OFANSİF ZARARLI YAZILIM ANALİZİ

İÇERİK

Neden zararlı yazılım analizi ?

Klasik zararlı yazılım analizi

Ofansif zararlı yazılım analizi

Araçlar üzerine

Sonuç

BEN KİMİM?

Ahlaklı Korsan (E.H)	**Mesai saatlerinde...**
Zararlı Yazılım Analisti	**Boş zamanlarımda...**
Blog Yazarı	**http://www.mertsarica.com**
Güvenlik TV	**http://www.guvenliktv.org**
Python Programcısı	**http://www.mertsarica.com/programlar**
Sertifika Kolleksiyoncusu	**CISSP , SSCP , OSCP , OPST , CREA**

MESLEĞİM ?

NBG Grup şirketlerinden Finansbank'ın Bilgi Teknolojileri iştiraki olan IBTech firmasında Bilişim Güvenliği Uzmanı (Senior Penetration Tester / Ethical Hacker) olarak çalışmaktayım.

http://www.finansbank.com.tr

http://www.ibtech.com.tr

İSTATİSTİKİ BİLGİLER

2012 yılında günde 74.000, toplamda 27 milyon zararlı yazılım tespit edildi.

En çok zararlı yazılım bulaşan sisteme sahip ülkeler arasında Türkiye, Çin, Kuzey Kore ve Tayvan'dan sonra 4. sırada yer aldı.

Tespit edilen zararlı yazılımlardan %99.82'si Windows işletim sistemi kullanıcılarını hedef aldı.

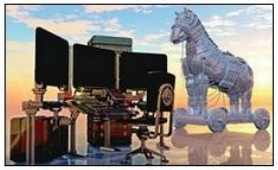
Tespit edilen zararlı yazılımlardan %76.56'sı truva atı, %8'i virüs, %6.44'ü solucan, %5.72'si reklam/casus yazılımıydı.

Android işletim sistemini hedef alan zararlı yazılım sayısı 2012 yılının ilk 6 ayı ile son 6 ayı arasında 5 kat arttı.

GÜNCEL HABERLER

Truva atı zaferi

Asliye Ticaret Mahkemesi, banka hesaplarında internet korsanlarının kurbanı olan Hülya S.'yi bilgisayarında yeterli güvenlik önlemi almadığı ve 'Truva atı' virüsü tespit edildiği için yüzde 50 oranında kusurlu buldu. Yargıtay bu kararı bozarak, müşterinin uğradığı zarardan yüzde 100 bankayı sorumlu tuttu.



YARGITAY Hukuk Genel Kurulu, (YHGK) hesapları internet korsanlarının kurbanı olan Hülya S.'nin ortaya çıkan zararında yüzde 100 bankayı sorumlu tuttu. Yargıtay emsal kararında, hesaptaki paranın güvenliğinden de kötü niyetli kişilere karşı gerekli önlemleri almaktan da bankanın sorumlu olduğuna dikkat çekti. Kararda, internet korsanlarınca usulsüz işlemle çekilen paranın doğrudan doğruya "banka zararı" niteliğinde olduğu ve mevduat sahibinin bankaya karşı alacağının aynen devam ettiği de belirtildi.

BANKA ÖDEMEDİ DAVA AÇTI

8 Haziran 2005'te, İzmir'de bankaya cüzdanını işletmeye giden Hülya S'nin, internet bankacılığı hizmetlerine açık olan hesaplarından altı kez para çekildiği ve 16 bin 150 lirasının Adnan Ö. adlı kişiye havale edildiği anlaşıldı. Hülya S. parasının rızası ve bilgisi dışında çekildiğini belirterek, bankadan parayı talep etti. Ancak, banka parayı ödemedi. Hülya S. internet korsanının çektiği 16 bin 150 TL yanı sıra tasarruf hesabındaki fonun bozulduğu için uğradığı 442 TL ve hesabı boşaltıldığı için para tedariki için harcadığı 68 TL'lik faiz olmak üzere bankaya toplam 17 bin 85 liralık maddi ve 20 bin liralık da manevi tazminat istemiyle İzmir 8. Asliye Ticaret Mahkemesi'nde dava açtı. Mahkeme bilirkişi incelemesi yaptırdı.

TRUVA ATI VİRÜSÜ BULDU

Bilirkişi raporunda, davacı Hülya S'nin bilgisiyarında yeterli güvenlik önlemi almadığı ve 'Trojan horse' (Truva atı) virüsü tespit edildiği kaydedildi. Raporda, bilgisayarında virüs tespit edilen davacının da banka gibi yüzde 50 oranında kusurlu olduğu savunuldu. Parayı çeken Adnan Ö. hakkında da nitelikli dolandırıcılıktan dava açıldı. Mahkeme 6 Kasım 2008 tarihli kararıyla internet bankacılığı sistemini kullanan kişilerin risk bulunduğunu bildiğine dikkat çekti ve banka ile birlikte davacıyı da yüzde 50 oranında kusurlu saydı. Çekilen 16 bin 150 liranın yüzde 50'si 8 bin 75 TL maddi tazminatın bankaca ödenmesine, manevi tazminat talebinin ise reddine karar verildi.

YÜZDE 100 BANKA SORUMLU

Temyizde, Yargıtay 11. Hukuk Dairesi, mahkemenin banka müşterisini de yüzde 50 kusurlu bulan kararını 3 Mayıs 2011'de oybirliği ile bozdu. Kararda özetle şöyle denildi: "Bankalar kendilerine yatırılan paraları mudilere istendiğinde veya belli bir vadede aynı veya misli olarak iade etmekle yükümlüdür. Bu tanımlamaya göre mevduat ödünç ile usulsüz tevdi sözleşmelerinin niteliklerini taşıyan kendine özgü bir sözleşmedir. Borçlar Kanunu hükümleri uyarınca ödünç alan akdin sonunda ödünç verilen parayı eğer kararlaştırılmışsa faizi ile iadeye mecburdur. Bu açıdan değerlendirildiğinde, usulsüz işlemle çekilen paralar aslında doğrudan doğruya bankanın zararı niteliğinde olup, mevduat sahibinin bankaya karşı alacağı aynen davam etmektedir."

Banka zararın tamamını ödesin

MAHKEME, ilk kararında direndi. Bunun üzerine dava, 21 Kasım Çarşamba günü YHGK'nın önüne geldi. Kurul, davalı bankanın paranın güvenliğini sağlayamadığı, müşterisini kötü niyetli kişilerin işlemlerine karşı koruyamadığı için yüzde 100 kusurlu bulan daire kararını onarken, direnme kararını oyçokluğu ile bozdu. Kurul, davacı müşterisinin hesabından çekilen paranın yüzde 100'ünün ödemesine hükmetti. Kurul kararı kesin nitelik taşıyor.

Banka nerelerde kusurlu

· Bu kişilerin eylem ve işlemlerine karşı koruyacak etkili mekanizmayı güvenlik önlemlerini geliştirmediği,
· Bu önlemleri kullanmayı müşterileri için zorunlu hale getirmediği anlaşıldı.
· Bu durum karşısında davacının yarı oranında kusurlu olduğu kabul edilerek hüküm kurulması doğru görülmemiş ve kararın bozulması gerekmiştir.

GÜNCEL HABERLER

BDDK'dan banka müşterilerini hedef alan "FATMAL" yazılım uyarısı

29.12.2012 | A A

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Türkiye'deki banka müşterilerini hedef alan, içeriğinde zararlı "FATMAL" yazılımı barındıran e-postalara karşı uyarıda bulundu.

BDDK'nın internet sitesinde yer alan açıklamaya göre, 19 Aralık 2012 tarihinden itibaren özellikle Türkiye'deki banka müşterilerini hedef alan, içeriğinde zararlı "FATMAL" yazılımı barındıran ve oltalama (phishing) tabir edilen bir e-posta trafiğinin başladığı TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü tarafından rapor edildi.

Söz konusu e-postalar, bazı telekom operatörlerinden veya havayolu firmalarından gelen ve içinde fatura bildirimi yapıldığı izlenimi uyandıran bir dosya (.pdf.exe uzantılı) taşıyor.

Açılması istenen bu dosyanın barındırdığı ikinci bir dosya (truva atı) ile de öncelikle bankacılık hizmetleri olmak üzere kullanıcı yetkilendirme ve parola bilgilerini çalmak amaçlanıyor.

Açıklamada, bankacılık hizmetlerinden yararlanan tüm kullanıcıların bu tür sahte e-postalara itibar etmeden silmeleri gerektiği, kurumların da saldırı tespit sistemlerindeki önlemleri güncellemelerinin yararlı olacağı belirtildi.

GÜNCEL HABERLER

Zeus'lu vurguna polis operasyonu

Habip ATAM / İSTANBUL, (DHA) 22 Şubat 2013

İstanbul Bilişim Suçlarla Mücadele Şube Müdürlüğü ekipleri banka müşterilerinin internet hesaplarına "Zeus" adlı virüsle girerek boşalttığı öne sürülen şüphelilere operasyon düzenledi. İstanbul, Antalya ve Kocaeli'de düzenlenen operasyonlarda 18 kişi gözaltına alındı. Şebekenin, 19 hesaptan 742 bin 206 TL'yi kendi belirledikleri hesaba aktardıkları öğrenildi

İstanbul Bilişim Suçlarla Mücadele Şube Müdürlüğü ekipleri, 4 ay önce virüs göndererek banka müşterilerinin internet hesaplarına giren bir şebekeyi tespit et Yapılan takipte şebekenin ele başlığını Ayhan A.'nın yaptığı, şebeke üyesi 2 bilgisayar korsanının da Rusya'da olduğu belirlendi. Ayrıca şebeke üyesi 6 kişi ile hesaplarını şebekeye kullandıran 9 kişi daha tespit edildi. Tespitlerin ardından 4 gün önce yapılan operasyonla şebeke elebaşının da aralarında bulunduğu 15 şüpheli İstanbul'da, 2 şüpheli Antalya'da, 1 şüpheli ise Kocaeli'de gözaltına alındı.

742 BİN 206 TL PARAYI BELİRLENEN HESAPLARA AKTARDILAR

Polisin takip ettiği şebekenin Rusya'daki 2 Türk bilgisayar korsanı yardımıyla 19 ayrı hesaptan toplam 742 bin TL'yi belirlenen hesaplara aktardığı tespit edildi. EFT ve havale yoluyla aktardığı tespit edilen bu paranın 210 bin 772 TL'lik kısmına polis bloke koydurdu. 531 bin 434 TL'sinin bir kısmının Türkiye'deki şebeke üyeleri arasında paylaşıldığı büyük kısmının ise Rusya'daki bazı hesaplara aktarıldığı belirtildi.

"ZEUS" VE "ZİTMO" VİRÜSLERİNİ KULLANDILAR

Şebeke üyelerinin bilgisayardaki internet hesaplarını ele geçirmek için genellikle mail yoluyla gönderdikleri "Zeus" adlı virüs programını kullandıkları belirtildi. Cep telefonu bilgilerini ele geçirmek için ise şebeke üyesi 2 bilgisayar korsanının "Zitmo" adlı virüsü kullandıkları öğrenildi.

KOMİSYON KARŞILIĞI HESAPLARINI KULLANDIRDILAR

Polisin yaptığı çalışmada şebeke üyelerinin dikkat çekmesin diye farklı hesaplara para havale ettikleri tespit edildi. Bunun için şebeke üyelerinin bankada hesabı olan bazı kişilerle komisyon karşılığı anlaştığı iddia edildi. .

GÖRÜNTÜLER KAMERALARA DA YANSIDI

Yapılan operasyon görüntüleri polis kameralarına da yansıdı. Görüntülerde polisin bir adrese girmesi bir şüpheliyi yere yatırarak gözaltına alması ve evde arama yapması görülüyor. Ayrıca şebekenin anlaştığı ve komisyon karşılığı hesaplarını kullandığı iddia edilen şüphelilerin bankadan para çekme anları da banka güvenlik kameralarına yansıdı. O görüntülerde şüphelilerin banka veznesine gelerek para çekme anları görülüyor.

POLİS UYARDI

Polis, bilgisayar kullanıcılarını özellikle lisanslı yeni sürüm antivirüs programı kullanmaları konusunda uyardı. Polisin yaptığı operasyonda gözaltına alınan 18 kişi Çaglayan'daki İstanbul Adliyesi'ne sevk edildi.

GÜNCEL HABERLER

‘Hırsız virüs’ alarmı

Nerdun Hacıoğlu /MOSKOVA

10.08.2012 | A A

Siber casus yazılım Flame, Stuxnet ve Duqu virüslerini ortaya çıkartan Rusya’daki antivirüs laboratuarı Kaspersky, şimdi de bankalardan kimlik bilgisi ve para çalmaya başlayan süper hırsız “Gauss” virüsü alarmı verdi.

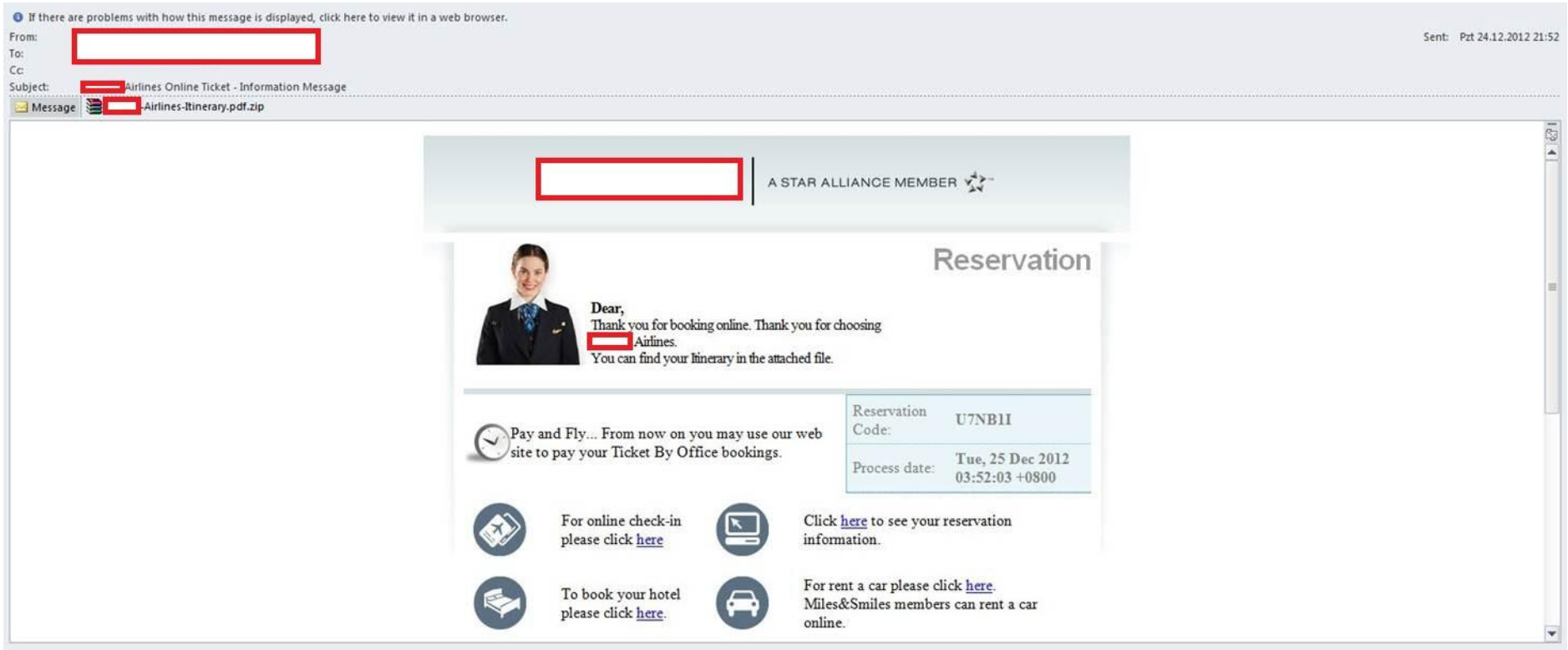
Kaspersky şirketinin Moskova’daki merkezinden basına yapılan açıklamada yeni Truva atı virüsü ünlü Alman matematikçi Carl Friedrich Gauss adını taşıyor ve “Gauss” olarak tanımlanıyor. Yazılımın ilk şifreleri çözüldüğünde bunun da Flami, Stuxnet ve Doqu virüslerini hazırlayan kişi veya ülke tarafından hazırlandığının tespit edildiğini de belirten Kaspersky, “Önceki üç komplike virüs sıradan insanlara zarar vermiyordu. Sadece sabotaj ve sanayi casusluğu için kullanılıyordu.

Ancak yeni bulgu “Gauss” virüsü siber savaşın yön değiştirdiğini ve gezegenimizde herkesi yakından ilgilendirdiğini göstermeye başladı. Bu virüs şu an Lübnan’daki bankalar ağırlıklı olmak üzere müşterilerin kimlik bilgileriyle hesaplarından para çalmaya başladı. Truva atı Gauss virüsünü keşfettiğimizden beri Lübnan’da 1660, İsrail’de 483 ve Filistin topraklarında 261 kişinin banka hesabı hacklandı” açıklamasını yaptı.

Kaspersky laboratuarı “Gauss” virüsünü etkisiz hale getirmek için şu anda alınacak önlemler üzerinde çalışmaya devam ettiklerini de bildirdi. Nerdun

FATMAL

Ekteki dosyayı çalıştırmayacak kaç kişi tanıyorsunuz ?



FATMAL

Ekteki dosyayı çalıştırmayacak kaç kişi tanıyorsunuz ?

Message Fatura_Bildirimi.pdf.zip (36 KB)

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

[redacted] www.[redacted].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
[redacted] İletişim Hizmetleri A.Ş.

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

[redacted] Faturanızı Hemen Ödemek İçin Tıklayınız

[redacted] Ödeme Kanallarını Görmek İçin Tıklayınız

NEDEN ZARARLI YAZILIM ANALİZİ ?

«Düşmanı tanımak, tehlikeyi bertaraf etmek demektir.»
Fatih Sultan Mehmet

Bir sonraki hedef çalışanlarınız ve/veya müşterileriniz olabilir!

Bilgisayar olayları müdahalesinde acil aksiyon almak için kilit nokta olabilir.

Basit sızma girişimleri yerini APT saldırılarına bıraktı. (NYT)

Güvenlik yazılımları/cihazları/sistemleri zararlı yazılımları tespit etmekte yetersiz!

BLACKHOLE vs ANTIVIRUS

Tarih: 22.06.2012

Zararlı Site Ziyaret Tarihi	URL	AV Tespit Tarihi	Ülke
18/06/2012 14:33:00 EEST	http://bell.madhousedomains.com/Set.jar	-	Rusya
18/06/2012 14:33:00 EEST	http://bowl.taxpainkiller.com/Set.jar	-	Rusya
11/06/2012 21:10:58 EEST	http://tellmeonlygoodnews.org/l/Set.jar	-	Rusya
11/06/2012 21:10:58 EEST	http://diving-pleasure.com/l/Set.jar	-	Rusya
08/06/2012 12:05:44 EEST	http://zhdrzfkzq.changeip.name/images/334857960/c17267280eeb8b395c2abca7085a2944.jar	-	-
08/06/2012 11:56:06 EEST	http://ca.miraclestove.org/Half.jar	-	Rusya
08/06/2012 11:56:06 EEST	http://home-page.ezua.com/Half.jar	-	Kazakistan
08/06/2012 11:56:06 EEST	http://shop.rxpillcenter.com/Half.jar	-	Rusya
06/06/2012 19:20:43 EEST	http://kioiwrsd.tk/33982.jar	22.06.2012	Rusya
06/06/2012 19:20:43 EEST	http://gkiqaue.tk/33982.jar	-	-

NELER YAPABİLİRİZ?

Davranışsal (Behavioral) Analizi:

Artısı: Yazılım hakkında kolay ve kısa sürede bilgi toplanır
Eksisi: Bilgilerin doğruluğundan emin olmak oldukça güçtür.

Kod Analizi:

Artısı: Yazılım hakkında detaylı ve doğru bilgi elde edilir.
Eksisi: Zor ve zaman alıcıdır.

Bellek Analizi:

Artısı: Zararlı yazılımın en korunmasız hali elde edilir.
Eksisi: Bilgilerin doğruluğundan emin olmak oldukça güçtür

Ofansif Analiz:

Artısı: Çalınan bilgiler tespit edilebilir.
Eksisi: Deliller istenmeden karartılabilir.

LAB 101

Fiziksel Makine:

Yüksek maliyet, Kullanım zorluğu vs Anti VM kontrolleri

Sanal Makine:

Düşük maliyet, Pratik kullanım vs Anti VM kontrolleri

Her iki durumda da üretim ortamından izole edilmelidir.

Sanal makine kullanılacak ise Host Only Networking kullanılmalıdır!

Sanal makine uygulamasının yamaları güncel olmalıdır!

VMWare Tools ve eşlenikleri kaldırılmalıdır!

DAVRANIŞSAL ANALİZ

Çevrim Dışı Analiz:

İzleme araçları sanal makineye kopyalanır ve çalıştırılır.

Zararlı yazılım sanal/fiziksel makineye kopyalanır ve çalıştırılır.

