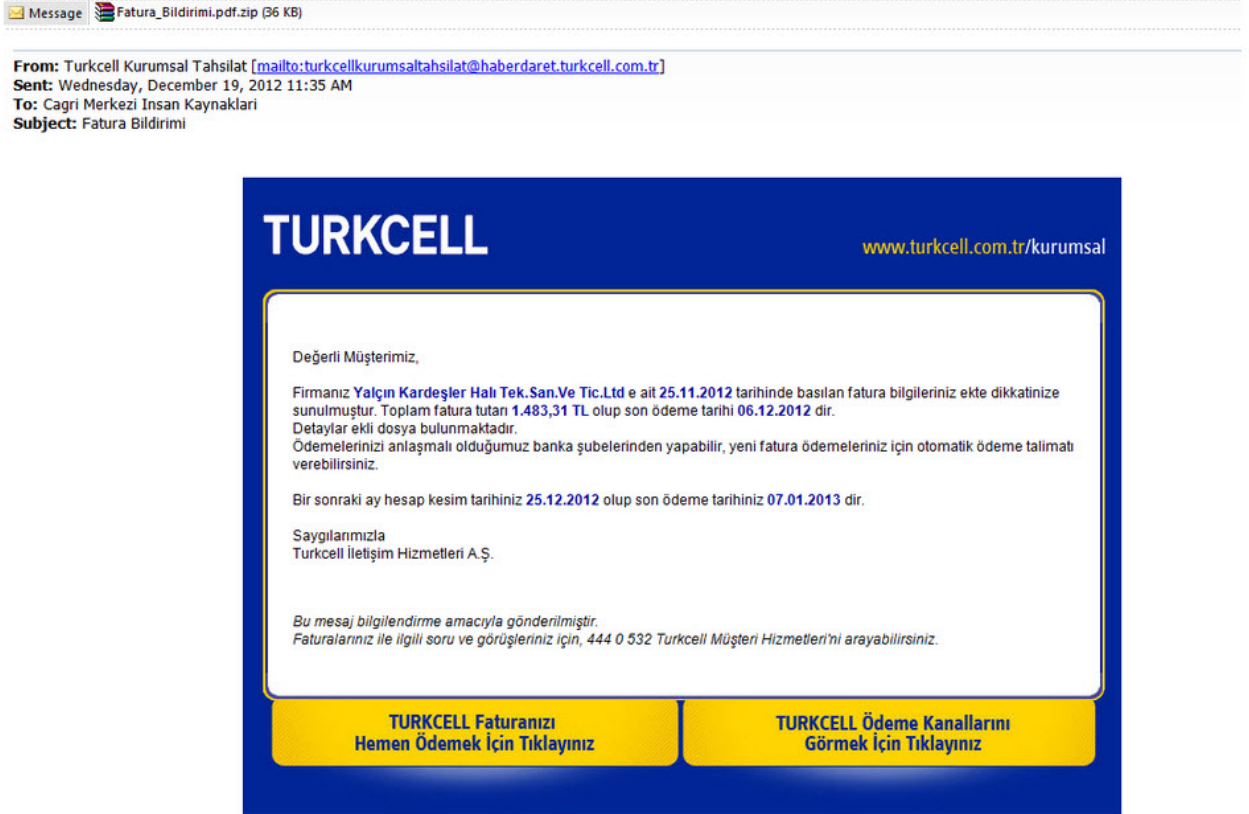


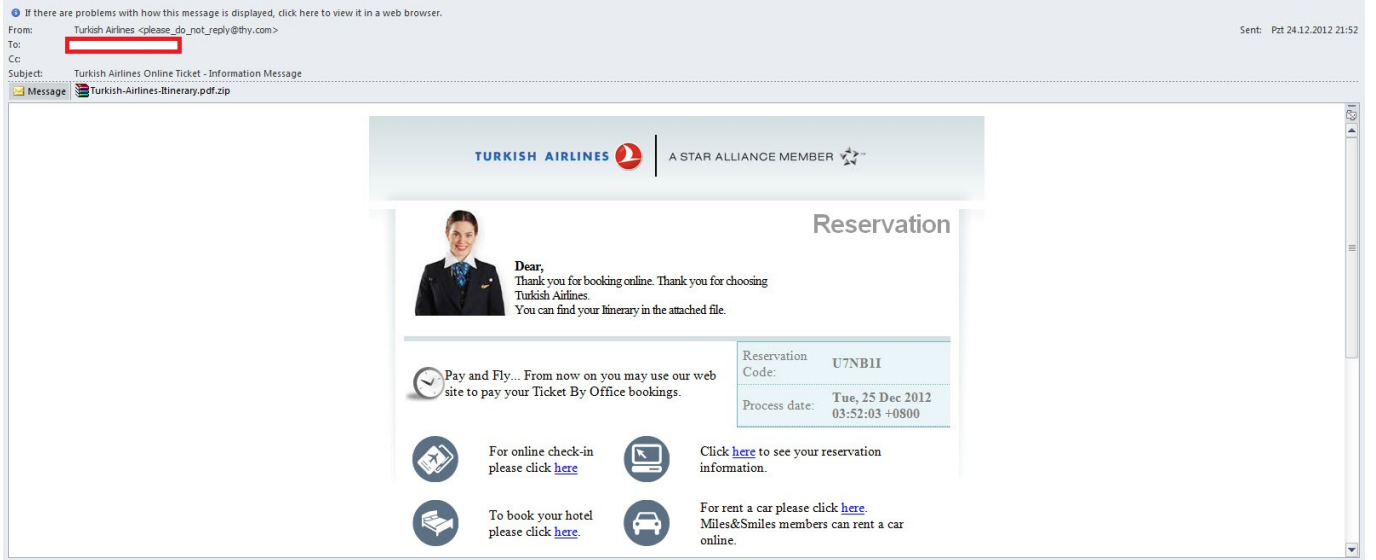
Şeytan Ayrıntıda Gizlidir

written by Mert SARICA | 1 January 2013

19 Aralık 2012 tarihinde birçok banka müşterilerinden gelen ihbarları değerlendirmek ile güne başladı. Aynı anda sosyal medyada ve NetSec bilişim güvenliği e-posta listesinde Turkcell ve Vodafone'dan gönderildiği ve ekinde zararlı yazılım bulunduğu öne sürülen e-postalar yer almaya başladı.



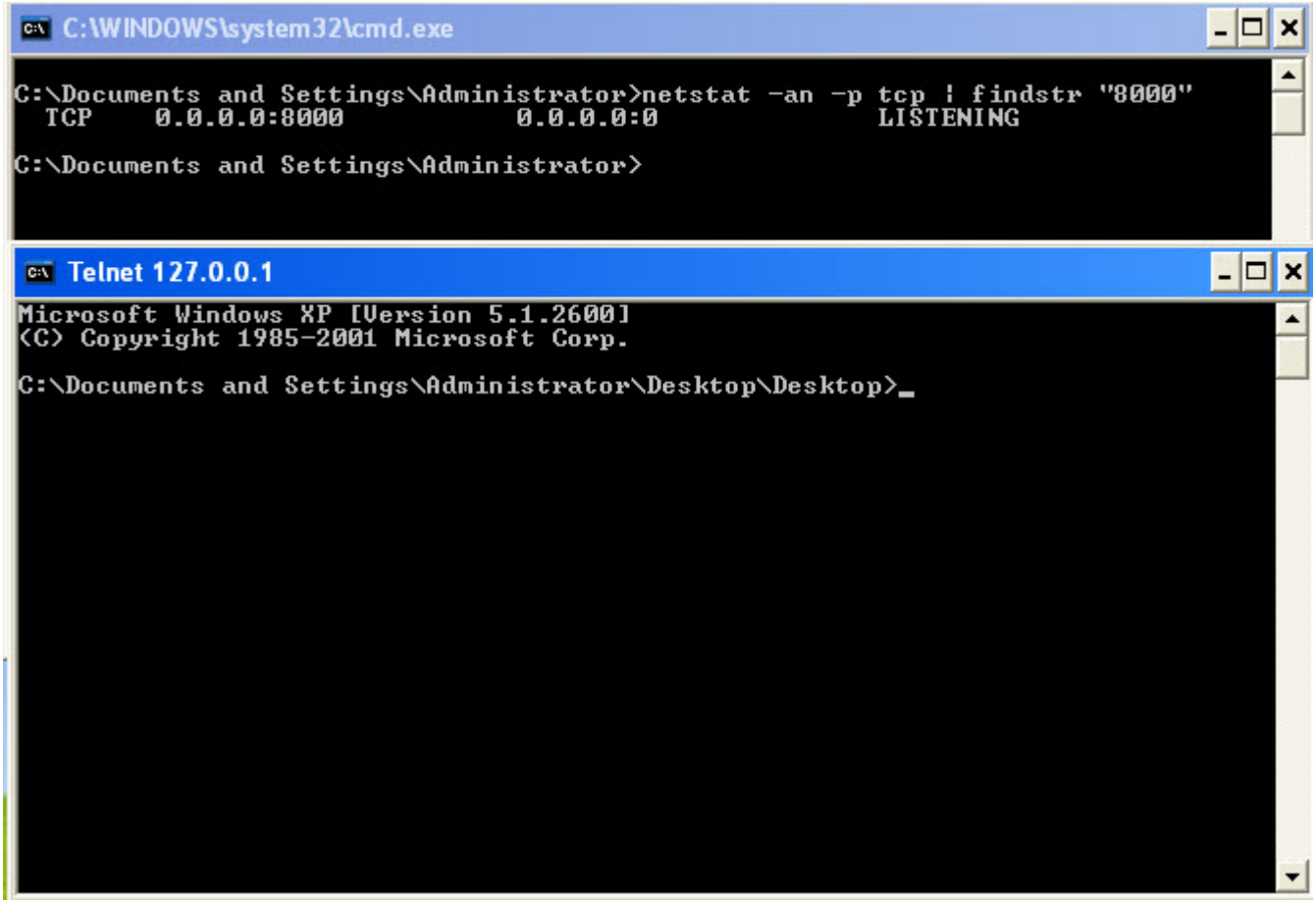
24 Aralık 2012 tarihinde ise bu defa THY'den gönderildiği ve ekinde zararlı yazılım bulunduğu öne sürülen e-postalar gündemi meşgul etmeye başladı.



