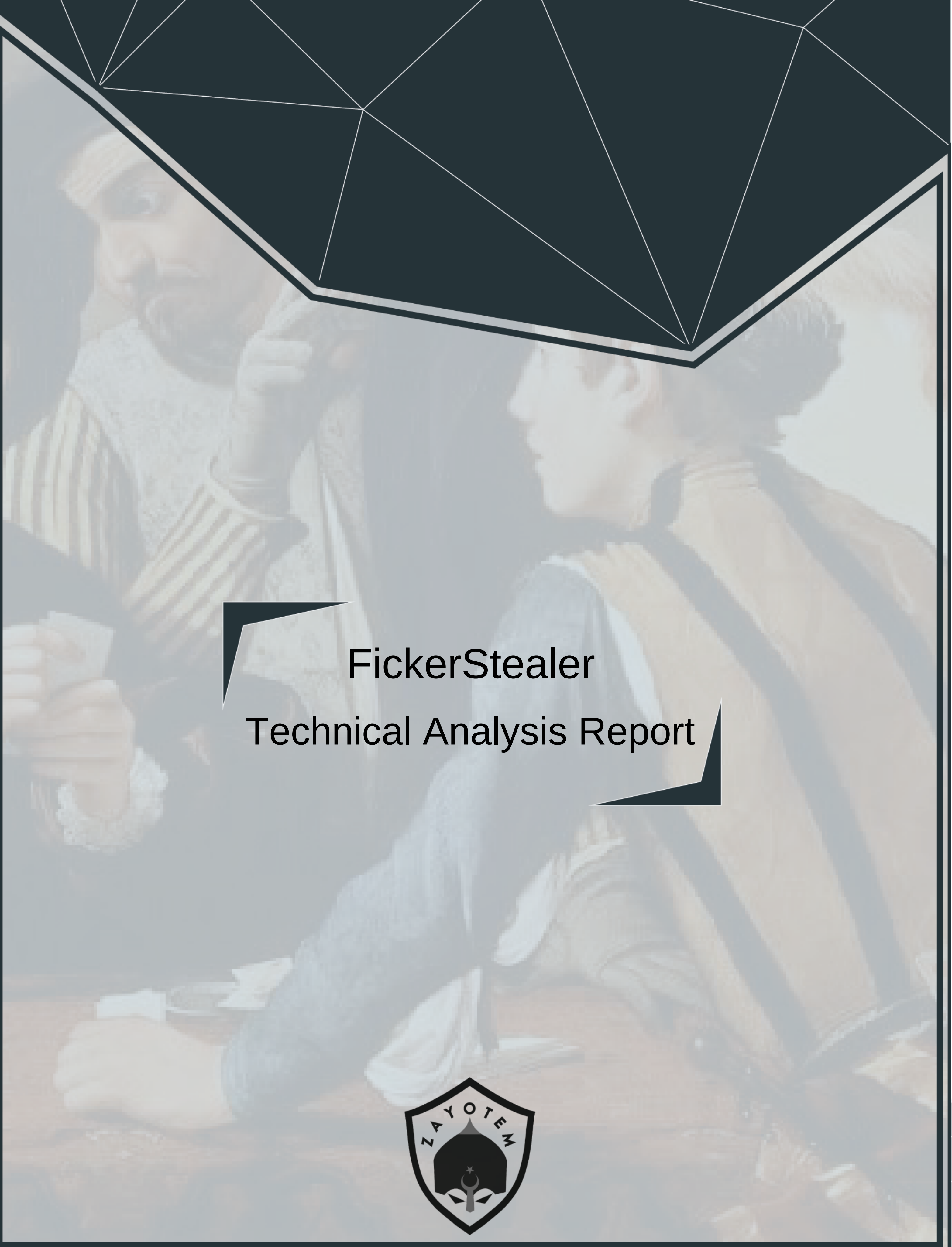


FickerStealer

Technical Analysis Report

ZAYOTEM

Contents

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;

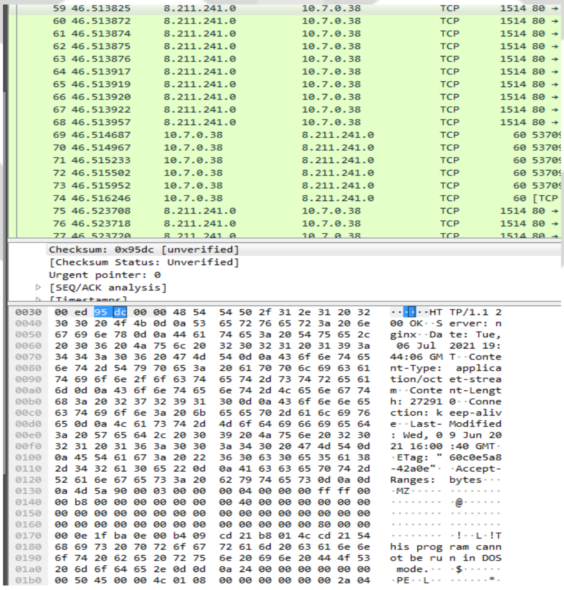
- Credentials saved in web browsers,
- Desktop messaging clients,
- To FTP clients,
- Blockchain wallets,
- It provides access to computer documents.

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	fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8ad4

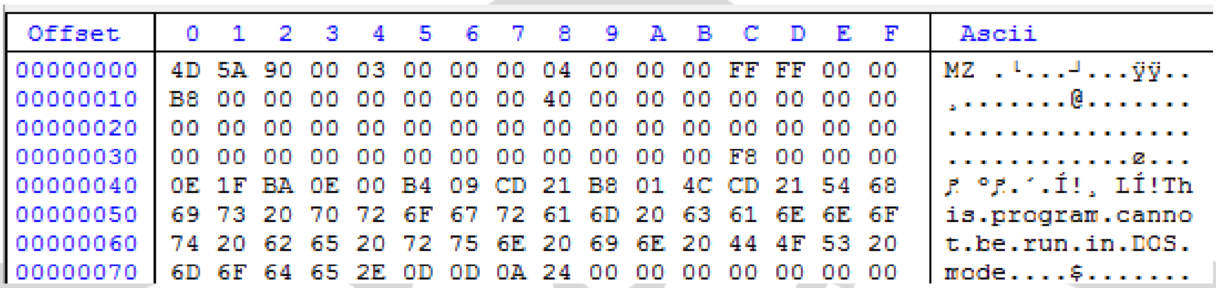
It has been observed that the file.dll malware downloads a file titled MZ when network traffic is monitored.



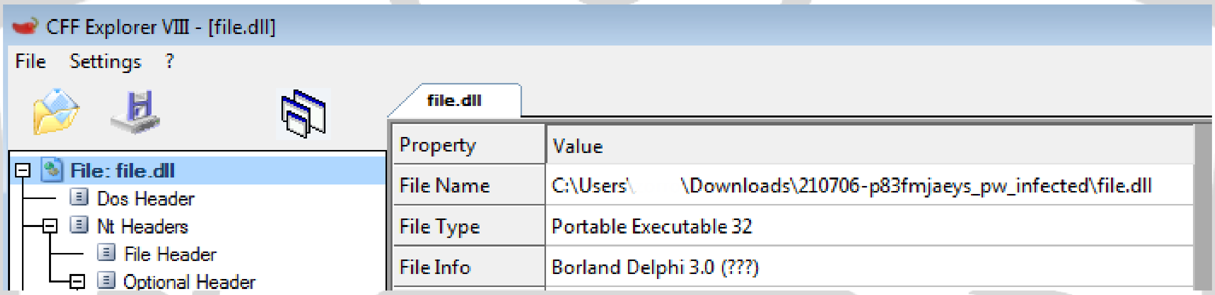
```
59 46.513825    8.211.241.0    10.7.0.38      TCP    1514 80 →
60 46.513872    8.211.241.0    10.7.0.38      TCP    1514 80 →
61 46.513874    8.211.241.0    10.7.0.38      TCP    1514 80 →
62 46.513875    8.211.241.0    10.7.0.38      TCP    1514 80 →
63 46.513876    8.211.241.0    10.7.0.38      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 46.515502    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 46.523708    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 46.523720    8.211.241.0    10.7.0.38      TCP    1514 80 →

    Checksum: 0x95dc [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▷ [SEQ/ACK analysis]
  ▷ [Timestamps]

0030  00 ed 95 dc 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 0d 0a 44 61  74 65 3a 20 54 75 65 2c   ginx··Da te: Tue,
0060  20 30 36 20 4a 75 6c 20  32 30 32 31 20 31 39 3a    06 Jul  2021 19:
0070  34 34 3a 30 36 20 47 4d  54 0d 0a 43 6f 6e 74 65   44:06 GM T··Conte
0080  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:  applica
0090  74 69 6f 6e 2f 6f 63 74  65 74 2d 73 74 72 65 61   tion/oct et-strea
00a0  6d 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   m··Conte nt-Lengt
00b0  68 3a 20 32 37 32 39 31  30 0d 0a 43 6f 6e 6e 65   h: 27291 0··Conne
00c0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00d0  65 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   e··Last- Modified
00e0  3a 20 57 65 64 2c 20 30  39 20 4a 75 6e 20 32 30   : Wed, 0 9 Jun 20
00f0  32 31 20 31 36 3a 30 30  3a 34 30 20 47 4d 54 0d   21 16:00 :40 GMT·
0100  0a 45 54 61 67 3a 20 22  36 30 63 30 65 35 61 38   ·ETag: " 60c0e5a8
0110  2d 34 32 61 30 65 22 0d  0a 41 63 63 65 70 74 2d   -42a0e"· ·Accept-
0120  52 61 6e 67 65 73 3a 20  62 79 74 65 73 0d 0a 0d   Ranges:  bytes···
0130  0a 4d 5a 90 00 03 00 00  00 04 00 00 00 ff ff 00   ·MZ····· ········
0140  00 b8 00 00 00 00 00 00  00 40 00 00 00 00 00 00   ········ ·@······
0150  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 80 00 00   ········ ········
0170  00 0e 1f ba 0e 00 b4 09  cd 21 b8 01 4c cd 21 54   ········ ·!··L·!T
0180  68 69 73 20 70 72 6f 67  72 61 6d 20 63 61 6e 6e   his prog ram cann
0190  6f 74 20 62 65 20 72 75  6e 20 69 6e 20 44 4f 53   ot be ru n in DOS
01a0  20 6d 6f 64 65 2e 0d 0d  0a 24 00 00 00 00 00 00    mode.·· ·$······
01b0  00 50 45 00 00 4c 01 08  00 00 00 00 00 00 2a 04   ·PE··L·· ······*·
```

file.dll ANALYSIS

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

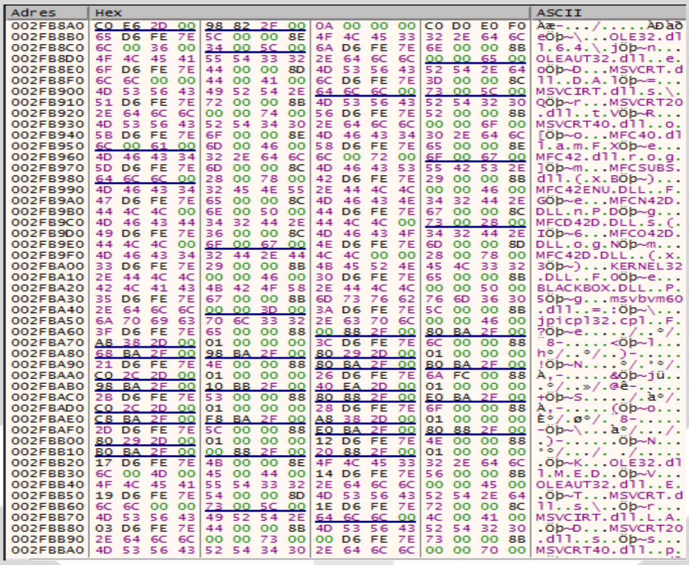


```
Offset     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   Ascii
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ .└...┘...ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  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  ♬ º♬.´.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....$.......
```