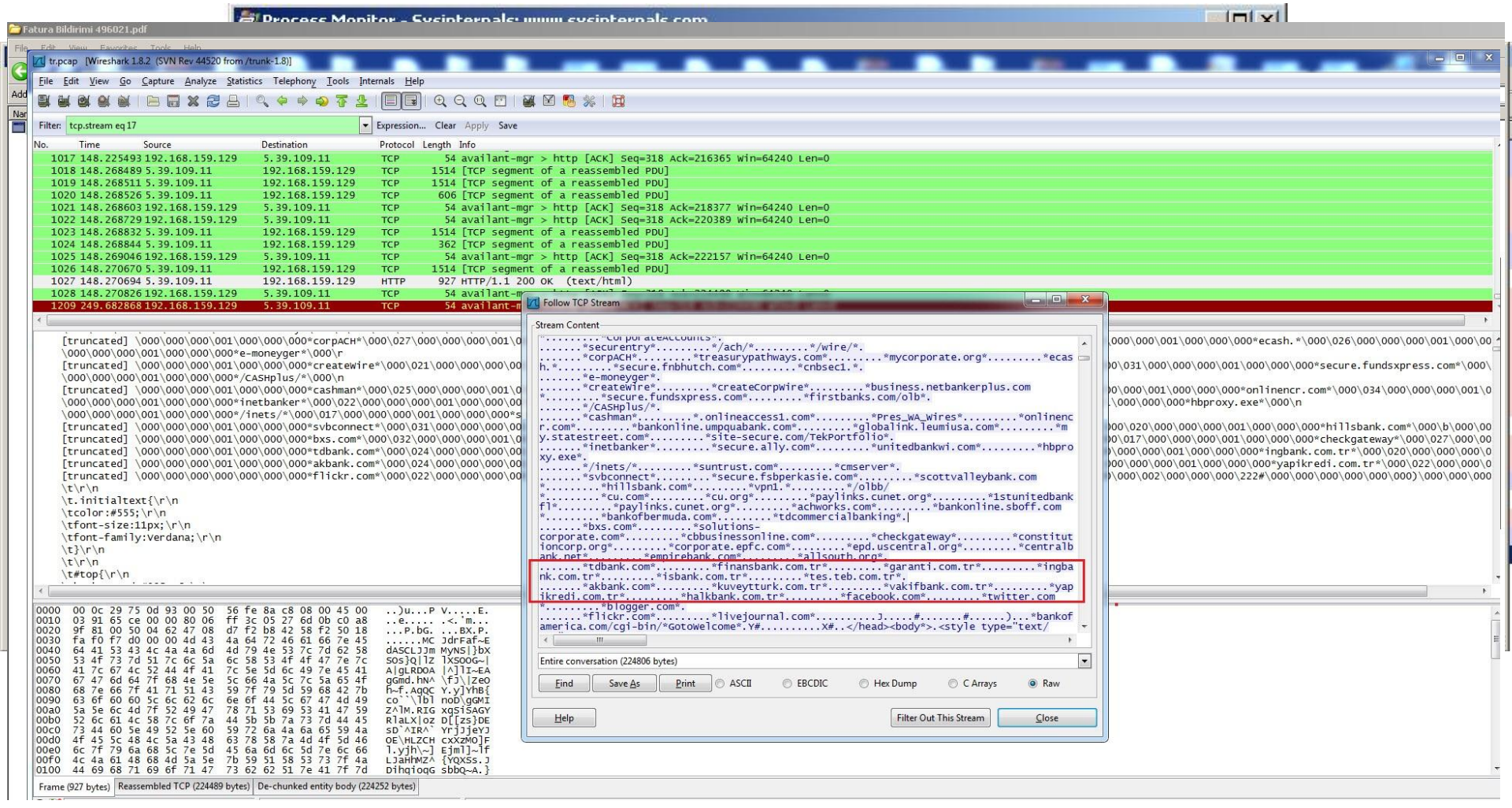
Zararlı yazılım ve izleme araçları sonlandırılır.

Kayıtlar incelenerek şüpheli hareketler tespit edilir.

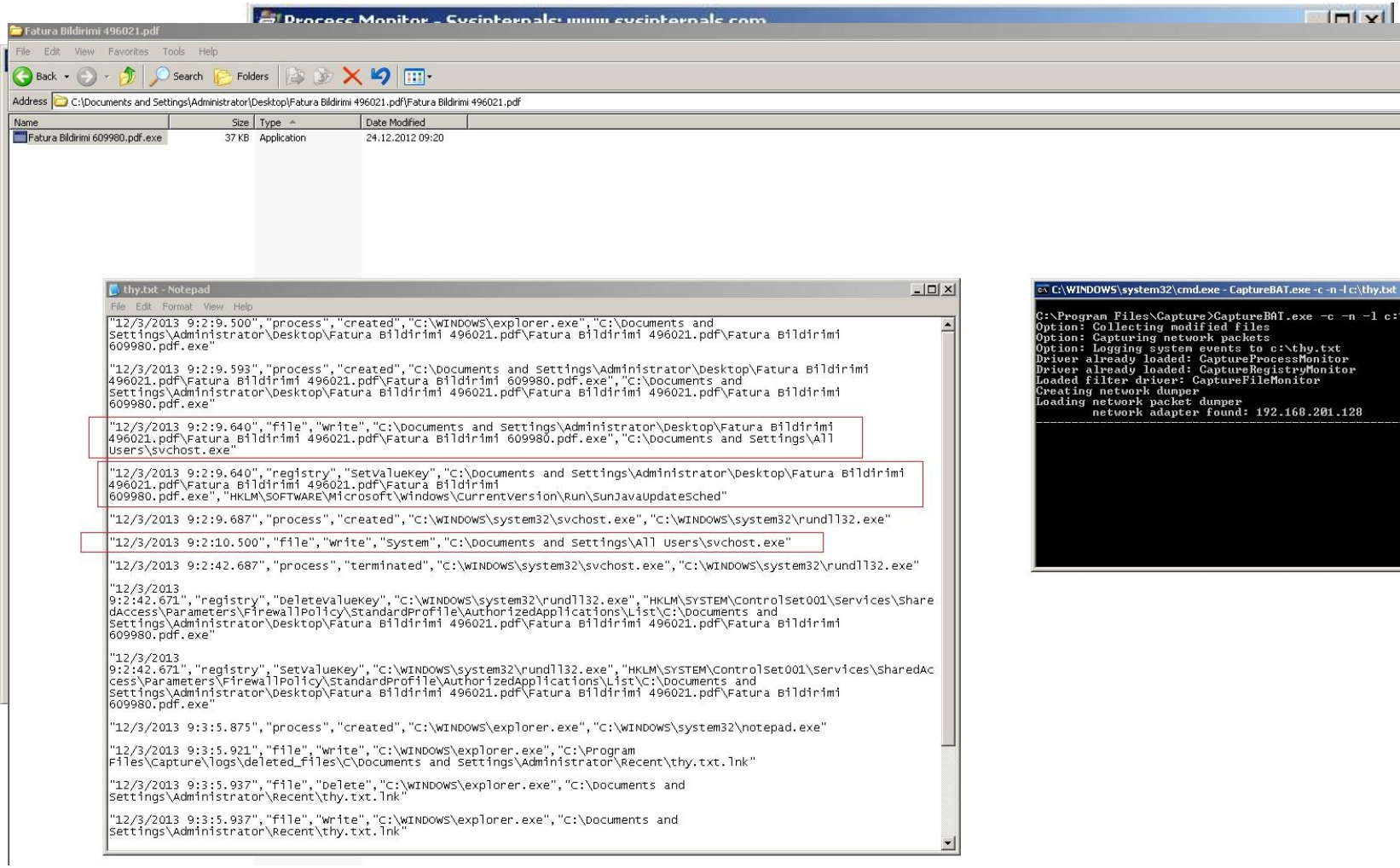
Popüler Araçlar: Process Monitor, Process Explorer, Wireshark, CaptureBat, Cuckoo Sandbox

Çevrim İçi Analiz: ThreatExpert, Anubis, Malwr, VirusTotal

ARAÇLAR


Process Monitor - Sysinternals: www.sysinternals.com
Fatura Bildirimi 496021.pdf
tr.pcap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 17
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1017 148.225493 192.168.159.129 5.39.109.11 TCP 54 availant-mgr > http [ACK] Seq=318 Ack=216365 Win=64240 Len=0
1018 148.268489 5.39.109.11 192.168.159.129 TCP 1514 [TCP segment of a reassembled PDU]
1019 148.268511 5.39.109.11 192.168.159.129 TCP 1514 [TCP segment of a reassembled PDU]
1020 148.268526 5.39.109.11 192.168.159.129 TCP 606 [TCP segment of a reassembled PDU]
1021 148.268603 192.168.159.129 5.39.109.11 TCP 54 availant-mgr > http [ACK] Seq=318 Ack=218377 Win=64240 Len=0
1022 148.268729 192.168.159.129 5.39.109.11 TCP 54 availant-mgr > http [ACK] Seq=318 Ack=220389 Win=64240 Len=0
1023 148.268832 5.39.109.11 192.168.159.129 TCP 1514 [TCP segment of a reassembled PDU]
1024 148.268844 5.39.109.11 192.168.159.129 TCP 362 [TCP segment of a reassembled PDU]
1025 148.269046 192.168.159.129 5.39.109.11 TCP 54 availant-mgr > http [ACK] Seq=318 Ack=222157 Win=64240 Len=0
1026 148.270670 5.39.109.11 192.168.159.129 TCP 1514 [TCP segment of a reassembled PDU]
1027 148.270694 5.39.109.11 192.168.159.129 HTTP 927 HTTP/1.1 200 OK (text/html)
1028 148.270826 192.168.159.129 5.39.109.11 TCP 54 availant-mgr
1209 249.682868 192.168.159.129 5.39.109.11 TCP 54 availant-mgr
Follow TCP Stream
Stream Content
Entire conversation (224806 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
Frame (927 bytes) Reassembled TCP (224489 bytes) De-chunked entity body (224252 bytes)

ARAÇLAR


Process Monitor - Sysinternals: www.sysinternals.com
Fatura Bildirimi 496021.pdf
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 496021.pdf
Name Size Type Date Modified
Fatura Bildirimi 609980.pdf.exe 37 KB Application 24.12.2012 09:20
thy.txt - Notepad
File Edit Format View Help
"12/3/2013 9:2:9.500","process","created","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 609980.pdf.exe"
"12/3/2013 9:2:9.593","process","created","C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 609980.pdf.exe","C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 609980.pdf.exe"
"12/3/2013 9:2:9.640","file","Write","C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 609980.pdf.exe","C:\Documents and Settings\All Users\svchost.exe"
"12/3/2013 9:2:9.640","registry","SetValueKey","C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 609980.pdf.exe","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SunJavaUpdateSched"
"12/3/2013 9:2:9.687","process","created","C:\WINDOWS\system32\svchost.exe","C:\WINDOWS\system32\rundll32.exe"
"12/3/2013 9:2:10.500","file","Write","System","C:\Documents and Settings\All Users\svchost.exe"
"12/3/2013 9:2:42.687","process","terminated","C:\WINDOWS\system32\svchost.exe","C:\WINDOWS\system32\rundll32.exe"
"12/3/2013 9:2:42.671","registry","DeleteValueKey","C:\WINDOWS\system32\rundll32.exe","HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 609980.pdf.exe"
"12/3/2013 9:2:42.671","registry","SetValueKey","C:\WINDOWS\system32\rundll32.exe","HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 496021.pdf\Fatura Bildirimi 609980.pdf.exe"
"12/3/2013 9:3:5.875","process","created","C:\WINDOWS\explorer.exe","C:\WINDOWS\system32\notepad.exe"
"12/3/2013 9:3:5.921","file","Write","C:\WINDOWS\explorer.exe","C:\Program Files\Capture\logs\deleted_files\C\Documents and Settings\Administrator\Recent\thy.txt.lnk"
"12/3/2013 9:3:5.937","file","Delete","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Recent\thy.txt.lnk"
"12/3/2013 9:3:5.937","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Recent\thy.txt.lnk"
C:\WINDOWS\system32\cmd.exe - CaptureBAT.exe -c -n -l c:\thy.txt
C:\Program Files\Capture>CaptureBAT.exe -c -n -l c:\thy.txt
Option: Collecting modified files
Option: Capturing network packets
Option: Logging system events to c:\thy.txt
Driver already loaded: CaptureProcessMonitor
Driver already loaded: CaptureRegistryMonitor
Loaded filter driver: CaptureFileMonitor
Creating network dumper
Loading network packet dumper
network adapter found: 192.168.201.128

ARAÇLAR

1. General Information

- Information about Anubis' invocation

Time needed:	82 s
Report created:	12/24/12, 13:47:04 UTC
Termination reason:	All tracked processes have exited
Program version:	1.76.3886

2. Turkish-Ai.exe

- General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	Turkish-Ai.exe
MD5:	c7c39fea16c34d867b586fd155dca77a
SHA-1:	9883922c5d1dd23494db58effa3098046e25164f
File Size:	37376 Bytes
Command Line:	"C:\Turkish-Ai.exe"
Process-status at analysis end:	dead
Exit Code:	0

- Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000

2.a) Turkish-Ai.exe - File Activities

- File System Control Communication:

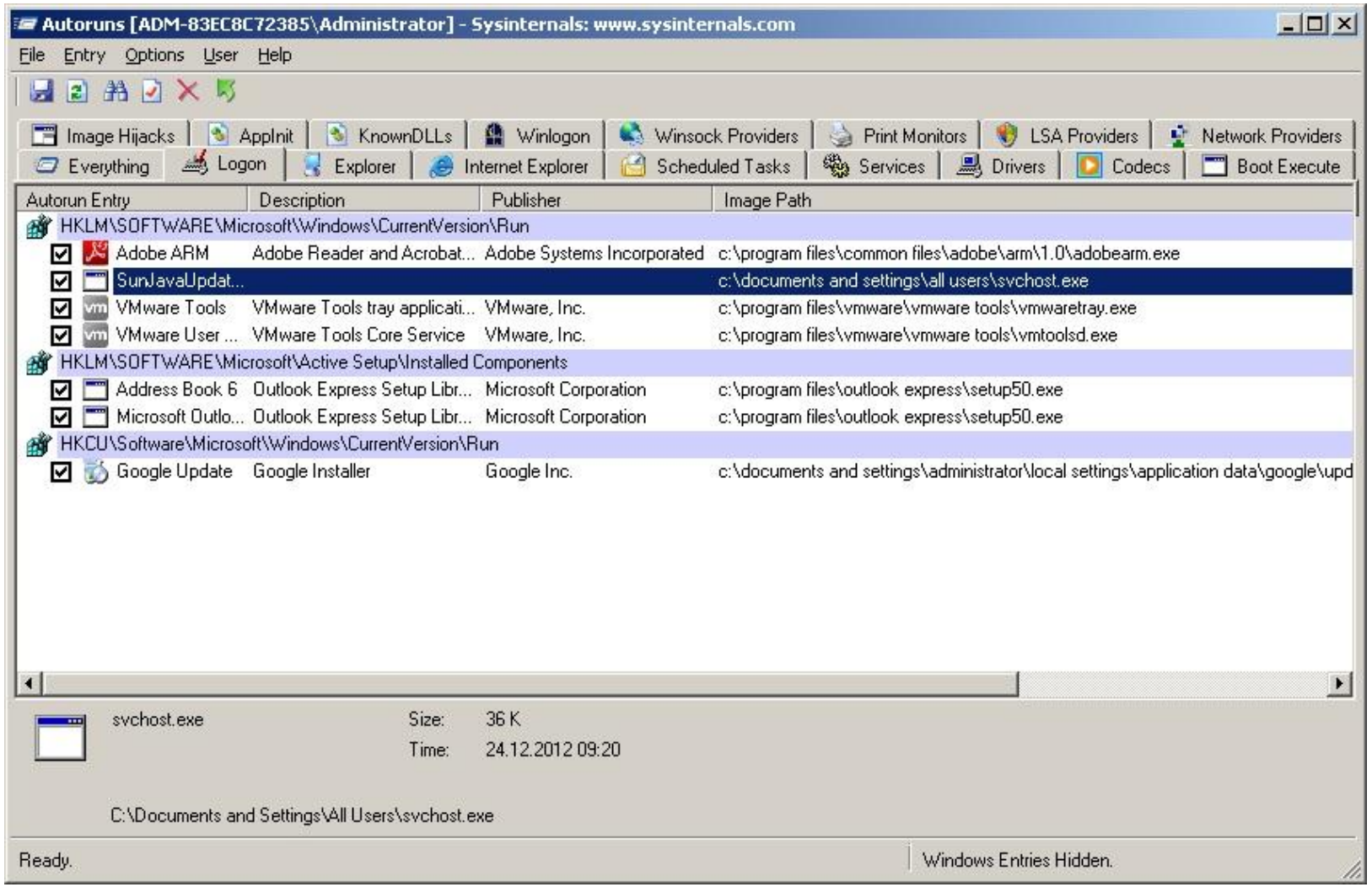
File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1

2.b) Turkish-Ai.exe - Other Activities

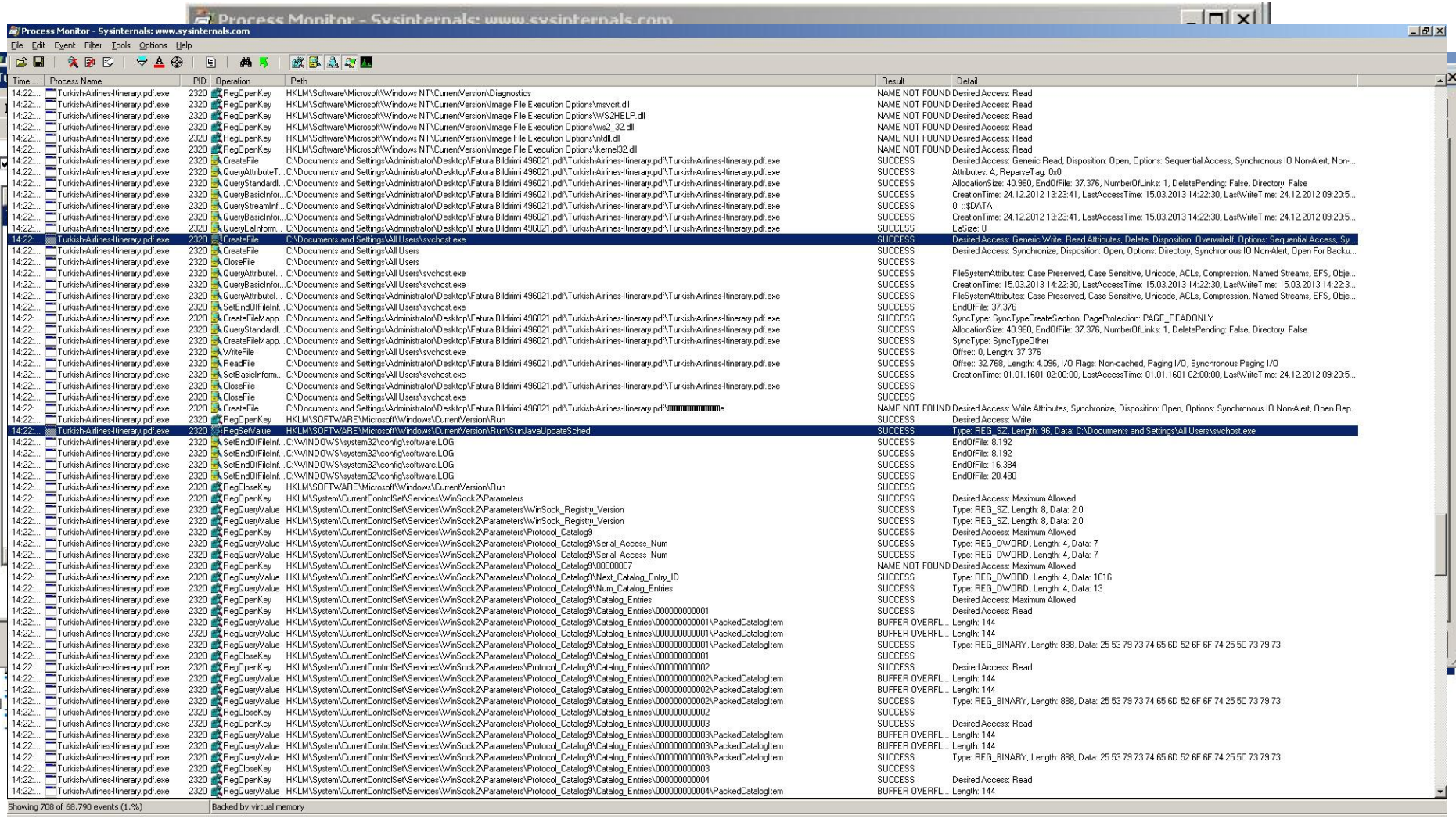
- Windows SEH exceptions:

Description	Times
Exception 0xc0000005 (STATUS_ACCESS_VIOLATION) at 0x401121	1

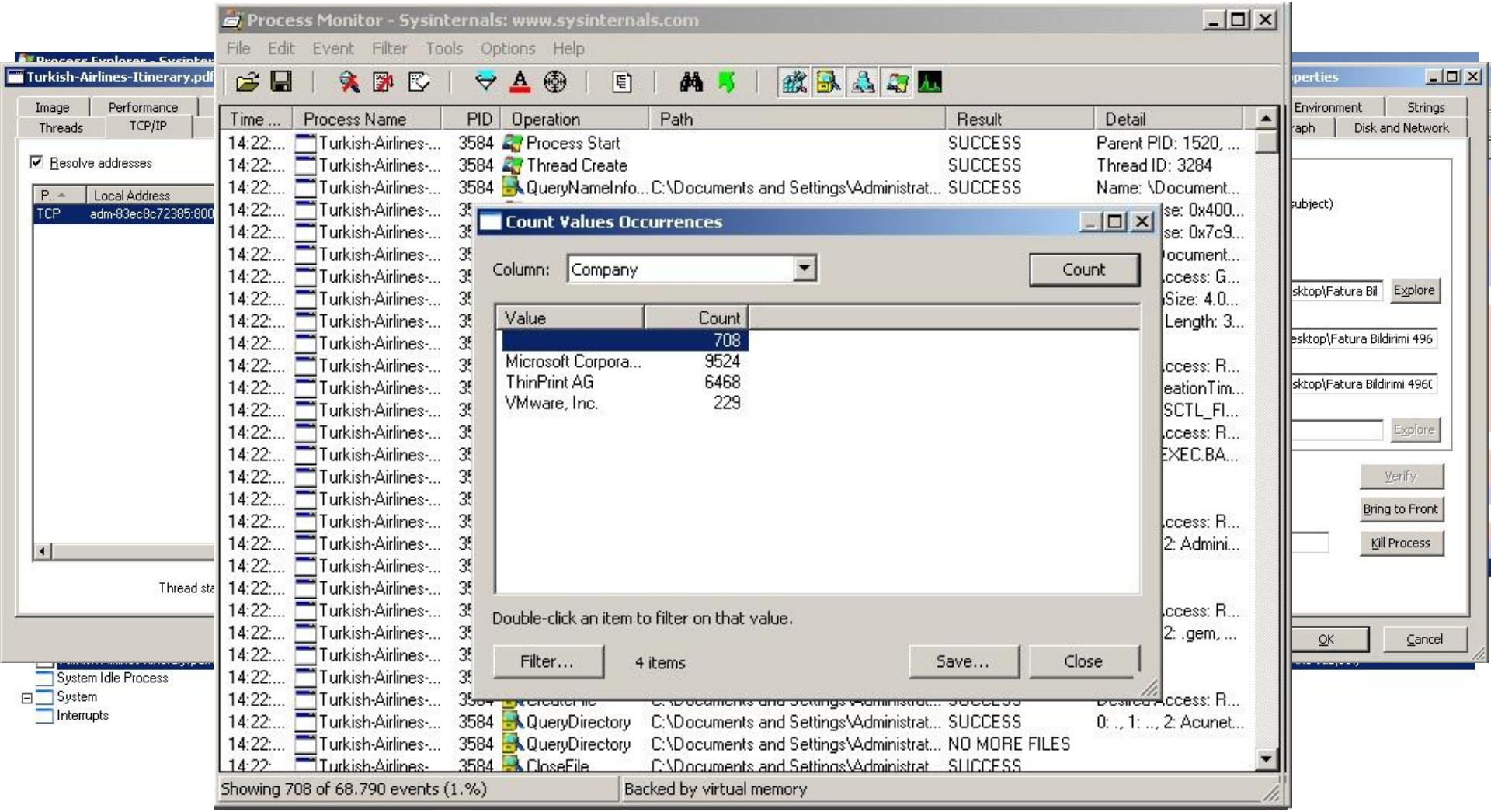
ARAÇLAR


Autoruns [ADM-83EC8C72385\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Image Hijacks AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute
Autorun Entry Description Publisher Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Adobe ARM Adobe Reader and Acrobat... Adobe Systems Incorporated c:\program files\common files\adobe\arm\1.0\adobearm.exe
SunJavaUpdat... c:\documents and settings\all users\svchost.exe
VMware Tools VMware Tools tray applicati... VMware, Inc. c:\program files\vmware\vmware tools\vmwaretray.exe
VMware User ... VMware Tools Core Service VMware, Inc. c:\program files\vmware\vmware tools\vmtoolsd.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
Address Book 6 Outlook Express Setup Libr... Microsoft Corporation c:\program files\outlook express\setup50.exe
Microsoft Outlo... Outlook Express Setup Libr... Microsoft Corporation c:\program files\outlook express\setup50.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Google Update Google Installer Google Inc. c:\documents and settings\administrator\local settings\application data\google\upd
svchost.exe
Size: 36 K
Time: 24.12.2012 09:20
C:\Documents and Settings\All Users\svchost.exe
Ready.
Windows Entries Hidden.

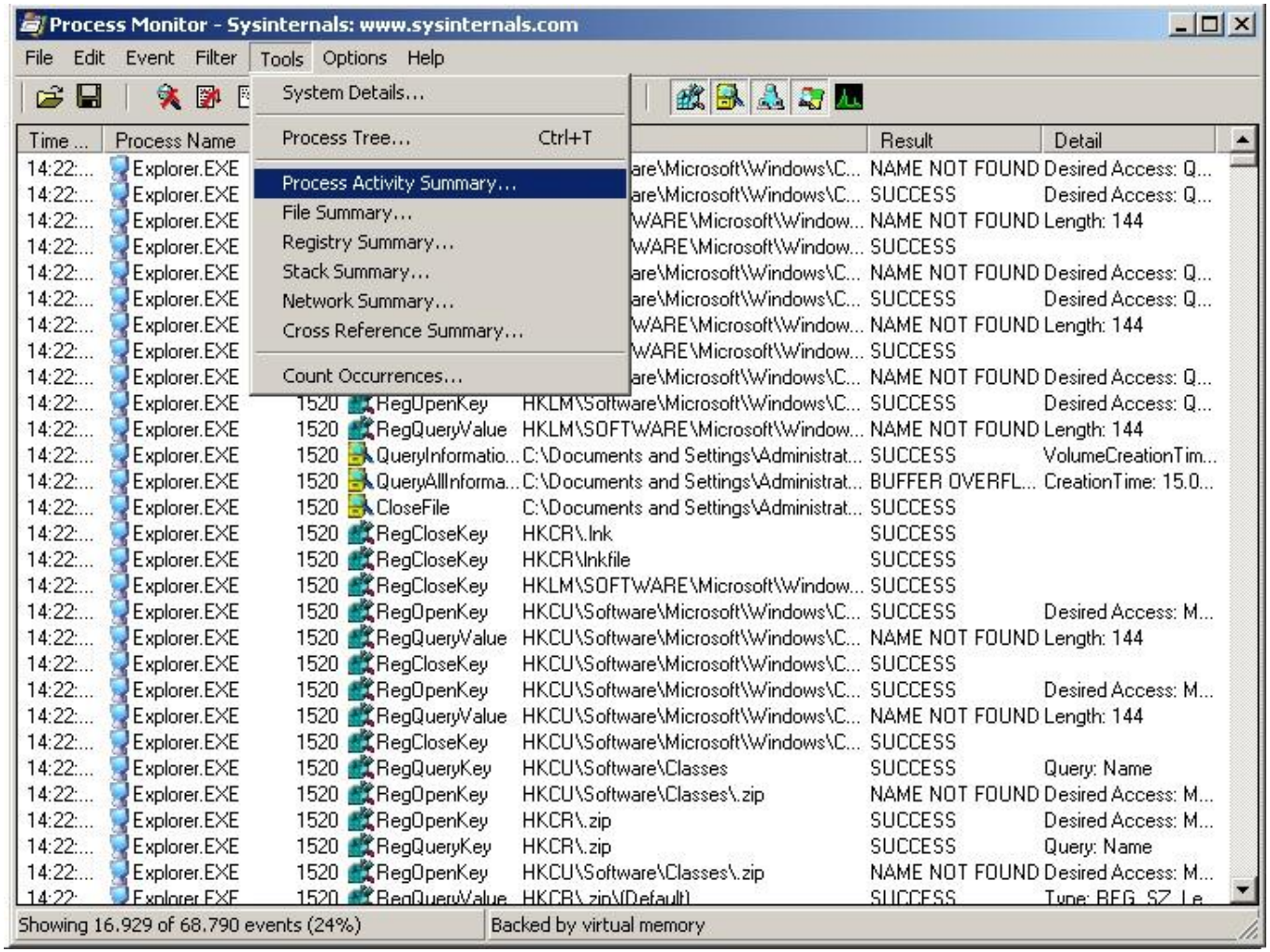
ARAÇLAR


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Showing 708 of 68.790 events (1.%)
Backed by virtual memory

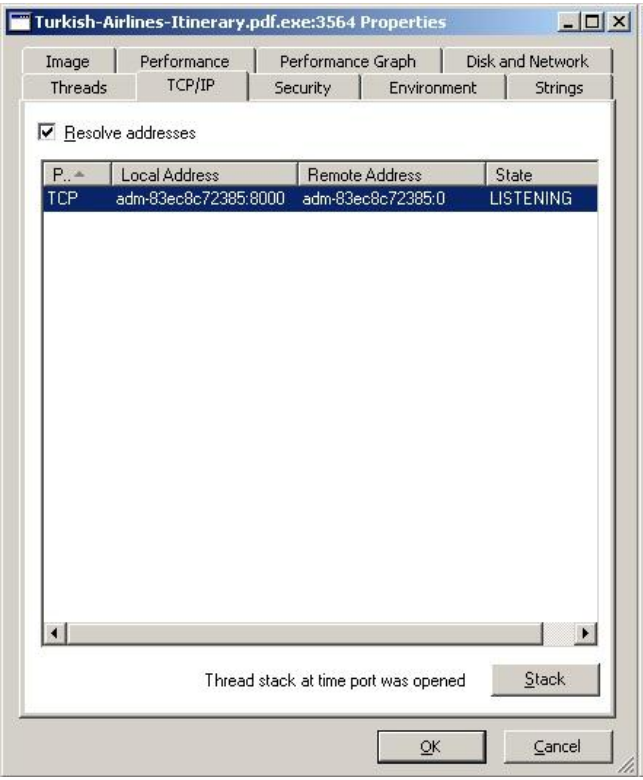
ARAÇLAR

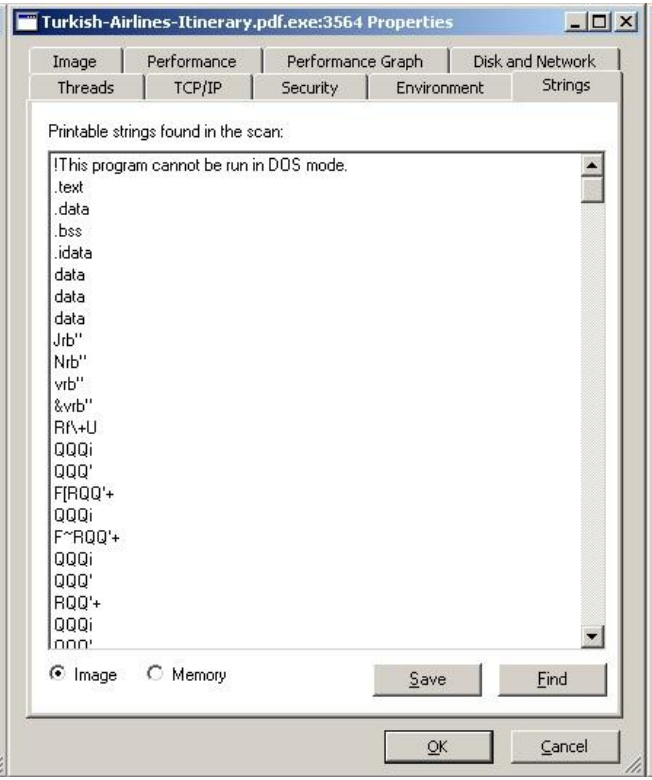

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
14:22:... Turkish-Airlines-... 3584 Process Start SUCCESS Parent PID: 1520, ...
14:22:... Turkish-Airlines-... 3584 Thread Create SUCCESS Thread ID: 3284
14:22:... Turkish-Airlines-... 3584 QueryNameInfo... C:\Documents and Settings\Administrat... SUCCESS Name: \Document...
Count Values Occurrences
Column: Company
Count
Value Count
708
Microsoft Corpora... 9524
ThinPrint AG 6468
VMware, Inc. 229
Double-click an item to filter on that value.
Filter...
4 items
Save...
Close
14:22:... Turkish-Airlines-... 3584 QueryDirectory C:\Documents and Settings\Administrat... SUCCESS 0: ., 1: .., 2: Acunet...
14:22:... Turkish-Airlines-... 3584 QueryDirectory C:\Documents and Settings\Administrat... NO MORE FILES
Showing 708 of 68.790 events (1.%)
Backed by virtual memory
Turkish-Airlines-Itinerary.pdf
Resolve addresses
Local Address
TCP adm-83ec8c72385:800
System Idle Process
System
Interrupts
Explore
Verify
Bring to Front
Kill Process
OK
Cancel

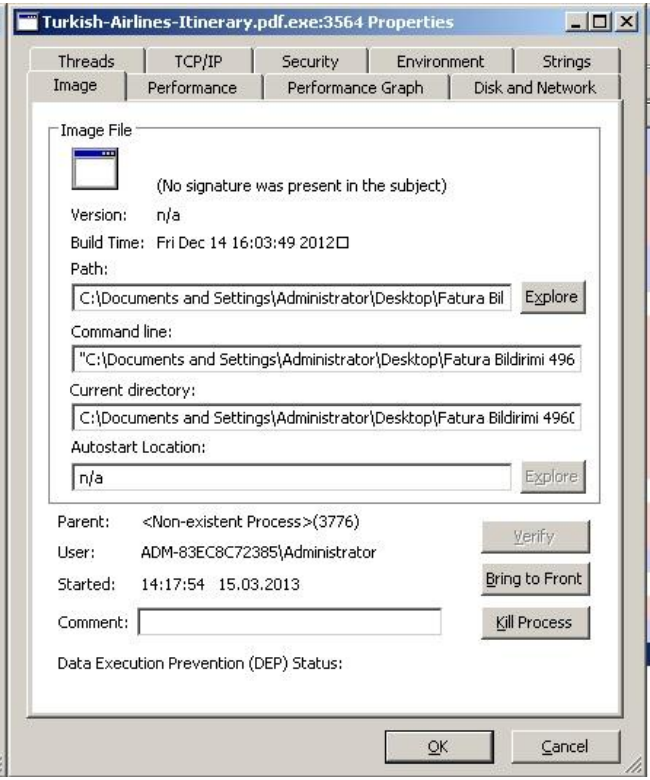
ARAÇLAR


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
System Details...
Process Tree... Ctrl+T
Process Activity Summary...
File Summary...
Registry Summary...
Stack Summary...
Network Summary...
Cross Reference Summary...
Count Occurrences...
Time ... Process Name Result Detail
Showing 16.929 of 68.790 events (24%)
Backed by virtual memory

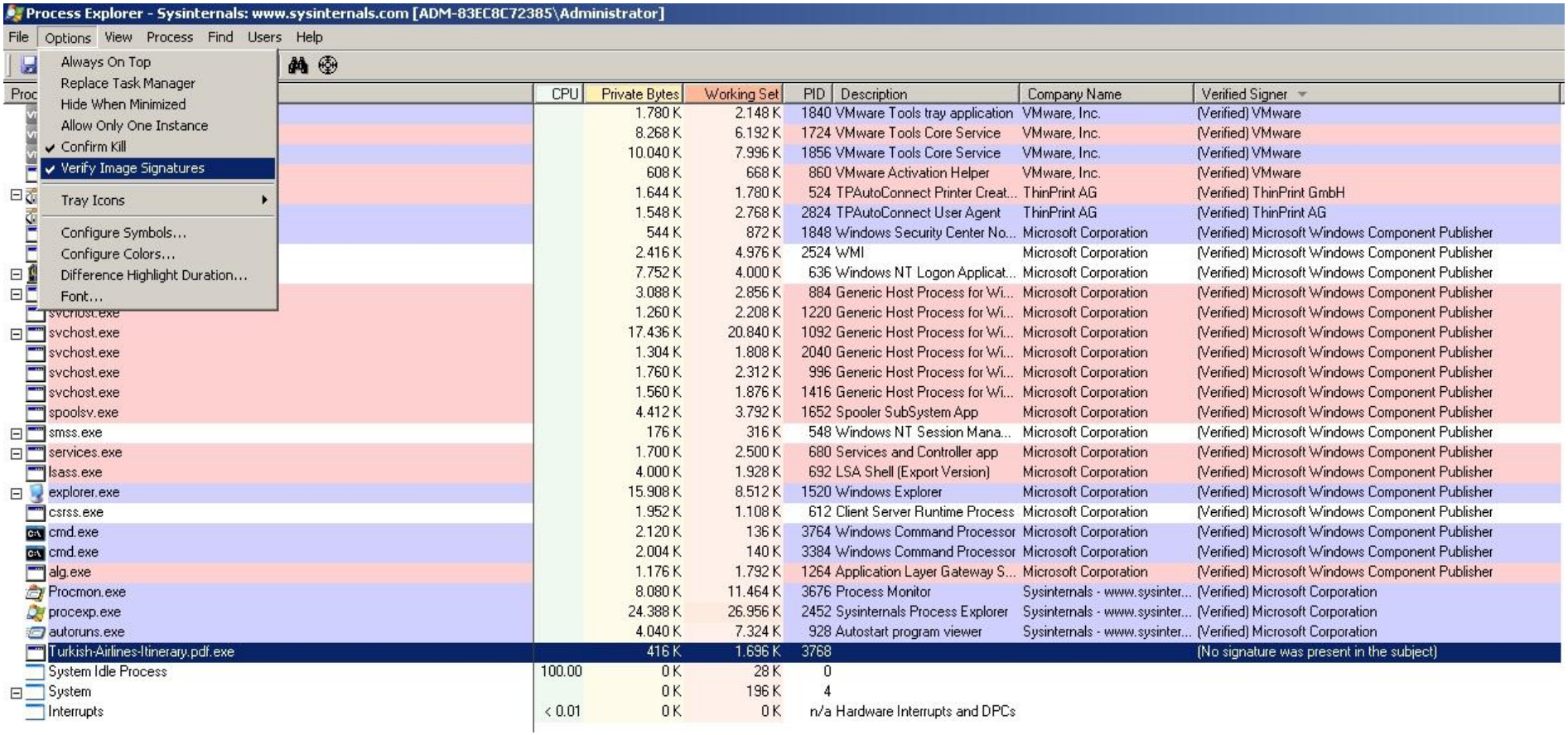
ARAÇLAR


Turkish-Airlines-Itinerary.pdf.exe:3564 Properties
Image
Performance
Performance Graph
Disk and Network
Threads
TCP/IP
Security
Environment
Strings
Resolve addresses
P..
Local Address
Remote Address
State
TCP
adm-83ec8c72385:8000
adm-83ec8c72385:0
LISTENING
Thread stack at time port was opened
Stack
OK
Cancel


Turkish-Airlines-Itinerary.pdf.exe:3564 Properties
Image
Performance
Performance Graph
Disk and Network
Threads
TCP/IP
Security
Environment
Strings
Printable strings found in the scan:
!This program cannot be run in DOS mode.
.text
.data
.bss
.idata
data
data
data
Jrb''
Nrb''
vrb''
&vrb''
Rf\+U
QQQi
QQQ'
F[RQQ'+
QQQi
F^RQQ'+
QQQi
QQQ'
RQQ'+
QQQi
Image
Memory
Save
Find
OK
Cancel


Turkish-Airlines-Itinerary.pdf.exe:3564 Properties
Threads
TCP/IP
Security
Environment
Strings
Image
Performance
Performance Graph
Disk and Network
Image File
(No signature was present in the subject)
Version: n/a
Build Time: Fri Dec 14 16:03:49 2012
Path:
C:\Documents and Settings\Administrator\Desktop\Fatura Bil
Explore
Command line:
"C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496
Current directory:
C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496(
Autostart Location:
n/a
Explore
Parent: <Non-existent Process>(3776)
User: ADM-83EC8C72385\Administrator
Started: 14:17:54 15.03.2013
Comment:
Verify
Bring to Front
Kill Process
Data Execution Prevention (DEP) Status:
OK
Cancel

ARAÇLAR


Process Explorer - Sysinternals: www.sysinternals.com [ADM-83EC8C72385\Administrator]
File Options View Process Find Users Help
Always On Top
Replace Task Manager
Hide When Minimized
Allow Only One Instance
Confirm Kill
Verify Image Signatures
Tray Icons
Configure Symbols...
Configure Colors...
Difference Highlight Duration...
Font...
CPU Private Bytes Working Set PID Description Company Name Verified Signer
svchost.exe 17.436 K 20.840 K 1092 Generic Host Process for Wi... Microsoft Corporation [Verified] Microsoft Windows Component Publisher
svchost.exe 1.304 K 1.808 K 2040 Generic Host Process for Wi... Microsoft Corporation [Verified] Microsoft Windows Component Publisher
svchost.exe 1.760 K 2.312 K 996 Generic Host Process for Wi... Microsoft Corporation [Verified] Microsoft Windows Component Publisher
svchost.exe 1.560 K 1.876 K 1416 Generic Host Process for Wi... Microsoft Corporation [Verified] Microsoft Windows Component Publisher
spoolsv.exe 4.412 K 3.792 K 1652 Spooler SubSystem App Microsoft Corporation [Verified] Microsoft Windows Component Publisher
smss.exe 176 K 316 K 548 Windows NT Session Mana... Microsoft Corporation [Verified] Microsoft Windows Component Publisher
services.exe 1.700 K 2.500 K 680 Services and Controller app Microsoft Corporation [Verified] Microsoft Windows Component Publisher
lsass.exe 4.000 K 1.928 K 692 LSA Shell (Export Version) Microsoft Corporation [Verified] Microsoft Windows Component Publisher
explorer.exe 15.908 K 8.512 K 1520 Windows Explorer Microsoft Corporation [Verified] Microsoft Windows Component Publisher
csrss.exe 1.952 K 1.108 K 612 Client Server Runtime Process Microsoft Corporation [Verified] Microsoft Windows Component Publisher
cmd.exe 2.120 K 136 K 3764 Windows Command Processor Microsoft Corporation [Verified] Microsoft Windows Component Publisher
cmd.exe 2.004 K 140 K 3384 Windows Command Processor Microsoft Corporation [Verified] Microsoft Windows Component Publisher
alg.exe 1.176 K 1.792 K 1264 Application Layer Gateway S... Microsoft Corporation [Verified] Microsoft Windows Component Publisher
Procmon.exe 8.080 K 11.464 K 3676 Process Monitor Sysinternals - www.sysinter... [Verified] Microsoft Corporation
procexp.exe 24.388 K 26.956 K 2452 Sysinternals Process Explorer Sysinternals - www.sysinter... [Verified] Microsoft Corporation
autoruns.exe 4.040 K 7.324 K 928 Autostart program viewer Sysinternals - www.sysinter... [Verified] Microsoft Corporation
Turkish-Airlines-Itinerary.pdf.exe 416 K 1.696 K 3768 (No signature was present in the subject)
System Idle Process 100.00 0 K 28 K 0
System 0 K 196 K 4
Interrupts < 0.01 0 K 0 K n/a Hardware Interrupts and DPCs

STATİK KOD ANALİZİ

Yazılım çalıştırılmadan assembly seviyesinde analiz edilir.

