52 00 00 00	R...e.s..E.S...	00667504	4C 00 43 00	L.C..M.O.N.E.T.
002F7420	66 00 69 00	f.i..F.I...f.r.	00667514	41 00 52 00	A.R.Y.=T.u.r.k.
002F7430	20 00 46 00	..F.R...d.e..D.	00667524	69 00 73 00	i.s.h..T.u.r.k.
002F7440	45 00 00 00	E...h.e..I.L..	00667534	65 00 79 00	e.y...1.2.5.4.;
002F7450	68 00 75 00	h.u..H.U...i.t.	00667544	4C 00 43 00	L.C..N.U.M.E.R.
002F7460	20 00 49 00	..I.T...j.a..J.	00667554	49 00 43 00	I.C.=T.u.r.k.i.
002F7470	50 00 00 00	P...k.o..K.R...	00667564	73 00 68 00	s.h..T.u.r.k.e.
002F7480	6E 00 6C 00	n.l..N.L...n.b.	00667574	79 00 2E 00	y...1.2.5.4.;
002F7490	20 00 4E 00	..N.O...p.l..P.	00667584	43 00 5F 00	C..T.I.M.E.=T.
002F74A0	4C 00 00 00	L...p.t..P.T...	00667594	75 00 72 00	u.r.k.i.s.h..T.
002F74B0	72 00 75 00	r.u..R.U...s.v.	006675A4	75 00 72 00	u.r.k.e.y...1.2.
002F74C0	20 00 53 00	..S.E...t.r..T.	006675B4	35 00 34 00	5.4.....
002F74D0	52 00 00 00	R...b.g..B.G..	006675C4	00 00 00 00	.....
002F74E0	68 00 72 00	h.r..H.R...e.t.			
002F74F0	20 00 45 00	..E.E...l.v..L.			
002F7500	56 00 00 00	V...l.t..L.T...			
002F7510	72 00 6F 00	r.o..R.O...s.r.			
002F7520	20 00 4C 00	..L.a.t.n..C.S.			
002F7530	00 00 73 00	..s.k..S.K...s.			
002F7540	6C 00 20 00	..S.I...t.h..			
002F7550	54 00 48 00	T.H...u.k..U.A.			
002F7560	00 00 66 00	..f.y..N.L...q.			
002F7570	70 00 73 00	p.s..p.l.o.c...			
002F7580	71 00 70 00	q.p.s..p.l.o.c...			
002F7590	60 00 00 00	m.....öüü..			



cmd.exe path:

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
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	OE 0 SE 0 DF 0
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	CE 0 TF 0 IF 1
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"	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="
6F199800 66:3906 cmp word ptr ds:[esi],ax	esi:L"USERNAME="
6F199802 75 F0 jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F1997F7	esi:L"USERNAME="
6F199804 56 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 fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F199802	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	esi:L"NUMBER_OF_PROCESSORS=1"
jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4.6F1997F7	esi:L"NUMBER_OF_PROCESSORS=1"

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 ANALYSIS

File Name:	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

When we look at the imports of the pest, it uses important libraries such as USER32 and WS2\_32. When we look at the WS2\_32 library, it is understood that it has the capacity to perform network operations, as can be seen from the functions it uses.

When we examine the important DLL and functions in the pest;

- CreateToolhelp32Snapshot
- WriteFile
- GetSystemInfo
- CreateMutexA

It is seen that the malware can Access system information, create a mutex object, get information about the system and files, write files, and take a snapshot of the process.