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

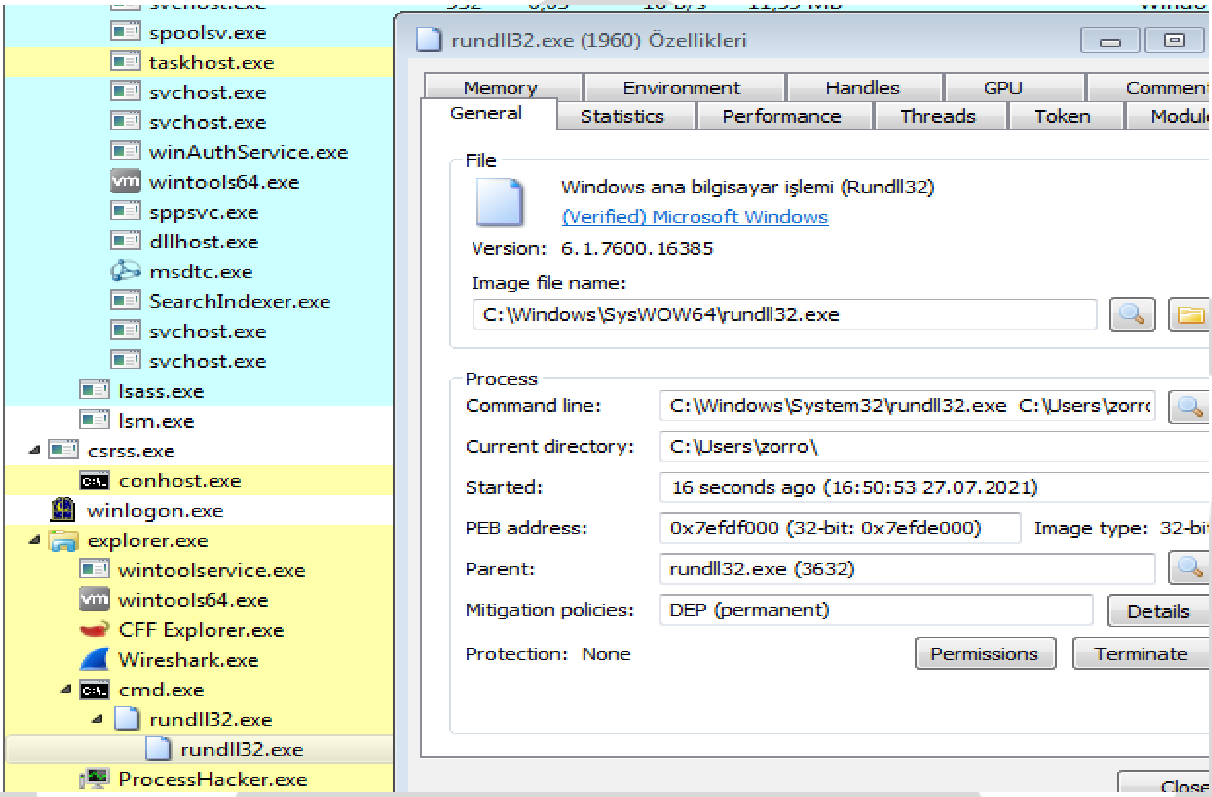
Dynamically loaded DLLs:



```
Adres     Hex                                              ASCII
002FB8A0  C0 E6 2D 00 98 82 2F 00 0A 00 00 00 C0 D0 E0 F0  Àæ-.../.....ÀÐàð
002FB8B0  65 D6 FE 7E 5C 00 00 8E 4F 4C 45 33 32 2E 64 6C  eÖþ~\...OLE32.dl
002FB8C0  6C 00 36 00 34 00 5C 00 6A D6 FE 7E 6E 00 00 8B  l.6.4.\.jÖþ~n...
002FB8D0  4F 4C 45 41 55 54 33 32 2E 64 6C 6C 00 00 65 00  OLEAUT32.dll..e.
002FB8E0  6F D6 FE 7E 44 00 00 8D 4D 53 56 43 52 54 2E 64  oÖþ~D...MSVCRT.d
002FB8F0  6C 6C 00 00 44 00 41 00 6C D6 FE 7E 3D 00 00 8C  ll..D.A.lÖþ~=...
002FB900  4D 53 56 43 49 52 54 2E 64 6C 6C 00 73 00 5C 00  MSVCIRT.dll.s.\.
002FB910  51 D6 FE 7E 72 00 00 8B 4D 53 56 43 52 54 32 30  QÖþ~r...MSVCRT20
002FB920  2E 64 6C 6C 00 00 74 00 56 D6 FE 7E 52 00 00 8B  .dll..t.VÖþ~R...
002FB930  4D 53 56 43 52 54 34 30 2E 64 6C 6C 00 00 6F 00  MSVCRT40.dll..o.
002FB940  5B D6 FE 7E 6F 00 00 8E 4D 46 43 34 30 2E 64 6C  [Öþ~o...MFC40.dl
002FB950  6C 00 61 00 6D 00 46 00 58 D6 FE 7E 65 00 00 8E  l.a.m.F.XÖþ~e...
002FB960  4D 46 43 34 32 2E 64 6C 6C 00 72 00 6F 00 67 00  MFC42.dll.r.o.g.
002FB970  5D D6 FE 7E 6D 00 00 8C 4D 46 43 53 55 42 53 2E  ]Öþ~m...MFCSUBS.
002FB980  64 6C 6C 00 28 00 78 00 42 D6 FE 7E 29 00 00 8B  dll.(.x.BÖþ~)...
002FB990  4D 46 43 34 32 45 4E 55 2E 44 4C 4C 00 00 46 00  MFC42ENU.DLL..F.
002FB9A0  47 D6 FE 7E 65 00 00 8C 4D 46 43 4E 34 32 44 2E  GÖþ~e...MFCN42D.
002FB9B0  44 4C 4C 00 6E 00 50 00 44 D6 FE 7E 67 00 00 8C  DLL.n.P.DÖþ~g...
002FB9C0  4D 46 43 44 34 32 44 2E 44 4C 4C 00 73 00 28 00  MFCD42D.DLL.s.(.
002FB9D0  49 D6 FE 7E 36 00 00 8C 4D 46 43 4F 34 32 44 2E  IÖþ~6...MFCO42D.
002FB9E0  44 4C 4C 00 6F 00 67 00 4E D6 FE 7E 6D 00 00 8D  DLL.o.g.NÖþ~m...
002FB9F0  4D 46 43 34 32 44 2E 44 4C 4C 00 00 28 00 78 00  MFC42D.DLL..(.x.
002FBA00  33 D6 FE 7E 29 00 00 8B 4B 45 52 4E 45 4C 33 32  3Öþ~)...KERNEL32
002FBA10  2E 44 4C 4C 00 00 46 00 30 D6 FE 7E 65 00 00 8B  .DLL..F.0Öþ~e...
002FBA20  42 4C 41 43 4B 42 4F 58 2E 44 4C 4C 00 00 50 00  BLACKBOX.DLL..P.
002FBA30  35 D6 FE 7E 67 00 00 8B 6D 73 76 62 76 6D 36 30  5Öþ~g...msvbvm60
002FBA40  2E 64 6C 6C 00 00 3D 00 3A D6 FE 7E 5C 00 00 8B  .dll..=.:Öþ~\...
002FBA50  6A 70 69 63 70 6C 33 32 2E 63 70 6C 00 00 46 00  jpicpl32.cpl..F.
002FBA60  3F D6 FE 7E 65 00 00 88 00 88 2F 00 80 BA 2F 00  ?Öþ~e...../..°/.
002FBA70  A8 38 2D 00 01 00 00 00 3C D6 FE 7E 6C 00 00 88  ¨8-.....<Öþ~l...
002FBA80  68 BA 2F 00 98 BA 2F 00 80 29 2D 00 01 00 00 00  h°/..°/..)-.....
002FBA90  21 D6 FE 7E 4E 00 00 88 80 BA 2F 00 B0 BA 2F 00  !Öþ~N....°/.°°/.
002FBAA0  C0 2C 2D 00 01 00 00 00 26 D6 FE 7E 6A FC 00 88  À,-.....&Öþ~jü..
002FBAB0  98 BA 2F 00 10 BB 2F 00 40 EA 2D 00 01 00 00 00  .°/..»/.@ê-.....
002FBAC0  2B D6 FE 7E 53 00 00 88 80 88 2F 00 E0 BA 2F 00  +Öþ~S...../.à°/.
002FBAD0  C0 2C 2D 00 01 00 00 00 28 D6 FE 7E 6F 00 00 88  À,-.....(Öþ~o...
002FBAE0  C8 BA 2F 00 F8 BA 2F 00 A8 38 2D 00 01 00 00 00  È°/.ø°/.¨8-.....
002FBAF0  2D D6 FE 7E 5C 00 00 88 E0 BA 2F 00 80 88 2F 00  -Öþ~\...à°/.../.
002FBB00  80 29 2D 00 01 00 00 00 12 D6 FE 7E 4E 00 00 88  .)-......Öþ~N...
002FBB10  B0 BA 2F 00 00 88 2F 00 20 88 2F 00 01 00 00 00  °°/.../. ./.....
002FBB20  17 D6 FE 7E 4B 00 00 8E 4F 4C 45 33 32 2E 64 6C  .Öþ~K...OLE32.dl
002FBB30  6C 00 4D 00 45 00 44 00 14 D6 FE 7E 56 00 00 8B  l.M.E.D..Öþ~V...
002FBB40  4F 4C 45 41 55 54 33 32 2E 64 6C 6C 00 00 45 00  OLEAUT32.dll..E.
002FBB50  19 D6 FE 7E 54 00 00 8D 4D 53 56 43 52 54 2E 64  .Öþ~T...MSVCRT.d
002FBB60  6C 6C 00 00 73 00 5C 00 1E D6 FE 7E 72 00 00 8C  ll..s.\..Öþ~r...
002FBB70  4D 53 56 43 49 52 54 2E 64 6C 6C 00 4C 00 41 00  MSVCIRT.dll.L.A.
002FBB80  03 D6 FE 7E 44 00 00 8B 4D 53 56 43 52 54 32 30  .Öþ~D...MSVCRT20
002FBB90  2E 64 6C 6C 00 00 73 00 00 D6 FE 7E 73 00 00 8B  .dll..s..Öþ~s...
002FBBA0  4D 53 56 43 52 54 34 30 2E 64 6C 6C 00 00 70 00  MSVCRT40.dll..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.



```
spoolsv.exe
taskhost.exe
svchost.exe
svchost.exe
winAuthService.exe
wintools64.exe
sppsvc.exe
dllhost.exe
msdtc.exe
SearchIndexer.exe
svchost.exe
svchost.exe
lsass.exe
lsm.exe
csrss.exe
  conhost.exe
winlogon.exe
explorer.exe
  wintoolservice.exe
  wintools64.exe
  CFF Explorer.exe
  Wireshark.exe
  cmd.exe
    rundll32.exe
      rundll32.exe
  ProcessHacker.exe
```

rundll32.exe (1960) Özellikleri

File

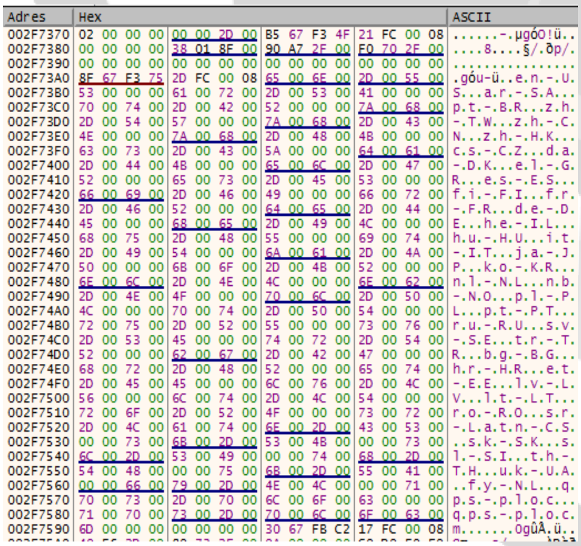
Windows ana bilgisayar işlemi (Rundll32)
(Verified) Microsoft Windows
Version: 6.1.7600.16385
Image file name: C:\Windows\SysWOW64\rundll32.exe

Process

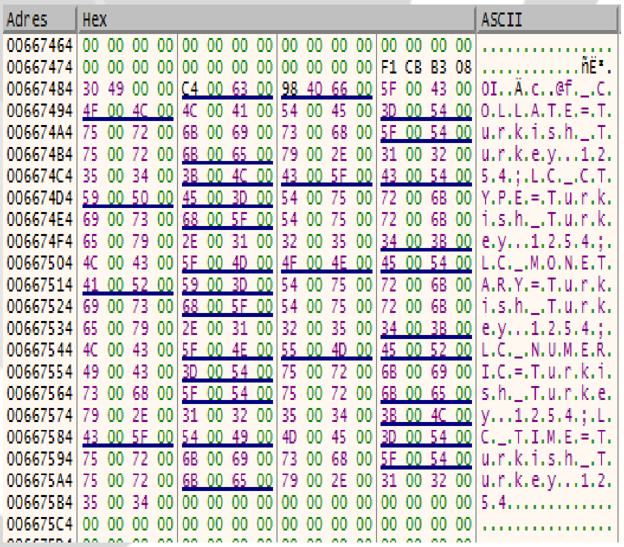
Command line: C:\Windows\System32\rundll32.exe C:\Users\zorro
Current directory: C:\Users\zorro\
Started: 16 seconds ago (16:50:53 27.07.2021)
PEB address: 0x7efdf000 (32-bit: 0x7efde000) Image type: 32-bi
Parent: rundll32.exe (3632)
Mitigation policies: DEP (permanent)
Protection: None

Information Collected:

Targeted languages and countries:

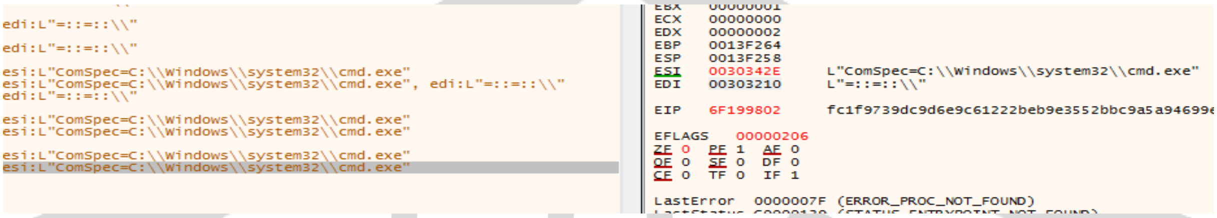


```
Adres     Hex                                              ASCII
002F7370  02 00 00 00 00 00 2D 00 B5 67 F3 4F 21 FC 00 08  ......-.µgóO!ü..
002F7380  00 00 00 00 38 01 8F 00 90 A7 2F 00 F0 70 2F 00  ....8....§/.ðp/.
002F7390  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
002F73A0  8F 67 F3 75 2D FC 00 08 65 00 6E 00 2D 00 55 00  .góu-ü..e.n.-.U.
002F73B0  53 00 00 00 61 00 72 00 2D 00 53 00 41 00 00 00  S...a.r.-.S.A...
002F73C0  70 00 74 00 2D 00 42 00 52 00 00 00 7A 00 68 00  p.t.-.B.R...z.h.
002F73D0  2D 00 54 00 57 00 00 00 7A 00 68 00 2D 00 43 00  -.T.W...z.h.-.C.
002F73E0  4E 00 00 00 7A 00 68 00 2D 00 48 00 4B 00 00 00  N...z.h.-.H.K...
002F73F0  63 00 73 00 2D 00 43 00 5A 00 00 00 64 00 61 00  c.s.-.C.Z...d.a.
002F7400  2D 00 44 00 4B 00 00 00 65 00 6C 00 2D 00 47 00  -.D.K...e.l.-.G.
002F7410  52 00 00 00 65 00 73 00 2D 00 45 00 53 00 00 00  R...e.s.-.E.S...
002F7420  66 00 69 00 2D 00 46 00 49 00 00 00 66 00 72 00  f.i.-.F.I...f.r.
002F7430  2D 00 46 00 52 00 00 00 64 00 65 00 2D 00 44 00  -.F.R...d.e.-.D.
002F7440  45 00 00 00 68 00 65 00 2D 00 49 00 4C 00 00 00  E...h.e.-.I.L...
002F7450  68 00 75 00 2D 00 48 00 55 00 00 00 69 00 74 00  h.u.-.H.U...i.t.
002F7460  2D 00 49 00 54 00 00 00 6A 00 61 00 2D 00 4A 00  -.I.T...j.a.-.J.
002F7470  50 00 00 00 6B 00 6F 00 2D 00 4B 00 52 00 00 00  P...k.o.-.K.R...
002F7480  6E 00 6C 00 2D 00 4E 00 4C 00 00 00 6E 00 62 00  n.l.-.N.L...n.b.
002F7490  2D 00 4E 00 4F 00 00 00 70 00 6C 00 2D 00 50 00  -.N.O...p.l.-.P.
002F74A0  4C 00 00 00 70 00 74 00 2D 00 50 00 54 00 00 00  L...p.t.-.P.T...
002F74B0  72 00 75 00 2D 00 52 00 55 00 00 00 73 00 76 00  r.u.-.R.U...s.v.
002F74C0  2D 00 53 00 45 00 00 00 74 00 72 00 2D 00 54 00  -.S.E...t.r.-.T.
002F74D0  52 00 00 00 62 00 67 00 2D 00 42 00 47 00 00 00  R...b.g.-.B.G...
002F74E0  68 00 72 00 2D 00 48 00 52 00 00 00 65 00 74 00  h.r.-.H.R...e.t.
002F74F0  2D 00 45 00 45 00 00 00 6C 00 76 00 2D 00 4C 00  -.E.E...l.v.-.L.
002F7500  56 00 00 00 6C 00 74 00 2D 00 4C 00 54 00 00 00  V...l.t.-.L.T...
002F7510  72 00 6F 00 2D 00 52 00 4F 00 00 00 73 00 72 00  r.o.-.R.O...s.r.
002F7520  2D 00 4C 00 61 00 74 00 6E 00 2D 00 43 00 53 00  -.L.a.t.n.-.C.S.
002F7530  00 00 73 00 6B 00 2D 00 53 00 4B 00 00 00 73 00  ..s.k.-.S.K...s.
002F7540  6C 00 2D 00 53 00 49 00 00 00 74 00 68 00 2D 00  l.-.S.I...t.h.-.
002F7550  54 00 48 00 00 00 75 00 6B 00 2D 00 55 00 41 00  T.H...u.k.-.U.A.
002F7560  00 00 66 00 79 00 2D 00 4E 00 4C 00 00 00 71 00  ..f.y.-.N.L...q.
002F7570  70 00 73 00 2D 00 70 00 6C 00 6F 00 63 00 00 00  p.s.-.p.l.o.c...
002F7580  71 00 70 00 73 00 2D 00 70 00 6C 00 6F 00 63 00  q.p.s.-.p.l.o.c.
002F7590  6D 00 00 00 00 00 00 00 30 67 FB C2 17 FC 00 08  m.......0gûÂ.ü..
```