PE başlık bilgileri analiz edilerek yazılım hakkında bilgi toplanır.

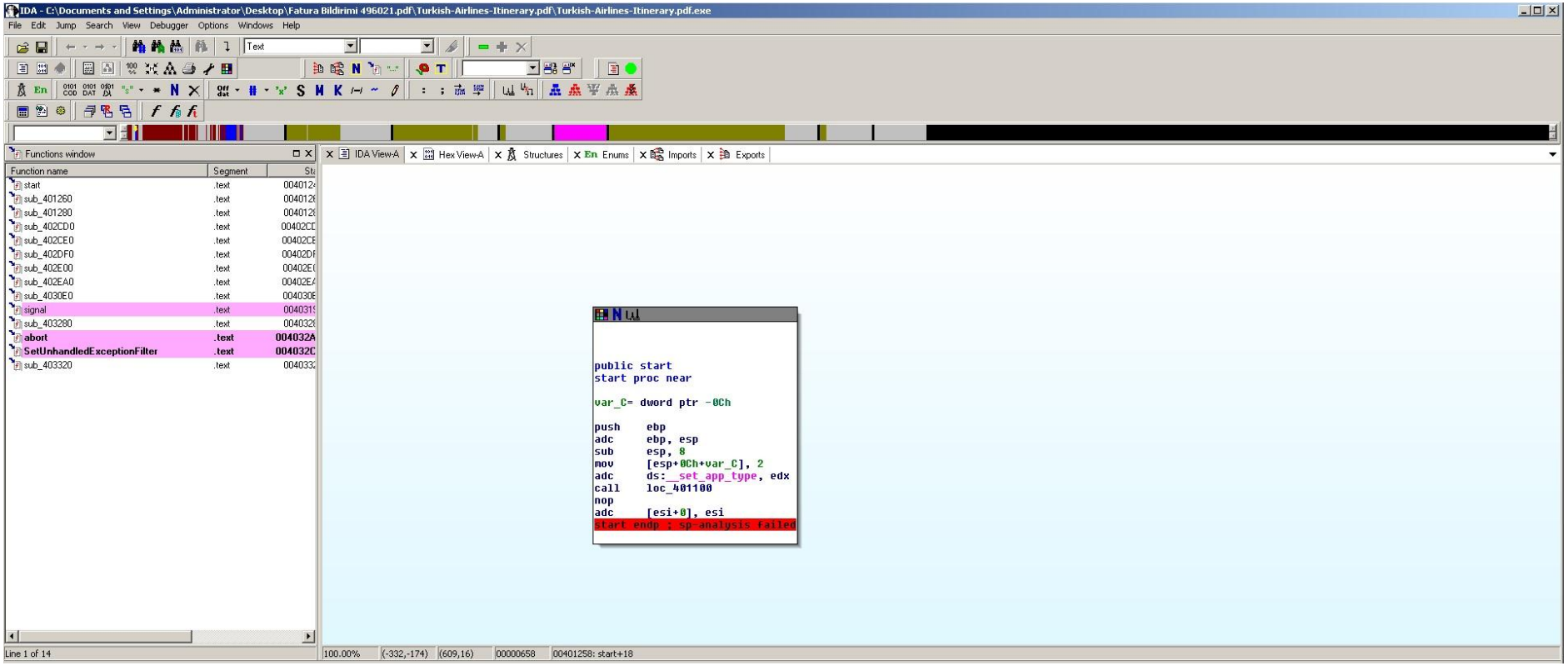
Import/Export tabloları şüpheli fonksiyonları içerebilir.

Karakter dizilerinden ipucu elde edilmeye çalışılır. (strings)

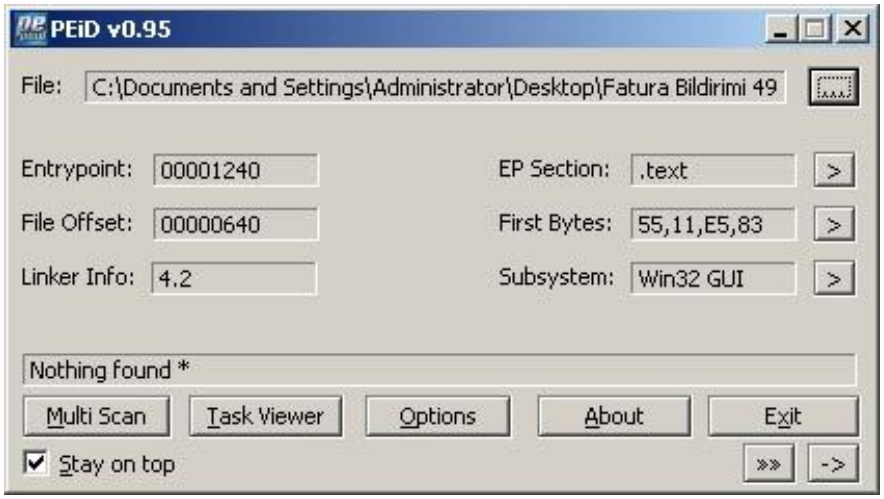
Decompiler ile yazılım detaylı analiz için kaynak koduna çevrilebilir.

Popüler Araçlar: BinText, strings, PE Explorer, IDA Pro, Dependency Walker, dumpbin, PEiD, Peview, JAD, Hex-Rays, Reflector

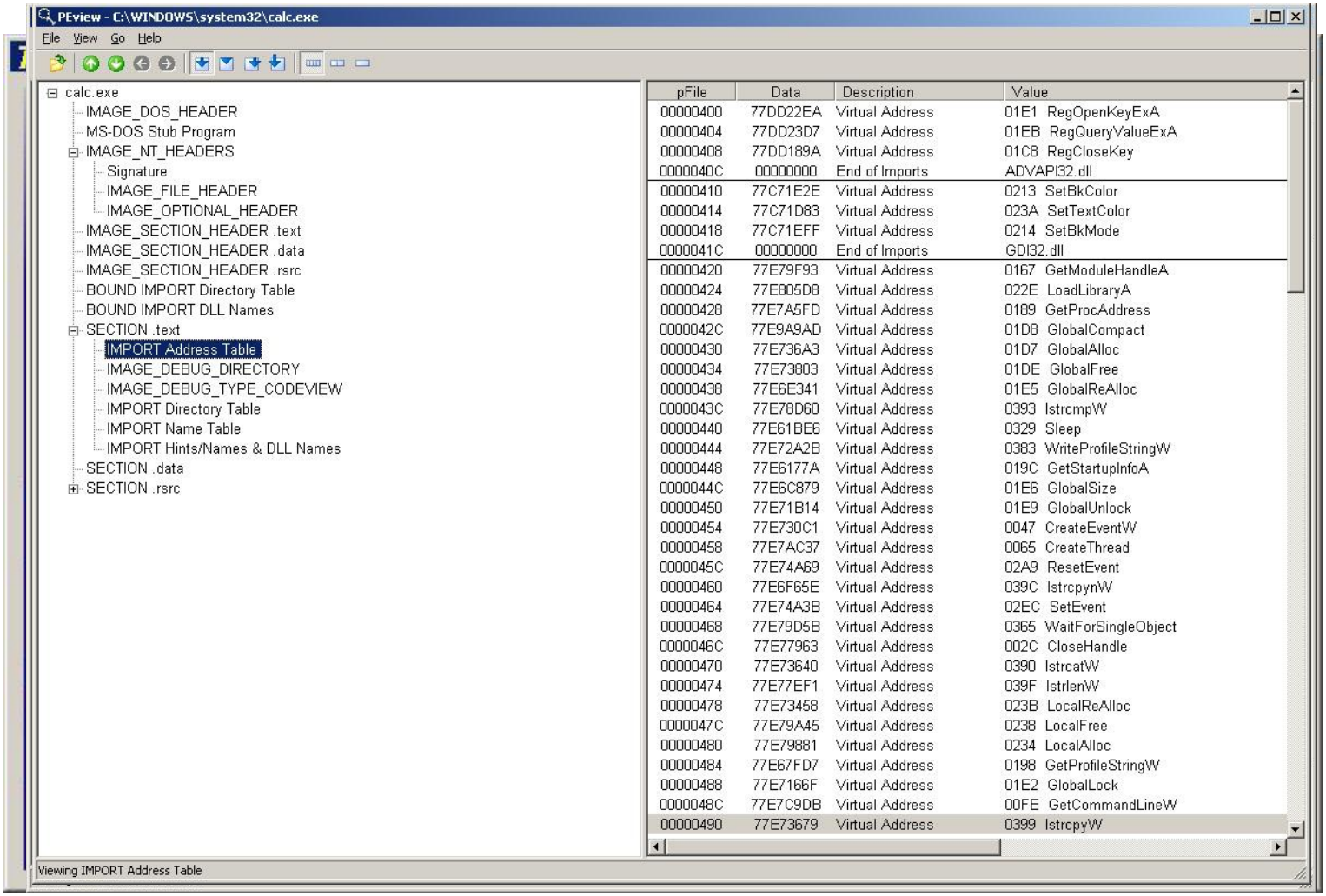
ARAÇLAR


IDA - C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Turkish-Airlines-Itinerary.pdf\Turkish-Airlines-Itinerary.pdf.exe
File Edit Jump Search View Debugger Options Windows Help
Functions window
Function name
Segment
start .text
sub_401260 .text
sub_401280 .text
sub_402CD0 .text
sub_402CE0 .text
sub_402DF0 .text
sub_402E00 .text
sub_402EA0 .text
sub_4030E0 .text
signal .text
sub_403280 .text
abort .text
SetUnhandledExceptionFilter .text
sub_403320 .text
IDA View-A
Hex View-A
Structures
Enums
Imports
Exports
public start
start proc near
var_C= dword ptr -0Ch
push ebp
adc ebp, esp
sub esp, 8
mov [esp+0Ch+var_C], 2
adc ds:__set_app_type, edx
call loc_401100
nop
adc [esi+0], esi
start endp ; sp-analysis failed
Line 1 of 14
100.00% (-332,-174) (609,16) 00000658 00401258: start+18

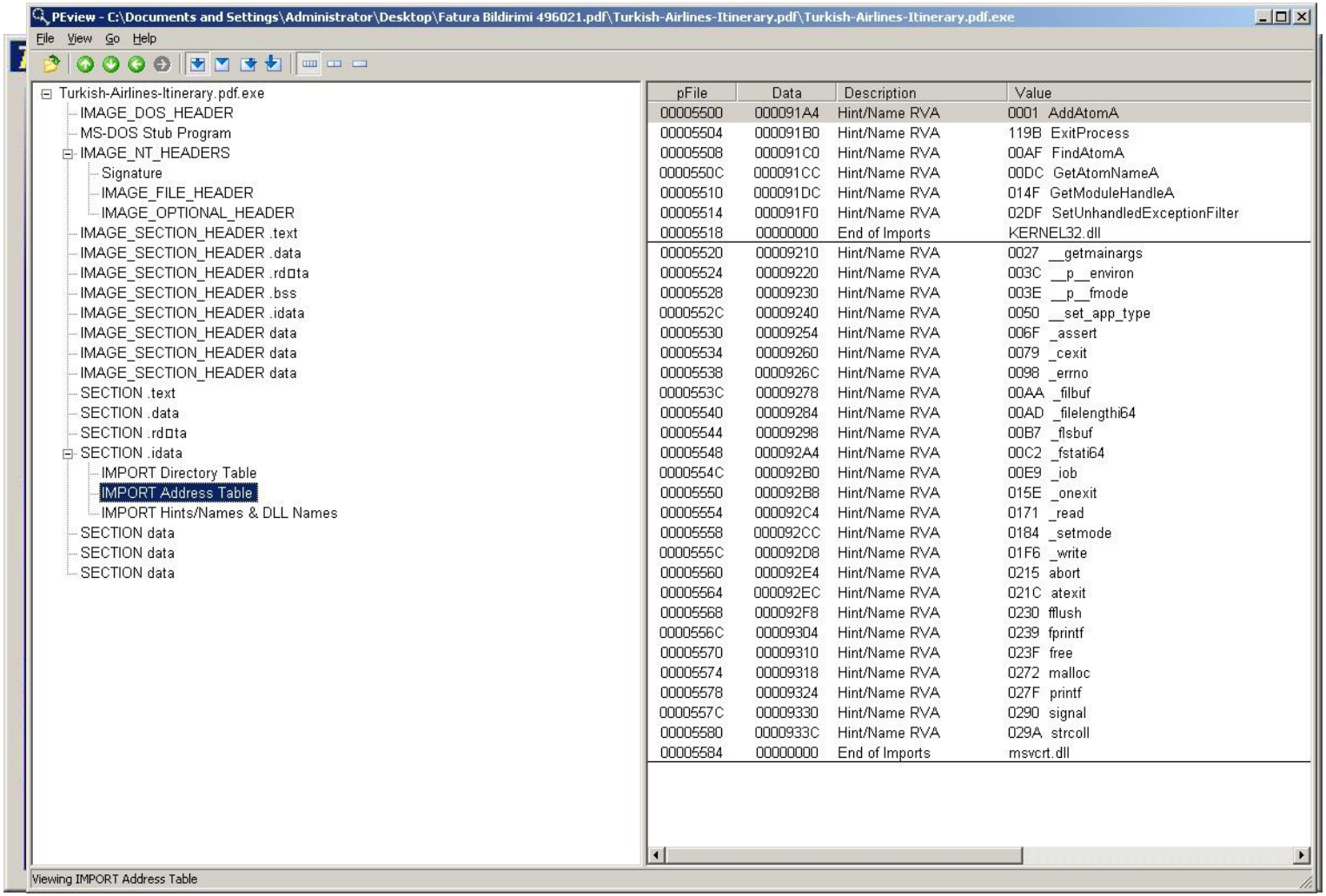
ARAÇLAR


PEiD v0.95
File:
C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 49
Entrypoint:
00001240
EP Section:
.text
File Offset:
00000640
First Bytes:
55,11,E5,83
Linker Info:
4.2
Subsystem:
Win32 GUI
Nothing found *
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
->>

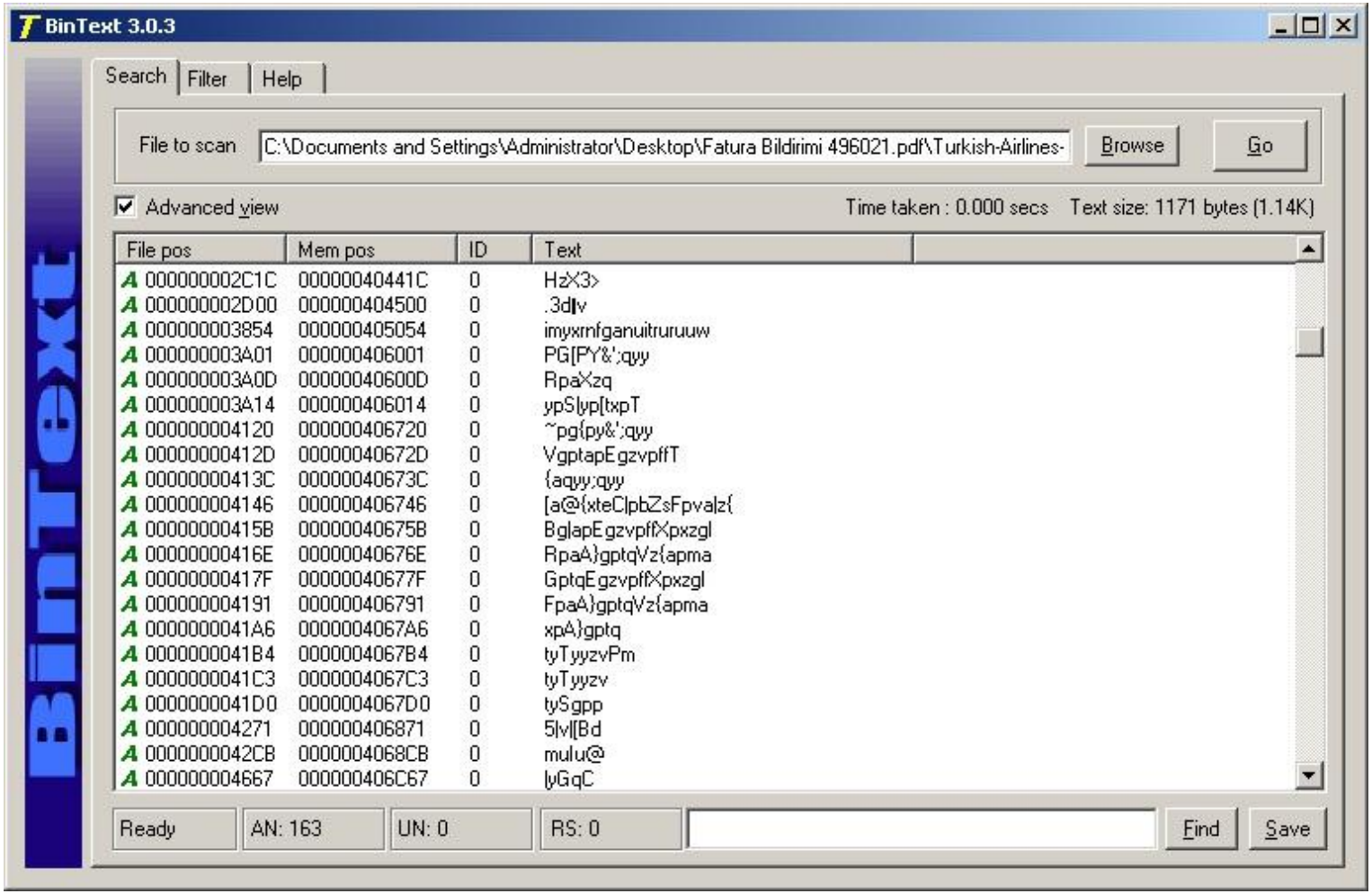
ARAÇLAR


PEview - C:\WINDOWS\system32\calc.exe
File View Go Help
calc.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
BOUND IMPORT Directory Table
BOUND IMPORT DLL Names
SECTION .text
IMPORT Address Table
IMAGE_DEBUG_DIRECTORY
IMAGE_DEBUG_TYPE_CODEVIEW
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION .rsrc
pFile Data Description Value
00000400 77DD22EA Virtual Address 01E1 RegOpenKeyExA
00000404 77DD23D7 Virtual Address 01EB RegQueryValueExA
00000408 77DD189A Virtual Address 01C8 RegCloseKey
0000040C 00000000 End of Imports ADVAPI32.dll
00000410 77C71E2E Virtual Address 0213 SetBkColor
00000414 77C71D83 Virtual Address 023A SetTextColor
00000418 77C71EFF Virtual Address 0214 SetBkMode
0000041C 00000000 End of Imports GDI32.dll
00000420 77E79F93 Virtual Address 0167 GetModuleHandleA
00000424 77E805D8 Virtual Address 022E LoadLibraryA
00000428 77E7A5FD Virtual Address 0189 GetProcAddress
0000042C 77E9A9AD Virtual Address 01D8 GlobalCompact
00000430 77E736A3 Virtual Address 01D7 GlobalAlloc
00000434 77E73803 Virtual Address 01DE GlobalFree
00000438 77E6E341 Virtual Address 01E5 GlobalReAlloc
0000043C 77E78D60 Virtual Address 0393 lstrcmpW
00000440 77E61BE6 Virtual Address 0329 Sleep
00000444 77E72A2B Virtual Address 0383 WriteProfileStringW
00000448 77E6177A Virtual Address 019C GetStartupInfoA
0000044C 77E6C879 Virtual Address 01E6 GlobalSize
00000450 77E71B14 Virtual Address 01E9 GlobalUnlock
00000454 77E730C1 Virtual Address 0047 CreateEventW
00000458 77E7AC37 Virtual Address 0065 CreateThread
0000045C 77E74A69 Virtual Address 02A9 ResetEvent
00000460 77E6F65E Virtual Address 039C lstrcpynW
00000464 77E74A3B Virtual Address 02EC SetEvent
00000468 77E79D5B Virtual Address 0365 WaitForSingleObject
0000046C 77E77963 Virtual Address 002C CloseHandle
00000470 77E73640 Virtual Address 0390 lstrcatW
00000474 77E77EF1 Virtual Address 039F lstrlenW
00000478 77E73458 Virtual Address 023B LocalReAlloc
0000047C 77E79A45 Virtual Address 0238 LocalFree
00000480 77E79881 Virtual Address 0234 LocalAlloc
00000484 77E67FD7 Virtual Address 0198 GetProfileStringW
00000488 77E7166F Virtual Address 01E2 GlobalLock
0000048C 77E7C9DB Virtual Address 00FE GetCommandLineW
00000490 77E73679 Virtual Address 0399 lstrcpyW
Viewing IMPORT Address Table