E-postaların başlık bilgileri incelendiğinde e-postaların Turkcell ve THY'den gönderiliyormuş gibi gösterilmeye çalışıldığı anlaşılmıyordu. Fakat dikkatlice bakıldığında son adımda e-postanın Tayvan'da ki bir sunucudan alınmış olduğu bu nedenle başlık bilgilerinin manipüle edildiği açıkça anlaşılmıyordu.

```
Received: from mail.gff.com.tw (60.250.9.34) by [redacted]
[redacted] with Microsoft SMTP Server id 14.1.355.2; Mon, 24 Dec 2012
21:52:04 +0200
Received: from ISTEXCEDGE1.thynet.thy.com ([212.175.83.159]) by
ip226.226.onofis.com (Icewarp 9.3.1) with ESMTP (SSL) id 6QR95678 for
[redacted] Tue, 25 Dec 2012 03:52:03 +0800
Received: from javabatchp3 (192.168.254.165) by ISTEXCEDGE1.thynet.thy.com
(10.11.91.138) with Microsoft SMTP Server id 14.1.218.12; Tue, 25 Dec 2012
03:52:03 +0800
Message-ID: <16728329.8371489790626.JavaMail.otbatch@javabatchp3>
From: Turkish Airlines <please_do_not_reply@thy.com>
To: [redacted]
Subject: Turkish Airlines Online Ticket - Information Message
Date: Tue, 25 Dec 2012 03:52:03 +0800
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="-----a_cazmn_87_11_29"
Return-Path: artistes@thy.com
X-MS-Exchange-Organization-AuthSource: [redacted]
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Organization-SCL: 0
X-MS-Exchange-Organization-PCL: 2
X-MS-Exchange-Organization-Antispam-Report: DV:3.3.5705.600;OrigIP:60.250.9.34
```

Ardından bazı web sitelerinde ve NetSec bilişim güvenliği e-posta listesinde zararlı yazılım üzerinde yapılan kısa analizlere yer verildi ve bu analizlerde zararlı yazılımın trojan olmadığı, çalıştırıldıktan sonra 8000 numaralı bağlantı noktasında (port) dinlemeye geçtiği ve bu bağlantı noktasından sisteme bağlanan kişilere komut satırı erişimi (shell) verildiği belirtiliyordu.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -an -p tcp | findstr "8000"
TCP      0.0.0.0:8000      0.0.0.0:0        LISTENING
C:\Documents and Settings\Administrator>

C:\ Telnet 127.0.0.1
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator\Desktop\Desktop>_
```

Emek ve zaman harcandığı açıkça belli olan profesyonelce hazırlanmış iki farklı sahte e-posta ve sadece çalıştırıldığı sistemde 8000 numaralı bağlantı noktasında komut satırı erişimi veren zararlı bir yazılım ? Muhtemelen okurken size de inandırıcı gelmeyen bu senaryo bana da hiç inandırıcı gelmediği için sahte THY e-postasında yer alan zararlı yazılıma kısaca göz atmaya karar verdim. Özellikle yazılım seviyesine inilmeden sistem seviyesinde yapılan analizler, zararlı yazılımın sanal makine, debugger, sandbox tespitine yönelik kontroller içermesi durumunda farklı sonuçlar ortaya çıkarabilmektedir bu nedenle yazılım seviyesine inilmeden yapılan bir analiz sonucuna göre bir karara varmak çok doğru değildir. Yazılım seviyesine inilse dahi kimi zaman yanıltma payı olabilmektedir.

Immunity Debugger aracı ile zararlı yazılımı analiz etmeye başladığımda ilk dikkatimi çeken Immunity Debugger tarafından karşıma çıkan şüpheli uyarı mesajları oldu.

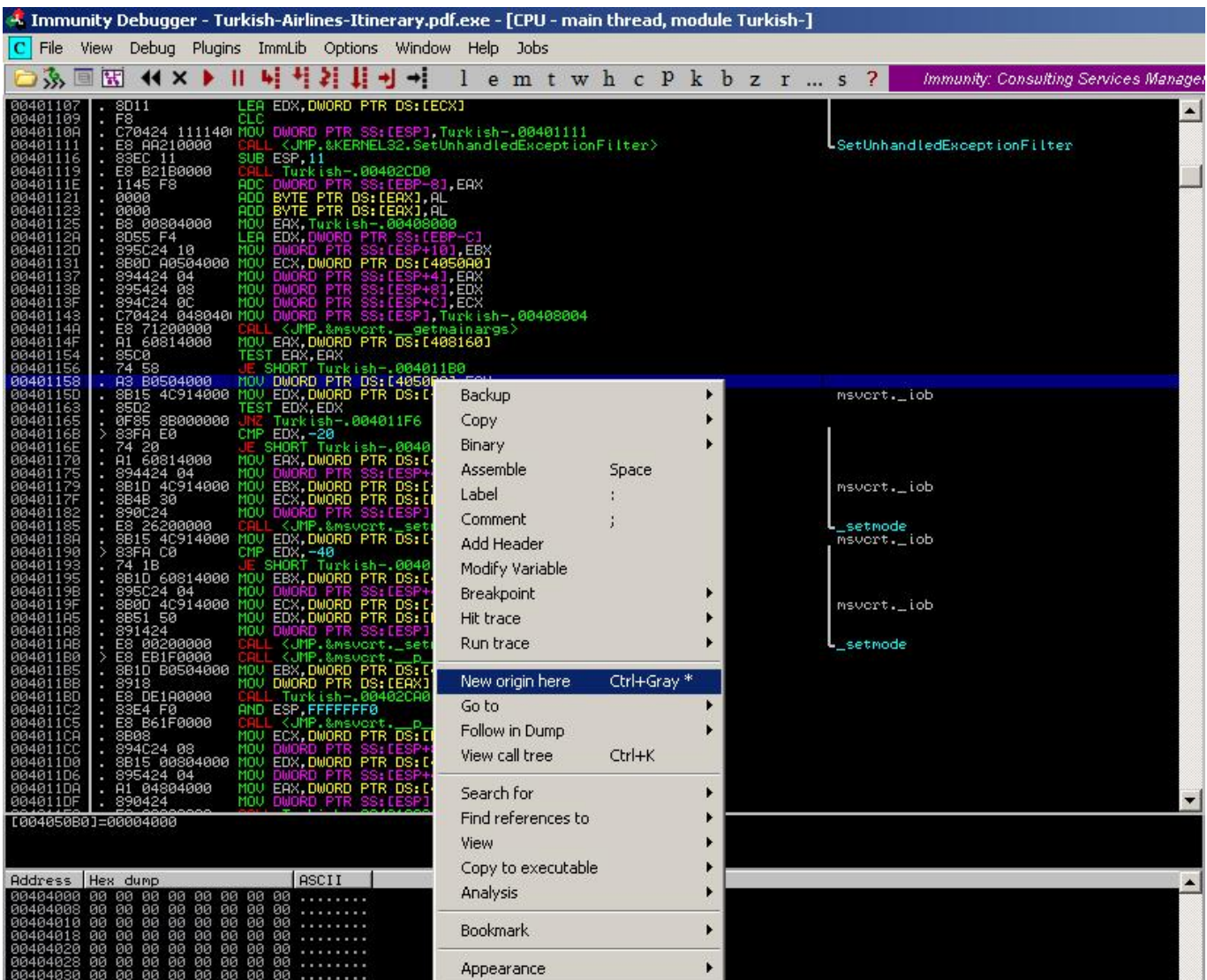


Ardından bir Anti Debugging tekniği olan ve zararlı yazılımlarda sıkça karşılaşılan SetUnhandledExceptionFilter dikkatimi çekti. Normalde bir yazılım çalışma esnasında ortaya çıkabilecek potansiyel hataları, istisnai durumları tespit eder ve ona göre aksiyon alır ancak öngörülemeyen hatalar için bir yazılımcı SetUnhandledExceptionFilter filtresi ile öngörülemeyen hataların da tespit edilmesini ve buna göre aksiyon almasını sağlayabilir. Hata ayıklayıcı (debugger) ile çalıştırılan bir yazılımda ise debugger yazılımın çalışması esnasında ortaya çıkan hataları, istisnai durumları kendisi yönetmeye çalışır. Bunu bilen zararlı yazılım geliştiricileri de bu filtreden faydalanarak sayısal hatalara yol açacak bir kod parçası çalıştırır ve bu hatayı bu filtrenin ayıklamasını ve yazılımın akışına devam etmesini sağlar. Ancak bunu bilmeyen bir hata ayıklayıcı böyle bir hata ile karşılaştığında yazılımın akışını devam ettiremez ve yazılım çökmüş olur kısaca SetUnhandledExceptionFilter ile debuggerlar bu şekilde devre dışı bırakılmaya çalışılır.

```
Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c p k b z r ... s ? Immunity: Consulting Services Manage

00401100 55 PUSH EBP
00401101 89E5 MOV EBP,ESP
00401103 53 PUSH EBX
00401104 83EC 24 SUB ESP,24
00401107 8D11 LEA EDI,DWORD PTR DS:[ECX]
00401109 F5 SC
0040110A C70424 111140 MOV DWORD PTR SS:[ESP],Turkish-.00401111
00401111 E9 A2100000 CALL <JMP.&KERNEL32.SetUnhandledExceptionFilter> SetUnhandledExceptionFilter
00401116 83EC 11 SUB ESP,11
00401119 E8 B2100000 CALL Turkish-.00402C00
0040111E 1145 F8 ADC DWORD PTR SS:[EBP-8],EAX
00401121 0000 ADD BYTE PTR DS:[EAX],AL
00401123 0000 ADD BYTE PTR DS:[EAX],AL
00401125 B8 00804000 MOV EAX,Turkish-.00408000
0040112A 8D55 F4 LEA EDI,DWORD PTR SS:[EBP-C],EAX
0040112D 895C24 10 MOV DWORD PTR SS:[ESP+10],EBX
00401131 8B00 A0504000 MOV ECX,DWORD PTR DS:[4050A0]
00401137 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
0040113B 895424 08 MOV DWORD PTR SS:[ESP+8],EDX
0040113F 894C24 0C MOV DWORD PTR SS:[ESP+C],ECX
00401143 C70424 040040 MOV DWORD PTR SS:[ESP],Turkish-.00408004
0040114A E9 71200000 CALL <JMP.&msvrt._getmainargs>
0040114F A1 60814000 MOV EAX,DWORD PTR DS:[408160]
00401154 85C0 TEST EAX,EAX
00401156 74 58 JF SHORT Turkish-.004011B0
00401158 A3 B0504000 MOV DWORD PTR DS:[4050B0],EAX
0040115D 8B15 4C914000 MOV EDI,DWORD PTR DS:[&msvrt._iob] msvrt._iob
00401163 8502 TEST EDI,EDI
00401165 0F85 8B000000 JNZ Turkish-.004011F6
0040116B > 83FA E0 CMP EDI,-20
0040116E 74 20 JF SHORT Turkish-.004011B0
00401170 A1 60814000 MOV EAX,DWORD PTR DS:[408160]
00401175 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
00401179 8B1D 4C914000 MOV EDI,DWORD PTR DS:[&msvrt._iob] msvrt._iob
0040117F 8B4B 30 MOV ECX,DWORD PTR DS:[EBX+30]
00401182 890C24 00 MOV DWORD PTR SS:[ESP],ECX
00401185 E8 26200000 CALL <JMP.&msvrt._setmode> _setmode
0040118A 8B15 4C914000 MOV EDI,DWORD PTR DS:[&msvrt._iob] msvrt._iob
00401190 > 83FA C0 CMP EDI,-40
00401193 74 18 JF SHORT Turkish-.004011B0
00401195 8B1D 60814000 MOV EDI,DWORD PTR DS:[408160]
00401198 895C24 04 MOV DWORD PTR SS:[ESP+4],EBX
0040119F 8B0D 4C914000 MOV ECX,DWORD PTR DS:[&msvrt._iob] msvrt._iob
004011A5 8B51 50 MOV EDI,DWORD PTR DS:[ECX+50]
004011A8 891424 00 MOV DWORD PTR SS:[ESP],EDI
004011AB E8 00200000 CALL <JMP.&msvrt._setmode> _setmode
004011B0 > E8 EB1F0000 CALL <JMP.&msvrt._p__fmode>
004011B5 8B1D B0504000 MOV EDI,DWORD PTR DS:[4050B0]
004011B8 8918 MOV DWORD PTR DS:[EAX],EBX
004011BD E8 DE1A0000 CALL Turkish-.00402CA0
004011C2 83E4 F0 AND ESP,FFFFFFF0
004011C5 E8 B61F0000 CALL <JMP.&msvrt._p__environ>
004011CA 8B08 MOV ECX,DWORD PTR DS:[EAX]
004011CC 894C24 08 MOV DWORD PTR SS:[ESP+8],ECX
004011D0 894C24 08 MOV DWORD PTR SS:[ESP+8],ECX
EBP=0045FFB0
Local calls/jumps from 004010F1, 00401253
```

Bu adımları geçtikten ve zararlı yazılımın paketlenmiş (packed) bölümlerini açtığını farkettim



Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]

File View Debug Plugins ImmLib Options Window Help Jobs

Code auditor and software assessment