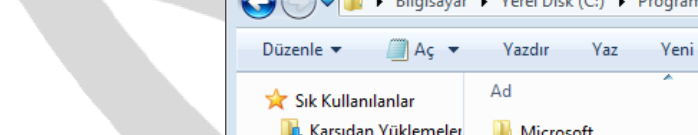
Address	Disassembly	Comment	Module Name
00415833	0303	add esp, dword ptr [esi], ebx	EDI:"C:\Program Files\...
00415837	74 00	je esp, esi	
00415839	58	pop esi	
0041583B	58	pop esi	
0041583D	58	pop esi	EDI:"C:\Program Files\...
0041583F	58	pop esi	
00415841	58 04 0C	add esp, 0C	EDI:"C:\Program Files\...
00415843	EB 6CF91000	CALL 6CF91000	
00415845	BE 6CF91000	mov esi, 6CF91000	
00415847	BE 6CF91000	mov esi, 6CF91000	
00415849	BE 6CF91000	mov esi, 6CF91000	
0041584B	BE 6CF91000	mov esi, 6CF91000	
0041584D	BE 6CF91000	mov esi, 6CF91000	
0041584F	BE 6CF91000	mov esi, 6CF91000	
00415851	BE 6CF91000	mov esi, 6CF91000	
00415853	BE 6CF91000	mov esi, 6CF91000	
00415855	BE 6CF91000	mov esi, 6CF91000	
00415857	BE 6CF91000	mov esi, 6CF91000	
00415859	BE 6CF91000	mov esi, 6CF91000	
0041585B	BE 6CF91000	mov esi, 6CF91000	
0041585D	BE 6CF91000	mov esi, 6CF91000	
0041585F	BE 6CF91000	mov esi, 6CF91000	
00415861	BE 6CF91000	mov esi, 6CF91000	
00415863	BE 6CF91000	mov esi, 6CF91000	
00415865	BE 6CF91000	mov esi, 6CF91000	
00415867	BE 6CF91000	mov esi, 6CF91000	
00415869	BE 6CF91000	mov esi, 6CF91000	
0041586B	BE 6CF91000	mov esi, 6CF91000	
0041586D	BE 6CF91000	mov esi, 6CF91000	
0041586F	BE 6CF91000	mov esi, 6CF91000	
00415871	BE 6CF91000	mov esi, 6CF91000	
00415873	BE 6CF91000	mov esi, 6CF91000	
00415875	BE 6CF91000	mov esi, 6CF91000	
00415877	BE 6CF91000	mov esi, 6CF91000	
00415879	BE 6CF91000	mov esi, 6CF91000	
0041587B	BE 6CF91000	mov esi, 6CF91000	
0041587D	BE 6CF91000	mov esi, 6CF91000	
0041587F	BE 6CF91000	mov esi, 6CF91000	
00415881	BE 6CF91000	mov esi, 6CF91000	
00415883	BE 6CF91000	mov esi, 6CF91000	
00415885	BE 6CF91000	mov esi, 6CF91000	
00415887	BE 6CF91000	mov esi, 6CF91000	
00415889	BE 6CF91000	mov esi, 6CF91000	
0041588B	BE 6CF91000	mov esi, 6CF91000	
0041588D	BE 6CF91000	mov esi, 6CF91000	
0041588F	BE 6CF91000	mov esi, 6CF91000	
00415891	BE 6CF91000	mov esi, 6CF91000	
00415893	BE 6CF91000	mov esi, 6CF91000	
00415895	BE 6CF91000	mov esi, 6CF91000	
00415897	BE 6CF91000	mov esi, 6CF91000	
00415899	BE 6CF91000	mov esi, 6CF91000	
0041589B	BE 6CF91000	mov esi, 6CF91000	
0041589D	BE 6CF91000	mov esi, 6CF91000	
0041589F	BE 6CF91000	mov esi, 6CF91000	
004158A1	BE 6CF91000	mov esi, 6CF91000	
004158A3	BE 6CF91000	mov esi, 6CF91000	
004158A5	BE 6CF91000	mov esi, 6CF91000	
004158A7	BE 6CF91000	mov esi, 6CF91000	
004158A9	BE 6CF91000	mov esi, 6CF91000	
004158AB	BE 6CF91000	mov esi, 6CF91000	
004158AD	BE 6CF91000	mov esi, 6CF91000	
004158AF	BE 6CF91000	mov esi, 6CF91000	
004158B1	BE 6CF91000	mov esi, 6CF91000	
004158B3	BE 6CF91000	mov esi, 6CF91000	
004158B5	BE 6CF91000	mov esi, 6CF91000	
004158B7	BE 6CF91000	mov esi, 6CF91000	
004158B9	BE 6CF91000	mov esi, 6CF91000	
004158BB	BE 6CF91000	mov esi, 6CF91000	
004158BD	BE 6CF91000	mov esi, 6CF91000	
004158BF	BE 6CF91000	mov esi, 6CF91000	
004158C1	BE 6CF91000	mov esi, 6CF91000	