```
Adres     Hex                                              ASCII
00667464  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00667474  00 00 00 00 00 00 00 00 00 00 00 00 F1 CB B3 08  ............ñË³.
00667484  30 49 00 00 C4 00 63 00 98 40 66 00 5F 00 43 00  0I..Ä.c..@f._.C.
00667494  4F 00 4C 00 4C 00 41 00 54 00 45 00 3D 00 54 00  O.L.L.A.T.E.=.T.
006674A4  75 00 72 00 6B 00 69 00 73 00 68 00 5F 00 54 00  u.r.k.i.s.h._.T.
006674B4  75 00 72 00 6B 00 65 00 79 00 2E 00 31 00 32 00  u.r.k.e.y...1.2.
006674C4  35 00 34 00 3B 00 4C 00 43 00 5F 00 43 00 54 00  5.4.;.L.C._.C.T.
006674D4  59 00 50 00 45 00 3D 00 54 00 75 00 72 00 6B 00  Y.P.E.=.T.u.r.k.
006674E4  69 00 73 00 68 00 5F 00 54 00 75 00 72 00 6B 00  i.s.h._.T.u.r.k.
006674F4  65 00 79 00 2E 00 31 00 32 00 35 00 34 00 3B 00  e.y...1.2.5.4.;.
00667504  4C 00 43 00 5F 00 4D 00 4F 00 4E 00 45 00 54 00  L.C._.M.O.N.E.T.
00667514  41 00 52 00 59 00 3D 00 54 00 75 00 72 00 6B 00  A.R.Y.=.T.u.r.k.
00667524  69 00 73 00 68 00 5F 00 54 00 75 00 72 00 6B 00  i.s.h._.T.u.r.k.
00667534  65 00 79 00 2E 00 31 00 32 00 35 00 34 00 3B 00  e.y...1.2.5.4.;.
00667544  4C 00 43 00 5F 00 4E 00 55 00 4D 00 45 00 52 00  L.C._.N.U.M.E.R.
00667554  49 00 43 00 3D 00 54 00 75 00 72 00 6B 00 69 00  I.C.=.T.u.r.k.i.
00667564  73 00 68 00 5F 00 54 00 75 00 72 00 6B 00 65 00  s.h._.T.u.r.k.e.
00667574  79 00 2E 00 31 00 32 00 35 00 34 00 3B 00 4C 00  y...1.2.5.4.;.L.
00667584  43 00 5F 00 54 00 49 00 4D 00 45 00 3D 00 54 00  C._.T.I.M.E.=.T.
00667594  75 00 72 00 6B 00 69 00 73 00 68 00 5F 00 54 00  u.r.k.i.s.h._.T.
006675A4  75 00 72 00 6B 00 65 00 79 00 2E 00 31 00 32 00  u.r.k.e.y...1.2.
006675B4  35 00 34 00 00 00 00 00 00 00 00 00 00 00 00 00  5.4.............
006675C4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

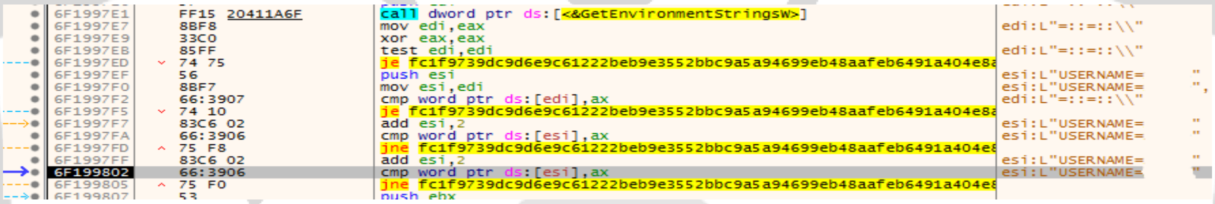
cmd.exe path:



```
edi:L"=::=::\\"

edi:L"=::=::\\"

esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe", edi:L"=::=::\\"
edi:L"=::=::\\"

esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"

esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
esi:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
```

```
ECX      00000000
EDX      00000002
EBP      0013F264
ESP      0013F258
ESI      0030342E       L"ComSpec=C:\\Windows\\system32\\cmd.exe"
EDI      00303210       L"=::=::\\"

EIP      6F199802       fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699e

EFLAGS     00000206
ZF 0   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1

LastError   0000007F (ERROR_PROC_NOT_FOUND)
```

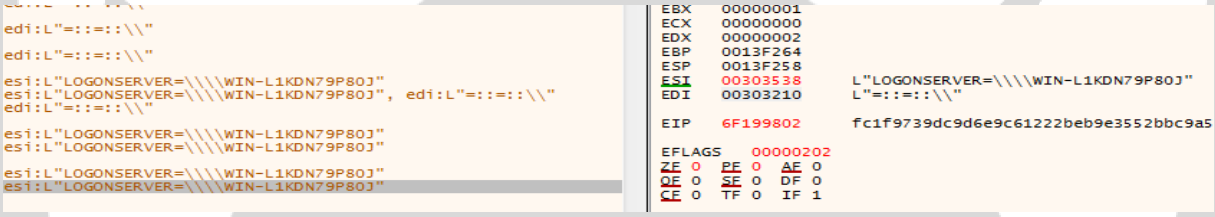
username:



```
6F1997E1      FF15 20411A6F     call dword ptr ds:[<&GetEnvironmentStringsW>]
6F1997E7      8BF8              mov edi,eax
6F1997E9      33C0              xor eax,eax
6F1997EB      85FF              test edi,edi
6F1997ED    ˅ 74 75             je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8a
6F1997EF      56                push esi
6F1997F0      8BF7              mov esi,edi
6F1997F2      66:3907           cmp word ptr ds:[edi],ax
6F1997F5    ˅ 74 10             je fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8a
6F1997F7      83C6 02           add esi,2
6F1997FA      66:3906           cmp word ptr ds:[esi],ax
6F1997FD    ^ 75 F8             jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8
6F1997FF      83C6 02           add esi,2
6F199802      66:3906           cmp word ptr ds:[esi],ax
6F199805    ^ 75 F0             jne fc1f9739dc9d6e9c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8
```

```
edi:L"=::=::\\"

edi:L"=::=::\\"

esi:L"USERNAME=       "
esi:L"USERNAME=       ",
edi:L"=::=::\\"

esi:L"USERNAME=       "
esi:L"USERNAME=       "

esi:L"USERNAME=       "
esi:L"USERNAME=       "
```

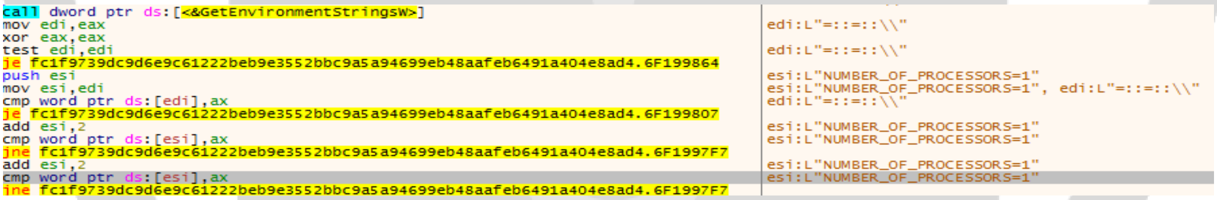
LOGONSERVER:



```
edi:L"=::=::\\"

edi:L"=::=::\\"

esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J", edi:L"=::=::\\"
edi:L"=::=::\\"

esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"

esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
esi:L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
```

```
EBX      00000001
ECX      00000000
EDX      00000002
EBP      0013F264
ESP      0013F258
ESI      00303538       L"LOGONSERVER=\\\\WIN-L1KDN79P80J"
EDI      00303210       L"=::=::\\"

EIP      6F199802       fc1f9739dc9d6e9c61222beb9e3552bbc9a5

EFLAGS     00000202
ZF 0   PE 0   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1
```

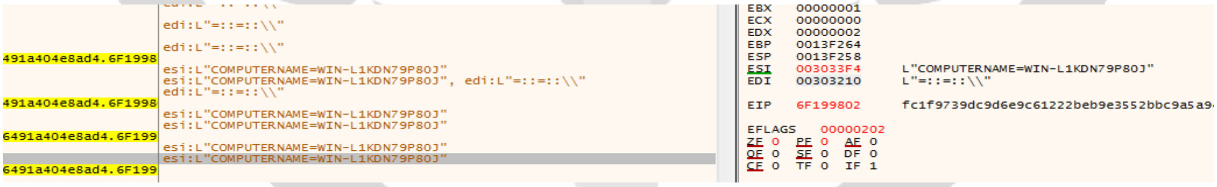
NUMBER_OF_PROCESSOR:



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

```
edi:L"=::=::\\"

edi:L"=::=::\\"

esi:L"NUMBER_OF_PROCESSORS=1"
esi:L"NUMBER_OF_PROCESSORS=1", edi:L"=::=::\\"
edi:L"=::=::\\"

esi:L"NUMBER_OF_PROCESSORS=1"
esi:L"NUMBER_OF_PROCESSORS=1"

esi:L"NUMBER_OF_PROCESSORS=1"
esi:L"NUMBER_OF_PROCESSORS=1"
```

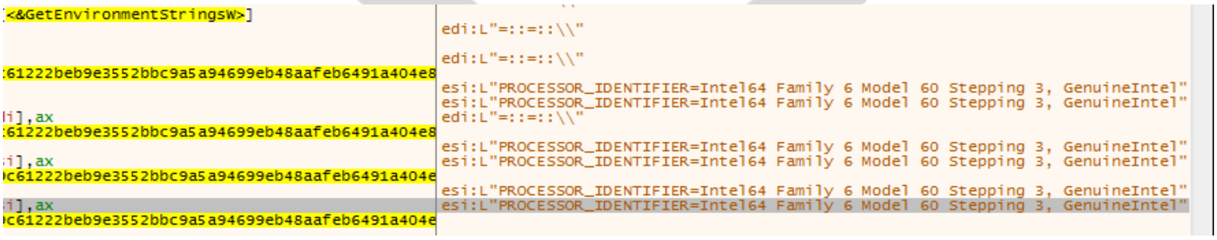
COMPUTERNAME:



```
                       edi:L"=::=::\\"

                       edi:L"=::=::\\"
491a404e8ad4.6F1998
                       esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
                       esi:L"COMPUTERNAME=WIN-L1KDN79P80J", edi:L"=::=::\\"
                       edi:L"=::=::\\"
491a404e8ad4.6F1998
                       esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
                       esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
6491a404e8ad4.6F199
                       esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
                       esi:L"COMPUTERNAME=WIN-L1KDN79P80J"
6491a404e8ad4.6F199
```

```
EBX      00000001
ECX      00000000
EDX      00000002
EBP      0013F264
ESP      0013F258
ESI      003033F4       L"COMPUTERNAME=WIN-L1KDN79P80J"
EDI      00303210       L"=::=::\\"

EIP      6F199802       fc1f9739dc9d6e9c61222beb9e3552bbc9a5a9

EFLAGS     00000202
ZF 0   PE 0   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1
```

PROCESSOR:

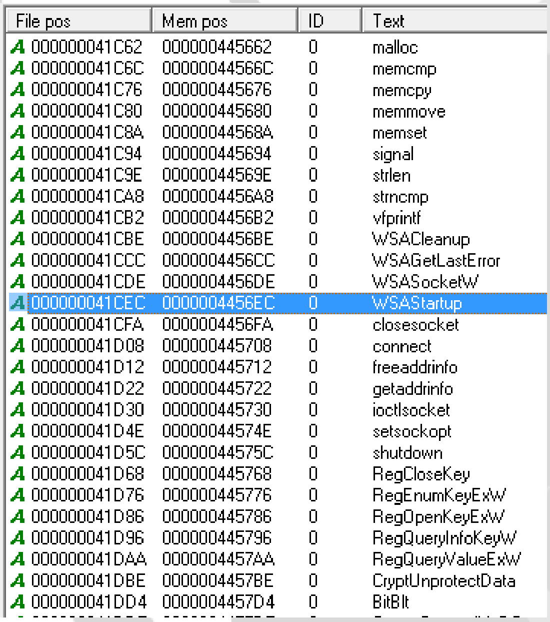


```
<&GetEnvironmentStringsW>]


:61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8

li],ax
:61222beb9e3552bbc9a5a94699eb48aafeb6491a404e8

:i],ax
c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e

:i],ax
c61222beb9e3552bbc9a5a94699eb48aafeb6491a404e
```

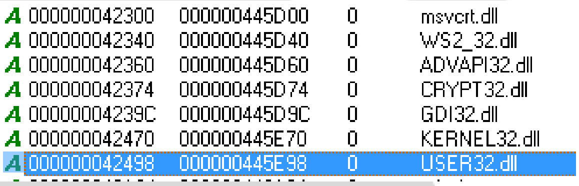
```
edi:L"=::=::\\"

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"
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"
```

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	memcmp
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	strncmp
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 000000041DAA	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

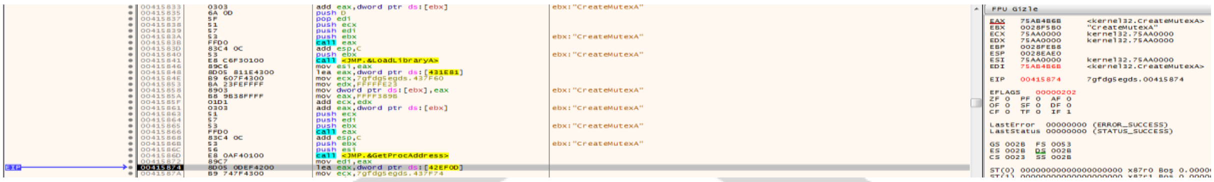
When we look at the imports of the pest, it uses important libraries such as USER32 and WS2_32. When we look at again the WS2_32 library, it is understood that it has the capacity to perform network operations, as can be seen from the functions it uses.