ARAÇLAR


PEview - C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Turkish-Airlines-Itinerary.pdf\Turkish-Airlines-Itinerary.pdf.exe
File View Go Help
Turkish-Airlines-Itinerary.pdf.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .bss
IMAGE_SECTION_HEADER .idata
IMAGE_SECTION_HEADER data
IMAGE_SECTION_HEADER data
IMAGE_SECTION_HEADER data
SECTION .text
SECTION .data
SECTION .rdata
SECTION .idata
IMPORT Directory Table
IMPORT Address Table
IMPORT Hints/Names & DLL Names
SECTION data
SECTION data
SECTION data
pFile Data Description Value
00005500 000091A4 Hint/Name RVA 0001 AddAtomA
00005504 000091B0 Hint/Name RVA 119B ExitProcess
00005508 000091C0 Hint/Name RVA 00AF FindAtomA
0000550C 000091CC Hint/Name RVA 00DC GetAtomNameA
00005510 000091DC Hint/Name RVA 014F GetModuleHandleA
00005514 000091F0 Hint/Name RVA 02DF SetUnhandledExceptionFilter
00005518 00000000 End of Imports KERNEL32.dll
00005520 00009210 Hint/Name RVA 0027 __getmainargs
00005524 00009220 Hint/Name RVA 003C __p__environ
00005528 00009230 Hint/Name RVA 003E __p__fmode
0000552C 00009240 Hint/Name RVA 0050 __set_app_type
00005530 00009254 Hint/Name RVA 006F _assert
00005534 00009260 Hint/Name RVA 0079 _cexit
00005538 0000926C Hint/Name RVA 0098 _errno
0000553C 00009278 Hint/Name RVA 00AA _filbuf
00005540 00009284 Hint/Name RVA 00AD _filelengthi64
00005544 00009298 Hint/Name RVA 00B7 _flsbuf
00005548 000092A4 Hint/Name RVA 00C2 _fstati64
0000554C 000092B0 Hint/Name RVA 00E9 _iob
00005550 000092B8 Hint/Name RVA 015E _onexit
00005554 000092C4 Hint/Name RVA 0171 _read
00005558 000092CC Hint/Name RVA 0184 _setmode
0000555C 000092D8 Hint/Name RVA 01F6 _write
00005560 000092E4 Hint/Name RVA 0215 abort
00005564 000092EC Hint/Name RVA 021C atexit
00005568 000092F8 Hint/Name RVA 0230 fflush
0000556C 00009304 Hint/Name RVA 0239 fprintf
00005570 00009310 Hint/Name RVA 023F free
00005574 00009318 Hint/Name RVA 0272 malloc
00005578 00009324 Hint/Name RVA 027F printf
0000557C 00009330 Hint/Name RVA 0290 signal
00005580 0000933C Hint/Name RVA 029A strcoll
00005584 00000000 End of Imports msvcrt.dll
Viewing IMPORT Address Table

ARAÇLAR


BinText 3.0.3
Search
Filter
Help
File to scan
C:\Documents and Settings\Administrator\Desktop\Fatura Bildirimi 496021.pdf\Turkish-Airlines-
Browse
Go
Advanced view
Time taken : 0.000 secs
Text size: 1171 bytes (1.14K)
File pos
Mem pos
ID
Text
A 000000002C1C 00000040441C 0 HzX3>
A 000000002D00 000000404500 0 .3dlv
A 000000003854 000000405054 0 imyxrnfganuitruruuw
A 000000003A01 000000406001 0 PG[PY&';qyy
A 000000003A0D 00000040600D 0 RpaXzq
A 000000003A14 000000406014 0 ypSlyp[txpT
A 000000004120 000000406720 0 ~pg{py&';qyy
A 00000000412D 00000040672D 0 VgptapEgzvpffT
A 00000000413C 00000040673C 0 {aqyy;qyy
A 000000004146 000000406746 0 [a@{xteClpbZsFpvalz{
A 00000000415B 00000040675B 0 BglapEgzvpffXpxzgl
A 00000000416E 00000040676E 0 RpaA}gptqVz{apma
A 00000000417F 00000040677F 0 GptqEgzvpffXpxzgl
A 000000004191 000000406791 0 FpaA}gptqVz{apma
A 0000000041A6 0000004067A6 0 xpA}gptq
A 0000000041B4 0000004067B4 0 tyTyyzvPm
A 0000000041C3 0000004067C3 0 tyTyyzv
A 0000000041D0 0000004067D0 0 tySgpp
A 000000004271 000000406871 0 5lvl[Bd
A 0000000042CB 0000004068CB 0 mulu@
A 000000004667 000000406C67 0 lyGqC
Ready
AN: 163
UN: 0
RS: 0
Find
Save
BinText

DİNAMİK KOD ANALİZİ

Yazılım çalıştırılarak assembly seviyesinde incelenir.

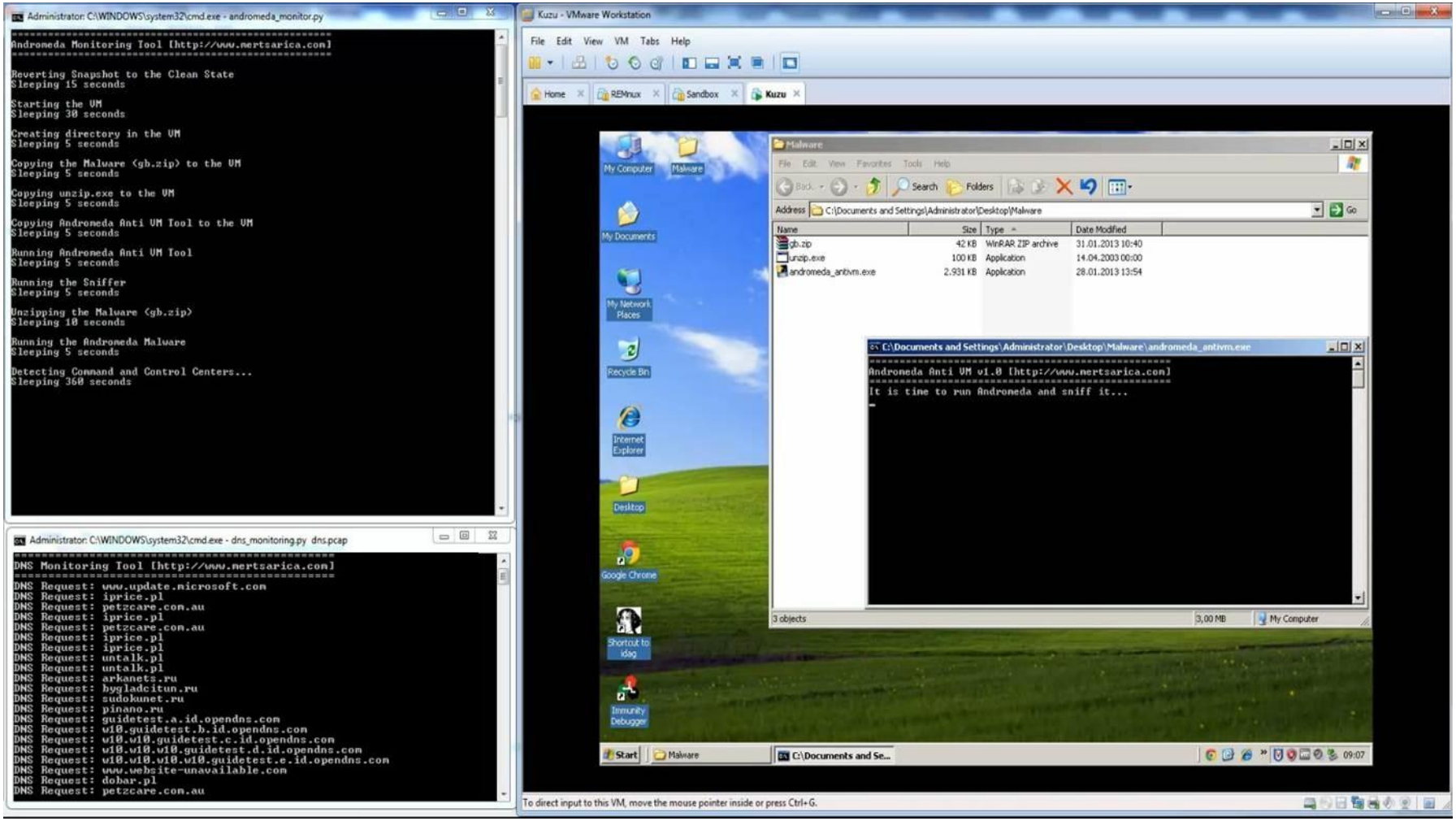
Diğer analiz yöntemlerine kıyasla en detaylı bilgi elde edilir.

Anti VM/Debugger/Disassembler kontrolleri devrede olabilir.

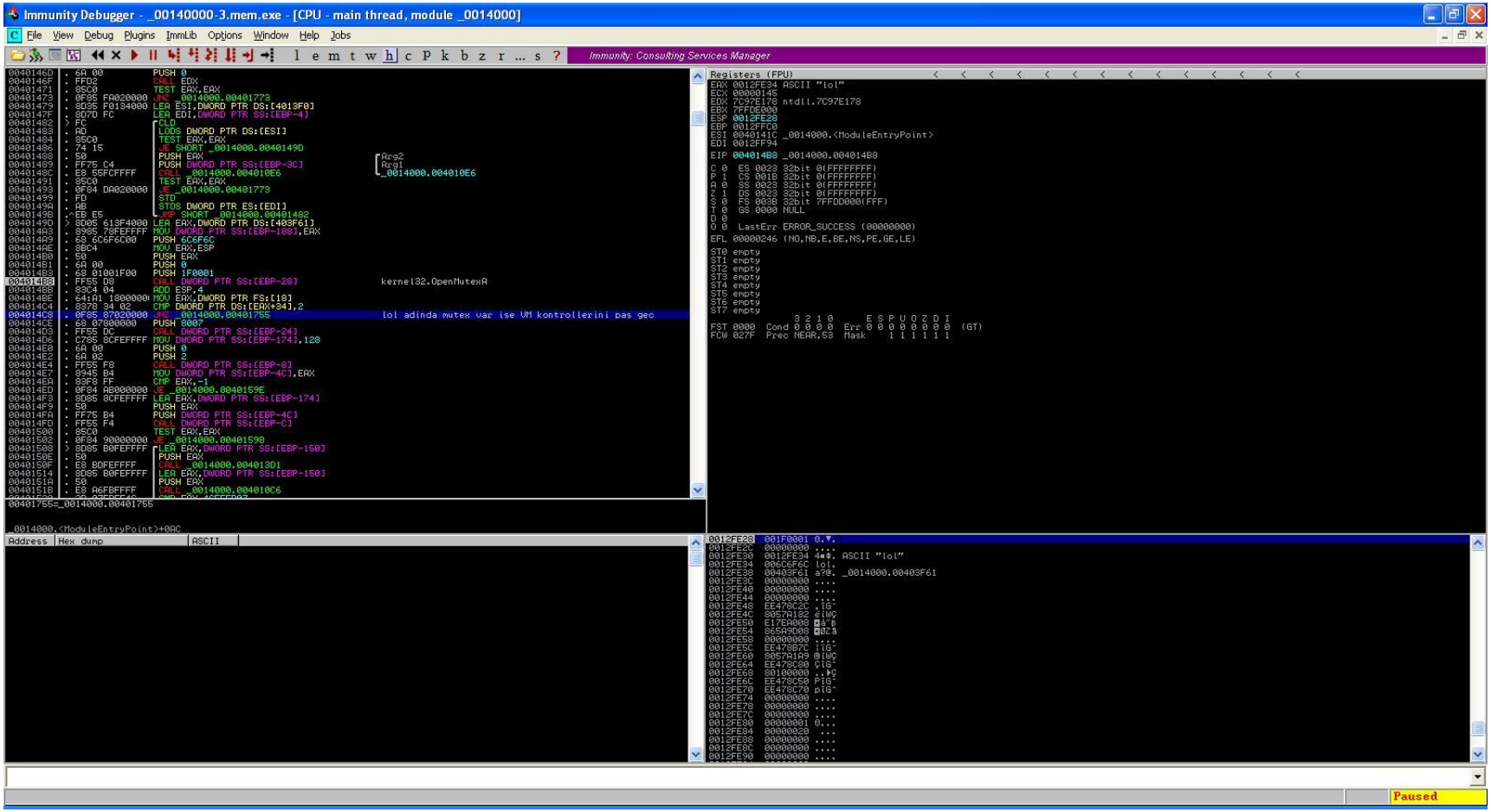
Paketi açılan, şifresi çözülen yazılımlar statik kod analizi için araçlar ve eklentiler yardımı ile DUMP edilebilir.

Popüler Araçlar: IDA Pro, Ollydbg, Immunity Debugger, Windbg, LordPE, OllyDump, ImpREC

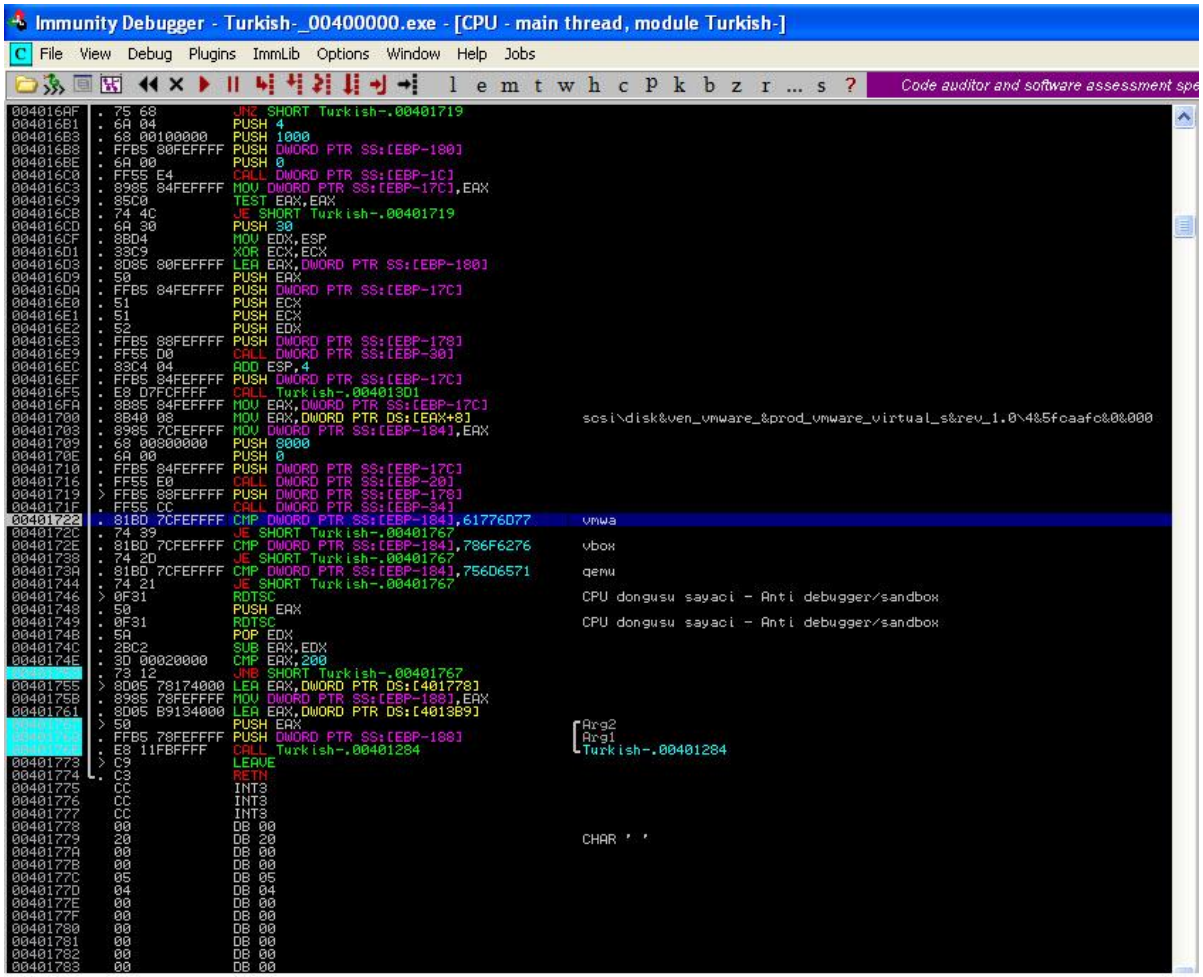
ARAÇLAR


Administrator: C:\WINDOWS\system32\cmd.exe - andromeda_monitor.py
Andromeda Monitoring Tool [http://www.mertsarica.com]
Reverting Snapshot to the Clean State
Sleeping 15 seconds
Starting the VM
Sleeping 30 seconds
Creating directory in the VM
Sleeping 5 seconds
Copying the Malware (gb.zip) to the VM
Sleeping 5 seconds
Copying unzip.exe to the VM
Sleeping 5 seconds
Copying Andromeda Anti VM Tool to the VM
Sleeping 5 seconds
Running Andromeda Anti VM Tool
Sleeping 5 seconds
Running the Sniffer
Sleeping 5 seconds
Unzipping the Malware (gb.zip)
Sleeping 10 seconds
Running the Andromeda Malware
Sleeping 5 seconds
Detecting Command and Control Centers...
Sleeping 360 seconds
Administrator: C:\WINDOWS\system32\cmd.exe - dns_monitoring.py dns.pcap
DNS Monitoring Tool [http://www.mertsarica.com]
DNS Request: www.update.microsoft.com
DNS Request: iprice.pl
DNS Request: petzcare.com.au
DNS Request: iprice.pl
DNS Request: petzcare.com.au
DNS Request: iprice.pl
DNS Request: iprice.pl
DNS Request: untalk.pl
DNS Request: untalk.pl
DNS Request: arkanets.ru
DNS Request: bygladcitun.ru
DNS Request: sudokunet.ru
DNS Request: pinano.ru
DNS Request: guidetest.a.id.opendns.com
DNS Request: w10.guidetest.b.id.opendns.com
DNS Request: w10.w10.guidetest.c.id.opendns.com
DNS Request: w10.w10.w10.guidetest.d.id.opendns.com
DNS Request: w10.w10.w10.w10.guidetest.e.id.opendns.com
DNS Request: www.website-unavailable.com
DNS Request: dobar.pl
DNS Request: petzcare.com.au
Kuzu - VMware Workstation
File Edit View VM Tabs Help
Home REMnux Sandbox Kuzu
Malware
Name Size Type Date Modified
gb.zip 42 KB WinRAR ZIP archive 31.01.2013 10:40
unzip.exe 100 KB Application 14.04.2003 00:00
andromeda_antivm.exe 2.931 KB Application 28.01.2013 13:54
C:\Documents and Settings\Administrator\Desktop\Malware\andromeda_antivm.exe
Andromeda Anti VM v1.0 [http://www.mertsarica.com]
It is time to run Andromeda and sniff it...
3 objects
3,00 MB
My Computer
Start
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