0004A200	3B	CALL ECX	EBX	0004B580	"serher/sheer/sheerF"
0004A201	8B	CALL 40100	EDI	0004B58C	"serher/sheerF"
0004A202	8B	CALL 40100	EDI	0004B594	0004B594
0004A203	74	JMP 40100	EDI	0004B598	0004B598
0004A204	74	JMP 40100	EDI	0004B59C	0004B59C
0004A205	74	JMP 40100	EDI	0004B5A0	0004B5A0
0004A206	74	JMP 40100	EDI	0004B5A4	0004B5A4
0004A207	74	JMP 40100	EDI	0004B5A8	0004B5A8
0004A208	74	JMP 40100	EDI	0004B5AC	0004B5AC
0004A209	74	JMP 40100	EDI	0004B5B0	0004B5B0
0004A20A	74	JMP 40100	EDI	0004B5B4	0004B5B4
0004A20B	74	JMP 40100	EDI	0004B5B8	0004B5B8
0004A20C	74	JMP 40100	EDI	0004B5BC	0004B5BC
0004A20D	74	JMP 40100	EDI	0004B5C0	0004B5C0
0004A20E	74	JMP 40100	EDI	0004B5C4	0004B5C4
0004A20F	74	JMP 40100	EDI	0004B5C8	0004B5C8
0004A210	74	JMP 40100	EDI	0004B5CC	0004B5CC
0004A211	74	JMP 40100	EDI	0004B5D0	0004B5D0
0004A212	74	JMP 40100	EDI	0004B5D4	0004B5D4
0004A213	74	JMP 40100	EDI	0004B5D8	0004B5D8
0004A214	74	JMP 40100	EDI	0004B5DC	0004B5DC
0004A215	74	JMP 40100	EDI	0004B5E0	0004B5E0
0004A216	74	JMP 40100	EDI	0004B5E4	0004B5E4
0004A217	74	JMP 40100	EDI	0004B5E8	0004B5E8
0004A218	74	JMP 40100	EDI	0004B5EC	0004B5EC
0004A219	74	JMP 40100	EDI	0004B5F0	0004B5F0
0004A21A	74	JMP 40100	EDI	0004B5F4	0004B5F4
0004A21B	74	JMP 40100	EDI	0004B5F8	0004B5F8
0004A21C	74	JMP 40100	EDI	0004B5FC	0004B5FC
0004A21D	74	JMP 40100	EDI	0004B600	0004B600
0004A21E	74	JMP 40100	EDI	0004B604	0004B604
0004A21F	74	JMP 40100	EDI	0004B608	0004B608
0004A220	74	JMP 40100	EDI	0004B60C	0004B60C
0004A221	74	JMP 40100	EDI	0004B610	0004B610
0004A222	74	JMP 40100	EDI	0004B614	0004B614
0004A223	74	JMP 40100	EDI	0004B618	0004B618
0004A224	74	JMP 40100	EDI	0004B61C	0004B61C
0004A225	74	JMP 40100	EDI	0004B620	0004B620
0004A226	74	JMP 40100	EDI	0004B624	0004B624
0004A227	74	JMP 40100	EDI	0004B628	0004B628
0004A228	74	JMP 40100	EDI	0004B62C	0004B62C
0004A229	74	JMP 40100	EDI	0004B630	0004B630
0004A22A	74	JMP 40100	EDI	0004B634	0004B634
0004A22B	74	JMP 40100	EDI	0004B638	0004B638
0004A22C	74	JMP 40100	EDI	0004B63C	0004B63C
0004A22D	74	JMP 40100	EDI	0004B640	0004B640
0004A22E	74	JMP 40100	EDI	0004B644	0004B644
0004A22F	74	JMP 40100	EDI	0004B648	0004B648
0004A230	74	JMP 40100	EDI	0004B64C	0004B64C
0004A231	74	JMP 40100	EDI	0004B650	0004B650
0004A232	74	JMP 40100	EDI	0004B654	0004B654
0004A233	74	JMP 40100	EDI	0004B658	0004B658
0004A234	74	JMP 40100	EDI	0004B65C	0004B65C
0004A235	74	JMP 40100	EDI	0004B660	0004B660
0004A236	74	JMP 40100	EDI	0004B664	0004B664
0004A237	74	JMP 40100	EDI	0004B668	0004B668
0004A238	74	JMP 40100	EDI	0004B66C	0004B66C
0004A239	74	JMP 40100	EDI	0004B670	0004B670
0004A23A	74	JMP 40100	EDI	0004B6	

Some other DLL's and APIs it loads dynamically:

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 esi	
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	
00415BA4	E8 CD F0 01 00	call <JMP.<GetProcAddress>	
00415BAF	894424 04	mov dword ptr ss:[esp+4],eax	
00415BB3	8D05 B9BD4200	lea eax,dword ptr ds:[4280B9]	
00415BB9	8D00 2A7E4300	lea ecx,dword ptr ds:[437E2A]	
00415BBF	8907	mov dword ptr ds:[edi],	edi:"URLDownloadToFileA"
00415BC1	EB 63 99FFFF	mov eax,FFF9963	
00415BC6	0307	add eax,dword ptr ds:[edi]	edi:"URLDownloadToFileA"



The screenshot shows a Windows Explorer window with the address bar set to 'Bilgisayar > Yerel Disk (C:) > ProgramData'. The left sidebar is expanded, showing 'Sık Kullanılanlar' (Frequently Used) and 'Kitaplıklar' (Folders). The main pane displays a list of files and folders, with 'kaosdma.txt' selected. The status bar at the bottom indicates the file is a 'Not Defteri' (Notepad) file.