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.

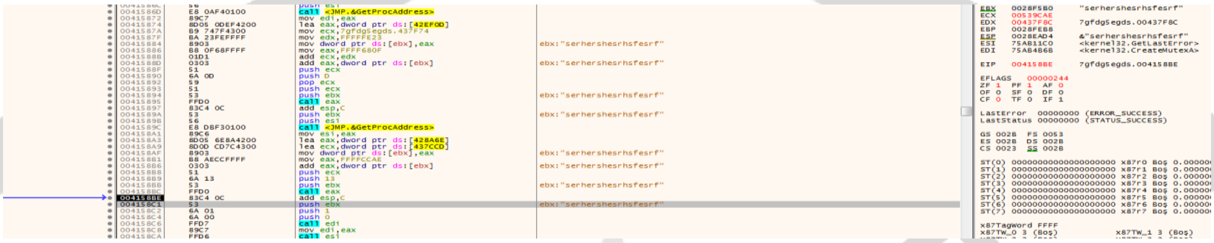
The malware first creates the mutex object with the "CreateMutexA" API that it loads dynamically.



```
00415833   0303           add eax,dword ptr ds:[ebx]            ebx:"CreateMutexA"
00415835   6A 0D          push D
00415837   5F             pop edi
00415838   51             push ecx
00415839   57             push edi
0041583A   53             push ebx                              ebx:"CreateMutexA"
0041583B   FFD0           call eax
0041583D   83C4 0C        add esp,C
00415840   53             push ebx                              ebx:"CreateMutexA"
00415841   E8 C6F30100    call <JMP.&LoadLibraryA>
00415846   89C6           mov esi,eax
00415848   8D05 811E4300  lea eax,dword ptr ds:[431E81]
0041584E   B9 607F4300    mov ecx,7gfdg5egds.437F60
00415853   BA 23FEFFFF    mov edx,FFFFFE23
00415858   8903           mov dword ptr ds:[ebx],eax            ebx:"CreateMutexA"
0041585A   B8 9B38FFFF    mov eax,FFFF389B
0041585F   01D1           add ecx,edx
00415861   0303           add eax,dword ptr ds:[ebx]            ebx:"CreateMutexA"
00415863   51             push ecx
00415864   57             push edi
00415865   53             push ebx                              ebx:"CreateMutexA"
00415866   FFD0           call eax
00415868   83C4 0C        add esp,C
0041586B   53             push ebx                              ebx:"CreateMutexA"
0041586C   56             push esi
0041586D   E8 0AF40100    call <JMP.&GetProcAddress>
00415872   89C7           mov edi,eax
00415874   8D05 0DEF4200  lea eax,dword ptr ds:[42EF0D]
0041587A   B9 747F4300    mov ecx,7gfdg5egds.437F74
```

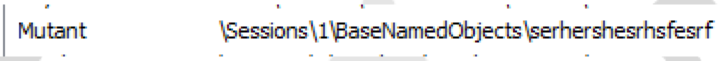
```
FPU Gizle
EAX    75AB4B6B    <kernel32.CreateMutexA>
EBX    0028F5B0    "CreateMutexA"
ECX    75AA0000    kernel32.75AA0000
EDX    75AA0000    kernel32.75AA0000
EBP    0028FEB8
ESP    0028EAE0
ESI    75AA0000    kernel32.75AA0000
EDI    75AB4B6B    <kernel32.CreateMutexA>

EIP    00415874    7gfdg5egds.00415874

EFLAGS   00000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus 00000000 (STATUS_SUCCESS)

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

ST(0) 0000000000000000000000 x87r0 Boş 0.0000
```

Name of mutex object:



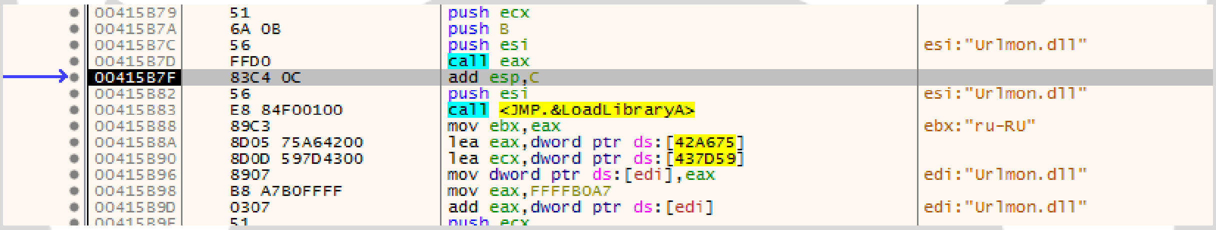
```
0041586D   E8 0AF40100    call <JMP.&GetProcAddress>
00415872   89C7           mov edi,eax
00415874   8D05 0DEF4200  lea eax,dword ptr ds:[42EF0D]
0041587A   B9 747F4300    mov ecx,7gfdg5egds.437F74
0041587F   BA 23FEFFFF    mov edx,FFFFFE23
00415884   8903           mov dword ptr ds:[ebx],eax            ebx:"serhershesrhsfesrf"
00415886   B8 0F68FFFF    mov eax,FFFF680F
0041588B   01D1           add ecx,edx
0041588D   0303           add eax,dword ptr ds:[ebx]            ebx:"serhershesrhsfesrf"
0041588F   51             push ecx
00415890   6A 0D          push D
00415892   59             pop ecx
00415893   51             push ecx
00415894   53             push ebx                              ebx:"serhershesrhsfesrf"
00415895   FFD0           call eax
00415897   83C4 0C        add esp,C
0041589A   53             push ebx                              ebx:"serhershesrhsfesrf"
0041589B   56             push esi
0041589C   E8 DBF30100    call <JMP.&GetProcAddress>
004158A1   89C6           mov esi,eax
004158A3   8D05 6E8A4200  lea eax,dword ptr ds:[428A6E]
004158A9   8D0D CD7C4300  lea ecx,dword ptr ds:[437CCD]
004158AF   8903           mov dword ptr ds:[ebx],eax            ebx:"serhershesrhsfesrf"
004158B1   B8 AECCFFFF    mov eax,FFFFCCAE
004158B6   0303           add eax,dword ptr ds:[ebx]            ebx:"serhershesrhsfesrf"
004158B8   51             push ecx
004158B9   6A 13          push 13
004158BB   53             push ebx                              ebx:"serhershesrhsfesrf"
004158BC   FFD0           call eax
004158BE   83C4 0C        add esp,C
004158C1   53             push ebx                              ebx:"serhershesrhsfesrf"
004158C2   6A 01          push 1
004158C4   6A 00          push 0
004158C6   FFD7           call edi
004158C8   89C7           mov edi,eax
004158CA   FFD6           call esi
```

```
EBX    0028F5B0    "serhershesrhsfesrf"
ECX    00539CAE
EDX    00437F8C    7gfdg5egds.00437F8C
EBP    0028FEB8
ESP    0028EAD4    &"serhershesrhsfesrf"
ESI    75AB11C0    <kernel32.GetLastError>
EDI    75AB4B6B    <kernel32.CreateMutexA>

EIP    004158BE    7gfdg5egds.004158BE

EFLAGS   00000244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus 00000000 (STATUS_SUCCESS)

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

ST(0) 0000000000000000000000 x87r0 Boş 0.00000
ST(1) 0000000000000000000000 x87r1 Boş 0.00000
ST(2) 0000000000000000000000 x87r2 Boş 0.00000
ST(3) 0000000000000000000000 x87r3 Boş 0.00000
ST(4) 0000000000000000000000 x87r4 Boş 0.00000
ST(5) 0000000000000000000000 x87r5 Boş 0.00000
ST(6) 0000000000000000000000 x87r6 Boş 0.00000
ST(7) 0000000000000000000000 x87r7 Boş 0.00000

x87TagWord FFFF
x87TW_0 3 (Boş)          x87TW_1 3 (Boş)
```

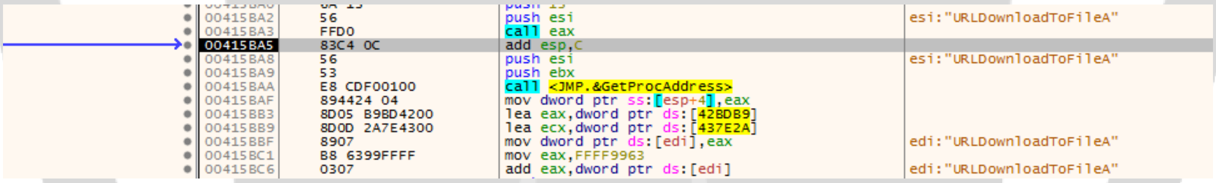


```
Mutant        \Sessions\1\BaseNamedObjects\serhershesrhsfesrf
```

Some other DLL's and APIs it loads dynamically:

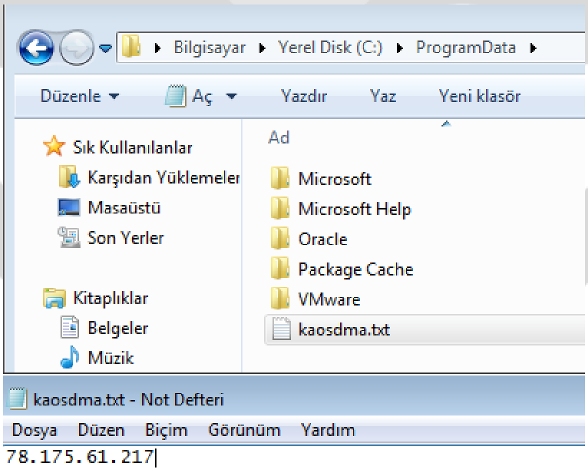


```
00415B79   51             push ecx
00415B7A   6A 0B          push B
00415B7C   56             push esi                      esi:"Urlmon.dll"
00415B7D   FFD0           call eax
00415B7F   83C4 0C        add esp,C
00415B82   56             push esi                      esi:"Urlmon.dll"
00415B83   E8 84F00100    call <JMP.&LoadLibraryA>
00415B88   89C3           mov ebx,eax                   ebx:"ru-RU"
00415B8A   8D05 75A64200  lea eax,dword ptr ds:[42A675]
00415B90   8D0D 597D4300  lea ecx,dword ptr ds:[437D59]
00415B96   8907           mov dword ptr ds:[edi],eax    edi:"Urlmon.dll"
00415B98   B8 A7B0FFFF    mov eax,FFFFB0A7
00415B9D   0307           add eax,dword ptr ds:[edi]    edi:"Urlmon.dll"
```



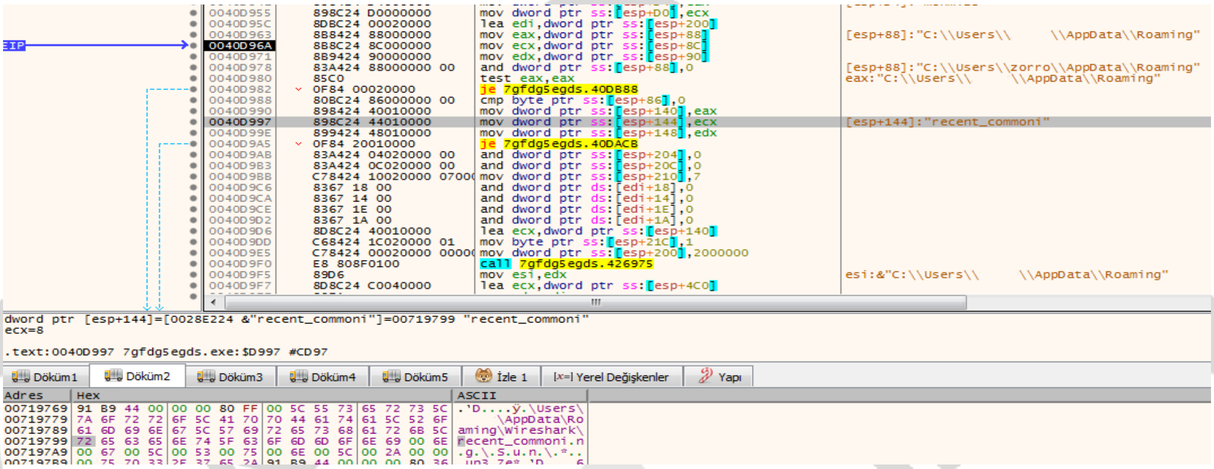
```
00415BA2   56             push esi                          esi:"URLDownloadToFileA"
00415BA3   FFD0           call eax
00415BA5   83C4 0C        add esp,C
00415BA8   56             push esi                          esi:"URLDownloadToFileA"
00415BA9   53             push ebx
00415BAA   E8 CDF00100    call <JMP.&GetProcAddress>
00415BAF   894424 04      mov dword ptr ss:[esp+4],eax
00415BB3   8D05 B9BD4200  lea eax,dword ptr ds:[42BDB9]
00415BB9   8D0D 2A7E4300  lea ecx,dword ptr ds:[437E2A]
00415BBF   8907           mov dword ptr ds:[edi],eax        edi:"URLDownloadToFileA"
00415BC1   B8 6399FFFF    mov eax,FFFF9963
00415BC6   0307           add eax,dword ptr ds:[edi]        edi:"URLDownloadToFileA"
```

The malware then drops the .txt file with an ip address into ProgramData.