```
0040116B > 83FA E0 CMP EDX,-20
0040116E . 74 20 JE SHORT Turkish-.00401190
00401170 . A1 60814000 MOV EAX,DWORD PTR DS:[408160]
00401175 . 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
00401179 . 8B1D 4C914000 MOV EBX,DWORD PTR DS:[<msvrt._iob>]
0040117F . 8B4B 30 MOV ECX,DWORD PTR DS:[EBX+30]
00401182 . 890C24 MOV DWORD PTR SS:[ESP],ECX
00401185 . E8 26200000 CALL <JMP.&msvrt._setmode>
0040118A . 8B15 4C914000 MOV EDI,DWORD PTR DS:[<msvrt._iob>]
00401190 > 83FA C0 CMP EDI,-40
00401193 . 74 1B JE SHORT Turkish-.004011B0
00401195 . 8B1D 60814000 MOV EBX,DWORD PTR DS:[408160]
0040119B . 895C24 04 MOV DWORD PTR SS:[ESP+4],EBX
0040119F . 8B0D 4C914000 MOV ECX,DWORD PTR DS:[<msvrt._iob>]
004011A5 . 8B51 50 MOV EDI,DWORD PTR DS:[ECX+50]
004011A8 . 891424 MOV DWORD PTR SS:[ESP],EDI
004011AB . E8 00200000 CALL <JMP.&msvrt._setmode>
004011B0 > EB1F0000 CALL <JMP.&msvrt._p_fmode>
004011B5 . 8B1D B0504000 MOV EBX,DWORD PTR DS:[405080]
004011B8 . 8918 MOV DWORD PTR DS:[EAX],EBX
004011BD . E8 DE1A0000 CALL Turkish-.00402CA0
004011C2 . 83E4 F0 AND ESP,FFFFFFF0
004011C5 . E8 B61F0000 CALL <JMP.&msvrt._p_environ>
004011CA . 8B08 MOV ECX,DWORD PTR DS:[EAX]
004011CC . 894C24 08 MOV DWORD PTR SS:[ESP+8],ECX
004011D0 . 8B15 00804000 MOV EDI,DWORD PTR DS:[408000]
004011D6 . 895424 04 MOV DWORD PTR SS:[ESP+4],EDI
004011DA . A1 04804000 MOV EAX,DWORD PTR DS:[408004]
004011DF . 890424 MOV DWORD PTR SS:[ESP],EAX
004011E2 . E8 A9000000 CALL Turkish-.00401290 Uyuyan devi uyandırma fonksiyon
004011E7 . 89C3 MOV EBX,EAX
004011E9 . E8 821F0000 CALL <JMP.&msvrt._cexit>
004011EE . 891C24 MOV DWORD PTR SS:[ESP],EBX
004011F1 . E8 0A200000 CALL <JMP.&KERNEL32.ExitProcess>
004011F6 > 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
004011FA . 8B15 4C914000 MOV EDI,DWORD PTR DS:[<msvrt._iob>]
00401200 . 8B42 10 MOV EAX,DWORD PTR DS:[EDI+10]
00401203 . 890424 MOV DWORD PTR SS:[ESP],EAX
00401206 . E8 A51F0000 CALL <JMP.&msvrt._setmode>
0040120B . 8B15 4C914000 MOV EDI,DWORD PTR DS:[<msvrt._iob>]
00401211 . E9 55FFFFFF JMP Turkish-.0040116B
00401216 . 8D76 00 LEA ESI,DWORD PTR DS:[ESI]
00401219 . 80 DB 80 DB 80
0040121A . BC DB BC
0040121B . 27 DB 27
0040121C . 00 DB 00
0040121D . 00 DB 00
0040121E . 00 DB 00
0040121F . 00 DB 00
00401220 . 55 DB 55
00401221 . 89 DB 89
00401222 . E5 DB E5
00401223 . 83 DB 83
00401224 . EC DB EC
00401225 . 55 DB 55
00401290=Turkish-.00401290
```

Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]

File View Debug Plugins ImmLib Options Window Help Jobs

Code auditor and software assessment