Ad
Microsoft
Microsoft Help
Oracle
Package Cache
VMware
<b>kaosdma.txt</b>

kaosdma.txt - Not Defteri

Dosya Düzen Biçim Görünüm Yardım

78.175.61.217



In general, it is seen that the malware has 2 basic behaviors. First, it scans the software installed on the system.

0028C700	00 00 00 00	00 00 00 00	90 CB 28 00	00 00 00 00	.....É(.....
0028C710	08 00 00 00	E0 C9 28 00	4C 00 00 00	08 00 0A 00	.....ðÉ(.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	5C 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	.....

Another behavior is to steal personal data and identity information from web browsers. Since most applications are not installed, it seems that it just checks.

## Google Chrome:

Phone number, credit card information kept in Google Chrome:

Adres	Hex	ASCII															
007895D0	43 6F 6E 69 72 6D 74 69 6F 6E	22 5D 7D 2C	Confirmation"];														
007895E0	22 7F 73 5F 63 72 79 70 74	22 3A 78 22 65 6E 63	"os_crypt";{"en														
007895F0	72 79 70 74 65 64 5F 6B 65 69	22 3A 22 62 66 63	rypted_crypt";{"RfE														
00789600	42 55 45 6B 42 41 41 41 41 41	40 39 79 64 33 77 45	BUEK6AAADtYd3wE														
00789610	56 30 52 47 4D 65 67 41 41 41	54 38 48 58 36 77 45	VORqEgBdAT8X6wE														
00789620	41 41 41 41 50 33 66 67 67 32	42 52 61 61 61	VORqEgBdAT8X6wE														
00789630	41 41 41 41 59 6D 41 41 41 41	41 41 41 41 41 51 41	KXCNVbYUuHwJjA														
00789640	41 41 41 41 41 41 42 42 6D 41	41 41 41 41 51 41	AAAAAAABmAAuAAQ														
00789650	41 49 41 41 41 41 4F 48 33 48	50 59 2F 74 6D	ATAAAA00H7P/ema														
00789660	30 33 33 36 34 58 4D 32 35 54	39 32 54 38 2B 35	03364XWZ22XYTMA														
00789670	79 68 48 2F 48 53 69 46 35 48	73 64 41 37 72 71	YH/HST5F5KsD7aT														
00789680	41 49 41 41 41 41 41 41 41 41	41 41 41 41 41 41 41	AAAAAAABmAAuAAQ														
00789690	41 49 41 41 41 41 41 41 41 41	41 41 41 41 41 41 41	AAAAAAABmAAuAAQ														
007896A0	64 66 58 5A 6D 47 6F 59 4A 52	51 73 64 46 46	fJf2XmQWJRQsDFD														
007896B0	54 38 25 71 43 63 6C 53 52 68	32 75 54 36 66 58	T8/CQ1SR1ZuTFX														
007896C0	48 4D 41 41 41 41 41 41 41 41	41 41 41 41 41 41 41	HMAAAALKwEDUyT2														
007896D0	56 4E 72 35 6E 42 39 43 50 64	76 41 64 4E 68	AAAAAAABmAAuAAQ														
007896E0	34 78 58 63 69 67 67 37 67 31	61 69 62 72 31 58 74	4XcW1cgW711nr1Lu														
007896F0	62 31 75 42 75 59 45 41 41 41	41 41 41 42 38 34 76 35	blubuyEAAAAB84Sv														
00789710	28 71 70 6A 51 64 63 34 58 6C	2F 79 62 65 65 34	+pQ1Q3JX1/y1Bn4														
00789720	56 4A 53 39 38 33 30 67 64 39	51 2A 2F 55 57	AAAAAAABmAAuAAQ														
00789730	41 41 41 41 41 41 41 41 41 41	41 41 41 41 41 41 41	A718/187WpHjJA8														
00789740	70 4C 51 53 66 77 38 75 52 45	6D 57 39 6A 61	pLQ5F8WqPEmW5jA														
00789750	78 4C 4E 45 36 48 46 65 71 61	6D 69 45 58 37	XLN8E6H8qumA1EX														
00789760	68 22 7D 2C 22 70 61 73 73 77	62 76 64 5F 6D 61 73	"},"password_ma														
00789770	6E 61 67 65 72 22 3A 73 73 77	63 73 5F 70 61 73 73	nager";{"os_pas														