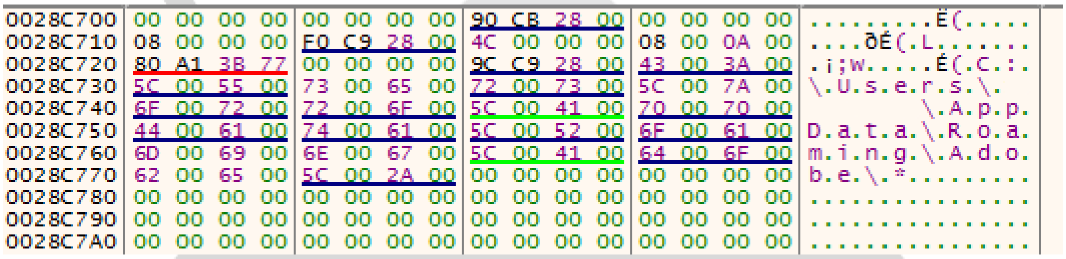
```
78.175.61.217
```

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



```
0040D955   898C24 D0000000       mov dword ptr ss:[esp+D0],ecx
0040D95C   8DBC24 00020000       lea edi,dword ptr ss:[esp+200]
0040D963   8B8424 88000000       mov eax,dword ptr ss:[esp+88]         [esp+88]:"C:\\Users\\     \\AppData\\Roaming"
0040D96A   8B8C24 8C000000       mov ecx,dword ptr ss:[esp+8C]
0040D971   8B9424 90000000       mov edx,dword ptr ss:[esp+90]
0040D978   83A424 88000000 00    and dword ptr ss:[esp+88],0           [esp+88]:"C:\\Users\\zorro\\AppData\\Roaming"
0040D980   85C0                  test eax,eax                          eax:"C:\\Users\\     \\AppData\\Roaming"
0040D982   0F84 00020000         je 7gfdg5egds.40DB88
0040D988   80BC24 86000000 00    cmp byte ptr ss:[esp+86],0
0040D990   898424 40010000       mov dword ptr ss:[esp+140],eax
0040D997   898C24 44010000       mov dword ptr ss:[esp+144],ecx        [esp+144]:"recent_commoni"
0040D99E   899424 48010000       mov dword ptr ss:[esp+148],edx
0040D9A5   0F84 20010000         je 7gfdg5egds.40DACB
0040D9AB   83A424 04020000 00    and dword ptr ss:[esp+204],0
0040D9B3   83A424 0C020000 00    and dword ptr ss:[esp+20C],0
0040D9BB   C78424 10020000 0700( mov dword ptr ss:[esp+210],7
0040D9C6   8367 18 00            and dword ptr ds:[edi+18],0
0040D9CA   8367 14 00            and dword ptr ds:[edi+14],0
0040D9CE   8367 1E 00            and dword ptr ds:[edi+1E],0
0040D9D2   8367 1A 00            and dword ptr ds:[edi+1A],0
0040D9D6   8D8C24 40010000       lea ecx,dword ptr ss:[esp+140]
0040D9DD   C68424 1C020000 01    mov byte ptr ss:[esp+21C],1
0040D9E5   C78424 00020000 0000( mov dword ptr ss:[esp+200],2000000
0040D9F0   E8 808F0100           call 7gfdg5egds.426975
0040D9F5   89D6                  mov esi,edx                           esi:&"C:\\Users\\     \\AppData\\Roaming"
0040D9F7   8D8C24 C0040000       lea ecx,dword ptr ss:[esp+4C0]

dword ptr [esp+144]=[0028E224 &"recent_commoni"]=00719799 "recent_commoni"
ecx=8

.text:0040D997 7gfdg5egds.exe:$D997 #CD97
```

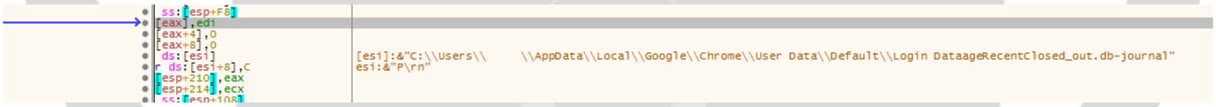
```
Adres     Hex                                              ASCII
00719769  91 B9 44 00 00 00 80 FF 00 5C 55 73 65 72 73 5C  .'D....ÿ.\Users\
00719779  7A 6F 72 72 6F 5C 41 70 70 44 61 74 61 5C 52 6F       \AppData\Ro
00719789  61 6D 69 6E 67 5C 57 69 72 65 73 68 61 72 6B 5C  aming\Wireshark\
00719799  72 65 63 65 6E 74 5F 63 6F 6D 6D 6F 6E 69 00 6E  recent_commoni.n
007197A9  00 67 00 5C 00 53 00 75 00 6E 00 5C 00 2A 00 00  .g.\.S.u.n.\.*..
```



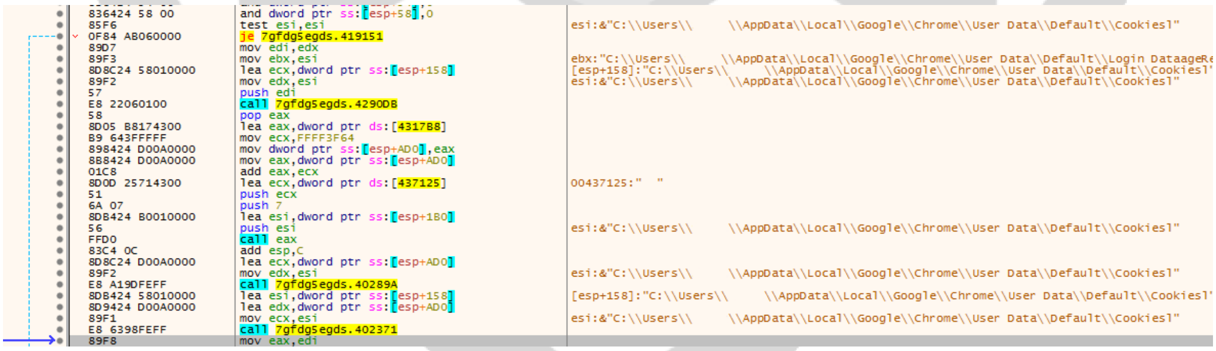
```
0028C700  00 00 00 00  00 00 00 00  90 CB 28 00  00 00 00 00  .........Ë(.....
0028C710  08 00 00 00  F0 C9 28 00  4C 00 00 00  08 00 0A 00  ....ðÉ(.L.......
0028C720  80 A1 3B 77  00 00 00 00  9C C9 28 00  43 00 3A 00  .¡;w.....É(.C.:.
0028C730  5C 00 55 00  73 00 65 00  72 00 73 00  5C 00 7A 00  \.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.\.*.........
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:

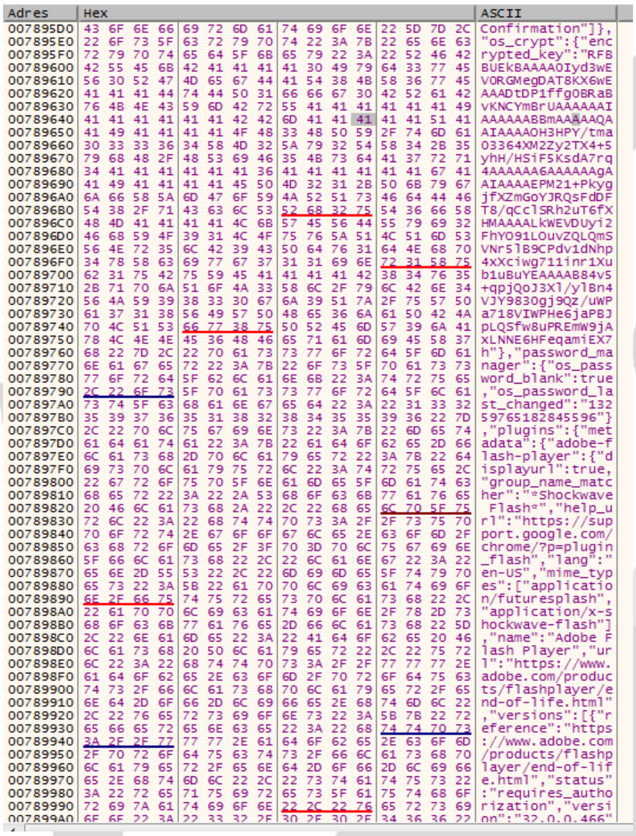


```
 ss:[esp+F8]
[eax],edi
[eax+4],0
[eax+8],0
 ds:[esi]         [esi]:&"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Login DataageRecentClosed_out.db-journal"
r ds:[esi+8],C    esi:&"P\rn"
[esp+210],eax
[esp+214],ecx
```

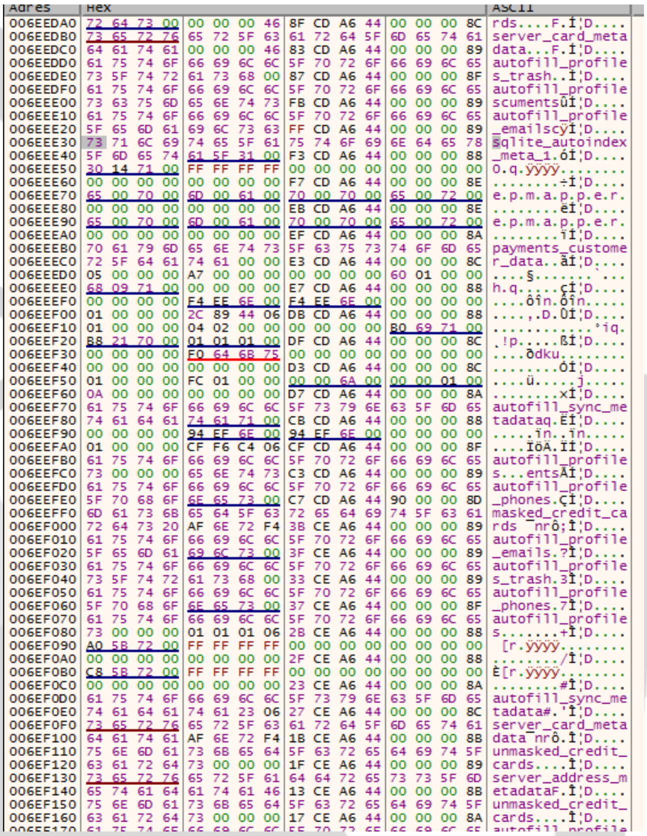


```
836424 58 00       and dword ptr ss:[esp+58],0
85F6               test esi,esi                       esi:&"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
0F84 AB060000      je 7gfdg5egds.419151
89D7               mov edi,edx
89F3               mov ebx,esi                        ebx:"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Login DataageRe
8D8C24 58010000    lea ecx,dword ptr ss:[esp+158]     [esp+158]:"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1'
89F2               mov edx,esi                        esi:&"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
57                 push edi
E8 22060100        call 7gfdg5egds.4290DB
58                 pop eax
8D05 B8174300      lea eax,dword ptr ds:[4317B8]
B9 643FFFFF        mov ecx,FFFF3F64
898424 D00A0000    mov dword ptr ss:[esp+AD0],eax
8B8424 D00A0000    mov eax,dword ptr ss:[esp+AD0]
01C8               add eax,ecx
8D0D 25714300      lea ecx,dword ptr ds:[437125]      00437125:"  "
51                 push ecx
6A 07              push 7
8DB424 B0010000    lea esi,dword ptr ss:[esp+1B0]
56                 push esi                           esi:&"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
FFD0               call eax
83C4 0C            add esp,C
8D8C24 D00A0000    lea ecx,dword ptr ss:[esp+AD0]
89F2               mov edx,esi                        esi:&"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
E8 A19DFEFF        call 7gfdg5egds.40289A
8DB424 58010000    lea esi,dword ptr ss:[esp+158]     [esp+158]:"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1'
8D9424 D00A0000    lea edx,dword ptr ss:[esp+AD0]
89F1               mov ecx,esi                        esi:&"C:\\Users\\     \\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Cookies1"
E8 6398FEFF        call 7gfdg5egds.402371
89F8               mov eax,edi
```

Phone number, credit card information kept in Google Chrome:

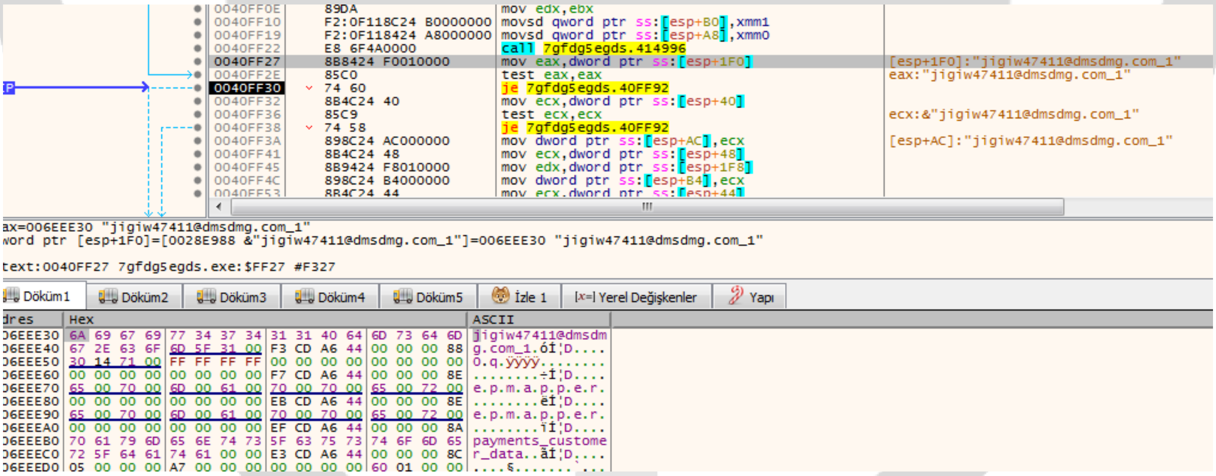