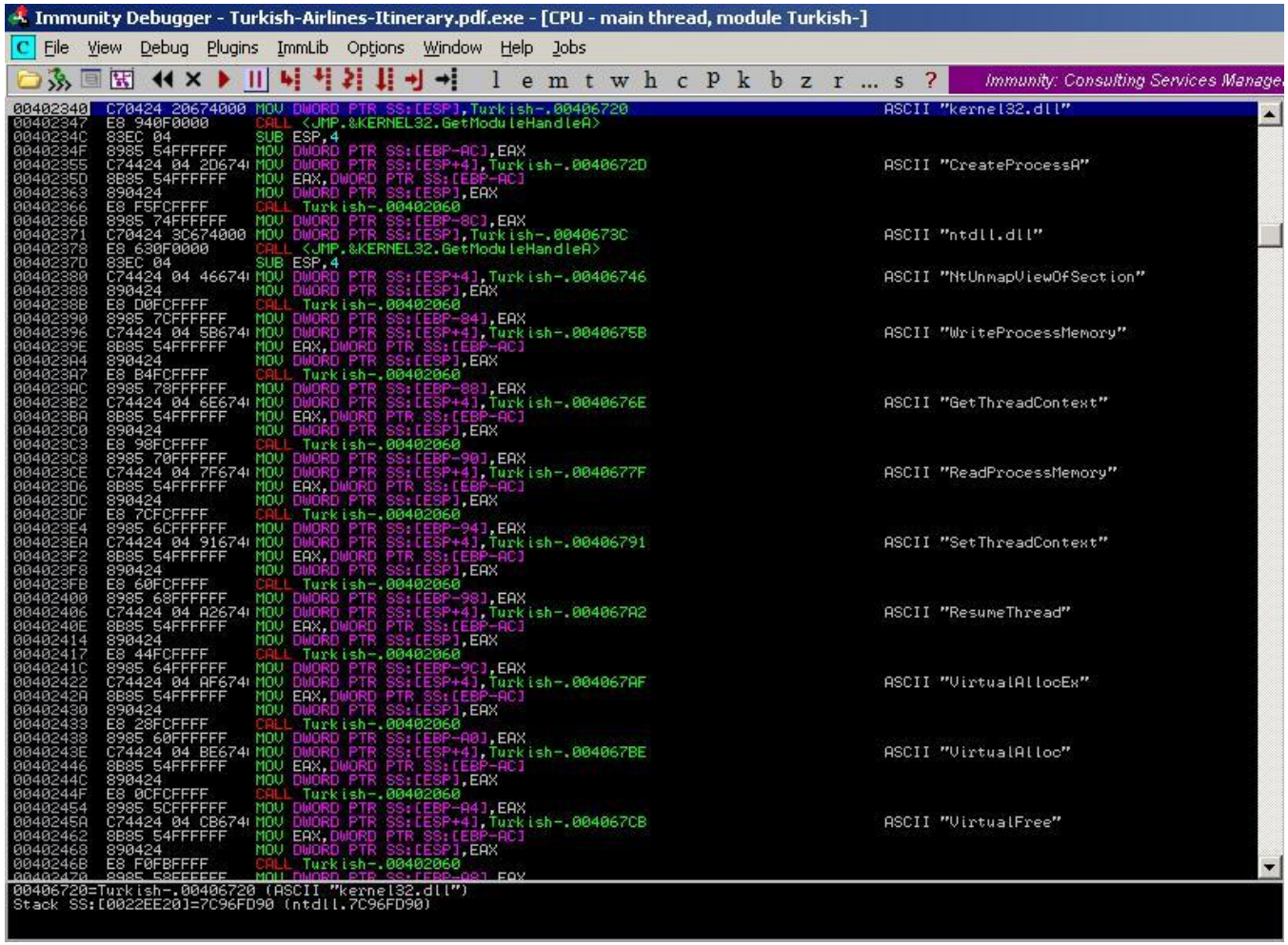
ARAÇLAR


Immunity Debugger - _00140000-3.mem.exe - [CPU - main thread, module _0014000]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
Registers (FPU)
EAX 0012FE34 ASCII "lol"
ECX 00000145
EDX 7C97E178 ntdll.7C97E178
EBX 7FFDE000
ESP 0012FE28
EBP 0012FFC0
ESI 0040141C _0014000.<ModuleEntryPoint>
EDI 0012FF94
EIP 004014B8 _0014000.004014B8
LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
Address Hex dump ASCII
Paused

ARAÇLAR


Immunity Debugger - Turkish-_00400000.exe - [CPU - main thread, module Turkish-]
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 . 68 00100000 PUSH 1000
004016B8 . FFB5 80FEFFFF PUSH DWORD PTR SS:[EBP-180]
004016BE . 6A 00 PUSH 0
004016C0 . FF55 E4 CALL DWORD PTR SS:[EBP-1C]
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 . 8BD4 MOV EDX,ESP
004016D1 . 33C9 XOR ECX,ECX
004016D3 . 8D85 80FEFFFF LEA EAX,DWORD PTR SS:[EBP-180]
004016D9 . 50 PUSH EAX
004016DA . FFB5 84FEFFFF PUSH DWORD PTR SS:[EBP-17C]
004016E0 . 51 PUSH ECX
004016E1 . 51 PUSH ECX
004016E2 . 52 PUSH EDX
004016E3 . FFB5 88FEFFFF PUSH DWORD PTR SS:[EBP-178]
004016E9 . FF55 D0 CALL DWORD PTR SS:[EBP-30]
004016EC . 83C4 04 ADD ESP,4
004016EF . FFB5 84FEFFFF PUSH DWORD PTR SS:[EBP-17C]
004016F5 . E8 D7FCFFFF CALL Turkish-.004013D1
004016FA . 8B85 84FEFFFF MOV EAX,DWORD PTR SS:[EBP-17C]
00401700 . 8B40 08 MOV EAX,DWORD PTR DS:[EAX+8]
00401703 . 8985 7CFEFFFF MOV DWORD PTR SS:[EBP-184],EAX
00401709 . 68 00800000 PUSH 8000
0040170E . 6A 00 PUSH 0
00401710 . FFB5 84FEFFFF PUSH DWORD PTR SS:[EBP-17C]
00401716 . FF55 E0 CALL DWORD PTR SS:[EBP-20]
00401719 > FFB5 88FEFFFF PUSH DWORD PTR SS:[EBP-178]
0040171F . FF55 CC CALL DWORD PTR SS:[EBP-34]
00401722 . 81BD 7CFEFFFF CMP DWORD PTR SS:[EBP-184],61776D77
0040172C . 74 39 JE SHORT Turkish-.00401767
0040172E . 81BD 7CFEFFFF CMP DWORD PTR SS:[EBP-184],786F6276
00401738 . 74 2D JE SHORT Turkish-.00401767
0040173A . 81BD 7CFEFFFF 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
00401753 . 73 12 JNB SHORT Turkish-.00401767
00401755 > 8D05 78174000 LEA EAX,DWORD PTR DS:[401778]
0040175B . 8985 78FEFFFF MOV DWORD PTR SS:[EBP-188],EAX
00401761 . 8D05 B9134000 LEA EAX,DWORD PTR DS:[4013B9]
00401767 > 50 PUSH EAX
00401768 . FFB5 78FEFFFF PUSH DWORD PTR SS:[EBP-188]
0040176E . 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
scsi\disk&ven_vmware_&prod_vmware_virtual_s&rev_1.0\4&5fcaafc&0&000
vmwa
vbox
qemu
CPU dongusu sayaci - Anti debugger/sandbox
CPU dongusu sayaci - Anti debugger/sandbox
Arg2
Arg1
Turkish-.00401284
CHAR ' '

ARAÇLAR


Immunity Debugger - Turkish-Airlines-Itinerary.pdf.exe - [CPU - main thread, module Turkish-]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manage
00402340 C70424 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 2D674 MOV DWORD PTR SS:[ESP+4],Turkish-.0040672D ASCII "CreateProcessA"
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 C70424 3C674000 MOV DWORD PTR SS:[ESP],Turkish-.0040673C ASCII "ntdll.dll"
00402378 E8 630F0000 CALL <JMP.&KERNEL32.GetModuleHandleA>
0040237D 83EC 04 SUB ESP,4
00402380 C74424 04 46674 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 5B674 MOV DWORD PTR SS:[ESP+4],Turkish-.0040675B ASCII "WriteProcessMemory"
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 6E674 MOV DWORD PTR SS:[ESP+4],Turkish-.0040676E ASCII "GetThreadContext"
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
00406720=Turkish-.00406720 (ASCII "kernel32.dll")
Stack SS:[0022EE20]=7C96FD90 (ntdll.7C96FD90)

BELLEK ANALİZİ

Bellekten çalışan programlara ait çeşitli bilgiler toplanır.

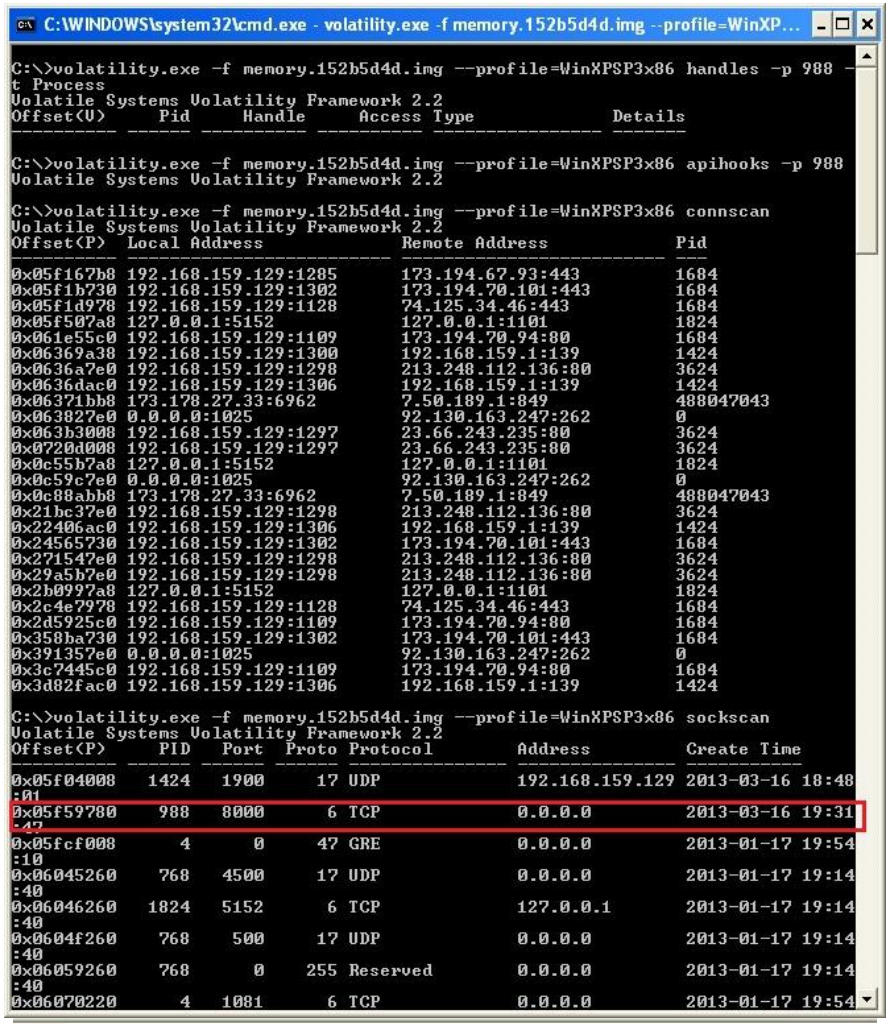
Bu bilgiler programlara ait ağ ve kayıt defteri bilgilerini de içermektedir.

Kendini gizlemeye çalışan zararlı yazılımlar daha kolay tespit edilebilir.

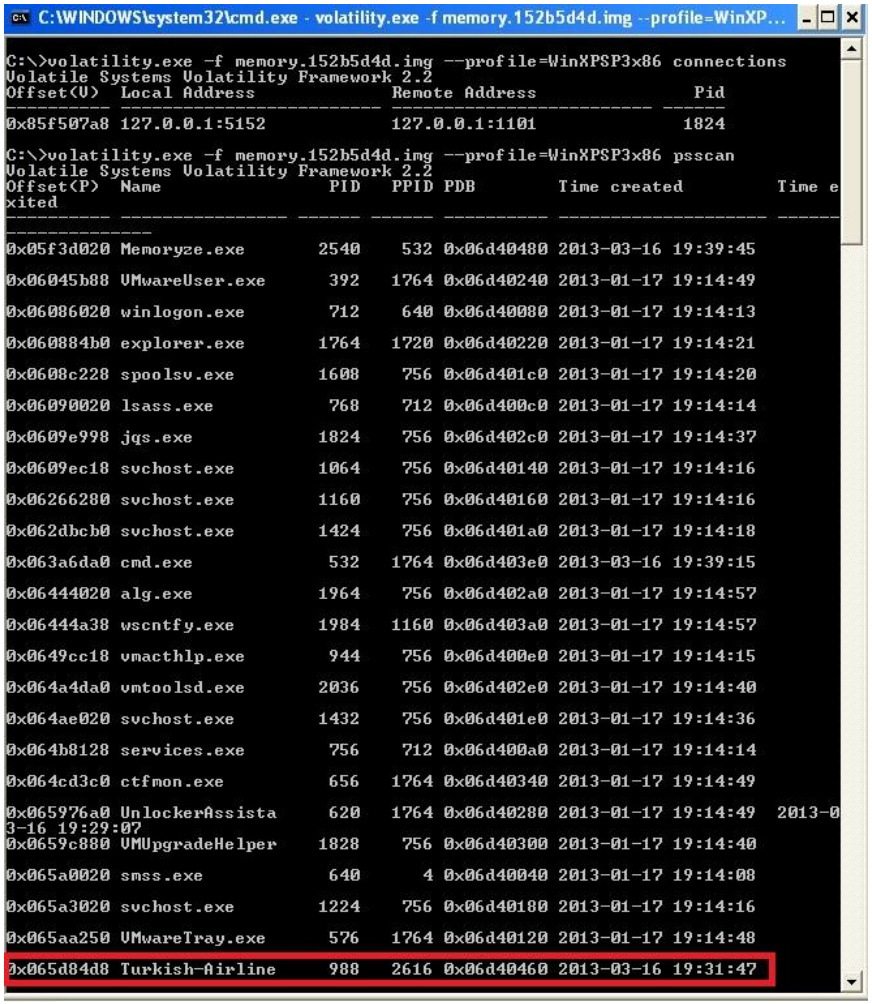
VMWare'de VMEM dosyası üzerinde analiz yapılabilir.

Popüler Araçlar: Volatility, Memoryze, Redline

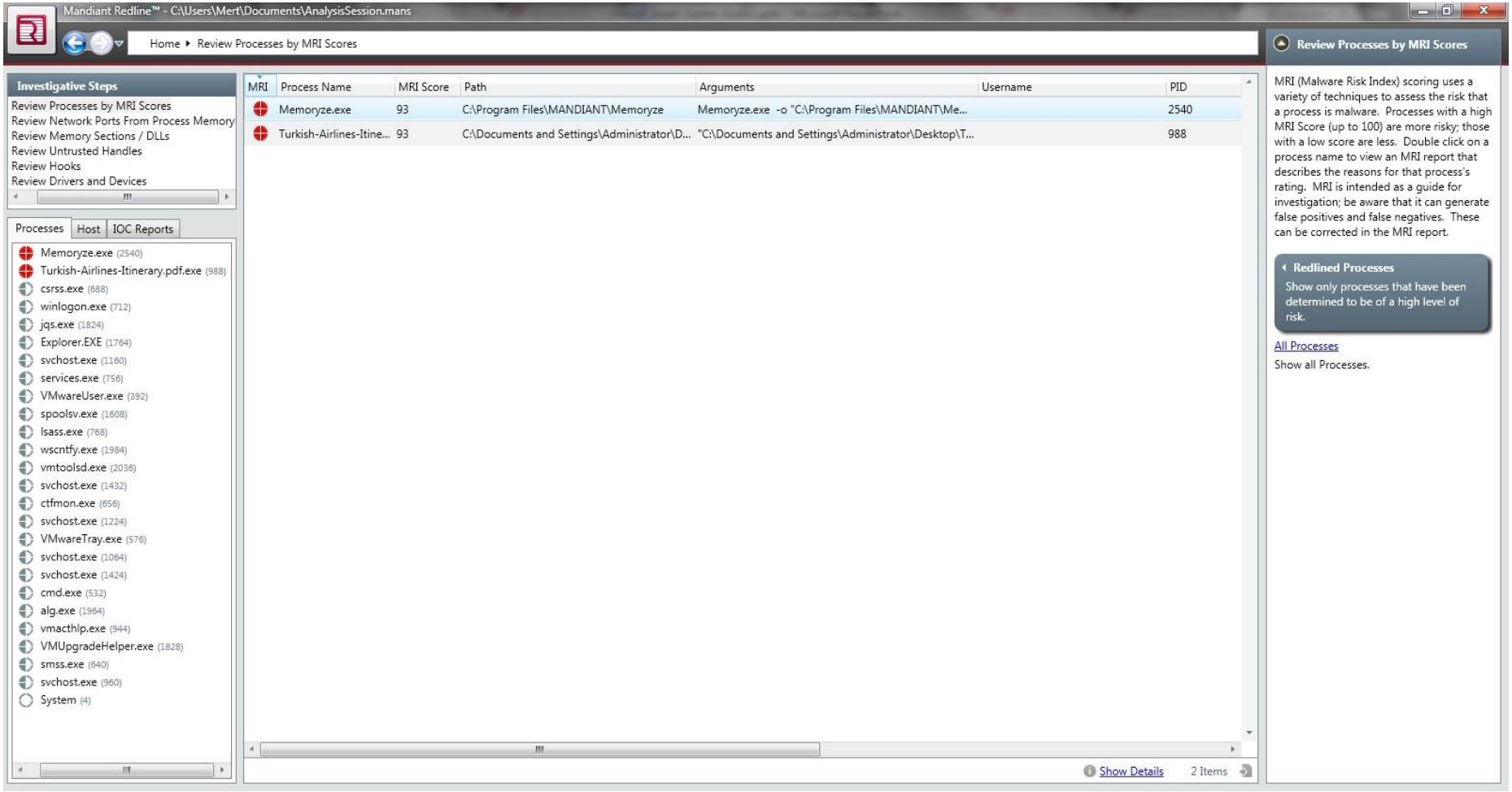
ARAÇLAR


C:\WINDOWS\system32\cmd.exe - volatility.exe -f memory.152b5d4d.img --profile=WinXP...
C:\>volatility.exe -f memory.152b5d4d.img --profile=WinXPSP3x86 handles -p 988 -t Process
Volatile Systems Volatility Framework 2.2
Offset(V) Pid Handle Access Type Details
C:\>volatility.exe -f memory.152b5d4d.img --profile=WinXPSP3x86 apihooks -p 988
Volatile Systems Volatility Framework 2.2
C:\>volatility.exe -f memory.152b5d4d.img --profile=WinXPSP3x86 connscan
Volatile Systems Volatility Framework 2.2
Offset(P) Local Address Remote Address Pid
0x05f167b8 192.168.159.129:1285 173.194.67.93:443 1684
0x05f1b730 192.168.159.129:1302 173.194.70.101:443 1684
0x05f1d978 192.168.159.129:1128 74.125.34.46:443 1684
0x05f507a8 127.0.0.1:5152 127.0.0.1:1101 1824
0x061e55c0 192.168.159.129:1109 173.194.70.94:80 1684
0x06369a38 192.168.159.129:1300 192.168.159.1:139 1424
0x0636a7e0 192.168.159.129:1298 213.248.112.136:80 3624
0x0636dac0 192.168.159.129:1306 192.168.159.1:139 1424
0x06371bb8 173.178.27.33:6962 7.50.189.1:849 488047043
0x063827e0 0.0.0.0:1025 92.130.163.247:262 0
0x063b3008 192.168.159.129:1297 23.66.243.235:80 3624
0x0720d008 192.168.159.129:1297 23.66.243.235:80 3624
0x0c55b7a8 127.0.0.1:5152 127.0.0.1:1101 1824
0x0c59c7e0 0.0.0.0:1025 92.130.163.247:262 0
0x0c88abb8 173.178.27.33:6962 7.50.189.1:849 488047043
0x21bc37e0 192.168.159.129:1298 213.248.112.136:80 3624
0x22406ac0 192.168.159.129:1306 192.168.159.1:139 1424
0x24565730 192.168.159.129:1302 173.194.70.101:443 1684
0x271547e0 192.168.159.129:1298 213.248.112.136:80 3624
0x29a5b7e0 192.168.159.129:1298 213.248.112.136:80 3624
0x2b0997a8 127.0.0.1:5152 127.0.0.1:1101 1824
0x2c4e7978 192.168.159.129:1128 74.125.34.46:443 1684
0x2d5925c0 192.168.159.129:1109 173.194.70.94:80 1684
0x358ba730 192.168.159.129:1302 173.194.70.101:443 1684
0x391357e0 0.0.0.0:1025 92.130.163.247:262 0
0x3c7445c0 192.168.159.129:1109 173.194.70.94:80 1684
0x3d82fac0 192.168.159.129:1306 192.168.159.1:139 1424
C:\>volatility.exe -f memory.152b5d4d.img --profile=WinXPSP3x86 sockscan
Volatile Systems Volatility Framework 2.2
Offset(P) PID Port Proto Protocol Address Create Time
0x05f04008 1424 1900 17 UDP 192.168.159.129 2013-03-16 18:48:01
0x05f59780 988 8000 6 TCP 0.0.0.0 2013-03-16 19:31:47
0x05fcf008 4 0 47 GRE 0.0.0.0 2013-01-17 19:54:10
0x06045260 768 4500 17 UDP 0.0.0.0 2013-01-17 19:14:40
0x06046260 1824 5152 6 TCP 127.0.0.1 2013-01-17 19:14:40
0x0604f260 768 500 17 UDP 0.0.0.0 2013-01-17 19:14:40
0x06059260 768 0 255 Reserved 0.0.0.0 2013-01-17 19:14:40
0x06070220 4 1081 6 TCP 0.0.0.0 2013-01-17 19:54