00789780	6E 61 67 65 72 22 3A 73 73 77	63 73 5F 70 61 73 73	nager";{"os_pas														
00789790	2C 62 66 73 5F 70 61 73 77 67	63 73 5F 6C 61	","os_password_1a														
007897A0	73 74 5F 63 68 61 6E 67 65 64	22 31 33 32	st_changed";{"132														
007897B0	35 39 37 36 35 31 38 32 38 34	35 35 39 36 22 7D	597618284596"														
007897C0	2C 22 70 6C 75 67 69 63 73 22	3A 78 22 6D 65 74	","plugins":["met														
007897D0	61 6A 61 61 68 20 70 6C 72 62	64 6A 62 65 2D 66	","plugins":["met														
007897E0	61 6A 61 68 20 70 6C 72 62 64	6A 62 65 2D 66	","plugins":["met														
007897F0	69 73 70 6C 61 79 5F 62 22 3A	74 72 75 65 61	","plugins":["met														
00789800	22 67 72 6F 75 70 5F 6E 61 6D	65 68 60 61 74 63	","group_name_mat														
00789810	68 65 72 22 3A 22 7A 53 68 61	63 68 77 71 76 65	","group_name_mat														
00789820	20 46 6C 61 73 68 2A 22 2C 22	68 65 6C 70 5F 74	Flash["help_u														
00789830	61 6A 61 68 20 70 6C 72 62 64	6A 62 65 2D 66	Flash["help_u														
00789840	70 6F 72 74 2E 67 6F 67 6C 65	2E 63 6F 6D 2F	http://google.co														
00789850	63 68 72 6F 6D 65 2F 3F 70 3D	70 6C 75 67 69 6E	chrome/?p=plugi														
00789860	5F 6E 6C 61 73 68 22 2C 22 6C	61 6E 67 22 3A 74	_flash","lang":														
00789870	65 6E 2D 55 52 74 22 2C 22 6D	69 6D 65 5F 74 79 70	en-us","mime_tyt														
00789880	61 6A 61 68 20 70 6C 72 62 64	6A 62 65 2D 66	","mime_type":														
00789890	2E 66 75 74 72 72 65 73 70 6C	71 63 73 68 22 7D	n/autocomplete"														
007898A0	22 61 70 70 6C 69 63 61 74 69	69 61 6F 2F 7D 2D	","application/x-s														
007898B0	68 6F 63 68 77 71 76 65 2D 66	6C 61 73 68 22 53	hockwave-flash"														
007898C0	2C 22 6E 61 6D 65 6E 2A 22 7A	62 64 6C 62 65 2D 46	1","name":"Adobe														
007898D0	6C 61 73 68 20 50 6C 79 65 72	61 72 2C 22 75 72	","name":"Adobe														
007898E0	61 6A 61 68 20 70 6C 72 62 64	6A 62 65 2D 66	","name":"Adobe														
007898F0	61 6A 61 68 20 70 6C 72 62 64	6A 62 65 2D 66	","name":"Adobe														
00789900	74 73 2F 66 61 73 68 70 6C 61	69 65 72 72 65	","name":"Adobe														
00789910	6E 64 2F 66 6D 6C 69 66 6E 2E	68 74 6D 6C 62 72	","name":"Adobe														
00789920	2C 22 76 65 72 73 69 6F 6E 73	22 3A 58 7B 22 72	","name":"Adobe														
00789930	61 6A 61 68 20 70 6C 72 62 64	6A 62 65 2D 66	","name":"Adobe														
00789940	3A 2E 2F 77 77 2E 61 64 2F 66	6C 65 2E 63 6F 6D	","name":"Adobe														
00789950	2F 70 72 72 6F 64 75 63 74 2F	66 6C 61 73 68 70	","name":"Adobe														
00789960	6C 61 79 68 72 72 65 64 2F 66	6D 6C 69 66 2D 6C	","name":"Adobe														
00789970	65 2E 76 74 8D 6C 2C 22 73 74	61 74 75 73 22 72	","name":"Adobe														
00789980	61 6A 2F 72 71 65 5F 6E 65 72	68 68 68 68 68 68	","name":"Adobe														
00789990	61 6A 2F 72 71 65 5F 6E 65 72	68 68 68 68 68 68	","name":"Adobe														
007899A0	6F 6E 22 3A 32 33 32 2F 20 2F	20 3A 36 36 22	","name":"Adobe														

