Spy-Net RAT Analizi

written by Mert SARICA | 1 November 2013

FatMal, Hesperbot, Zeus derken neredeyse 2013 yılını geride bırakıyoruz. Son yayımlanan tehdit raporlarına baktığımızda zararlı yazılım salgınlarında Türk kullanıcılarının eskiye kıyasla daha sık hedef alındığını görüyoruz. Zararlı yazılım analizi üzerine yan dal yapmaya çalışan bir sızma testi uzmanı olarak, son yıllarda artan siber saldırılara bir de bu salgınlar eklendiğinde, son kullanıcıların, kurumların geçmiş yıllara kıyasla güvenliğe, uzman personele daha çok önem vermeleri gerektiğini söyleyebilirim. Örneğin yıllar önce sızma testini 11. görev olarak gören ve 10 işi aynı anda götürmeye çalışan bir uzmana yükleyenlerin, bugün sadece sızma testi yaptırmak için 3-4 kişilik ekipler oluşturduklarını görebiliyoruz. Artan zararlı yazılım salgınları ve APT tehditleri ile zaman içinde zararlı yazılım analizi becerisine sahip uzmanlara da aynı şekilde talebin artacağını tahmin ediyorum dolayısıyla kendinizi yarına hazırlamak için zararlı analizi konusunda bol bol pratik yapmanızı tavsiye edebilirim. Pratik yapmak için benim gibi sağdan, soldan elde ettiğiniz örnek zararlı yazılımları inceleyebilirsiniz.

Geçtiğimiz günlerde yine bir arkadaşım, kendisine gelen bir sahte e-postayı benimle paylaştı. 2012 yılından bu yana gönderilen JAR uzantılı sahte KVK, Yurtiçi Kargo e-postalarına son olarak sahte Turkcell e-postası eklendi. Daha önce incelediğim benzer örneklerde, art niyetli kişiler Vodafone 3G modem üzerinden zararlı yazılım bulaşan sistemler ile iletişime geçiyorlardı. Zararlı yazılımlarda geçen Türkçe fonksiyon isimleri de geliştiricilerin yabancı olmadıklarını ortaya koyuyordu. Aradan uzun bir zaman geçtikten sonra gönderilen son örneğe göz atmaya ve bu konuda sizleri bilgilendirmeye karar verdim.

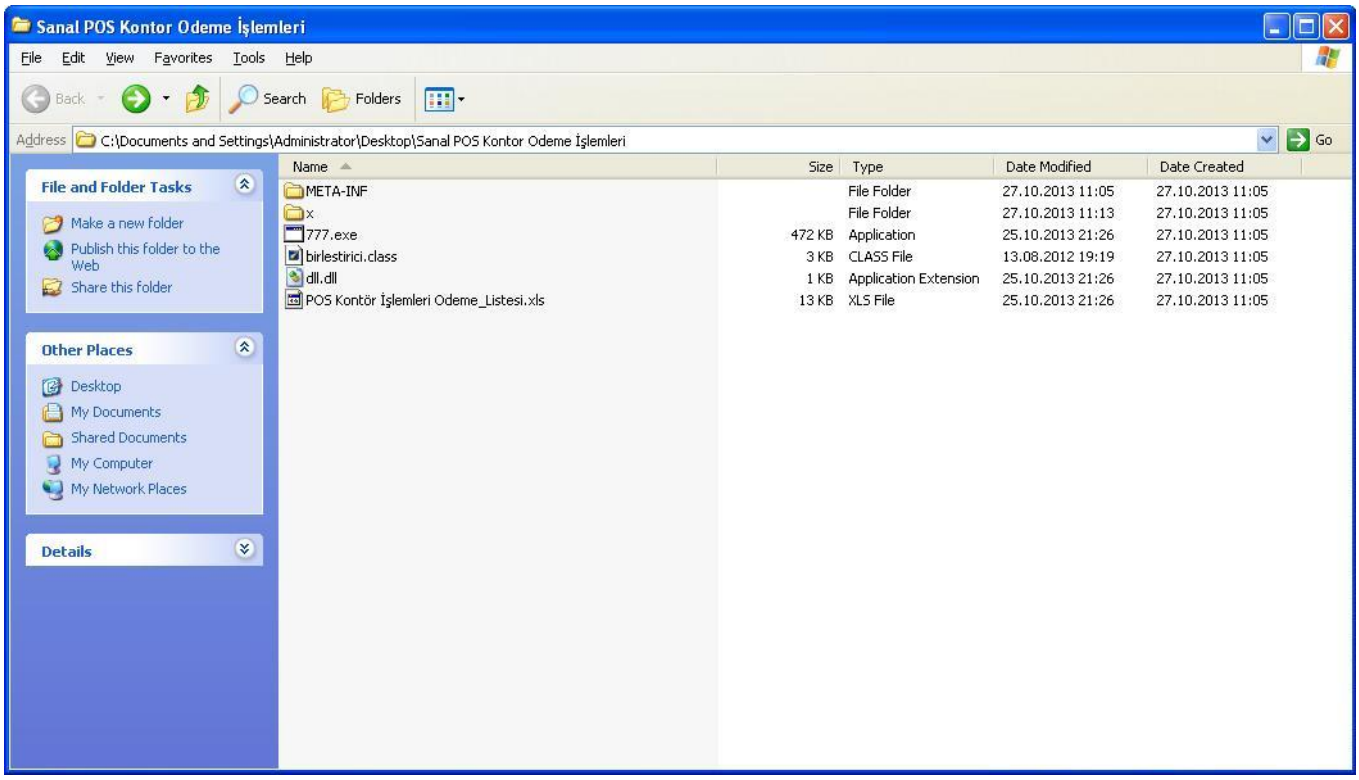
Sahte e-postanın ekinde Sanal POS Kontor Odeme İşlemleri.jar isimli bir dosya yer alıyordu.