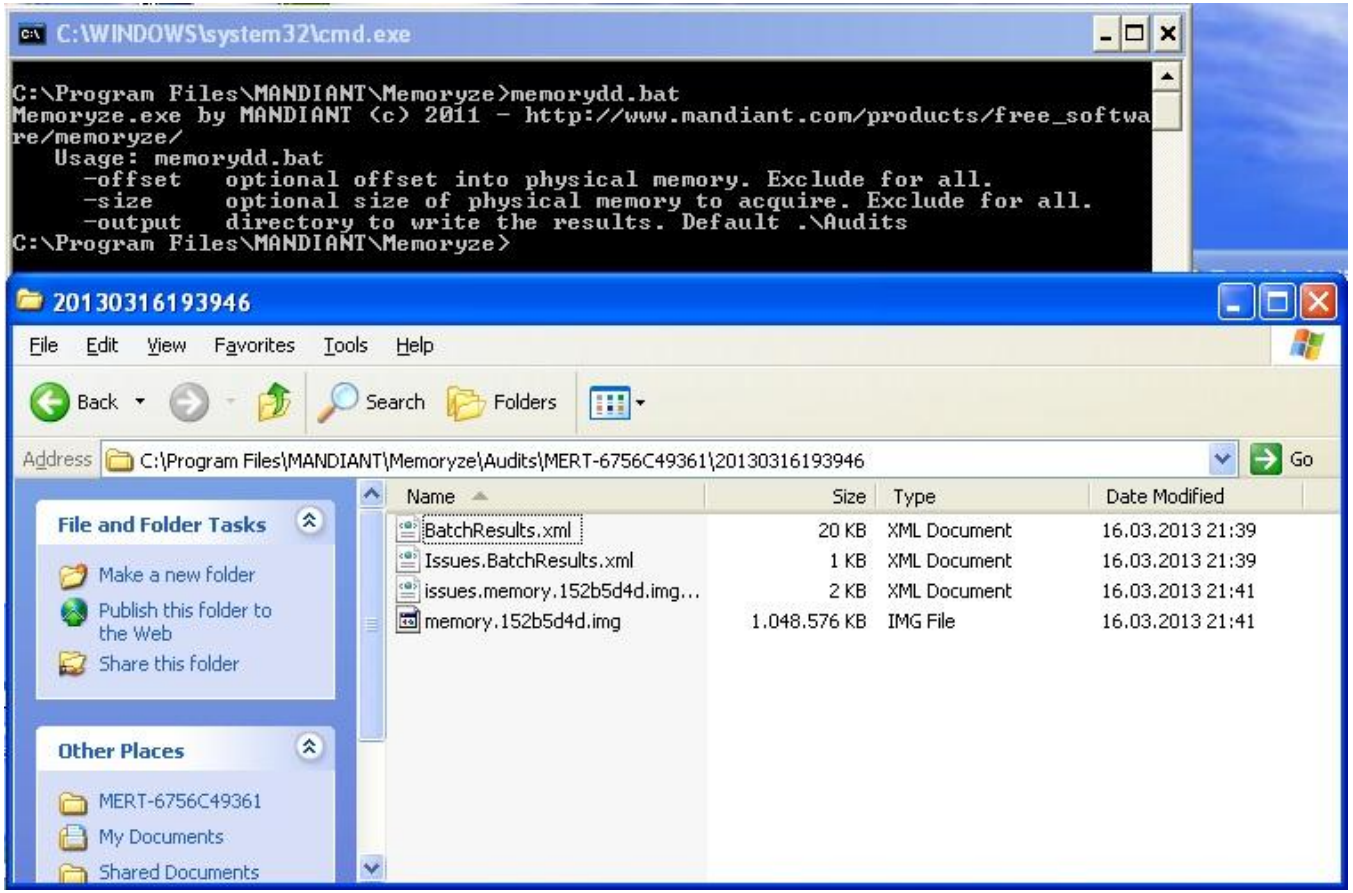
ARAÇLAR


C:\WINDOWS\system32\cmd.exe - volatility.exe -f memory.152b5d4d.img --profile=WinXP...
C:\>volatility.exe -f memory.152b5d4d.img --profile=WinXPSP3x86 connections
Volatile Systems Volatility Framework 2.2
Offset(V) Local Address Remote Address Pid
0x85f507a8 127.0.0.1:5152 127.0.0.1:1101 1824
C:\>volatility.exe -f memory.152b5d4d.img --profile=WinXPSP3x86 psscan
Volatile Systems Volatility Framework 2.2
Offset(P) Name PID PPID PDB Time created Time exited
0x05f3d020 Memoryze.exe 2540 532 0x06d40480 2013-03-16 19:39:45
0x06045b88 VMwareUser.exe 392 1764 0x06d40240 2013-01-17 19:14:49
0x06086020 winlogon.exe 712 640 0x06d40080 2013-01-17 19:14:13
0x060884b0 explorer.exe 1764 1720 0x06d40220 2013-01-17 19:14:21
0x0608c228 spoolsv.exe 1608 756 0x06d401c0 2013-01-17 19:14:20
0x06090020 lsass.exe 768 712 0x06d400c0 2013-01-17 19:14:14
0x0609e998 jqs.exe 1824 756 0x06d402c0 2013-01-17 19:14:37
0x0609ec18 svchost.exe 1064 756 0x06d40140 2013-01-17 19:14:16
0x06266280 svchost.exe 1160 756 0x06d40160 2013-01-17 19:14:16
0x062dbcb0 svchost.exe 1424 756 0x06d401a0 2013-01-17 19:14:18
0x063a6da0 cmd.exe 532 1764 0x06d403e0 2013-03-16 19:39:15
0x06444020 alg.exe 1964 756 0x06d402a0 2013-01-17 19:14:57
0x06444a38 wscntfy.exe 1984 1160 0x06d403a0 2013-01-17 19:14:57
0x0649cc18 vmacthlp.exe 944 756 0x06d400e0 2013-01-17 19:14:15
0x064a4da0 vmtoolsd.exe 2036 756 0x06d402e0 2013-01-17 19:14:40
0x064ae020 svchost.exe 1432 756 0x06d401e0 2013-01-17 19:14:36
0x064b8128 services.exe 756 712 0x06d400a0 2013-01-17 19:14:14
0x064cd3c0 ctfmon.exe 656 1764 0x06d40340 2013-01-17 19:14:49
0x065976a0 UnlockerAssista 620 1764 0x06d40280 2013-01-17 19:14:49 2013-03-16 19:29:07
0x0659c880 VMUpgradeHelper 1828 756 0x06d40300 2013-01-17 19:14:40
0x065a0020 smss.exe 640 4 0x06d40040 2013-01-17 19:14:08
0x065a3020 svchost.exe 1224 756 0x06d40180 2013-01-17 19:14:16
0x065aa250 VMwareTray.exe 576 1764 0x06d40120 2013-01-17 19:14:48
0x065d84d8 Turkish-Airline 988 2616 0x06d40460 2013-03-16 19:31:47

ARAÇLAR


Mandiant Redline™ - C:\Users\Mert\Documents\AnalysisSession.mans
Home ▸ Review Processes by MRI Scores
Investigative Steps
Review Processes by MRI Scores
Review Network Ports From Process Memory
Review Memory Sections / DLLs
Review Untrusted Handles
Review Hooks
Review Drivers and Devices
Processes
Host
IOC Reports
Memoryze.exe (2540)
Turkish-Airlines-Itinerary.pdf.exe (988)
csrss.exe (688)
winlogon.exe (712)
jqs.exe (1824)
Explorer.EXE (1764)
svchost.exe (1160)
services.exe (756)
VMwareUser.exe (392)
spoolsv.exe (1608)
lsass.exe (768)
wscntfy.exe (1984)
vmtoolsd.exe (2036)
svchost.exe (1432)
ctfmon.exe (656)
svchost.exe (1224)
VMwareTray.exe (576)
svchost.exe (1064)
svchost.exe (1424)
cmd.exe (532)
alg.exe (1964)
vmacthlp.exe (944)
VMUpgradeHelper.exe (1828)
smss.exe (640)
svchost.exe (960)
System (4)
MRI
Process Name
MRI Score
Path
Arguments
Username
PID
Memoryze.exe 93 C:\Program Files\MANDIANT\Memoryze Memoryze.exe -o "C:\Program Files\MANDIANT\Me... 2540
Turkish-Airlines-Itine... 93 C:\Documents and Settings\Administrator\D... "C:\Documents and Settings\Administrator\Desktop\T... 988
Show Details
2 Items
Review Processes by MRI Scores
MRI (Malware Risk Index) scoring uses a variety of techniques to assess the risk that a process is malware. Processes with a high MRI Score (up to 100) are more risky; those with a low score are less. Double click on a process name to view an MRI report that describes the reasons for that process's rating. MRI is intended as a guide for investigation; be aware that it can generate false positives and false negatives. These can be corrected in the MRI report.
Redlined Processes
Show only processes that have been determined to be of a high level of risk.
All Processes
Show all Processes.

ARAÇLAR


C:\WINDOWS\system32\cmd.exe
C:\Program Files\MANDIANT\Memoryze>memorydd.bat
Memoryze.exe by MANDIANT (c) 2011 - http://www.mandiant.com/products/free_software/memoryze/
Usage: memorydd.bat
-offset optional offset into physical memory. Exclude for all.
-size optional size of physical memory to acquire. Exclude for all.
-output directory to write the results. Default .\Audits
C:\Program Files\MANDIANT\Memoryze>
20130316193946
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Program Files\MANDIANT\Memoryze\Audits\MERT-6756C49361\20130316193946
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
MERT-6756C49361
My Documents
Shared Documents
Name Size Type Date Modified
BatchResults.xml 20 KB XML Document 16.03.2013 21:39
Issues.BatchResults.xml 1 KB XML Document 16.03.2013 21:39
issues.memory.152b5d4d.img... 2 KB XML Document 16.03.2013 21:41
memory.152b5d4d.img 1.048.576 KB IMG File 16.03.2013 21:41

OFANSİF ANALİZ

Komuta Kontrol Merkezi üzerinde denetimler gerçekleştirilir.

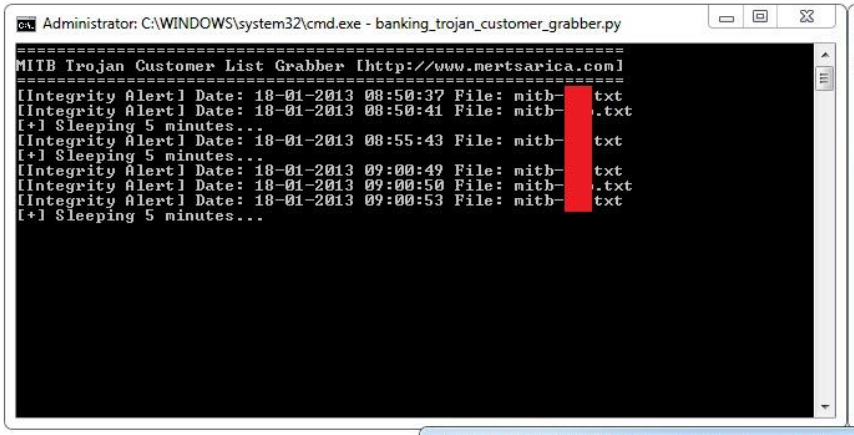
Amaç ele geçirilen kurum ve müşterileri bilgilerinin tespit edilmesidir.

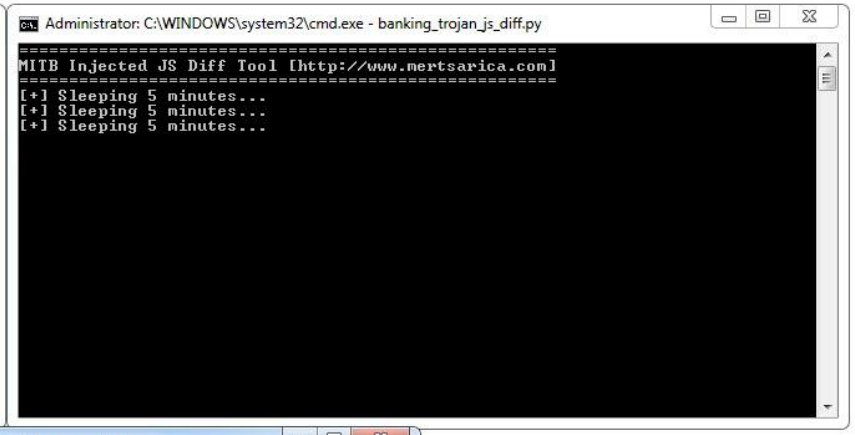
Duruma göre basit veya ileri seviye denetimler gerçekleştirilebilir.

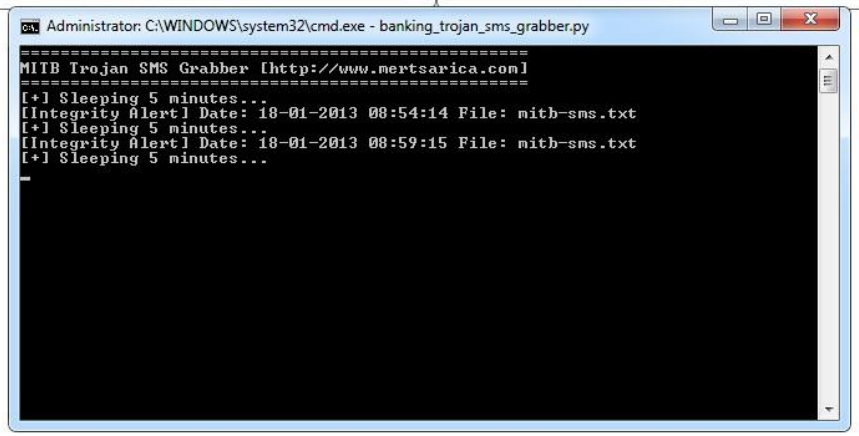
Dikkat edilmezse hedef sistemde hizmet kesintisi yaşanabilir.

Popüler Araçlar: Sızma testi yöntemleriniz & araçlarınız ☺

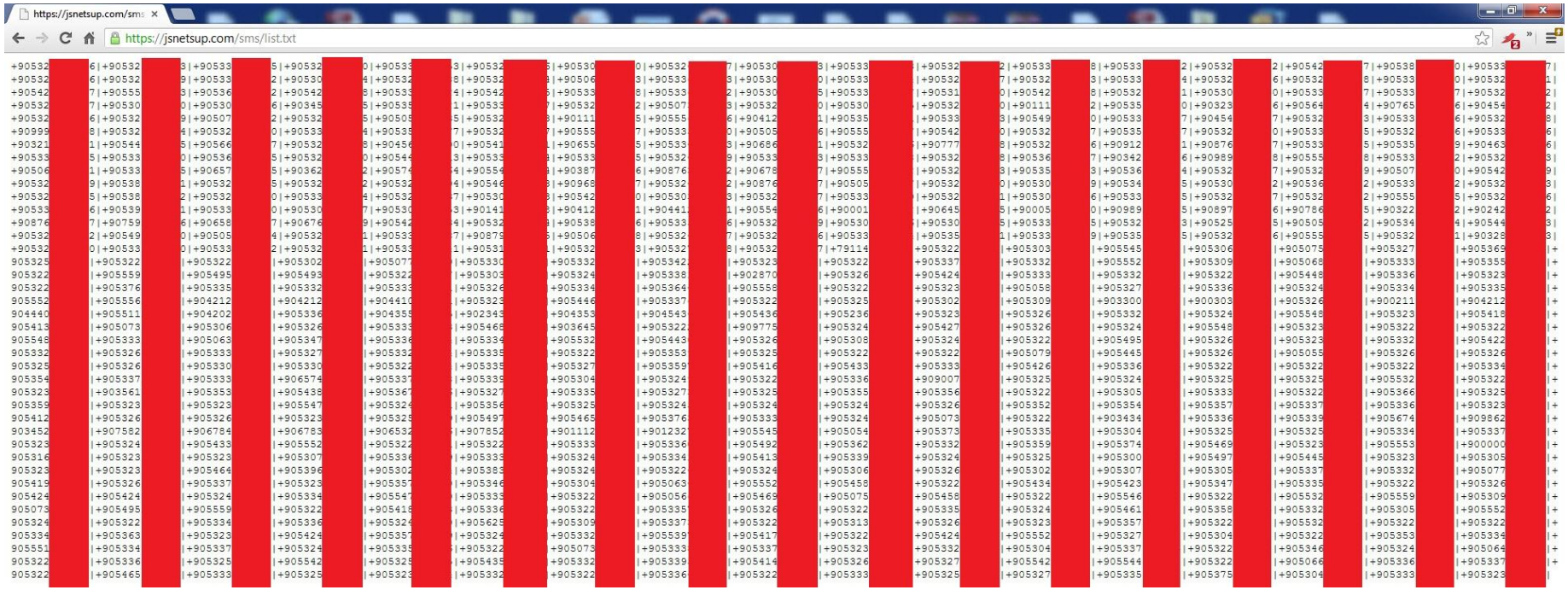
OFANSİF ANALİZ



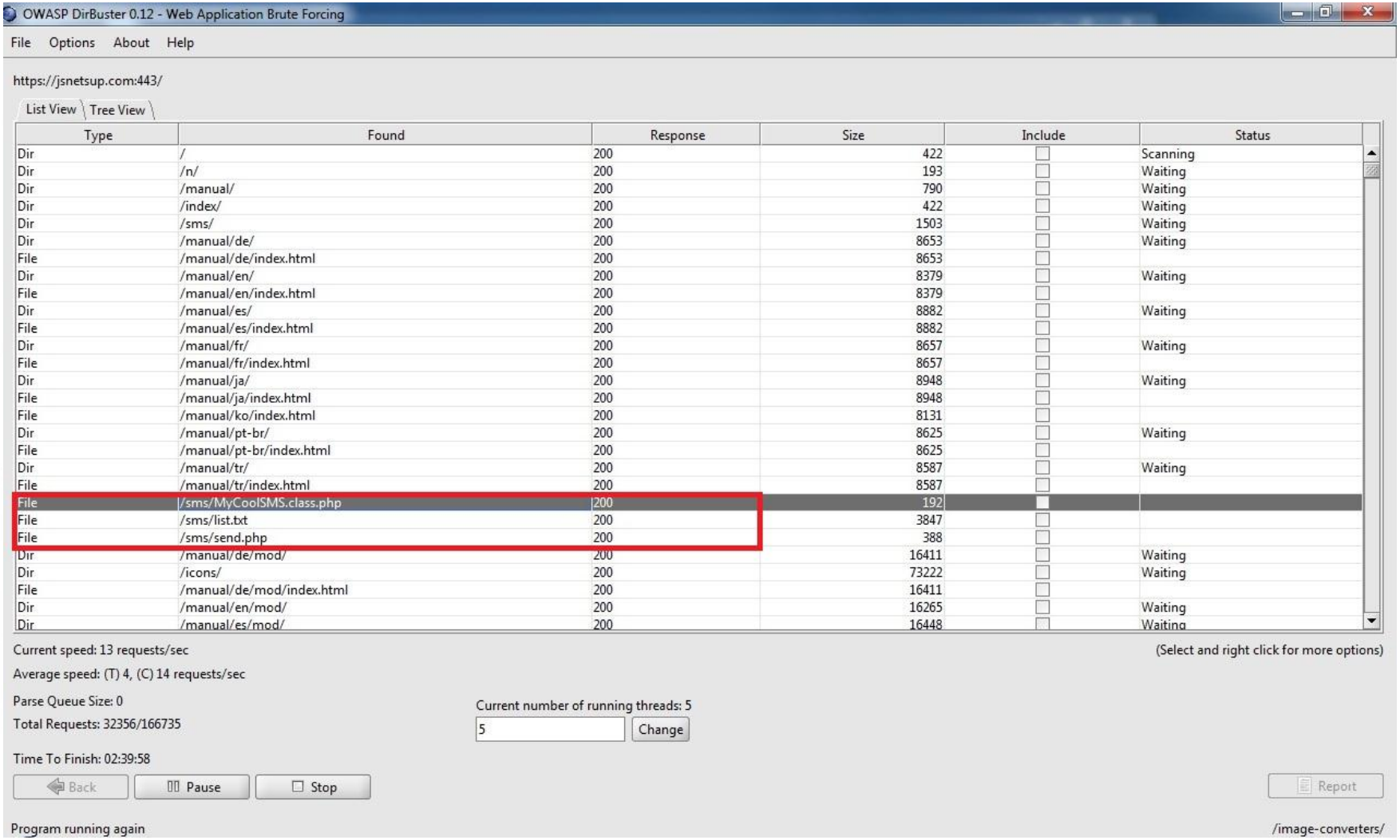




OFANSİF ANALİZ



OFANSİF ANALİZ



OFANSİF ANALİZ

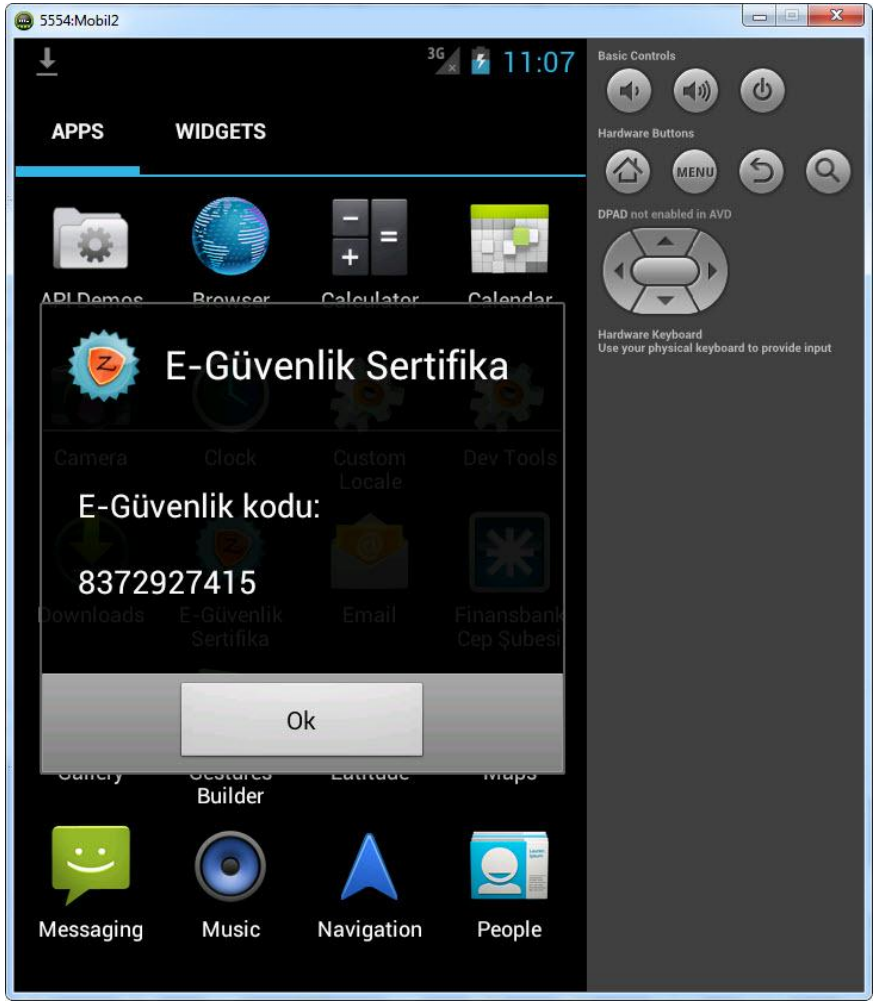
domain name - instances - first time reported - last time reported - nameserver - IP address - registrar