Address	Hex	Disassembly	
00EEEDA0	22 64 73 00	00 00 00 46 8F CD A6 44 00 00 00 8C	rsd...F.iD...
00EEEDB0	73 65 72 76	65 72 5F 63 61 72 64 5F 60 65 74 61	server_card_meta
00EEEDC0	64 61 74 76	00 00 00 46 83 CD A6 44 00 00 00 89	data...F.iD...
00EEEDD0	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEEDF0	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEEEE0	73 63 75 6D	65 6E 74 73 F8 CD A6 44 00 00 00 89	scumcentsUI.D...
00EEEEE10	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEEEE20	5F 65 60 61	69 6C 73 63 6F CD A6 44 00 00 00 89	emalicyiD...
00EEEEE30	73 6C 69	74 65 5F 61 75 76 69 6E 64 65 78	sqite_autoindex
00EEEEE40	FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00	data...iD...
00EEEEE50	30 14 71 00	FF FF FF FF 00 00 00 00 00 00 00 00	0.0.yyyy...
00EEEEE60	00 00 00 00	00 00 00 00 F7 CD A6 44 00 00 00 8E	...iD...
00EEEEE70	65 00 70 00	6D 00 61 00 70 00 70 00 65 00 72 00	e.p.m.a.p.p.e.r...
00EEEEE80	00 00 00 00	00 00 00 00 00 CD A6 44 00 00 00 8E	...iD...
00EEEEE90	65 00 70 00	6D 00 61 00 70 00 70 00 65 00 72 00	e.p.m.a.p.p.e.r...
00EEEEEA0	00 00 00 00	00 00 00 00 EF CD A6 44 00 00 00 8A	...iD...
00EEEEEB0	70 61 79 6D	65 6E 74 73 5F 63 75 74 74 6F 6D 65	payments_custom...
00EEEEEC0	72 5F 64 61	74 61 00 00 E3 CD A6 44 00 00 00 8C	r_data.iD...
00EEEEED0	05 00 00 00	A7 00 00 00 00 00 00 00 60 01 00 00	...s...
00EEEEEE0	68 09 71 00	67 00 00 00 E7 CD A6 44 00 00 00 88	h.q...iD...
00EEEEEF0	00 00 00 00	01 00 00 00 44 EE 65 60 00 00 00 00	0in.0in...
00EEEF00	00 00 00 00	2C 89 44 06 D8 CD A6 44 00 00 00 88	...D.iD...
00EEEF10	01 00 00 00	04 02 00 00 00 00 00 00 80 63 71 00	...iD...
00EEEF20	88 21 70 00	01 01 01 00 DF CD A6 44 00 00 00 8C	lp...iD...
00EEEF30	00 00 00 00	F0 64 68 75 00 00 00 00 00 00 00 00	0duku...
00EEEF40	00 00 00 00	00 00 00 00 D3 CD A6 44 00 00 00 8C	...0.iD...
00EEEF50	01 00 00 00	01 00 00 00 D7 CD A6 44 00 00 00 8A	...D...iD...
00EEEF60	0A 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00	...iD...
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 00 88	tadata.iD...
00EEEF90	00 00 00 00	94 EF 6E 00 94 EF 6E 00 00 00 00 00	...in...iD...
00EEFE00	01 00 00 00	CF FE C4 06 CF CD A6 44 00 00 00 8F	IOA.iD...
00EEFE10	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEFE20	00 00 00 00	00 00 00 00 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEFE30	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEFE40	73 5F 74 72	61 73 68 00 3C CD A6 44 00 00 00 89	s_trash.iD...
00EEFE50	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEFE60	5F 70 68 6F	6E 65 73 00 37 CD A6 44 00 00 00 8D	_phones.iD...
00EEFE70	6D 61 73 68	65 64 5F 63 72 65 64 69 74 5F 63 61	masked_credit_ca...
00EEF000	72 64 73 20	AF 6E 72 F4 38 CD A6 44 00 00 00 89	rds_nro.iD...
00EEF010	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEF020	00 00 00 00	00 00 00 00 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEF030	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEF040	73 5F 74 72	61 73 68 00 3C CD A6 44 00 00 00 89	s_trash.iD...
00EEF050	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEF060	5F 70 68 6F	6E 65 73 00 37 CD A6 44 00 00 00 8F	_phones.iD...
00EEF070	61 75 74 6F	66 69 6C 6C 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEF080	00 00 00 00	00 00 00 00 5F 70 72 6F 66 69 6C 65	autofill_profile
00EEF090	A0 5B 72 00	FF FF FF FF 00 00 00 00 00 00 00 00	[r.yyyy...
00EEF0A0	00 00 00 00	00 00 00 00 2F CD A6 44 00 00 00 88	...iD...
00EEF0B0	C8 5B 72 00	FF FF FF FF 00 00 00 00 00 00 00 00	E[r.yyyy...
00EEF0C0	00 00 00 00	00 00 00 00 23 CD A6 44 00 00 00 8A	...iD...
00EEF0D0	61 75 74 6F	66 69 6C 6C 5F 73 79 6E 63 5F 6D 65	autofill_sync_me...
00EEF0E0	74 61 64 61	74 61 71 00 C8 CD A6 44 00 00 00 88	server_card_meta
00EEF0F0	73 65 72 76	65 72 5F 63 61 72 64 5F 60 65 74 61	data_nro.iD...
00EEF100	64 61 74 61	AF 6E 72 F4 18 CD A6 44 00 00 00 88	unmasked_credit...
00EEF110	75 6E 6D 74	73 68 65 64 5F 63 72 65 64 69 74 5F	unmasked_credit...
00EEF120	63 61 72 64	73 00 00 00 1F CD A6 44 00 00 00 89	cards...iD...
00EEF130	00 00 00 00	00 00 00 00 64 64 65 63 60 00 00 00	scumcs_addres...
00EEF140	74 61 64 61	74 61 71 00 C8 CD A6 44 00 00 00 8D	tadata.iD...
00EEF150	75 6E 6D 61	73 68 65 64 5F 63 72 65 64 69 74 5F	unmasked_credit...
00EEF160	63 61 72 64	73 00 00 00 17 CD A6 44 00 00 00 8A	cards...iD...