```
00404518 55      PUSH EBP
00404519 8BEC    MOV EBP,ESP
0040451A 57      PUSH EDI
0040451B 52      PUSH EDX
0040451C 51      PUSH ECX
0040451D B9 26000000 MOV ECX,26
0040451E BA 5F000000 MOV EDX,5F
0040451F 8B7C24 10 MOV EDI,DWORD PTR SS:[ESP+10]
00404520 85C9    TEST ECX,ECX
00404521 74 06   JE SHORT Turkish-.00404531
00404522 3B17    XOR BYTE PTR DS:[EDI],DL
00404523 49      DEC ECX
00404524 47      INC EDI
00404525 ^EB F6  JMP SHORT Turkish-.00404527
00404526 59      POP ECX
00404527 5A      POP EDX
00404528 5F      POP EDI
00404529 5D      POP EBP
0040452A C3      RETN
0040452B 0000    ADD BYTE PTR DS:[EAX],AL
0040452C 1345 40  ADC EAX,DWORD PTR SS:[EBP+40]
0040452D 0000    ADD BYTE PTR DS:[EAX],AL
0040452E 55      PUSH EBP
0040452F 8BEC    MOV EBP,ESP
00404530 57      PUSH EDI
00404531 52      PUSH EDX
00404532 51      PUSH ECX
00404533 B9 26000000 MOV ECX,26
00404534 BA 5F000000 MOV EDX,5F
00404535 8B7C24 10 MOV EDI,DWORD PTR SS:[ESP+10]
00404536 83EF 08  SUB EDI,8
00404537 85C9    TEST ECX,ECX
00404538 74 06   JE SHORT Turkish-.0040455E
00404539 3B17    XOR BYTE PTR DS:[EDI],DL
0040453A 49      DEC ECX
0040453B 47      INC EDI
0040453C ^EB F6  JMP SHORT Turkish-.00404554
0040453D 59      POP ECX
0040453E 5A      POP EDX
0040453F 5F      POP EDI
00404540 5D      POP EBP
00404541 C3      RETN
00404542 0000    ADD BYTE PTR DS:[EAX],AL
00404543 3D 45400000 CMP EAX,4045
00404544 55      PUSH EBP
00404545 8BEC    MOV EBP,ESP
00404546 57      PUSH EDI
00404547 52      PUSH EDX
00404548 51      PUSH ECX
00404549 B9 F9000000 MOV ECX,0F9
0040454A BA 22000000 MOV EDX,22
0040454B 8B7C24 10 MOV EDI,DWORD PTR SS:[ESP+10]
0040454C 85C9    TEST ECX,ECX
0040454D 74 06   JE SHORT Turkish-.00404588
0040454E 3B17    XOR BYTE PTR DS:[EDI],DL
0040454F 49      DEC ECX
00404550 47      INC EDI
00404551 ^EB F6  JMP SHORT Turkish-.0040457E
00404552 59      POP ECX
00404553 5A      POP EDX
00404554 5F      POP EDI
00404555 5D      POP EBP
00404556 C3      RETN
00404557 0000    ADD BYTE PTR DS:[EAX],AL
00404558 6A 45   PUSH 45
00404559 40      INC EAX
0040455A 0000    ADD BYTE PTR DS:[EAX],AL
0040455B 55      PUSH EBP
0040455C 8BEC    MOV EBP,ESP
0040455D 57      PUSH EDI
0040455E 52      PUSH EDX
0040455F 51      PUSH ECX
00404560 B9 F9000000 MOV ECX,0F9
00404561 BA 22000000 MOV EDX,22
00404562 8B7C24 10 MOV EDI,DWORD PTR SS:[ESP+10]
00404563 83EF 08  SUB EDI,8
00404564 85C9    TEST ECX,ECX
00404565 74 06   JE SHORT Turkish-.004045B5
00404566 3B17    XOR BYTE PTR DS:[EDI],DL
00404567 49      DEC ECX
00404568 47      INC EDI
00404569 ^EB F6  JMP SHORT Turkish-.004045AB
0040456A 59      POP ECX
0040456B 5A      POP EDX
0040456C 5F      POP EDI
0040456D 5D      POP EBP
0040456E C3      RETN
```


Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]

FileViewDebugPluginsImmLibOptionsWindowHelpJobs

Code auditor and software assessment

0040132883307C50400001CMPDWORDPTRDS:[40507C],0

0040132A7410JESHORTTurkish-.00401349

0040132C8B1080504000MOVEBX,DWORDPTRDS:[405080]

00401332A178504000MOV EAX,DWORDPTRDS:[405078]

004013373018XORBYTEPTRDS:[EAX],BL

00401339B87C504000MOV EAX,Turkish-.0040507C

0040133EFA08DECDWORDPTRDS:[EAX]

00401340B878504000MOV EAX,Turkish-.00405078

00401345FF08INCDWORDPTRDS:[EAX]

00401347^EBDAJMPSHORTTurkish-.00401323

00401349A165454000MOV EAX,DWORDPTRDS:[404565]

0040134EFF08CALL EAX

00401350A18F454000MOV EAX,DWORDPTRDS:[40458F]

00401357FFD0CALL EAX

00401359E526IN EAX,26I/O command

0040135A06PUSH ES

0040135A224262ANDAL,BYTEPTRDS:[EDX+62]

0040135D22CAANDCL,DL

0040135F5FPUSH EDI

004013605D222A1CECMPEAX,CESI2222

0040136526E566JNE EAX,66I/O command

0040136806PUSH ES

00401369262FDBS

0040136B42INCEX

0040136C6222BOUND ESP,QWORDPTRDS:[EDX]

0040136EABSTOSDWORDPTRES:[EDI]

0040136F2606PUSH ES

00401371CA C82ERETF 2EC8Superfluous prefixFar return

004013742222ANDAH,BYTEPTRDS:[EDX]

004013768132A26222E5XORDWORDPTRDS:[EDX],E52262A2

0040137C6606PUSH ES

0040137E2A26SUBAH,BYTEPTRDS:[ESI]

004013802322ANDESP,DWORDPTRDS:[EDX]

0040138222E5ANDAH,CH

004013846606PUSH ES

004013862612A26222E52ADC AH,BYTEPTRES:[EDX+26E52262]

0040138D06PUSH ES

0040138E2222ANDAH,BYTEPTRDS:[EDX]

004013902222ANDAH,BYTEPTRDS:[EDX]

004013929332A2XORDWORDPTRDS:[EDX],FFFFFFFA2

004013956222BOUND ESP,QWORDPTRDS:[EDX]

00401397DDF2[ESI]EAX

00401399ABSTOSDWORDPTRES:[EDI]Illegal use of register

0040139A67D2A967D2SHRBYTEPTRDS:[EBX+D1+D267],CL

0040139F27DAA

004013A008A26222A21AORBYTEPTRDS:[EDX+1AA22262],AH

004013A757DEC EDI

004013A83EA967D22709TEST EAX,927D267

004013AE A26222A21AMOVBYTEPTRDS:[1AA22262],ALSuperfluous prefix

004013B352PUSH EDX

004013B457PUSH EDI

004013B52DE5A7B6CDSUB EAX,CDBA7E5

004013BA0000FSTP ST(5)

004013BC1122ADCDWORDPTRDS:[EDX],ESP

004013BE2222ANDAH,BYTEPTRDS:[EAX]

0040134FD0A18F454000SHLBYTEPTRDS:[ECX+40458F],1

00401357FFD0CALL EAX

0040135EC7042400604000MOV DWORDPTRSS:[ESP],Turkish-.00406000ASCII "KERNEL32.dll"

0040135EE87D1F0000CALL <JMP.&KERNEL32.GetModuleHandleA>

0040136383EC04SUBESP,4

00401366C7442404006040MOV DWORDPTRSS:[ESP+4],Turkish-.00406000ASCII "GetModuleFileNameA"

0040136839042404006040MOV DWORDPTRSS:[ESP],EAX

00401371E8E00C0000CALLTurkish-.00402060

00401376A310804000MOV DWORDPTRDS:[408010],EAX

00401378C7442408040101MOV DWORDPTRSS:[ESP+8],104

00401383C7442404308040MOV DWORDPTRSS:[ESP+4],Turkish-.00408030

00401388C7042400000000MOV DWORDPTRSS:[ESP],0

00401392A110804000MOV EAX,DWORDPTRDS:[408010]

00401397FFD0CALL EAX

004013998945F0MOV DWORDPTRSS:[EBP-10],EAX

0040139CB845F0MOV EAX,DWORDPTRSS:[EBP-10]

0040139F052A804000ADD EAX,Turkish-.0040802A

004013A480386DCHPBYTEPTRDS:[EAX],6D

004013A7751CJNZSHORTTurkish-.004013C5

004013A98B45F0MOV EAX,DWORDPTRSS:[EBP-10]

004013AC052B804000ADD EAX,Turkish-.0040802B

004013B1803870CHPBYTEPTRDS:[EAX],70

004013B4750FJNZSHORTTurkish-.004013C5

004013B6C78594FFFFFF3:MOV DWORDPTRSS:[EBP-106C],33

004013C0E99C000000JMPTurkish-.00401461

004013C58B45F0MOV EAX,DWORDPTRSS:[EBP-10]

004013C8052A804000ADD EAX,Turkish-.0040802A

004013CD803870CHPBYTEPTRDS:[EAX],70

004013D07519JNZSHORTTurkish-.004013EB

004013D28B45F0MOV EAX,DWORDPTRSS:[EBP-10]

004013D5052B804000ADD EAX,Turkish-.0040802B

004013DA803870CHPBYTEPTRDS:[EAX],70

004013DD750CJNZSHORTTurkish-.004013EB

004013DFC78594FFFFFF0:MOV DWORDPTRSS:[EBP-106C],0

004013E9ED76JMPSHORTTurkish-.00401461

004013EBA168504000MOV EAX,DWORDPTRDS:[405068]

004013F08945ECMOV DWORDPTRSS:[EBP-14],EAX

004013F3A16C504000MOV EAX,DWORDPTRDS:[40506C]

004013F88945E8MOV DWORDPTRSS:[EBP-18],EAX

004013FB C7042454504000MOV DWORDPTRSS:[ESP],Turkish-.00405054ASCII "imyxrnfganuituruuw"

00401402E833000000CALLTurkish-.0040213A

0040140789442408MOV DWORDPTRSS:[ESP+8],EAX

0040140BC7442404545040MOV DWORDPTRSS:[ESP+4],Turkish-.00405054ASCII "imyxrnfganuituruuw"

00401413808598FFFFFFLEA EAX,DWORDPTRSS:[EBP-1068]

00401419890424MOV DWORDPTRSS:[ESP],EAX

0040141CE8E1150000CALLTurkish-.00402A02

004014218B45ECMOV EAX,DWORDPTRSS:[EBP-14]

0040142489442408MOV DWORDPTRSS:[ESP+8],EAX

004014288B45E8MOV EAX,DWORDPTRSS:[EBP-18]

0040142B89442404MOV DWORDPTRSS:[ESP+4],EAX

0040142F808598FFFFFFLEA EAX,DWORDPTRSS:[EBP-1068]

00401435890424MOV DWORDPTRSS:[ESP],EAX

00401438E8D1170000CALLTurkish-.00402C0E

0040143DB845E8MOV EAX,DWORDPTRSS:[EBP-18]

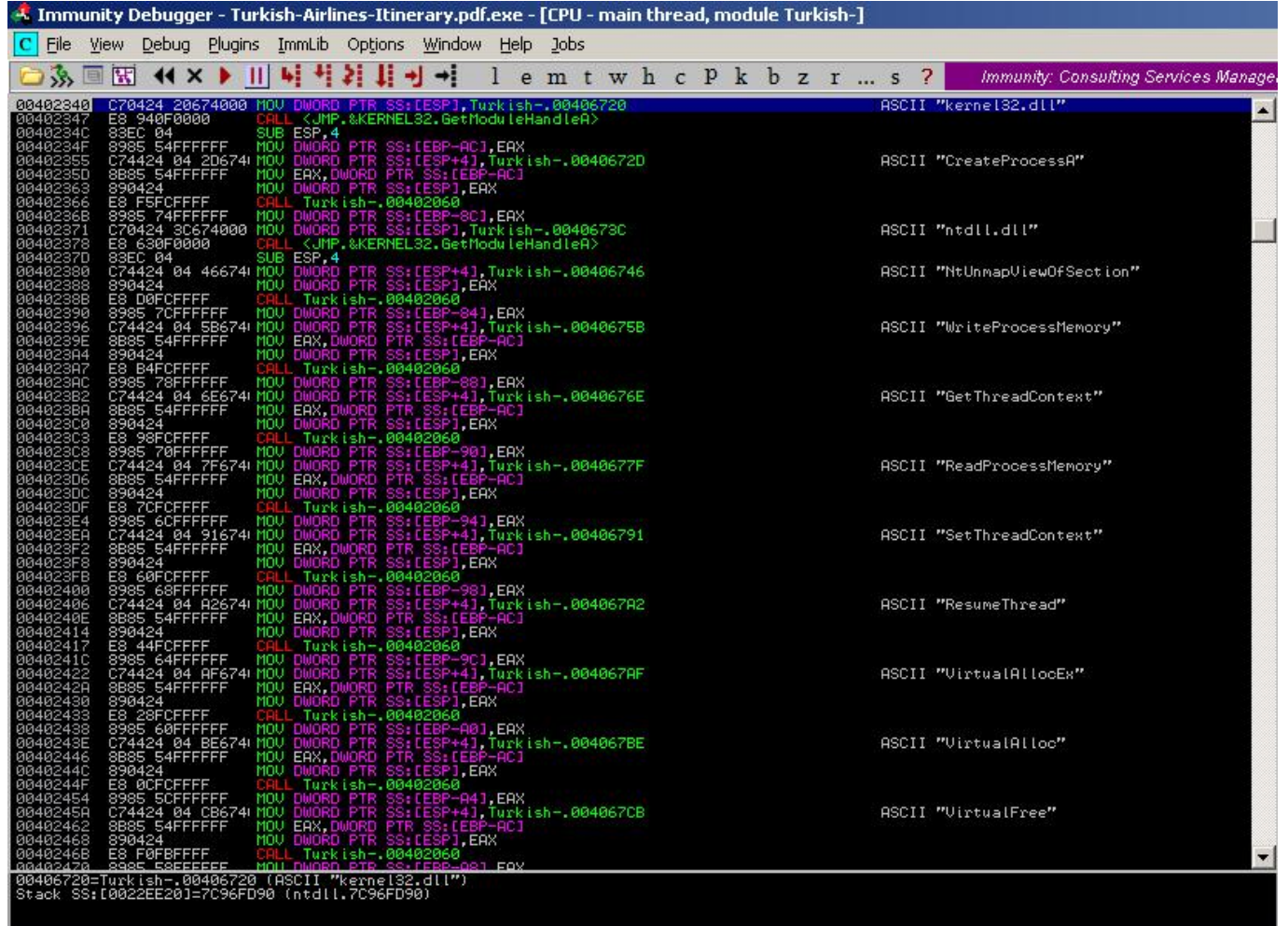
0040144089442404MOV DWORDPTRSS:[ESP+4],EAX

00401444C7042430804000MOV DWORDPTRSS:[ESP],Turkish-.00408030

00406000=Turkish-.00406000(ASCII "KERNEL32.dll")

StackSS:[0022EF14]=00070006

Son adımlara yaklaşıırken zararlı yazılımın işletim sistemi üzerinde çalışan potansiyel güvenlik yazılımlarını atlatmak için runPE (hafızadan işlem (process) çalıştırma) yöntemini kullanmak için hazırlık yaptığı anlaşılıyordu.