```
Adres     Hex                                              ASCII
007895D0  43 6F 6E 66 69 72 6D 61 74 69 6F 6E 22 5D 7D 2C  Confirmation"]},
007895E0  22 6F 73 5F 63 72 79 70 74 22 3A 7B 22 65 6E 63  "os_crypt":{"enc
007895F0  72 79 70 74 65 64 5F 6B 65 79 22 3A 22 52 46 42  rypted_key":"RFB
00789600  42 55 45 6B 42 41 41 41 41 30 49 79 64 33 77 45  BUEkBAAAA0Iyd3wE
00789610  56 30 52 47 4D 65 67 44 41 54 38 4B 58 36 77 45  V0RGMegDAT8KX6wE
00789620  41 41 41 44 74 44 50 31 66 66 67 30 42 52 61 42  AAADtDP1ffg0BRaB
00789630  76 4B 4E 43 59 6D 42 72 55 41 41 41 41 41 41 49  vKNCYmBrUAAAAAAI
00789640  41 41 41 41 41 41 42 42 6D 41 41 41 41 41 51 41  AAAAAABBmAAAAAQA
00789650  41 49 41 41 41 41 4F 48 33 48 50 59 2F 74 6D 61  AIAAAAOH3HPY/tma
00789660  30 33 33 36 34 58 4D 32 5A 79 32 54 58 34 2B 35  03364XM2Zy2TX4+5
00789670  79 68 48 2F 48 53 69 46 35 4B 73 64 41 37 72 71  yhH/HSiF5KsdA7rq
00789680  34 41 41 41 41 41 41 36 41 41 41 41 41 41 67 41  4AAAAAA6AAAAAAgA
00789690  41 49 41 41 41 41 45 50 4D 32 31 2B 50 6B 79 67  AIAAAAEPM21+Pkyg
007896A0  6A 66 58 5A 6D 47 6F 59 4A 52 51 73 46 64 44 46  jfXZmGoYJRQsFdDF
007896B0  54 38 2F 71 43 63 6C 53 52 68 32 75 54 36 66 58  T8/qCclSRh2uT6fX
007896C0  48 4D 41 41 41 41 4C 6B 57 45 56 44 55 79 69 32  HMAAAALkWEVDUyi2
007896D0  46 68 59 4F 39 31 4C 4F 75 76 5A 51 4C 51 6D 53  FhYO91LOuvZQLQmS
007896E0  56 4E 72 35 6C 42 39 43 50 64 76 31 64 4E 68 70  VNr5lB9CPdv1dNhp
007896F0  34 78 58 63 69 77 67 37 31 31 69 6E 72 31 58 75  4xXciwg711inr1Xu
00789700  62 31 75 42 75 59 45 41 41 41 41 42 38 34 76 35  b1uBuYEAAAAB84v5
00789710  2B 71 70 6A 51 6F 4A 33 58 6C 2F 79 6C 42 6E 34  +qpjQoJ3Xl/ylBn4
00789720  56 4A 59 39 38 33 30 67 6A 39 51 7A 2F 75 57 50  VJY9830gj9Qz/uWP
00789730  61 37 31 38 56 49 57 50 48 65 36 6A 61 50 42 4A  a718VIWPHe6jaPBJ
00789740  70 4C 51 53 66 77 38 75 50 52 45 6D 57 39 6A 41  pLQSfw8uPREmW9jA
00789750  78 4C 4E 4E 45 36 48 46 65 71 61 6D 69 45 58 37  xLNNE6HFeqamiEX7
00789760  68 22 7D 2C 22 70 61 73 73 77 6F 72 64 5F 6D 61  h"},"password_ma
00789770  6E 61 67 65 72 22 3A 7B 22 6F 73 5F 70 61 73 73  nager":{"os_pass
00789780  77 6F 72 64 5F 62 6C 61 6E 6B 22 3A 74 72 75 65  word_blank":true
00789790  2C 22 6F 73 5F 70 61 73 73 77 6F 72 64 5F 6C 61  ,"os_password_la
007897A0  73 74 5F 63 68 61 6E 67 65 64 22 3A 22 31 33 32  st_changed":"132
007897B0  35 39 37 36 35 31 38 32 38 34 35 35 39 36 22 7D  59765182845596"}
007897C0  2C 22 70 6C 75 67 69 6E 73 22 3A 7B 22 6D 65 74  ,"plugins":{"met
007897D0  61 64 61 74 61 22 3A 7B 22 61 64 6F 62 65 2D 66  adata":{"adobe-f
007897E0  6C 61 73 68 2D 70 6C 61 79 65 72 22 3A 7B 22 64  lash-player":{"d
007897F0  69 73 70 6C 61 79 75 72 6C 22 3A 74 72 75 65 2C  isplayurl":true,
00789800  22 67 72 6F 75 70 5F 6E 61 6D 65 5F 6D 61 74 63  "group_name_matc
00789810  68 65 72 22 3A 22 2A 53 68 6F 63 6B 77 61 76 65  her":"*Shockwave
00789820  20 46 6C 61 73 68 2A 22 2C 22 68 65 6C 70 5F 75   Flash*","help_u
00789830  72 6C 22 3A 22 68 74 74 70 73 3A 2F 2F 73 75 70  rl":"https://sup
00789840  70 6F 72 74 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F  port.google.com/
00789850  63 68 72 6F 6D 65 2F 3F 70 3D 70 6C 75 67 69 6E  chrome/?p=plugin
00789860  5F 66 6C 61 73 68 22 2C 22 6C 61 6E 67 22 3A 22  _flash","lang":"
00789870  65 6E 2D 55 53 22 2C 22 6D 69 6D 65 5F 74 79 70  en-US","mime_typ
00789880  65 73 22 3A 5B 22 61 70 70 6C 69 63 61 74 69 6F  es":["applicatio
00789890  6E 2F 66 75 74 75 72 65 73 70 6C 61 73 68 22 2C  n/futuresplash",
007898A0  22 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 73  "application/x-s
007898B0  68 6F 63 6B 77 61 76 65 2D 66 6C 61 73 68 22 5D  hockwave-flash"]
007898C0  2C 22 6E 61 6D 65 22 3A 22 41 64 6F 62 65 20 46  ,"name":"Adobe F
007898D0  6C 61 73 68 20 50 6C 61 79 65 72 22 2C 22 75 72  lash Player","ur
007898E0  6C 22 3A 22 68 74 74 70 73 3A 2F 2F 77 77 77 2E  l":"https://www.
007898F0  61 64 6F 62 65 2E 63 6F 6D 2F 70 72 6F 64 75 63  adobe.com/produc
00789900  74 73 2F 66 6C 61 73 68 70 6C 61 79 65 72 2F 65  ts/flashplayer/e
00789910  6E 64 2D 6F 66 2D 6C 69 66 65 2E 68 74 6D 6C 22  nd-of-life.html"
00789920  2C 22 76 65 72 73 69 6F 6E 73 22 3A 5B 7B 22 72  ,"versions":[{"r
00789930  65 66 65 72 65 6E 63 65 22 3A 22 68 74 74 70 73  eference":"https
00789940  3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D  ://www.adobe.com
00789950  2F 70 72 6F 64 75 63 74 73 2F 66 6C 61 73 68 70  /products/flashp
00789960  6C 61 79 65 72 2F 65 6E 64 2D 6F 66 2D 6C 69 66  layer/end-of-lif
00789970  65 2E 68 74 6D 6C 22 2C 22 73 74 61 74 75 73 22  e.html","status"
00789980  3A 22 72 65 71 75 69 72 65 73 5F 61 75 74 68 6F  :"requires_autho
00789990  72 69 7A 61 74 69 6F 6E 22 2C 22 76 65 72 73 69  rization","versi
007899A0  6F 6E 22 3A 22 33 32 2E 30 2E 30 2E 34 36 36 22  on":"32.0.0.466"
```



```
Adres     Hex                                              ASCII
006EEDA0  72 64 73 00 00 00 00 46 8F CD A6 44 00 00 00 8C  rds....F.Í¦D....
006EEDB0  73 65 72 76 65 72 5F 63 61 72 64 5F 6D 65 74 61  server_card_meta
006EEDC0  64 61 74 61 00 00 00 46 83 CD A6 44 00 00 00 89  data...F.Í¦D....
006EEDD0  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EEDE0  73 5F 74 72 61 73 68 00 87 CD A6 44 00 00 00 8F  s_trash..Í¦D....
006EEDF0  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EEE00  73 63 75 6D 65 6E 74 73 FB CD A6 44 00 00 00 89  scumentsûÍ¦D....
006EEE10  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EEE20  5F 65 6D 61 69 6C 73 63 FF CD A6 44 00 00 00 89  _emailscÿÍ¦D....
006EEE30  73 71 6C 69 74 65 5F 61 75 74 6F 69 6E 64 65 78  sqlite_autoindex
006EEE40  5F 6D 65 74 61 5F 31 00 F3 CD A6 44 00 00 00 88  _meta_1.óÍ¦D....
006EEE50  30 14 71 00 FF FF FF FF 00 00 00 00 00 00 00 00  0.q.ÿÿÿÿ........
006EEE60  00 00 00 00 00 00 00 00 F7 CD A6 44 00 00 00 8E  ........÷Í¦D....
006EEE70  65 00 70 00 6D 00 61 00 70 00 70 00 65 00 72 00  e.p.m.a.p.p.e.r.
006EEE80  00 00 00 00 00 00 00 00 EB CD A6 44 00 00 00 8E  ........ëÍ¦D....
006EEE90  65 00 70 00 6D 00 61 00 70 00 70 00 65 00 72 00  e.p.m.a.p.p.e.r.
006EEEA0  00 00 00 00 00 00 00 00 EF CD A6 44 00 00 00 8A  ........ïÍ¦D....
006EEEB0  70 61 79 6D 65 6E 74 73 5F 63 75 73 74 6F 6D 65  payments_custome
006EEEC0  72 5F 64 61 74 61 00 00 E3 CD A6 44 00 00 00 8C  r_data..ãÍ¦D....
006EEED0  05 00 00 00 A7 00 00 00 00 00 00 00 60 01 00 00  ....§.......`...
006EEEE0  68 09 71 00 00 00 00 00 E7 CD A6 44 00 00 00 88  h.q.....çÍ¦D....
006EEEF0  00 00 00 00 F4 EE 6E 00 F4 EE 6E 00 00 00 00 00  ....ôîn.ôîn.....
006EEF00  01 00 00 00 2C 89 44 06 DB CD A6 44 00 00 00 88  ....,.D.ÛÍ¦D....
006EEF10  01 00 00 00 04 02 00 00 00 00 00 00 B0 69 71 00  ............°iq.
006EEF20  B8 21 70 00 01 01 01 00 DF CD A6 44 00 00 00 8C  ¸!p.....ßÍ¦D....
006EEF30  00 00 00 00 F0 64 6B 75 00 00 00 00 00 00 00 00  ....ðdku........
006EEF40  00 00 00 00 00 00 00 00 D3 CD A6 44 00 00 00 8C  ........ÓÍ¦D....
006EEF50  01 00 00 00 FC 01 00 00 00 00 6A 00 00 00 01 00  ....ü.....j.....
006EEF60  0A 00 00 00 00 00 00 00 D7 CD A6 44 00 00 00 8A  ........×Í¦D....
006EEF70  61 75 74 6F 66 69 6C 6C 5F 73 79 6E 63 5F 6D 65  autofill_sync_me
006EEF80  74 61 64 61 74 61 71 00 CB CD A6 44 00 00 00 88  tadataq.ËÍ¦D....
006EEF90  00 00 00 00 94 EF 6E 00 94 EF 6E 00 00 00 00 00  .....ïn..ïn.....
006EEFA0  01 00 00 00 CF F6 C4 06 CF CD A6 44 00 00 00 8F  ....ÏöÄ.ÏÍ¦D....
006EEFB0  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EEFC0  73 00 00 00 65 6E 74 73 C3 CD A6 44 00 00 00 89  s...entsÃÍ¦D....
006EEFD0  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EEFE0  5F 70 68 6F 6E 65 73 00 C7 CD A6 44 90 00 00 8D  _phones.ÇÍ¦D....
006EEFF0  6D 61 73 6B 65 64 5F 63 72 65 64 69 74 5F 63 61  masked_credit_ca
006EF000  72 64 73 20 AF 6E 72 F4 3B CE A6 44 00 00 00 89  rds ¯nrô;Î¦D....
006EF010  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EF020  5F 65 6D 61 69 6C 73 00 3F CE A6 44 00 00 00 89  _emails.?Î¦D....
006EF030  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EF040  73 5F 74 72 61 73 68 00 33 CE A6 44 00 00 00 89  s_trash.3Î¦D....
006EF050  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EF060  5F 70 68 6F 6E 65 73 00 37 CE A6 44 00 00 00 8F  _phones.7Î¦D....
006EF070  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
006EF080  73 00 00 00 01 01 01 06 2B CE A6 44 00 00 00 88  s.......+Î¦D....
006EF090  A0 5B 72 00 FF FF FF FF 00 00 00 00 00 00 00 00   [r.ÿÿÿÿ........
006EF0A0  00 00 00 00 00 00 00 00 2F CE A6 44 00 00 00 88  ......../Î¦D....
006EF0B0  C8 5B 72 00 FF FF FF FF 00 00 00 00 00 00 00 00  È[r.ÿÿÿÿ........
006EF0C0  00 00 00 00 00 00 00 00 23 CE A6 44 00 00 00 8A  ........#Î¦D....
006EF0D0  61 75 74 6F 66 69 6C 6C 5F 73 79 6E 63 5F 6D 65  autofill_sync_me
006EF0E0  74 61 64 61 74 61 23 06 27 CE A6 44 00 00 00 8C  tadata#.'Î¦D....
006EF0F0  73 65 72 76 65 72 5F 63 61 72 64 5F 6D 65 74 61  server_card_meta
006EF100  64 61 74 61 AF 6E 72 F4 1B CE A6 44 00 00 00 8B  data¯nrô.Î¦D....
006EF110  75 6E 6D 61 73 6B 65 64 5F 63 72 65 64 69 74 5F  unmasked_credit_
006EF120  63 61 72 64 73 00 00 00 1F CE A6 44 00 00 00 89  cards....Î¦D....
006EF130  73 65 72 76 65 72 5F 61 64 64 72 65 73 73 5F 6D  server_address_m
006EF140  65 74 61 64 61 74 61 46 13 CE A6 44 00 00 00 8B  etadataF.Î¦D....
006EF150  75 6E 6D 61 73 6B 65 64 5F 63 72 65 64 69 74 5F  unmasked_credit_
006EF160  63 61 72 64 73 00 00 00 17 CE A6 44 00 00 00 8A  cards....Î¦D....
006EF170  61 75 74 6F 66 69 6C 6C 5F 70 72 6F 66 69 6C 65  autofill_profile
```

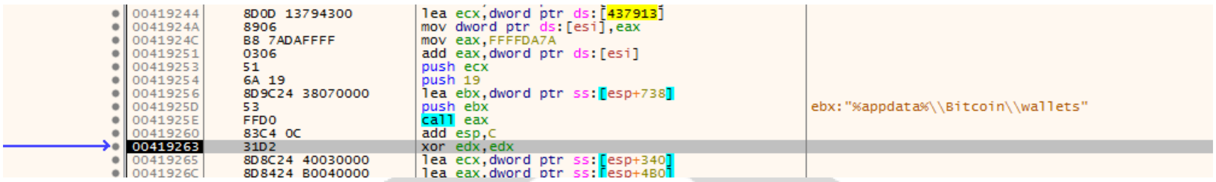
The email address that Google Chrome keeps after logging in:



```
0040FF0E  89DA                 mov edx,ebx
0040FF10  F2:0F118C24 B0000000 movsd qword ptr ss:[esp+B0],xmm1
0040FF19  F2:0F118424 A8000000 movsd qword ptr ss:[esp+A8],xmm0
0040FF22  E8 6F4A0000          call 7gfdg5egds.414996
0040FF27  8B8424 F0010000      mov eax,dword ptr ss:[esp+1F0]   [esp+1F0]:"jigiw47411@dmsdmg.com_1"
0040FF2E  85C0                 test eax,eax                     eax:"jigiw47411@dmsdmg.com_1"
0040FF30  74 60                je 7gfdg5egds.40FF92
0040FF32  8B4C24 40            mov ecx,dword ptr ss:[esp+40]    ecx:&"jigiw47411@dmsdmg.com_1"
0040FF36  85C9                 test ecx,ecx
0040FF38  74 58                je 7gfdg5egds.40FF92             [esp+AC]:"jigiw47411@dmsdmg.com_1"
0040FF3A  898C24 AC000000      mov dword ptr ss:[esp+AC],ecx
0040FF41  8B4C24 48            mov ecx,dword ptr ss:[esp+48]
0040FF45  8B9424 F8010000      mov edx,dword ptr ss:[esp+1F8]
0040FF4C  898C24 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 7gfdg5egds.exe:$FF27 #F327
```

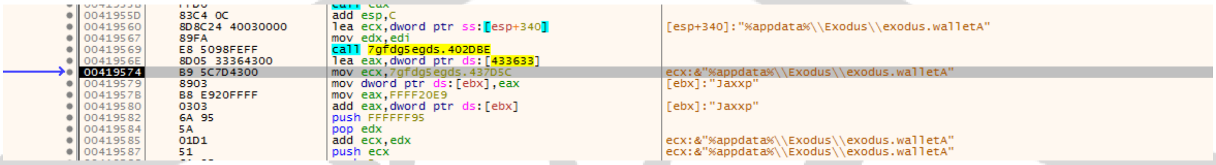
```
dres     Hex                                              ASCII
06EEE30  6A 69 67 69 77 34 37 34 31 31 40 64 6D 73 64 6D  jigiw47411@dmsdm
06EEE40  67 2E 63 6F 6D 5F 31 00 F3 CD A6 44 00 00 00 88  g.com_1.óÍ¦D....
06EEE50  30 14 71 00 FF FF FF FF 00 00 00 00 00 00 00 00  0.q.ÿÿÿÿ........
06EEE60  00 00 00 00 00 00 00 00 F7 CD A6 44 00 00 00 8E  ........÷Í¦D....
06EEE70  65 00 70 00 6D 00 61 00 70 00 70 00 65 00 72 00  e.p.m.a.p.p.e.r.
06EEE80  00 00 00 00 00 00 00 00 EB CD A6 44 00 00 00 8E  ........ëÍ¦D....
06EEE90  65 00 70 00 6D 00 61 00 70 00 70 00 65 00 72 00  e.p.m.a.p.p.e.r.
06EEEA0  00 00 00 00 00 00 00 00 EF CD A6 44 00 00 00 8A  ........ïÍ¦D....
06EEEB0  70 61 79 6D 65 6E 74 73 5F 63 75 73 74 6F 6D 65  payments_custome
06EEEC0  72 5F 64 61 74 61 00 00 E3 CD A6 44 00 00 00 8C  r_data..ãÍ¦D....
06EEED0  05 00 00 00 A7 00 00 00 00 00 00 00 60 01 00 00  ....§.......`...
```

Bitcoin wallet:



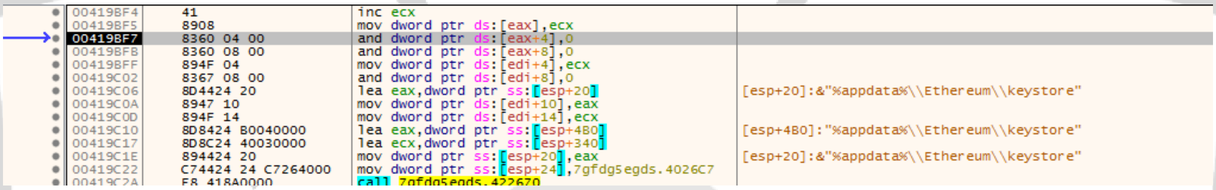
```
00419244  8D0D 13794300      lea ecx,dword ptr ds:[437913]
0041924A  8906               mov dword ptr ds:[esi],eax
0041924C  B8 7ADAFFFF        mov eax,FFFFDA7A
00419251  0306               add eax,dword ptr ds:[esi]
00419253  51                 push ecx
00419254  6A 19              push 19
00419256  8D9C24 38070000    lea ebx,dword ptr ss:[esp+738]
0041925D  53                 push ebx                            ebx:"%appdata%\\Bitcoin\\wallets"
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+4B0]
```

Exodus wallet:



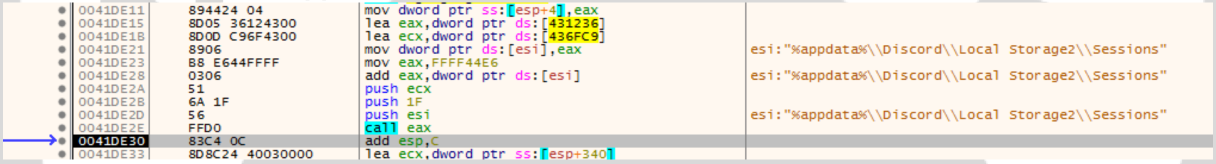
```
0041955D  83C4 0C            add esp,C
00419560  8D8C24 40030000    lea ecx,dword ptr ss:[esp+340]      [esp+340]:"%appdata%\\Exodus\\exodus.walletA"
00419567  89FA               mov edx,edi
00419569  E8 5098FEFF        call 7gfdg5egds.402DBE
0041956E  8D05 33364300      lea eax,dword ptr ds:[433633]
00419574  B9 5C7D4300        mov ecx,7gfdg5egds.437D5C           ecx:&"%appdata%\\Exodus\\exodus.walletA"
00419579  8903               mov dword ptr ds:[ebx],eax          [ebx]:"Jaxxp"
0041957B  B8 E920FFFF        mov eax,FFFF20E9
00419580  0303               add eax,dword ptr ds:[ebx]          [ebx]:"Jaxxp"
00419582  6A 95              push FFFFFF95
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:



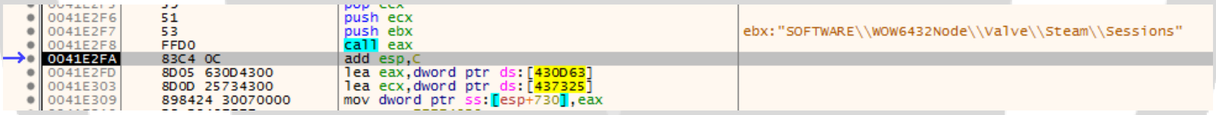
```
00419BF4  41                 inc ecx
00419BF5  8908               mov dword ptr ds:[eax],ecx
00419BF7  8360 04 00         and dword ptr ds:[eax+4],0
00419BFB  8360 08 00         and dword ptr ds:[eax+8],0
00419BFF  894F 04            mov dword ptr ds:[edi+4],ecx
00419C02  8367 08 00         and dword 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 B0040000    lea eax,dword ptr ss:[esp+4B0]      [esp+4B0]:"%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],7gfdg5egds.4026C7
00419C2A  E8 418A0000        call 7gfdg5egds.422670
```

Data from the Discord app:



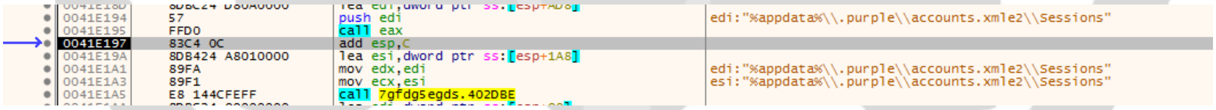
```
0041DE11  894424 04          mov dword ptr ss:[esp+4],eax
0041DE15  8D05 36124300      lea eax,dword ptr ds:[431236]
0041DE1B  8D0D C96F4300      lea ecx,dword ptr ds:[436FC9]
0041DE21  8906               mov dword ptr ds:[esi],eax          esi:"%appdata%\\Discord\\Local Storage2\\Sessions"
0041DE23  B8 E644FFFF        mov eax,FFFF44E6
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                            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:



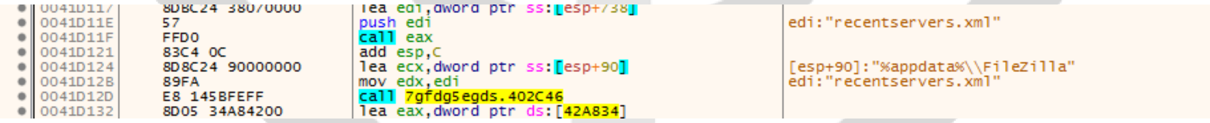
```
0041E2F6  51                 push ecx
0041E2F7  53                 push ebx                            ebx:"SOFTWARE\\WOW6432Node\\Valve\\Steam\\Sessions"
0041E2F8  FFD0               call eax
0041E2FA  83C4 0C            add esp,C
0041E2FD  8D05 630D4300      lea eax,dword ptr ds:[430D63]
0041E303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

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



```
0041E194  57                 push edi                            edi:"%appdata%\\.purple\\accounts.xmle2\\Sessions"
0041E195  FFD0               call eax
0041E197  83C4 0C            add esp,C
0041E19A  8DB424 A8010000    lea esi,dword ptr ss:[esp+1A8]
0041E1A1  89FA               mov edx,edi                         edi:"%appdata%\\.purple\\accounts.xmle2\\Sessions"
0041E1A3  89F1               mov ecx,esi                         esi:"%appdata%\\.purple\\accounts.xmle2\\Sessions"
0041E1A5  E8 144CFEFF        call 7gfdg5egds.402DBE
```

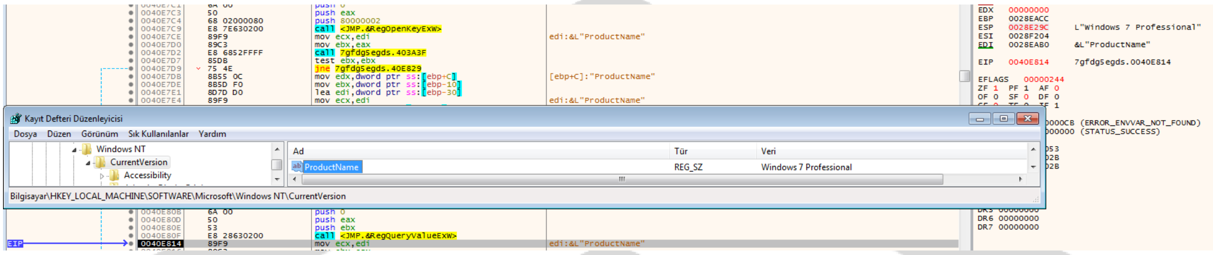
FileZilla:



```
0041D117  8DBC24 38070000    lea edi,dword ptr ss:[esp+738]
0041D11E  57                 push edi                            edi:"recentservers.xml"
0041D11F  FFD0               call eax
0041D121  83C4 0C            add esp,C
0041D124  8D8C24 90000000    lea ecx,dword ptr ss:[esp+90]       [esp+90]:"%appdata%\\FileZilla"
0041D12B  89FA               mov edx,edi                         edi:"recentservers.xml"
0041D12D  E8 145BFEFF        call 7gfdg5egds.402C46
0041D132  8D05 34A84200      lea eax,dword ptr ds:[42A834]
```

Here, the system information received by the malware is displayed.

OS:



```
0040E7C3   50                push eax
0040E7C4   68 02000080       push 80000002
0040E7C9   E8 7E630200       call <JMP.&RegOpenKeyExW>
0040E7CE   89F9              mov ecx,edi                         edi:&L"ProductName"
0040E7D0   89C3              mov ebx,eax
0040E7D2   E8 6852FFFF       call 7gfdg5egds.403A3F
0040E7D7   85DB              test ebx,ebx
0040E7D9   75 4E             jne 7gfdg5egds.40E829
0040E7DB   8B55 0C           mov edx,dword ptr ss:[ebp+C]        [ebp+C]:"ProductName"
0040E7DE   8B5D F0           mov ebx,dword ptr ss:[ebp-10]
0040E7E1   8D7D D0           lea edi,dword ptr ss:[ebp-30]
0040E7E4   89F9              mov ecx,edi                         edi:&L"ProductName"
...
0040E80B   6A 00             push 0
0040E80D   50                push eax
0040E80E   53                push ebx
0040E80F   E8 28630200       call <JMP.&RegQueryValueExW>
0040E814   89F9              mov ecx,edi                         edi:&L"ProductName"
```

```
EDX   00000000
EBP   0028EACC
ESP   0028E29C     L"Windows 7 Professional"
ESI   0028F204
EDI   0028EAB0     &L"ProductName"

EIP   0040E814     7gfdg5egds.0040E814

EFLAGS   00000244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0

0000CB (ERROR_ENVVAR_NOT_FOUND)
000000 (STATUS_SUCCESS)

DR6 00000000
DR7 00000000
```

Kayıt Defteri Düzenleyicisi

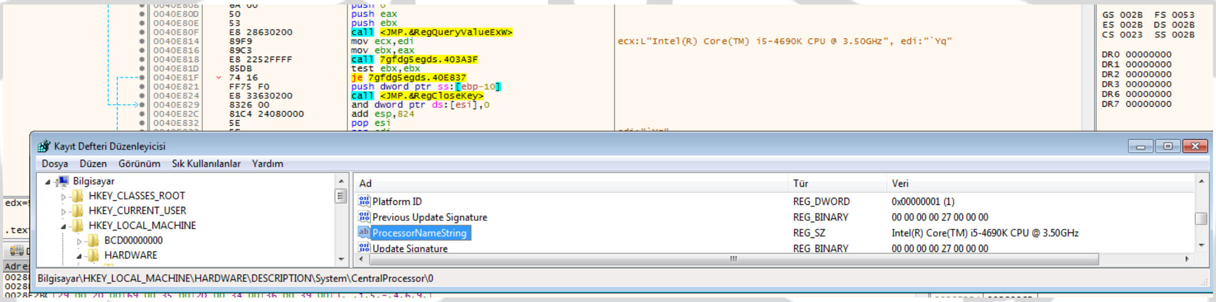
Dosya Düzen Görünüm Sık Kullanılanlar Yardım