The email address that Google Chrome keeps after logging in:

Address	Disassembly	Comment
0040FF0E	89DA	mov edx,ebx
0040FF10	F2:0F118C24 80000000	movsd qword ptr ss:[esp+80],xmm1
0040FF19	F2:0F118424 A8000000	movsd qword ptr ss:[esp+A8],xmm0
0040FF22	E8 6F4A0000	call 79fdgsegds.414996
0040FF27	88424 F0010000	mov eax,dword ptr ss:[esp+1F0]
0040FF2E	85C0	test eax,eax
0040FF30	74 60	jz 79fdgsegds.40FF92
0040FF32	884C24 40	mov ecx,dword ptr ss:[esp+40]
0040FF36	85C9	test ecx,ecx
0040FF38	74 58	jz 79fdgsegds.40FF92
0040FF3A	998C24 AC000000	mov dword ptr ss:[esp+AC],ecx
0040FF41	884C24 48	mov ecx,dword ptr ss:[esp+48]
0040FF45	89424 F8010000	mov edx,dword ptr ss:[esp+1F8]
0040FF4C	998C24 B4000000	mov dword ptr ss:[esp+B4],ecx
0040FF53	884C24 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			igigiw47411@dmsdm	
06EEEE40	67 2E 63 6F 6D 5F 31 00	F3 CD A6 44	00 00 00 88			g.com_1.0i'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	
06EEEC0	72 5F 64 00	74 10 A6 44	00 00 00 8C			_data..ai'D....	
06EEED0	05 09 00 00	A7 00 00 00	09 00 00 00			.....s.....	

## Bitcoin wallet:

00419244	800D 13794300	lea ecx,dword ptr ds:[437913]	
0041924A	8906	mov dword ptr ds:[esi],eax	
0041924C	B8 7ADAF7FF	mov eax,FFFFFFA7A	
00419253	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]	
0041925D	53	push ebx	
0041925E	FFD0	call eax	ebx:"%appdata%\Bitcoin\wallets"
00419263	83C4 0C	add esp,C	
00419265	8D8C24 40030000	lea ecx,dword ptr ss:[esp+340]	
0041926C	8D8424 80040000	lea eax,dword ptr ss:[esp+480]	

## Exodus wallet:

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.4020B6	
0041956E	8D05 33364300	lea eax,dword ptr ds:[433633]	ecx:"%appdata%\Exodus\exodus.walletA"
00419574	89 5C7D4300	mov ecx,79fdg5egds.4020B6	[ebx]:"%axxp"
00419579	8903	mov dword ptr ds:[ebx],eax	[ebx]:"%axxp"
00419578	B8 E920FFFF	mov eax,FFFFFF0E9	
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 wallet:

004198F4	41	inc ecx	
004198F5	8908	mov dword ptr ds:[eax],ecx	
004198F7	8360 04 00	and dword ptr ds:[eax+4],0	
004198F8	8360 08 00	and dword ptr ds:[eax+8],0	
004198FF	834F 04	mov dword ptr ds:[edi+4],ecx	
00419C02	8367 08 00	and dword ptr ds:[edi+8],0	
00419C06	8D4424 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 80040000	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 418A0000	call 79fdg5egds.4026C0	

## Data from the Discord app:

0041DE11	894424 04	mov dword ptr ss:[esp+4],eax	
0041DE15	8D05 36124300	lea eax,dword ptr ds:[431236]	
0041DE1E	8D0D 396F4300	lea ecx,dword ptr ds:[436FC9]	
0041DE21	8906	mov dword ptr ds:[esi],eax	esi:"%appdata%\Discord\Local Storage2\Sessions"
0041DE23	B8 E644FFFF	mov eax,FFFFFF4E6	
0041DE28	0306	add eax,dword ptr ds:[esi]	esi:"%appdata%\Discord\Local Storage2\Sessions"
0041DE2A	51	push ecx	
0041DE2B	6A 1F	push 1F	
0041DE2D	56	push esi	
0041DE2E	FFD0	call eax	esi:"%appdata%\Discord\Local Storage2\Sessions"
0041DE30	83C4 0C	add esp,C	
0041DE33	8D8C24 40030000	lea ecx,dword ptr ss:[esp+340]	