```
Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c p k b z r ... s ? Immunity: Consulting Services Manage

00402340 C74424 20674000 MOV DWORD PTR SS:[ESP],Turkish-.00406720 ASCII "kernel32.dll"
00402347 E8 940F0000 CALL <JMP.&KERNEL32.GetModuleHandleA>
0040234C 83EC 04 SUB ESP,4
0040234F 8985 54FFFFFF MOV DWORD PTR SS:[EBP-AC],EAX
00402355 C74424 04 2D6741 MOV DWORD PTR SS:[ESP+4],Turkish-.0040672D
0040235D 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402363 890424 MOV DWORD PTR SS:[ESP],EAX
00402366 E8 F5FCFFFF CALL Turkish-.00402060
0040236B 8985 74FFFFFF MOV DWORD PTR SS:[EBP-8C],EAX
00402371 C74424 3C674000 MOV DWORD PTR SS:[ESP],Turkish-.0040673C
00402378 E8 630F0000 CALL <JMP.&KERNEL32.GetModuleHandleA>
0040237D 83EC 04 SUB ESP,4
00402380 C74424 04 466741 MOV DWORD PTR SS:[ESP],EAX
00402388 E8 06FCFFFF CALL Turkish-.00402060
00402390 8985 7CFFFFFF MOV DWORD PTR SS:[EBP-84],EAX
00402396 C74424 04 5B6741 MOV DWORD PTR SS:[ESP+4],Turkish-.0040675B
0040239E 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023A4 890424 MOV DWORD PTR SS:[ESP],EAX
004023A7 E8 B4FCFFFF CALL Turkish-.00402060
004023AC 8985 78FFFFFF MOV DWORD PTR SS:[EBP-88],EAX
004023B2 C74424 04 6E6741 MOV DWORD PTR SS:[ESP+4],Turkish-.0040676E
004023BA 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023C0 890424 MOV DWORD PTR SS:[ESP],EAX
004023C3 E8 98FCFFFF CALL Turkish-.00402060
004023C8 8985 70FFFFFF MOV DWORD PTR SS:[EBP-90],EAX
004023CE C74424 04 7F6741 MOV DWORD PTR SS:[ESP+4],Turkish-.0040677F
004023D6 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023DC 890424 MOV DWORD PTR SS:[ESP],EAX
004023DF E8 7CFCFFFF CALL Turkish-.00402060
004023E4 8985 6CFFFFFF MOV DWORD PTR SS:[EBP-94],EAX
004023EA C74424 04 916741 MOV DWORD PTR SS:[ESP+4],Turkish-.00406791
004023F2 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023F8 890424 MOV DWORD PTR SS:[ESP],EAX
004023FB E8 60FCFFFF CALL Turkish-.00402060
00402400 8985 68FFFFFF MOV DWORD PTR SS:[EBP-98],EAX
00402406 C74424 04 A26741 MOV DWORD PTR SS:[ESP+4],Turkish-.004067A2
0040240E 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402414 890424 MOV DWORD PTR SS:[ESP],EAX
00402417 E8 44FCFFFF CALL Turkish-.00402060
0040241C 8985 64FFFFFF MOV DWORD PTR SS:[EBP-9C],EAX
00402422 C74424 04 0F6741 MOV DWORD PTR SS:[ESP+4],Turkish-.004067AF
0040242A 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402430 890424 MOV DWORD PTR SS:[ESP],EAX
00402433 E8 28FCFFFF CALL Turkish-.00402060
00402438 8985 60FFFFFF MOV DWORD PTR SS:[EBP-A0],EAX
0040243E C74424 04 BE6741 MOV DWORD PTR SS:[ESP+4],Turkish-.004067BE
00402446 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
0040244C 890424 MOV DWORD PTR SS:[ESP],EAX
0040244F E8 0CFCFFFF CALL Turkish-.00402060
00402454 8985 5CFFFFFF MOV DWORD PTR SS:[EBP-A4],EAX
0040245A C74424 04 CB6741 MOV DWORD PTR SS:[ESP+4],Turkish-.004067CB
00402462 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402469 890424 MOV DWORD PTR SS:[ESP],EAX
0040246B E8 F0FCFFFF CALL Turkish-.00402060
00402470 8985 58FFFFFF MOV DWORD PTR SS:[EBP-A8],EAX
00406720=Turkish-.00406720 (ASCII "kernel32.dll")
Stack SS:[0022EE20]=7C96FD90 (ntdll.7C96FD90)
```

Biraz daha ilerledikten sonra zararlı yazılımın paketinden çıkarmış olduğu işlemi (process) kontrol ettiğini farkettim ve diske kayıt edip, HEX editor ile fazlalık kısımları temizleyip Immunity Debugger ile çalıştırdım ve incelemeye başladım.

Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessment

```

004023BA 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023C0 890424 MOV DWORD PTR SS:[ESP],EAX
004023C3 E8 98FCFFFF CALL Turkish-.00402060
004023C8 8985 70FFFFFF MOV DWORD PTR SS:[EBP-90],EAX
004023CE C74424 04 7F6741 MOV DWORD PTR SS:[ESP+4],Turkish-.0040677F ASCII "ReadProcessMemory"
004023D6 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023DC 890424 MOV DWORD PTR SS:[ESP],EAX
004023DF E8 7CFCFFFF CALL Turkish-.00402060
004023E4 8985 60FFFFFF MOV DWORD PTR SS:[EBP-94],EAX
004023EA C74424 04 916741 MOV DWORD PTR SS:[ESP+4],Turkish-.00406791 ASCII "SetThreadContext"
004023F2 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023F8 890424 MOV DWORD PTR SS:[ESP],EAX
004023FB E8 60FCFFFF CALL Turkish-.00402060
00402400 8985 68FFFFFF MOV DWORD PTR SS:[EBP-98],EAX
00402406 C74424 04 A26741 MOV DWORD PTR SS:[ESP+4],Turkish-.004067A2 ASCII "ResumeThread"
0040240E 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402414 890424 MOV DWORD PTR SS:[ESP],EAX
00402417 E8 44FCFFFF CALL Turkish-.00402060
0040241C 8985 64FFFFFF MOV DWORD PTR SS:[EBP-9C],EAX
00402422 C74424 04 AF6741 MOV DWORD PTR SS:[ESP+4],Turkish-.004067AF ASCII "VirtualAllocEx"
0040242A 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402430 890424 MOV DWORD PTR SS:[ESP],EAX
00402433 E8 28FCFFFF CALL Turkish-.00402060
00402438 8985 60FFFFFF MOV DWORD PTR SS:[EBP-A0],EAX
0040243E C74424 04 BE6741 MOV DWORD PTR SS:[ESP+4],Turkish-.004067BE ASCII "VirtualAlloc"
00402446 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
0040244C 890424 MOV DWORD PTR SS:[ESP],EAX
0040244F E8 0CFCFFFF CALL Turkish-.00402060
00402454 8985 5CFFFFFF MOV DWORD PTR SS:[EBP-A4],EAX
0040245A C74424 04 CB6741 MOV DWORD PTR SS:[ESP+4],Turkish-.004067CB ASCII "VirtualFree"
00402462 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402468 890424 MOV DWORD PTR SS:[ESP],EAX
0040246B E8 F8FCFFFF CALL Turkish-.00402060
00402470 8985 58FFFFFF MOV DWORD PTR SS:[EBP-A8],EAX
00402476 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
00402479 8B45 F4 MOV DWORD PTR SS:[EBP-C],EAX
0040247C 8B45 F4 MOV EAX,DWORD PTR SS:[EBP-C]
0040247F 66:8138 4D5A CMP WORD PTR DS:[EAX],5A4D
00402484 0F85 47030000 JNZ Turkish-.004027D1
0040248A 8B55 F4 MOV EDX,DWORD PTR SS:[EBP-C]
0040248D 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
00402490 0342 3C ADD EAX,DWORD PTR DS:[EDX+3C]
00402493 8B45 F8 MOV EAX,DWORD PTR SS:[EBP-10]
00402496 8B45 F8 MOV EAX,DWORD PTR SS:[EBP-10]
00402499 8138 50450000 CMP DWORD PTR DS:[EAX],4550
0040249F 0F85 2C030000 JNZ Turkish-.004027D1
004024A5 C74424 08 440000 MOV DWORD PTR SS:[ESP+8],44
004024AD C74424 04 000000 MOV DWORD PTR SS:[ESP+4],0
004024B5 8D45 88 LEA EAX,DWORD PTR SS:[EBP-78]
004024B8 890424 MOV DWORD PTR SS:[ESP],EAX
004024BB E8 C6FCFFFF CALL Turkish-.00402286
004024C0 C74424 08 100000 MOV DWORD PTR SS:[ESP+8],10
004024C8 C74424 04 000000 MOV DWORD PTR SS:[ESP+4],0
004024D0 8D45 D8 LEA EAX,DWORD PTR SS:[EBP-28]
004024D3 890424 MOV DWORD PTR SS:[ESP],EAX
004024D6 E8 0BFCFFFF CALL Turkish-.00402286
DS:[0040A000]=5A4D

```

Address	Hex dump	ASCII
0040A000	4D 5A 90 00 03 00 00 00	NZE.♦...
0040A008	04 00 00 00 FF 00 00 00	♦....
0040A010	00 00 00 00 00 00 00 00	
0040A018	40 00 00 00 00 00 00 00	@.....
0040A020	00 00 00 00 00 00 00 00	
0040A028	00 00 00 00 00 00 00 00	
0040A030	00 00 00 00 00 00 00 00	
0040A038	00 00 00 00 80 00 00 00	C...
0040A040	00 00 00 00 00 00 00 00	
0040A048	00 00 00 00 00 00 00 00	
0040A050	00 00 00 00 00 00 00 00	
0040A058	00 00 00 00 00 00 00 00	
0040A060	00 00 00 00 00 00 00 00	
0040A068	00 00 00 00 00 00 00 00	
0040A070	00 00 00 00 00 00 00 00	
0040A078	00 00 00 00 00 00 00 00	
0040A080	00 00 00 00 00 00 00 00	
0040A088	00 00 00 00 00 00 00 00	
0040A090	00 00 00 00 00 00 00 00	
0040A098	00 00 00 00 00 00 00 00	
0040A0A0	00 00 00 00 00 00 00 00	
0040A0A8	00 00 00 00 00 00 00 00	
0040A0B0	00 00 00 00 00 00 00 00	
0040A0B8	00 00 00 00 00 00 00 00	
0040A0C0	00 00 00 00 00 00 00 00	
0040A0C8	00 00 00 00 00 00 00 00	
0040A0D0	00 00 00 00 00 00 00 00	
0040A0D8	00 00 00 00 00 00 00 00	
0040A0E0	00 00 00 00 00 00 00 00	
0040A0E8	00 00 00 00 00 00 00 00	
0040A0F0	00 00 00 00 00 00 00 00	
0040A0F8	00 00 00 00 00 00 00 00	
0040A100	00 00 00 00 00 00 00 00	
0040A108	00 00 00 00 00 00 00 00	
0040A110	00 00 00 00 00 00 00 00	
0040A118	00 00 00 00 00 00 00 00	
0040A120	00 00 00 00 00 00 00 00	
0040A128	00 00 00 00 00 00 00 00	
0040A130	00 00 00 00 00 00 00 00	
0040A138	00 00 00 00 00 00 00 00	
0040A140	00 00 00 00 00 00 00 00	

Backup

Create backup

Search for

Load backup from file

Go to

Save data to file

Hex

Text

Short

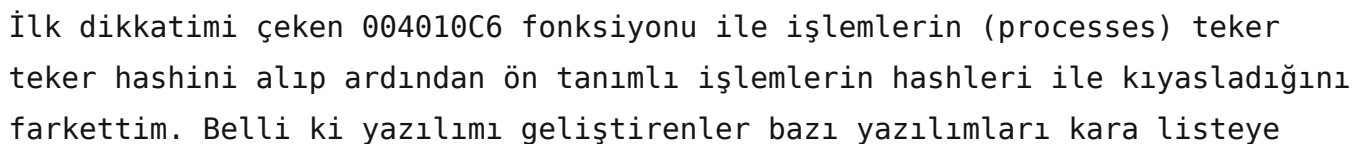
Long

Float

Disassemble

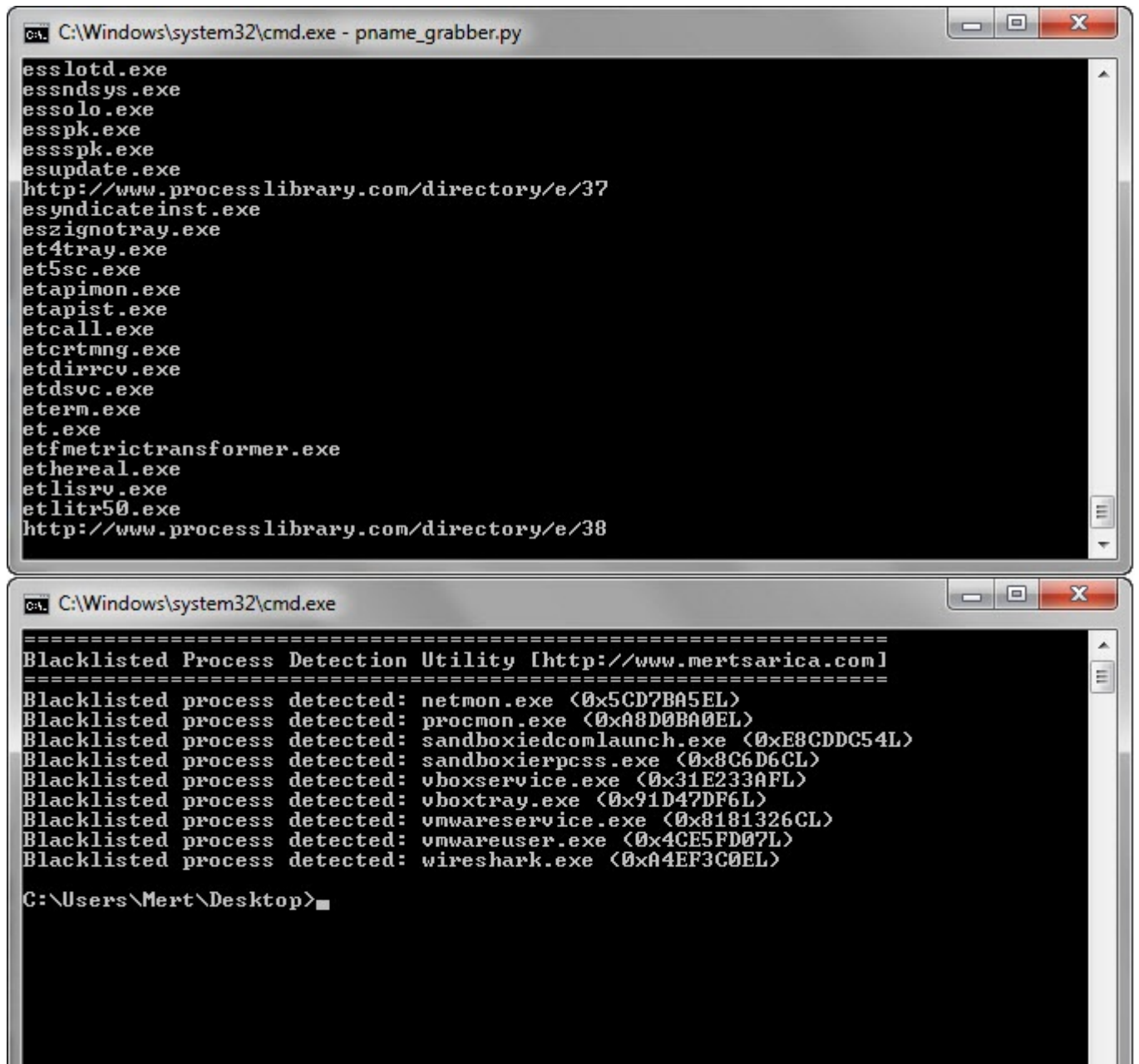
Special

Appearance



İlk dikkatimi çeken 004010C6 fonksiyonu ile işlemlerin (processes) teker teker hashini alıp ardından ön tanımlı işlemlerin hashleri ile kıyasladığını farkettim. Belli ki yazılımı geliştirenler bazı yazılımları kara listeye

almışlardı. Zararlı yazılımı VMWare içinde çalıştırdığım için vmwareuser.exe yazılımının kara listede olduğu hemen anlaşılıyordu. Ancak biraz çatlak olduğum için hangi yazılımların kara listede yer aldığını öğrenmek için Python ile <http://www.processlibrary.com/> adresinde kayıtlı olan tüm işlemlerin (processes) listesini oluşturan ufak bir araç hazırladım ve hash fonksiyonunu bire bir Python kodu ile oluşturarak tüm işlemleri bu araçtan geçirerek kara listede yer alan tüm yazılımları (netmon.exe, procmon.exe, sandboxiedcomlaunch.exe, sandboxierpcss.exe, vboxservice.exe, vboxtray.exe, vmwareservice.exe, vmwareuser.exe, wireshark.exe) tespit ettim.