Windows NT > CurrentVersion > Accessibility

Ad	Tür	Veri
ProductName	REG_SZ	Windows 7 Professional

Bilgisayar\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Processor:



```
0040E80D   50                push eax
0040E80E   53                push ebx
0040E80F   E8 28630200       call <JMP.&RegQueryValueExW>
0040E814   89F9              mov ecx,edi              ecx:L"Intel(R) Core(TM) i5-4690K CPU @ 3.50GHz", edi:"`Yq"
0040E816   89C3              mov ebx,eax
0040E818   E8 2252FFFF       call 7gfdg5egds.403A3F
0040E81D   85DB              test ebx,ebx
0040E81F   74 16             je 7gfdg5egds.40E837
0040E821   FF75 F0           push dword ptr ss:[ebp-10]
0040E824   E8 33630200       call <JMP.&RegCloseKey>
0040E829   8326 00           and dword ptr ds:[esi],0
0040E82C   81C4 24080000     add esp,824
0040E832   5E                pop esi
```

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

DR0 00000000
DR1 00000000
DR2 00000000
DR3 00000000
DR6 00000000
DR7 00000000
```

Kayıt Defteri Düzenleyicisi

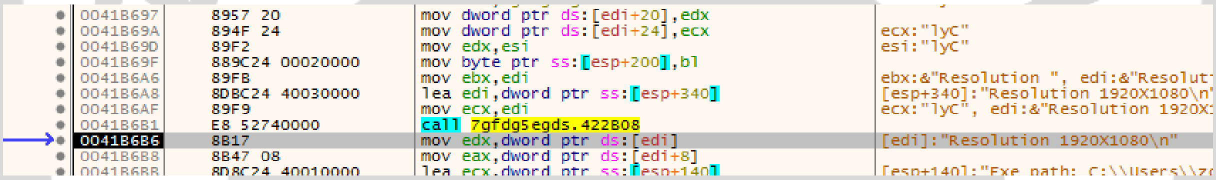
Dosya Düzen Görünüm Sık Kullanılanlar Yardım

Bilgisayar
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
  - BCD00000000
  - HARDWARE

Ad	Tür	Veri
Platform ID	REG_DWORD	0x00000001 (1)
Previous Update Signature	REG_BINARY	00 00 00 00 27 00 00 00
ProcessorNameString	REG_SZ	Intel(R) Core(TM) i5-4690K CPU @ 3.50GHz
Update Signature	REG_BINARY	00 00 00 00 27 00 00 00

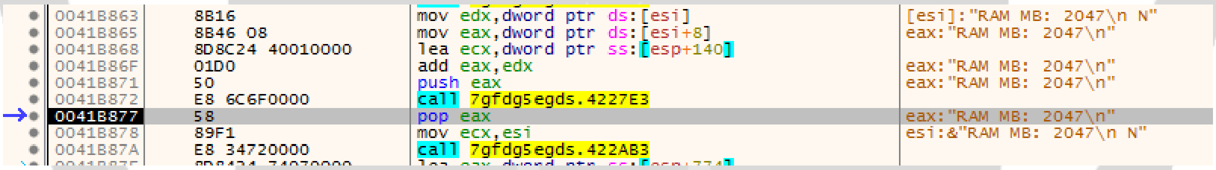
Bilgisayar\HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0

Resolution:



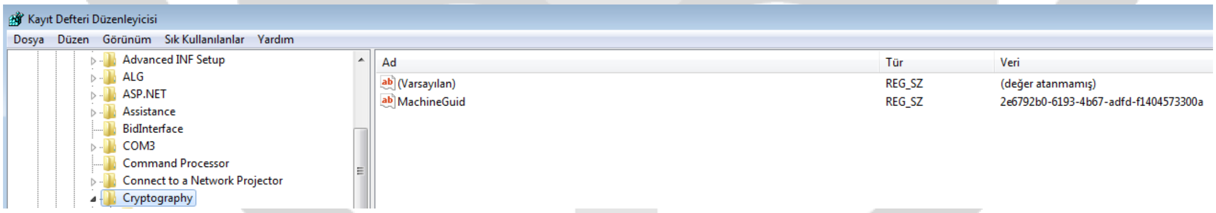
```
0041B697   8957 20           mov dword ptr ds:[edi+20],edx
0041B69A   894F 24           mov dword ptr ds:[edi+24],ecx     ecx:"lyC"
0041B69D   89F2              mov edx,esi                       esi:"lyC"
0041B69F   889C24 00020000   mov byte ptr ss:[esp+200],bl
0041B6A6   89FB              mov ebx,edi                       ebx:&"Resolution ", edi:&"Resolut
0041B6A8   8DBC24 40030000   lea edi,dword ptr ss:[esp+340]    [esp+340]:"Resolution 1920X1080\n"
0041B6AF   89F9              mov ecx,edi                       ecx:"lyC", edi:&"Resolution 1920X
0041B6B1   E8 52740000       call 7gfdg5egds.422B08
0041B6B6   8B17              mov edx,dword ptr ds:[edi]        [edi]:"Resolution 1920X1080\n"
0041B6B8   8B47 08           mov eax,dword ptr ds:[edi+8]
0041B6BB   8D8C24 40010000   lea ecx,dword ptr ss:[esp+140]    [esp+140]:"Exe path: C:\\Users\\z
```

Ram:



```
0041B863   8B16              mov edx,dword ptr ds:[esi]        [esi]:"RAM MB: 2047\n N"
0041B865   8B46 08           mov eax,dword ptr ds:[esi+8]      eax:"RAM MB: 2047\n"
0041B868   8D8C24 40010000   lea ecx,dword ptr ss:[esp+140]
0041B86F   01D0              add eax,edx                       eax:"RAM MB: 2047\n"
0041B871   50                push eax                          eax:"RAM MB: 2047\n"
0041B872   E8 6C6F0000       call 7gfdg5egds.4227E3
0041B877   58                pop eax                           eax:"RAM MB: 2047\n"
0041B878   89F1              mov ecx,esi                       esi:&"RAM MB: 2047\n N"
0041B87A   E8 34720000       call 7gfdg5egds.422AB3
```

Machine-Guid:

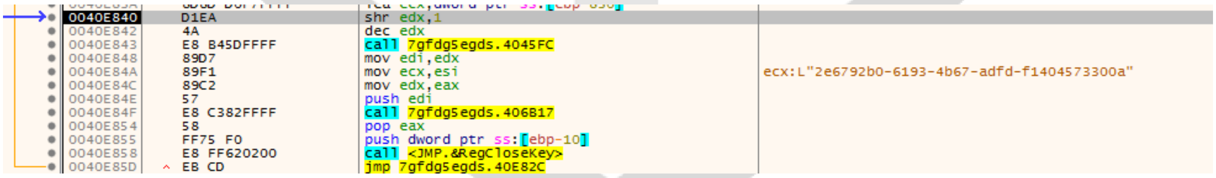


Kayıt Defteri Düzenleyicisi

Dosya Düzen Görünüm Sık Kullanılanlar Yardım

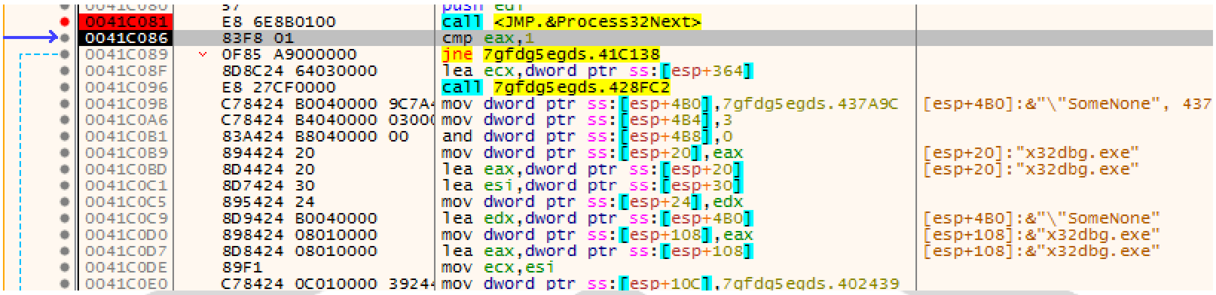
- Advanced INF Setup
- ALG
- ASP.NET
- Assistance
- BidInterface
- COM3
- Command Processor
- Connect to a Network Projector
- Cryptography

Ad	Tür	Veri
(Varsayılan)	REG_SZ	(değer atanmamış)
MachineGuid	REG_SZ	2e6792b0-6193-4b67-adfd-f1404573300a



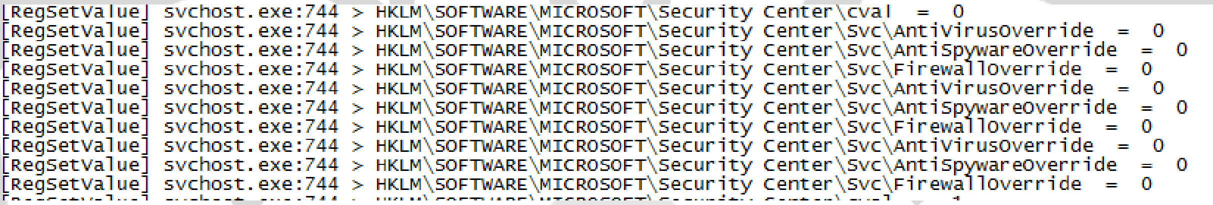
```
0040E840   D1EA              shr edx,1
0040E842   4A                dec edx
0040E843   E8 B45DFFFF       call 7gfdg5egds.4045FC
0040E848   89D7              mov edi,edx
0040E84A   89F1              mov ecx,esi                ecx:L"2e6792b0-6193-4b67-adfd-f1404573300a"
0040E84C   89C2              mov edx,eax
0040E84E   57                push edi
0040E84F   E8 C382FFFF       call 7gfdg5egds.406B17
0040E854   58                pop eax
0040E855   FF75 F0           push dword ptr ss:[ebp-10]
0040E858   E8 FF620200       call <JMP.&RegCloseKey>
0040E85D   EB CD             jmp 7gfdg5egds.40E82C
```

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



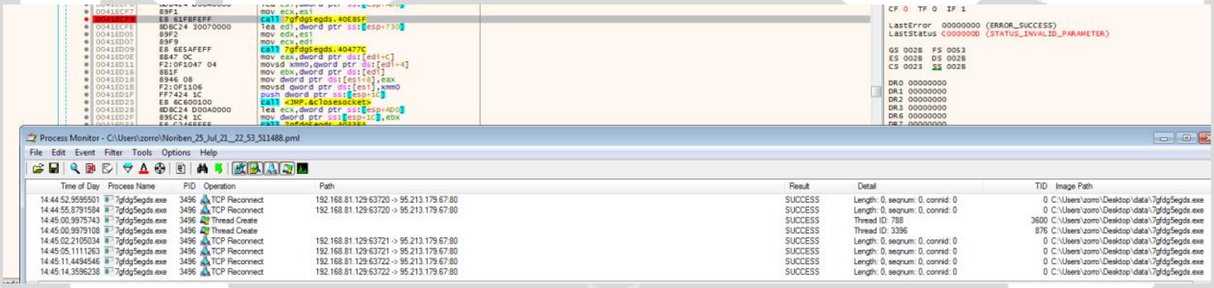
```
0041C080  57                    push edi
0041C081  E8 6E8B0100           call <JMP.&Process32Next>
0041C086  83F8 01               cmp eax,1
0041C089  0F85 A9000000         jne 7gfdg5egds.41C138
0041C08F  8D8C24 64030000       lea ecx,dword ptr ss:[esp+364]
0041C096  E8 27CF0000           call 7gfdg5egds.428FC2
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 3924  mov dword ptr ss:[esp+10C],7gfdg5egds.402439
```

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



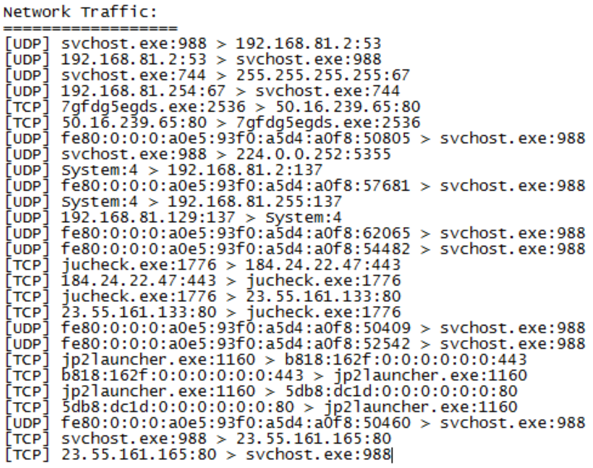
```
0041ECF7  89F1                 mov ecx,esi
0041ECF9  E8 61FBFEFF          call 7gfdg5egds.40E85F
0041ECFE  8D8C24 30070000      lea edi,dword ptr ss:[esp+730]
0041ED05  89F2                 mov edx,esi
0041ED07  89F9                 mov ecx,edi
0041ED09  E8 6E5AFEFF          call 7gfdg5egds.40477C
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  8D8C24 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
```

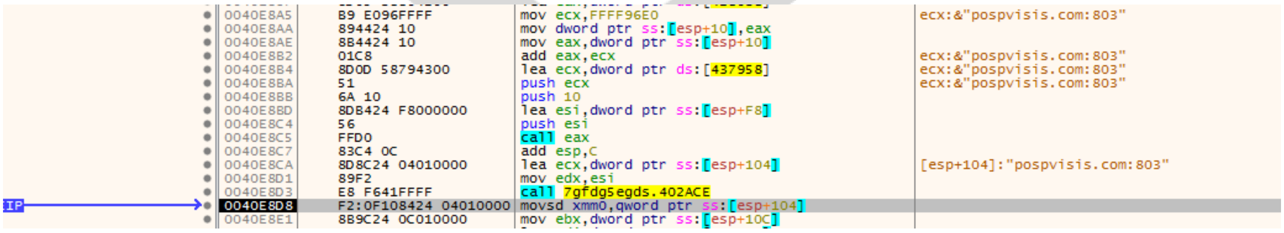
Process Monitor - C:\Users\zorro\Noriben_25_Jul_21__22_53_511488.pml

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

It has been seen that the malware tries to connect to the address 95[.]213[.]179[.]67[:]80 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] fe80:0:0:0: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]
```

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/