emailing-express.com - 7 - 1/29/2012 - 1/22/2013 - joker@axalone.com - A.NS.JOKER.COM - 159.25.16.217 - JOKER
maprosperite.com - 122 - 1/1/2013 - 1/22/2013 - admin@transmonde.com - A.NS.JOKER.COM - 69.195.32.117 - JOKER
kontaktimaili.com - 43 - 1/19/2013 - 1/21/2013 - hydrofobia@gmail.com - A.NS.JOKER.COM - 164.138.27.120 - JOKER
both.com - 7 - 1/19/2013 - 1/21/2013 - alasky@sover.net - A.NS.JOKER.COM - 216.158.160.82 - JOKER
dietfacts.com - 7 - 1/19/2013 - 1/21/2013 - info@computersites.com - A.NS.JOKER.COM - 72.51.35.238 - JOKER
freeholdentertainment.com - 4 - 1/15/2013 - 1/21/2013 - unormal@gmail.com - A.NS.JOKER.COM - 72.18.135.22 - JOKER
consolidatedunderwriters.com - 2 - 1/17/2013 - 1/19/2013 - ss@gocui.com - A.NS.JOKER.COM - 50.57.130.139 - JOKER
sexydeskbabes.com - 4 - 9/11/2012 - 1/16/2013 - mymodelsites@yahoo.com - A.NS.JOKER.COM - 184.107.219.178 - JOKER
phpguru.org - 281 - 10/13/2010 - 1/16/2013 - richardh@phpguru.org - A.NS.JOKER.COM - NOTFOUND - JOKER
clientbiz.net - 11 - 12/21/2012 - 1/15/2013 - info@forward.com.ua - A.NS.JOKER.COM - NOTFOUND - JOKER
jsnetsup.com - 5 - 1/11/2013 - 1/15/2013 - vladpetro@rocketmail.com - A.NS.JOKER.COM - 37.221.161.78 - JOKER
sumrandomguy.com - 8 - 1/11/2013 - 1/15/2013 - FAIL - A.NS.JOKER.COM - 50.116.98.191 - GODADDY
emails-express.com - 6 - 1/11/2013 - 1/15/2013 - joker@axalone.com - A.NS.JOKER.COM - 159.25.16.223 - JOKER
js-backup.com - 5 - 1/11/2013 - 1/15/2013 - vladpetro@rocketmail.com - A.NS.JOKER.COM - 78.138.100.151 - JOKER
clockss.org - 8 - 1/11/2013 - 1/15/2013 - vreich@stanford.edu - A.NS.JOKER.COM - 171.66.236.16 - JOKER
qolar.com - 3 - 1/7/2013 - 1/11/2013 - artoix@gmail.com - A.NS.JOKER.COM - 77.120.115.199 - JOKER
javafr.com - 17 - 3/29/2012 - 1/11/2013 - nicolas@sorel.org - A.NS.JOKER.COM - 213.251.145.123 - JOKER
royalacecampaign.com - 134 - 7/10/2012 - 1/11/2013 - domadmi@hotmail.com - A.NS.JOKER.COM - 50.23.120.59 - JOKER
phpcs.com - 16 - 4/6/2012 - 1/11/2013 - nicolas@sorel.org - A.NS.JOKER.COM - 213.251.145.123 - JOKER
topmeds10.com - 2720 - 1/3/2012 - 1/11/2013 - admin@foxseek.com - A.NS.JOKER.COM - 91.224.160.159 - JOKER

Only first 20 are displayed, for the rest contact us at contact@knujon.com.

db-updated: 2013-02-07 06:22:52

OFANSİF ANALİZ



OFANSİF ANALİZ

1. Talimatları içeren SMS mesajı

Cep telefonunuzun işletim sistemi için özel olarak seçilmiş E-Güvenlik sertifika linkini içeren mesaj aldınız, kuruluma devam etmek için SMS mesajındaki linke tıklayın.

2. Ürün hakkında bilgiler

Cep telefonunuzun ekranında E-Güvenlik sertifika hakkında detaylı bilgileri göreceksiniz.

3. Yükleme yeri

E-Güvenlik sertifika yüklenmesi için telefonun dahili belleğini kullanmanız önerilir.

4. E-Güvenlik kodu

E-Güvenlik sertifika uygulamasını kurduktan sonra, aktivasyon kodunu ve uygulamanın başarılı bir şekilde kurulduğuna dair onay mesajını alacaksınız.

E-Güvenlik kodu girin:

Örneğin, 1234567890

SAYILARLA FATMAL

19 Aralık'ta başlayan Andromeda/Zeus/Cridex salgını 9 yerli banka müşterisini hedef aldı.

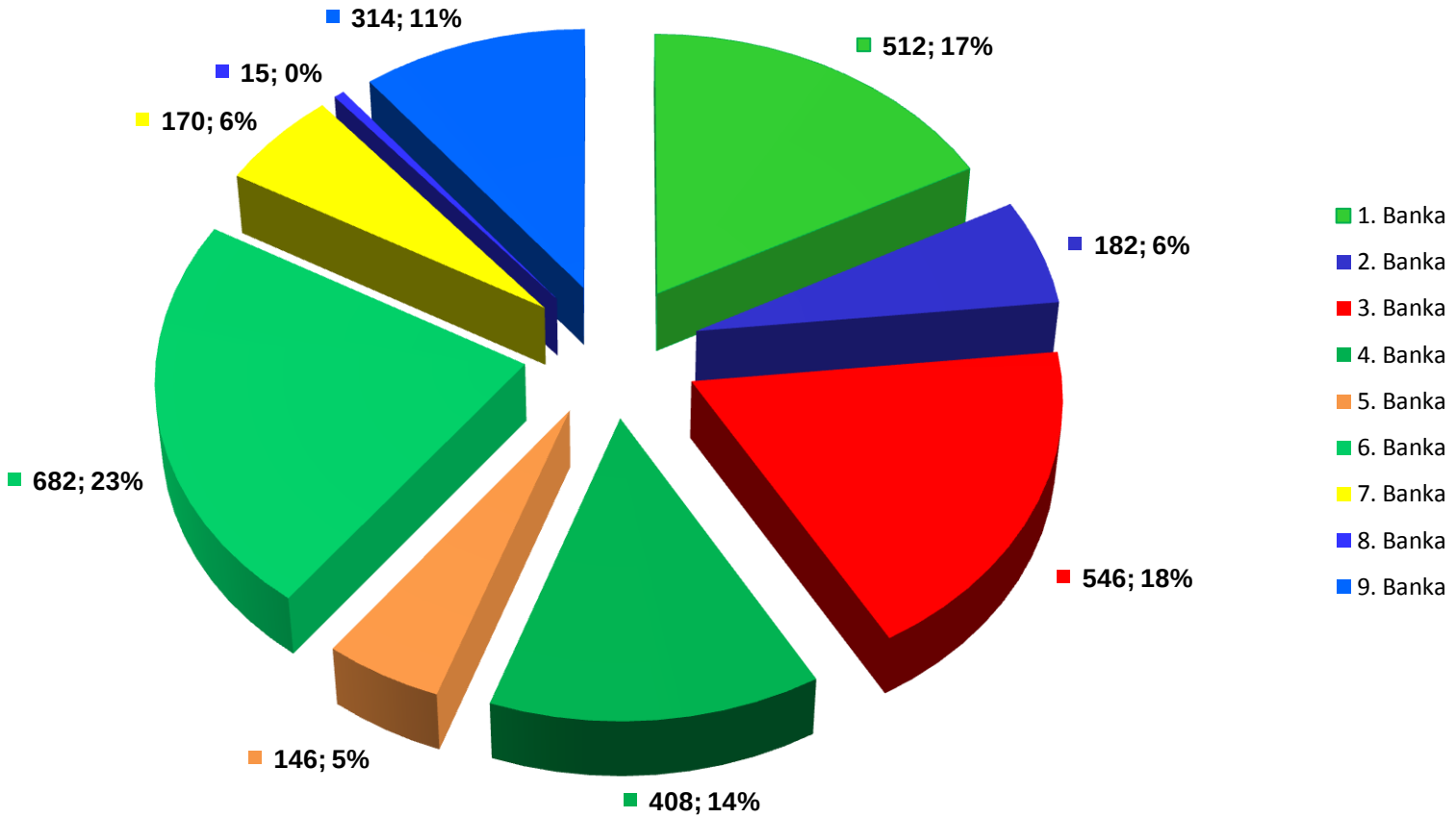
20 günde 1000 kişi zararlı yazılıma cep telefonu bilgisini verdi.

1 ayda, enjekte edilen Javascript dosyaları 32 defa güncellendi.

Sonuç olarak 1 ayda ~3000 sisteme bulaştı.

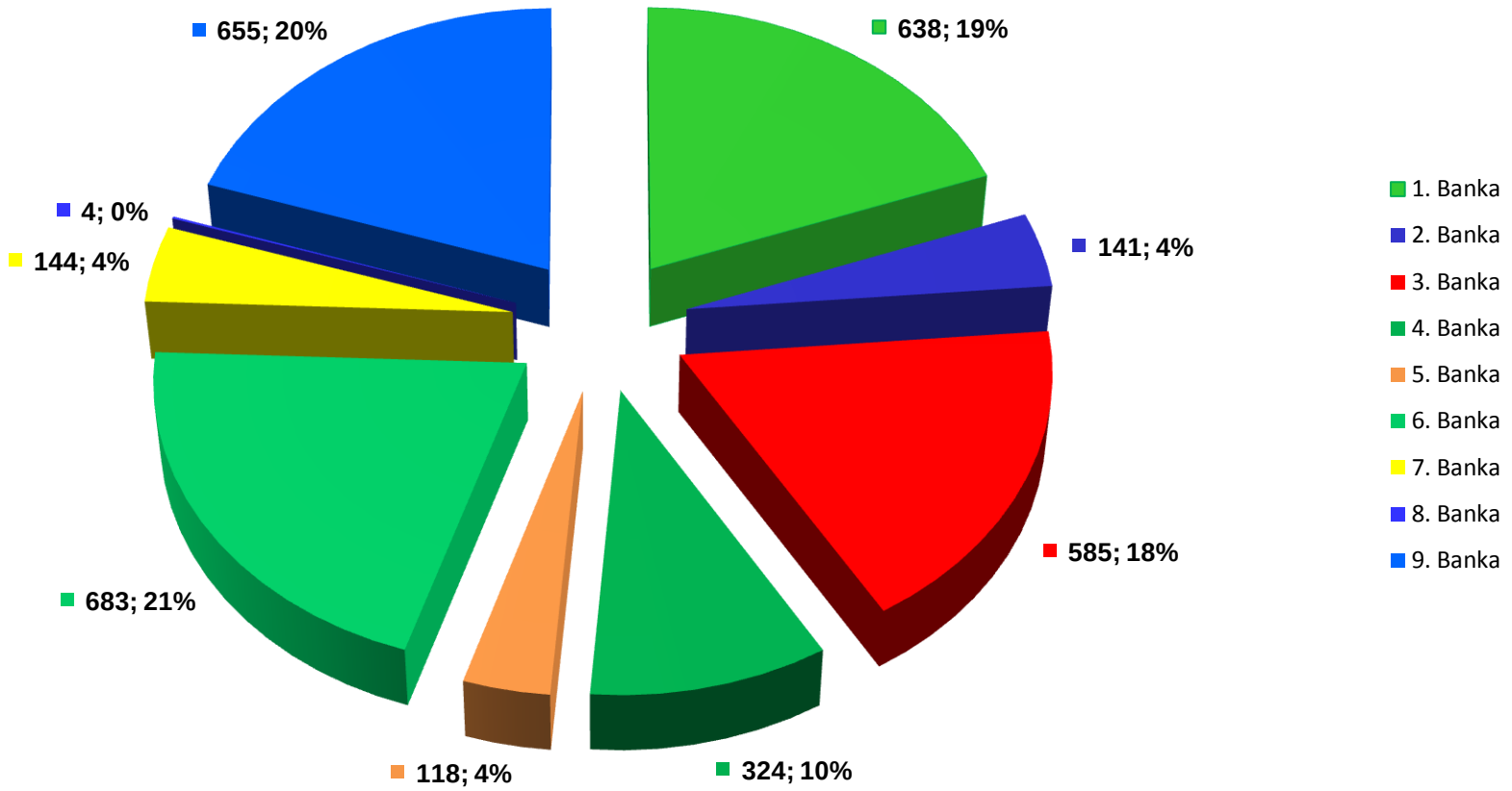
FATMAL

Aşağıdaki tablo 15 Ocak – 15 Şubat tarihleri arasında müşteri numaralarının yer aldığı ve bankaya özel olan sayfanın güncellenme sıklığını göstermektedir.



FATMAL

Aşağıdaki tablo 15 Şubat itibariyle banka bazında zararlı yazılım tarafından ele geçirilen müşteri numaralarının sayılarını göstermektedir.



SONUÇ

Zararlı yazılım analiz becerisine artık hemen hemen her kurum sahip olmalıdır.

Basit sızma girişimleri yerini APT saldırılarına bıraktı.

En detaylı ve doğru bilgi kod analizi ile ortaya çıkmaktadır.

Güvenlik sistemleri/cihazları zararlı yazılım tespiti konusunda kısıtlıdır.

Bellek analizi ile şüpheli yazılımları tespit etmek çok daha kolaydır.

Ofansif analiz ile klasik analiz yönetini bir adım öteye götürerek sizin için çok daha değerli bilgiler elde edebilirsiniz.

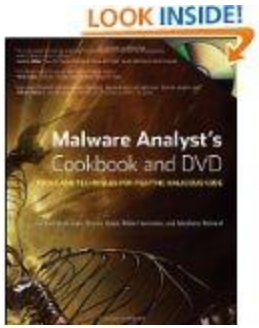
OKUNASI KİTAPLAR

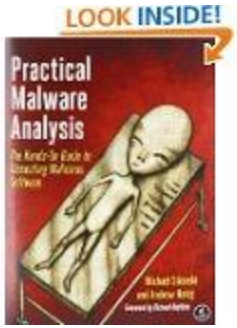
Malware Analyst's Cookbook

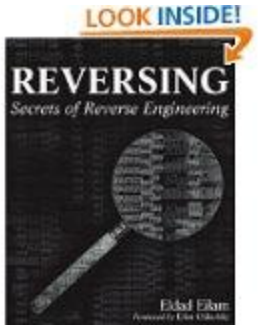
Practical Malware Analysis

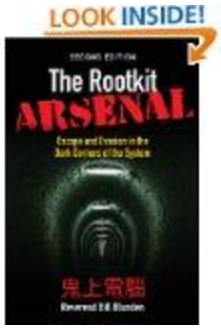
Secrets of Reverse Engineering

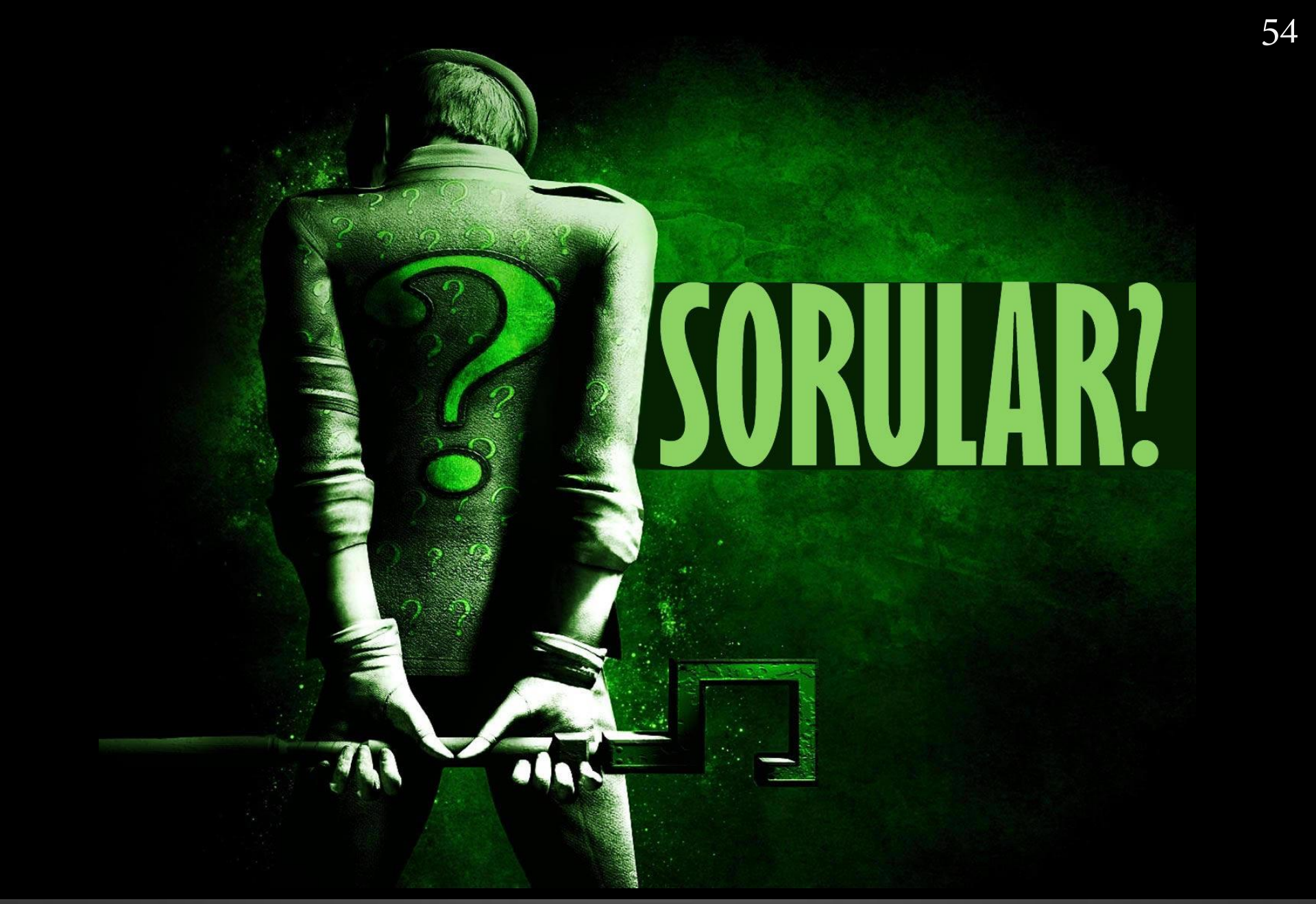
The Rootkit Arsenal










SORULAR?

TEŞEKKÜRLER