```
C:\Windows\system32\cmd.exe - pname_grabber.py
esslotd.exe
essndsys.exe
essolo.exe
esspk.exe
essspk.exe
esupdate.exe
http://www.processlibrary.com/directory/e/37
esyndicateinst.exe
eszignotray.exe
et4tray.exe
et5sc.exe
etapimon.exe
etapist.exe
etcall.exe
etcrtmng.exe
etdirrcv.exe
etdsvc.exe
eterm.exe
et.exe
etfmetrictransformer.exe
ethereal.exe
etlisrv.exe
etlitr50.exe
http://www.processlibrary.com/directory/e/38

C:\Windows\system32\cmd.exe
=====
Blacklisted Process Detection Utility [http://www.mertsarica.com]
=====
Blacklisted process detected: netmon.exe (0x5CD7BA5EL)
Blacklisted process detected: procmon.exe (0xA8D0BA0EL)
Blacklisted process detected: sandboxiedcomlaunch.exe (0xE8CDDC54L)
Blacklisted process detected: sandboxierpcss.exe (0x8C6D6CL)
Blacklisted process detected: vboxservice.exe (0x31E233AFL)
Blacklisted process detected: vboxtray.exe (0x91D47DF6L)
Blacklisted process detected: vmwareservice.exe (0x8181326CL)
Blacklisted process detected: vmwareuser.exe (0x4CE5FD07L)
Blacklisted process detected: wireshark.exe (0xA4EF3C0EL)
C:\Users\Mert\Desktop>
```

Bunun dışında zararlı yazılımın sbiedll.dll ile Sandboxie yazılımının sistemde yüklü olup olmadığını, vmware, vbox gibi sanal makinede çalışıp çalışmadığının kontrolü, qemu öykünücü (emulator) kontrolü ve RDTSC yönergesi

(instruction) ile yönergeler arası geçen sürenin kontrolü ile kum havuzu ve hata ayıklıkcı kontrolü yaptığını tespit ettim.

```
Immunity Debugger - Turkish_.00400000.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins Immlib Options Window Help Jobs
l e m t w h c p k b z r ... s ? Code auditor and software assessment spe

004016AF . 75 68 JNZ SHORT Turkish-.00401719
004016B1 . 6A 04 PUSH 4
004016B3 . 68 00100000 PUSH 1000
004016B8 . FFB5 80FFFFFF PUSH DWORD PTR SS:[EBP-180]
004016BE . 6A 00 PUSH 0
004016C0 . FF55 E4 CALL DWORD PTR SS:[EBP-1C]
004016C3 . 8985 84FFFFFF MOV DWORD PTR SS:[EBP-17C],EAX
004016C9 . 85C0 TEST EAX,EAX
004016CB . 74 4C JE SHORT Turkish-.00401719
004016CD . 6A 30 PUSH 30
004016CF . 8BD4 MOV EDX,ESP
004016D1 . 33C9 XOR ECX,ECX
004016D3 . 8085 80FFFFFF LEA EAX,DWORD PTR SS:[EBP-180]
004016D9 . 59 PUSH EAX
004016DA . FFB5 84FFFFFF PUSH DWORD PTR SS:[EBP-17C]
004016E0 . 51 PUSH ECX
004016E1 . 51 PUSH ECX
004016E2 . 52 PUSH EDX
004016E3 . FFB5 88FFFFFF PUSH DWORD PTR SS:[EBP-178]
004016E9 . FF55 D0 CALL DWORD PTR SS:[EBP-30]
004016EC . 83C4 04 ADD ESP,4
004016EF . FFB5 84FFFFFF PUSH DWORD PTR SS:[EBP-17C]
004016F5 . E8 D7CFFFFF CALL Turkish-.004013D1
004016FA . 3B85 84FFFFFF MOV EAX,DWORD PTR SS:[EBP-17C]
00401700 . 8B40 08 MOV EAX,DWORD PTR DS:[EAX+8]
00401703 . 8985 7CFFFFFF MOV DWORD PTR SS:[EBP-184],EAX
00401709 . 68 00800000 PUSH 8000
0040170E . 6A 00 PUSH 0
00401710 . FFB5 84FFFFFF PUSH DWORD PTR SS:[EBP-17C]
00401716 . FF55 E0 CALL DWORD PTR SS:[EBP-20]
00401719 . FFB5 88FFFFFF PUSH DWORD PTR SS:[EBP-178]
0040171F . FF55 CC CALL DWORD PTR SS:[EBP-34]
00401722 . 81B0 7CFFFFFF CMP DWORD PTR SS:[EBP-184],61776D77
0040172C . 74 39 JE SHORT Turkish-.00401767
0040172E . 81B0 7CFFFFFF CMP DWORD PTR SS:[EBP-184],786F6276
00401738 . 74 2D JE SHORT Turkish-.00401767
0040173A . 81B0 7CFFFFFF CMP DWORD PTR SS:[EBP-184],756D6571
00401744 . 74 21 JE SHORT Turkish-.00401767
00401746 . 0F31 RDTSC
00401748 . 50 PUSH EAX
00401749 . 0F31 RDTSC
0040174B . 5A POP EDX
0040174C . 2BC2 SUB EAX,EDX
0040174E . 3D 00020000 CMP EAX,200
00401755 . 73 12 JNB SHORT Turkish-.00401767
0040175B . 8085 78FFFFFF LEA EAX,DWORD PTR DS:[401778]
00401761 . 8085 B9134000 LEA EAX,DWORD PTR DS:[4013B9]
00401763 . 50 PUSH EAX
00401765 . FFB5 78FFFFFF PUSH DWORD PTR SS:[EBP-188]
00401767 . E8 11FBFFFF CALL Turkish-.00401284
00401773 . C9 LEAVE
00401774 . C3 RETN
00401775 . CC INT3
00401776 . CC INT3
00401777 . CC INT3
00401778 . 00 DB 00
00401779 . 20 DB 20
0040177A . 00 DB 00
0040177B . 00 DB 00
0040177C . 05 DB 05
0040177D . 04 DB 04
0040177E . 00 DB 00
0040177F . 00 DB 00
00401780 . 00 DB 00
00401781 . 00 DB 00
00401782 . 00 DB 00
00401783 . 00 DB 00