## Steam:

0041E2F6	51	push ecx	
0041E2F7	53	push ecx	
0041E2F8	FFD0	push ebx	ebx:"SOFTWARE\Wow6432Node\Valve\Steam\Sessions"
0041E2FA	83C4 0C	call eax	
0041E2FD	8D05 630D4300	add esp,C	
0041E303	8D0D 25734300	lea eax,dword ptr ds:[430063]	
0041E309	898424 30070000	lea ecx,dword ptr ds:[437325]	
		mov dword ptr ss:[esp+730],eax	

**.purple:** It is the configuration directory in Windows. Here you can find information about the account, including chat logs, pictures from other users, passwords.

0041E190	8D8C24 80040000	lea edi,dword ptr ss:[esp+480]	
0041E195	FFD0	push edi	edi:"%appdata%\purple\accounts.xml2\Sessions"
0041E197	83C4 0C	call eax	
0041E19A	8D8424 A8010000	add esp,C	
0041E1A1	89FA	lea esi,dword ptr ss:[esp+1A8]	
0041E1A3	89F1	mov edx,edi	edi:"%appdata%\purple\accounts.xml2\Sessions"
0041E1A5	E8 144CFE9F	mov ecx,esi	esi:"%appdata%\purple\accounts.xml2\Sessions"
0041E1A7	8D05 33364300	call 79fdg5egds.4020B6	

## 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 145BFE9F	call 79fdg5egds.402C46	
0041D132	8D05 34A84200	lea eax,dword ptr ds:[42A834]	

**OS:**





We see that the malware takes a snapshot of the operation.

```
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
```

[esp+480]:&"\"SomeNone", 437  
[esp+20]: "x32dbg.exe"  
[esp+20]: "x32dbg.exe"  
[esp+480]:&"\"SomeNone"  
[esp+108]:&"x32dbg.exe"  
[esp+108]:&"x32dbg.exe"

The values that the malware changes from the registry to escape antiviruses.

```
[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 ANALYSIS

It has been seen that the malware tries to connect to the address 95[.1213[.1179[.167[.180 after stealing data. But because the server is not active, it could not establish a connection.

### 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: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: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:a0e5:93f0:a5d4:a0f8:62065 > svchost.exe:988
[UDP] fe80:0:0:a0e5:93f0:a5d4:a0f8:54482 > svchost.exe:988
[TCP] juheck.exe:1776 > 184.24.22.47:443
[TCP] 184.24.22.47:443 > juheck.exe:1776
[TCP] juheck.exe:1776 > 23.55.161.133:80
[TCP] 23.55.161.133:80 > juheck.exe:1776
[UDP] fe80:0:0:a0e5:93f0:a5d4:a0f8:50409 > svchost.exe:988
[UDP] fe80:0:0: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: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
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
0040E8B4 800D 58794300 lea ecx,dword ptr ds:[437958]
0040E8BA 51: push ecx
0040E8BB 6A 10: push 10
0040E8BD 8D8424 F8000000 lea esi,dword ptr ss:[esp+F8]
0040E8C4 56: push esi
0040E8C5 FFD0: cadd eax,ecx
0040E8C7 83C4 0C: add esp,c
0040E8CA 8D8C24 04010000 lea ecx,dword ptr ss:[esp+104]
0040E8D1 89F2: mov edx,esi
0040E8D3 E8 F641FFFF call 7gfdg5egds.402ACE
0040E8D8 F20F108424 04010000 movsd xmm0,qword ptr ss:[esp+104]
0040E8E1 8B9C24 0C010000 mov ebx,dword ptr ss:[esp+10C]
```

ecx:&"pospvisis.com:803"  
ecx:&"pospvisis.com:803"  
ecx:&"pospvisis.com:803"  
ecx:&"pospvisis.com:803"  
[esp+104]: "pospvisis.com:803"





## **SOLUTION PROPOSALS**

- Actual and reliable anti-virus software should be used on the systems.
- Incoming e-mails should be read carefully, e-mails and URLs from unknown sources and files should not be opened without a full scan of attachments.
- All installed software and operating system should be kept up to date.
- Train users frequently to be aware of potential phishing schemas and how to handle them in the right way.
- The network movements of the processes running on the system should be examined.

# Yara Rules

```
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/>