vmwa
vbox
qemu
CPU dongusu sayaci - Anti debugger/sandbox
CPU dongusu sayaci - Anti debugger/sandbox
Arg2
Arg1
Turkish-.00401284
CHAR ' '

```

Zararlı yazılım bu kontrollerden herhangi birine takıldığı takdirde kendisini %ALLUSERSPROFILE% ortam değişkeninde (environment) yer alan klasöre kopyalamakta ve sistem yeniden başlatıldığında çalışabilmek için kayıt defterinde

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SunJavaUpdateSched anahtarı oluşturmaktadır. Çalıştığı zaman da hem e-posta hem de web sitelerine konu olduğu gibi 8000. numaralı bağlantı noktasında (port) dinlemeye geçmekte ve bu bağlantı noktasından sisteme bağlanan kişilere komut satırı erişimi (shell) vermektedir.

Immunity Debugger - Turkish_00400000.exe - [CPU - main thread]

File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c p k b z r ... s ? Python Developer Wanted

```
00380100 55      PUSH EBP
00380101 8BEC    MOV EBP,ESP
00380103 83C4 0C  ADD ESP,-74
00380106 E8 C3010000 CALL 003802CE      JMP to kernel32.GetProcessHeap
00380108 A3 20033800 MOV DWORD PTR DS:[380320],EAX
00380110 68 04010000 PUSH 104
00380115 6A 00    PUSH 0
00380117 FF35 20033800 PUSH DWORD PTR DS:[380320]
0038011D E8 B2010000 CALL 003802D4      JMP to ntdll.RtlAllocateHeap
00380122 8945 FC  MOV DWORD PTR SS:[EBP-4],EAX
00380125 3BF8 00  CMP EAX,0
00380128 0F84 76010000 JE 003802A4
0038012E 68 04010000 PUSH 104
00380133 6A 00    PUSH 0
00380135 FF35 20033800 PUSH DWORD PTR DS:[380320]
0038013B E8 94010000 CALL 003802D4      JMP to ntdll.RtlAllocateHeap
00380140 8945 F8  MOV DWORD PTR SS:[EBP-8],EAX
00380143 3BF8 00  CMP EAX,0
00380146 0F84 58010000 JE 003802A4
0038014C 68 04010000 PUSH 104
00380151 FF75 F8  PUSH DWORD PTR SS:[EBP-8]
00380154 68 60003800 PUSH 380060
00380159 E8 64010000 CALL 003802C2      ASCII "%ALLUSERSPROFILE%\suchost.exe"
0038015E 68 04010000 PUSH 104      JMP to kernel32.ExpandEnvironmentStringsA
00380163 FF75 FC  PUSH DWORD PTR SS:[EBP-4]
00380166 6A 00    PUSH 0
00380168 E8 58010000 CALL 003802C8      JMP to kernel32.GetModuleFileNameA
0038016D 6A 00    PUSH 0
0038016F FF75 F8  PUSH DWORD PTR SS:[EBP-8]
00380172 FF75 FC  PUSH DWORD PTR SS:[EBP-4]
00380175 E8 36010000 CALL 003802B0      JMP to kernel32.CopyFileA
0038017A 6A 06    PUSH 6
0038017C FF75 F8  PUSH DWORD PTR SS:[EBP-8]
0038017F E8 56010000 CALL 003802DA      JMP to kernel32.SetFileAttributesW
00380184 8D45 F4  LEA EAX,DWORD PTR SS:[EBP-C]
00380187 50      PUSH EAX
00380188 68 06000200 PUSH 20006
0038018D 6A 00    PUSH 0
0038018F 68 7E003800 PUSH 38007E      ASCII "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
00380194 68 02000000 PUSH 00000002
00380199 E8 72010000 CALL 00380310      JMP to ADVAPI32.RegOpenKeyExA
0038019E 3BF8 00  CMP EAX,0
003801A1 74 1F    JE SHORT 003801C2
003801A3 8D45 F4  LEA EAX,DWORD PTR SS:[EBP-C]
003801A6 50      PUSH EAX
003801A7 68 06000200 PUSH 20006
003801AC 6A 00    PUSH 0
003801AE 68 AC003800 PUSH 3800AC      ASCII "Software\Microsoft\Windows\CurrentVersion\Run"
003801B3 68 01000000 PUSH 00000001
003801B8 E8 53010000 CALL 00380310      JMP to ADVAPI32.RegOpenKeyExA
003801BD 3BF8 00  CMP EAX,0
003801C0 75 26    JNS SHORT 003801E8
003801C2 FF75 F8  PUSH DWORD PTR SS:[EBP-8]
003801C5 E8 16010000 CALL 003802E0      JMP to kernel32.lstrlenA
003801CA 40      INC EAX
003801CB 50      PUSH EAX
003801CC FF75 F8  PUSH DWORD PTR SS:[EBP-8]
003801CF 6A 01    PUSH 1
003801D1 6A 00    PUSH 0
003801D3 68 DA003800 PUSH 3800DA      ASCII "SunJavaUpdateSched"
003801D8 FF75 F4  PUSH DWORD PTR SS:[EBP-C]
003801DB E8 36010000 CALL 00380316      JMP to ADVAPI32.RegSetValueExA
003801E0 FF75 F4  PUSH DWORD PTR SS:[EBP-C]
003801E3 E8 22010000 CALL 0038030A      JMP to ADVAPI32.RegCloseKey
003801E8 68 24033800 PUSH 380324
003801ED 68 01010000 PUSH 101
003801F2 E8 F5000000 CALL 003802EC      JMP to ws2_32.WSASStartupA
EBP=0012FE28
```

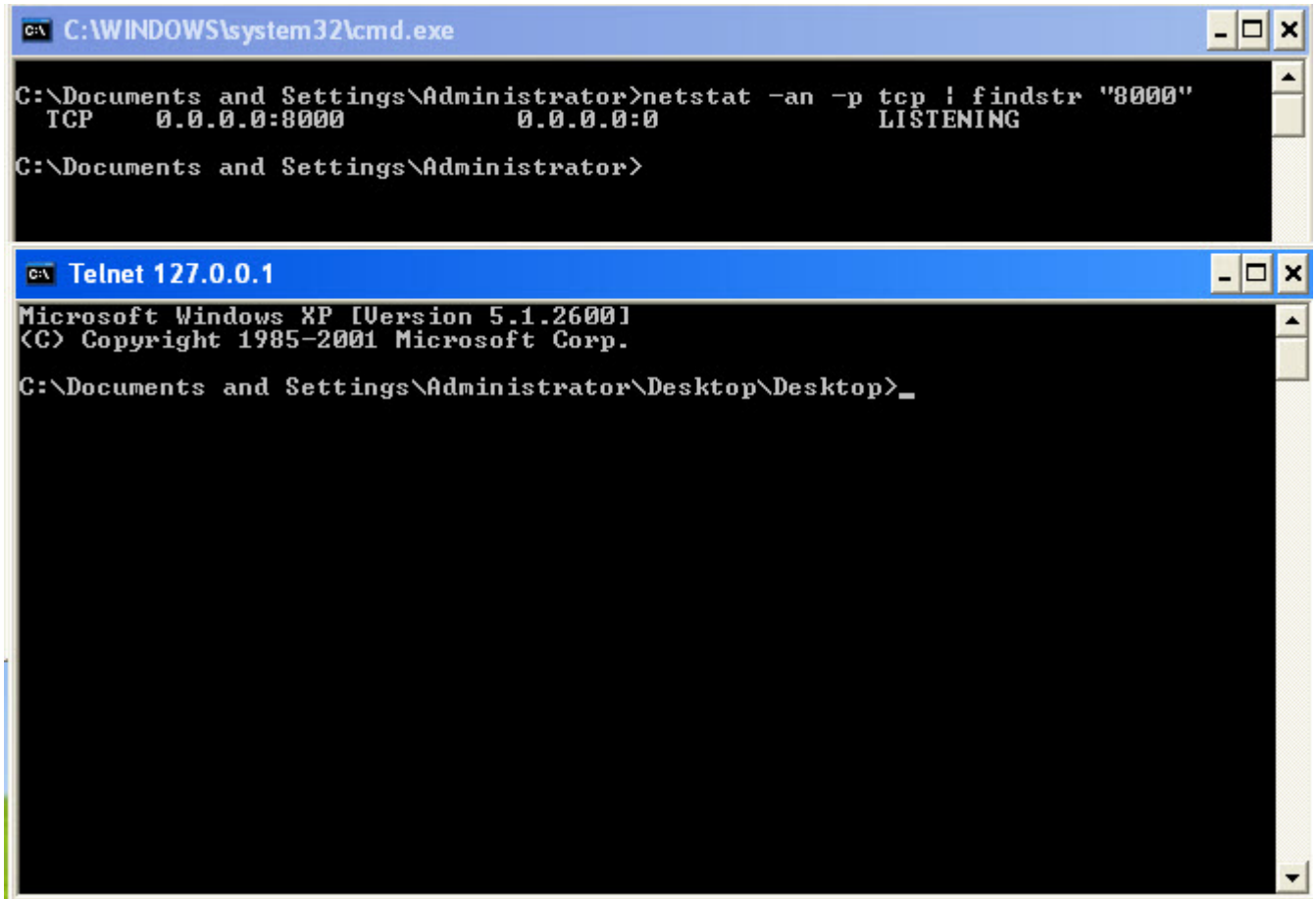

Immunity Debugger - Turkish_00400000.exe - [CPU - main thread]

File View Debug Plugins Immlib Options Window Help Jobs

Code auditor and software assessment

l e m t w h c p k b z r ... s ?

```
003801CF 6A 01      PUSH 1
003801D1 6A 00      PUSH 0
003801D3 68 DA003800  PUSH 3800DA
003801D8 FF75 F4    PUSH DWORD PTR SS:[EBP-C]
003801DB E8 36010000  CALL 00380316
003801E0 FF75 F4    PUSH DWORD PTR SS:[EBP-C]
003801E3 E8 22010000  CALL 0038030A
003801E8 68 24003800  PUSH 380324
003801ED 68 01010000  PUSH 101
003801F2 E8 F5000000  CALL 003802EC
003801F7 66:C745 E0 0200 MOV WORD PTR SS:[EBP-20],2
003801FD 68 401F0000  PUSH 1F40
00380202 E8 F7000000  CALL 003802FE
00380207 66:8945 E2    MOV WORD PTR SS:[EBP-1E],AX
0038020B C745 E4 00000000 MOV DWORD PTR SS:[EBP-1C],0
00380212 6A 00      PUSH 0
00380214 6A 00      PUSH 0
00380216 6A 00      PUSH 0
00380218 6A 06      PUSH 6
0038021A 6A 01      PUSH 1
0038021C 6A 02      PUSH 2
0038021E E8 C3000000  CALL 003802E6
00380223 8945 F0      MOV DWORD PTR SS:[EBP-10],EAX
00380226 83F8 FF      CMP EAX,-1
00380229 74 79      JE SHORT 003802A4
0038022B 6A 10      PUSH 10
0038022D 8D45 E0      LEA EAX,DWORD PTR SS:[EBP-20]
00380230 50          PUSH EAX
00380231 FF75 F0      PUSH DWORD PTR SS:[EBP-10]
00380234 E8 BF000000  CALL 003802F8
00380239 83F8 FF      CMP EAX,-1
0038023C 74 66      JE SHORT 003802A4
0038023E 6A 05      PUSH 5
00380240 FF75 F0      PUSH DWORD PTR SS:[EBP-10]
00380243 E8 BC000000  CALL 00380304
00380248 83F8 FF      CMP EAX,-1
0038024B 74 57      JE SHORT 003802A4
0038024D 33C0      XOR EAX,EAX
0038024F 8D7D 9C      LEA EDI,DWORD PTR SS:[EBP-64]
00380252 B9 44000000  MOV ECX,44
00380257 F3:AA      REP STOS BYTE PTR ES:[EDI]
00380259 6A 00      PUSH 0
0038025B 6A 00      PUSH 0
0038025D FF75 F0      PUSH DWORD PTR SS:[EBP-10]
00380260 E8 8D000000  CALL 003802F2
00380265 C745 9C 44000000 MOV DWORD PTR SS:[EBP-64],44
0038026C 8945 04      MOV DWORD PTR SS:[EBP-2C],EAX
0038026F 8945 08      MOV DWORD PTR SS:[EBP-28],EAX
00380272 8945 0C      MOV DWORD PTR SS:[EBP-24],EAX
00380275 66:C745 CC 0000 MOV WORD PTR SS:[EBP-34],0
0038027B C745 C8 01010000 MOV DWORD PTR SS:[EBP-30],101
00380282 8D45 8C      LEA EAX,DWORD PTR SS:[EBP-74]
00380285 50          PUSH EAX
00380286 8D45 9C      LEA EAX,DWORD PTR SS:[EBP-64]
00380289 50          PUSH EAX
0038028A 6A 00      PUSH 0
0038028C 6A 00      PUSH 0
0038028E 6A 00      PUSH 0
00380290 6A 01      PUSH 1
00380292 6A 00      PUSH 0
00380294 6A 00      PUSH 0
00380296 68 ED003800  PUSH 3800ED
0038029B 6A 00      PUSH 0
0038029D E8 14000000  CALL 003802B6
003802A2 EB A9      JMP SHORT 003802AD
003802A4 6A 00      PUSH 0
003802A6 E8 11000000  CALL 003802BC
003802AB C9          LEAVE
003802AC C2 0400      RETN 4
EBP=0012FE28
```



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -an -p tcp | findstr "8000"
TCP      0.0.0.0:8000      0.0.0.0:0        LISTENING
C:\Documents and Settings\Administrator>

C:\ Telnet 127.0.0.1
Microsoft Windows XP [Version 5.1.26001
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator\Desktop\Desktop>_
```

Ancak bu zararlı yazılım, kontrollerden herhangi birine takılmaz ise 32 bit işletim sisteminde windows\system32 klasörü altında wuaucvt.exe dosyası yaratmakta, 64 bit işletim sisteminde ise windows\syswow64 klasörü altında svchost.exe dosyası yaratmakta (windows file protection izin verirse), çalıştırmakta ardından kendisini bu işleme (process) enjekte ederek diğer faza geçmektedir. Son fazda ise sisteme bankacılık zararlı yazılımı bulaştırarak Zeus ve Spyeye'dan bildiğimiz gibi kullanıcının cep telefonuna da zararlı yazılım göndererek internet şubesini kullanan kullanıcının kullanıcı adını, şifresini ve sms doğrulama kodunu çalarak müşterilerin hesabını boşaltmaya çalışmaktadır.

```
00380000 55          PUSH EBP
00380001 8BEC       MOV EBP, ESP
00380003 31C4 ACFCFFF ADD ESP, -354
00380009 6A 00      PUSH 0
0038000B E8 96030000 CALL 00380466      JMP to kernel32.GetModuleHandleW
0038000D 8945 F8    MOV DWORD PTR SS:[EBP-8], EAX
0038000F 6A 04      PUSH 4
00380011 68 00100000 PUSH 1000
00380013 68 00000000 PUSH 0
00380015 6A 00      PUSH 0
00380017 E8 96030000 CALL 0038047E      JMP to kernel32.VirtualAlloc
00380019 8945 F4    MOV DWORD PTR SS:[EBP-C], EAX
0038001B 85C0      TEST EAX, EAX
0038001D JE 00380416
0038001F 68 00000000 PUSH 0
00380021 FF75 F4    PUSH DWORD PTR SS:[EBP-C]
00380023 6A 00      PUSH 0
00380025 E8 60030000 CALL 00380460      JMP to kernel32.GetModuleFileNameW
00380027 FF75 F4    PUSH DWORD PTR SS:[EBP-C]
00380029 68 00000000 PUSH 0
0038002B E8 60030000 CALL 00380478      UNICODE "src"
0038002D 68 00000000 PUSH 0
0038002F E8 60030000 CALL 00380472      JMP to kernel32.SetEnvironmentVariableW
00380031 FF75 F4    PUSH DWORD PTR SS:[EBP-C]
00380033 E8 58030000 CALL 00380472      JMP to kernel32.GetWindowsDirectoryW
00380035 85C0      TEST EAX, EAX
00380037 JE 00380407
00380039 0F84 E5020000 JBE 00380407
0038003B C745 FC 00000000 MOV DWORD PTR SS:[EBP-4], 0
0038003D 6A 00      PUSH 0
0038003F 6A 04      PUSH 4
00380041 8B45 FC    LEA EAX, DWORD PTR SS:[EBP-4]
00380043 50        PUSH EAX
00380045 6A 1A      PUSH 1A
00380047 6A FF      PUSH -1
00380049 E8 FC020000 CALL 00380436      JMP to ntdll.ZwQueryInformationProcess
0038004B 337D FC 00 CMP DWORD PTR SS:[EBP-4], 0
0038004D 75 0F     JNZ SHORT 0038014F
0038004F 68 00000000 PUSH 0
00380051 FF75 F4    PUSH DWORD PTR SS:[EBP-C]
00380053 E8 30030000 CALL 0038048A      UNICODE "\system32\wuauclt.exe"
00380055 E8 30030000 CALL 0038048A      JMP to kernel32.lstrcatW
00380057 E8 30030000 CALL 0038048A      UNICODE "\system32\svchost.exe"
00380059 E8 30030000 CALL 0038048A      JMP to kernel32.lstrcatW
0038005B 6A 00      PUSH 0
0038005D 68 00000000 PUSH 0
0038005F 6A 03      PUSH 3
00380061 6A 00      PUSH 0
00380063 6A 01      PUSH 1
00380065 68 00000000 PUSH 0
00380067 FF75 F4    PUSH DWORD PTR SS:[EBP-C]
00380069 E8 30030000 CALL 0038048A      JMP to kernel32.CreateFileW
0038006B 8945 F8    MOV DWORD PTR SS:[EBP-10], EAX
0038006D 83F8 FF    CMP EAX, -1
0038006F JE 00380407
00380071 FF75 F0    PUSH DWORD PTR SS:[EBP-10]
00380073 68 00000000 PUSH 0
00380075 6A 02      PUSH 2
00380077 6A 00      PUSH 0
00380079 6A 00      PUSH 0
0038007B 6A 04      PUSH 4
0038007D 8B45 EC    LEA EAX, DWORD PTR SS:[EBP-14]
0038007F 50        PUSH EAX
00380081 E8 8F020000 CALL 0038042A      JMP to ntdll.ZwCreateSection
00380083 85C0      TEST EAX, EAX
00380085 JL 003803FF
00380087 XOR ECX, ECX
00380089 894D E8    MOV DWORD PTR SS:[EBP-18], ECX
0038008B 50        PUSH EAX
EBP=0012FE28
```

Sonuç olarak yazının başında da bahsettiğim üzere yazılım seviyesine inilmeden sistem seviyesinde yapılan analizler, zararlı yazılımın sanal makine, debugger, sandbox tespitine yönelik kontroller içermesi durumunda farklı sonuçlar ortaya çıkarabilmektedir bu nedenle zararlı yazılım hakkında kesin bir sonuca varmak için mutlaka ama mutlaka yazılım seviyesinde de analiz yapılması gerekmektedir.

Türkiye’deki banka müşterilerini hedef alan bu zararlı yazılım ile ilgili daha fazla bilgi almak için Tübitak BİLGEM tarafından yayınlanan analiz yazısını da okumanızı öneririm.

Bu vesileyle herkesin yeni yılını kutlar, 2013 yılının herkese önce sağlık sonra güvenli günler getirmesini dilerim.

Not: Her ne kadar bu zararlı yazılım Tübitak BİLGEM’in yayınlamış olduğu analiz yazısında Zeus’un bir türevi olarak yer almış olsa da Zemana firmasından Emre TINAZTEPE’nin yapmış olduğu bir açıklamaya göreye zararlı

yazılım kimi zaman Zeus kimi zaman ise Cridex olarak son kullanıcının sistemine yüklenmektedir. Daha detaylı yeni analiz raporları/yazıları yayınlandıkça bu zararlı yazılım hakkında daha net bilgilere sahip olacağımıza inanıyorum.