From: info@turkcell.com.tr
To: [redacted]
Subject: Turkcell Dağıtım Merkezi (TDM
Date: Sat, 26 Oct 2013 12:17:40 +0300

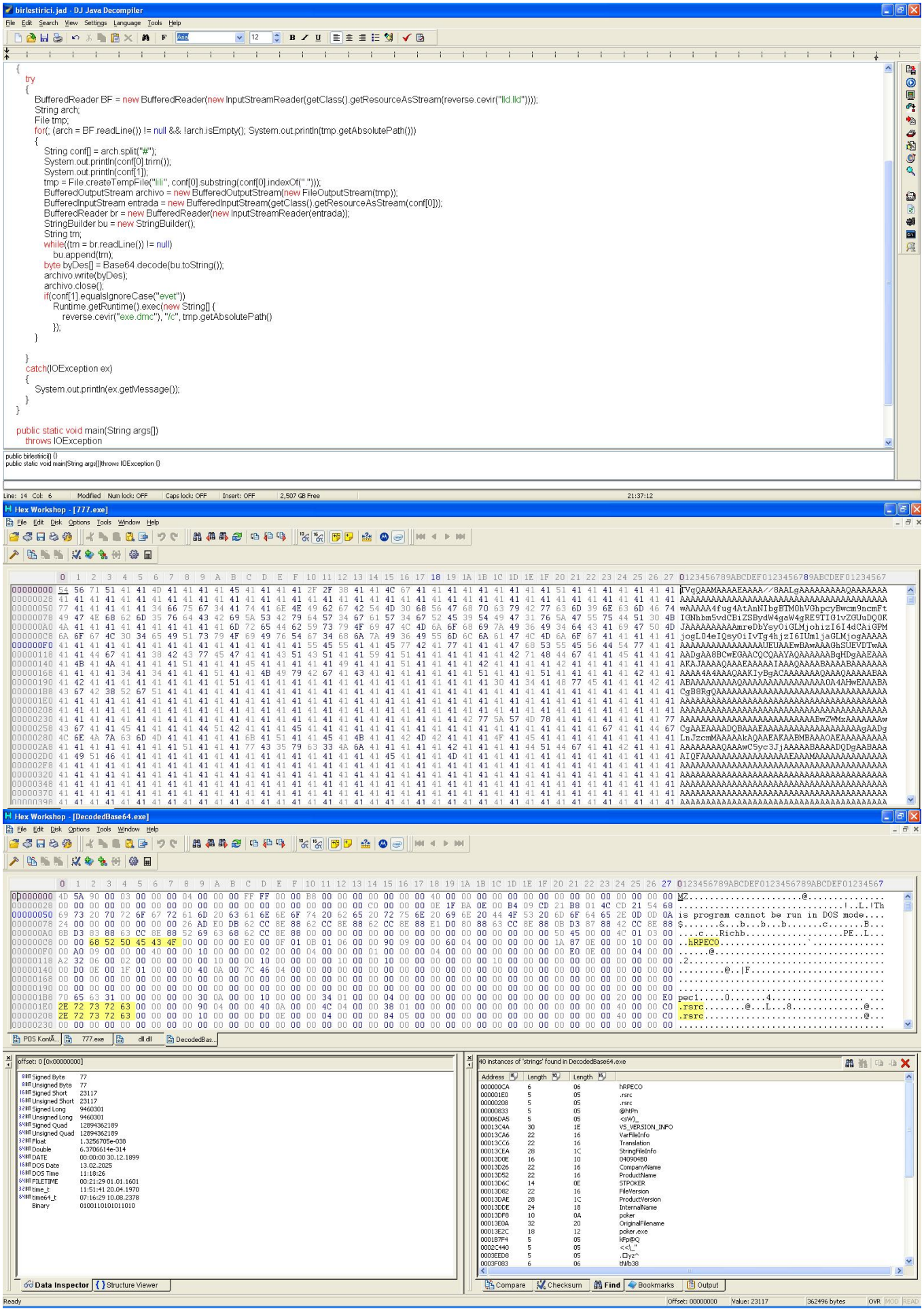
Turkcell Dağıtım Merkezi (TDM

Sanal POS Kontor Odeme İşlemleri.jar
490K Download

JAR uzantılı dosyayı açtığımda içinden BASE64 ile encode edilmiş 777.exe ve POS Kontör İşlemleri Odeme_Listesi.xls dosyaları ile birlestirici.class ve x/reverse.class dosyaları çıktı.

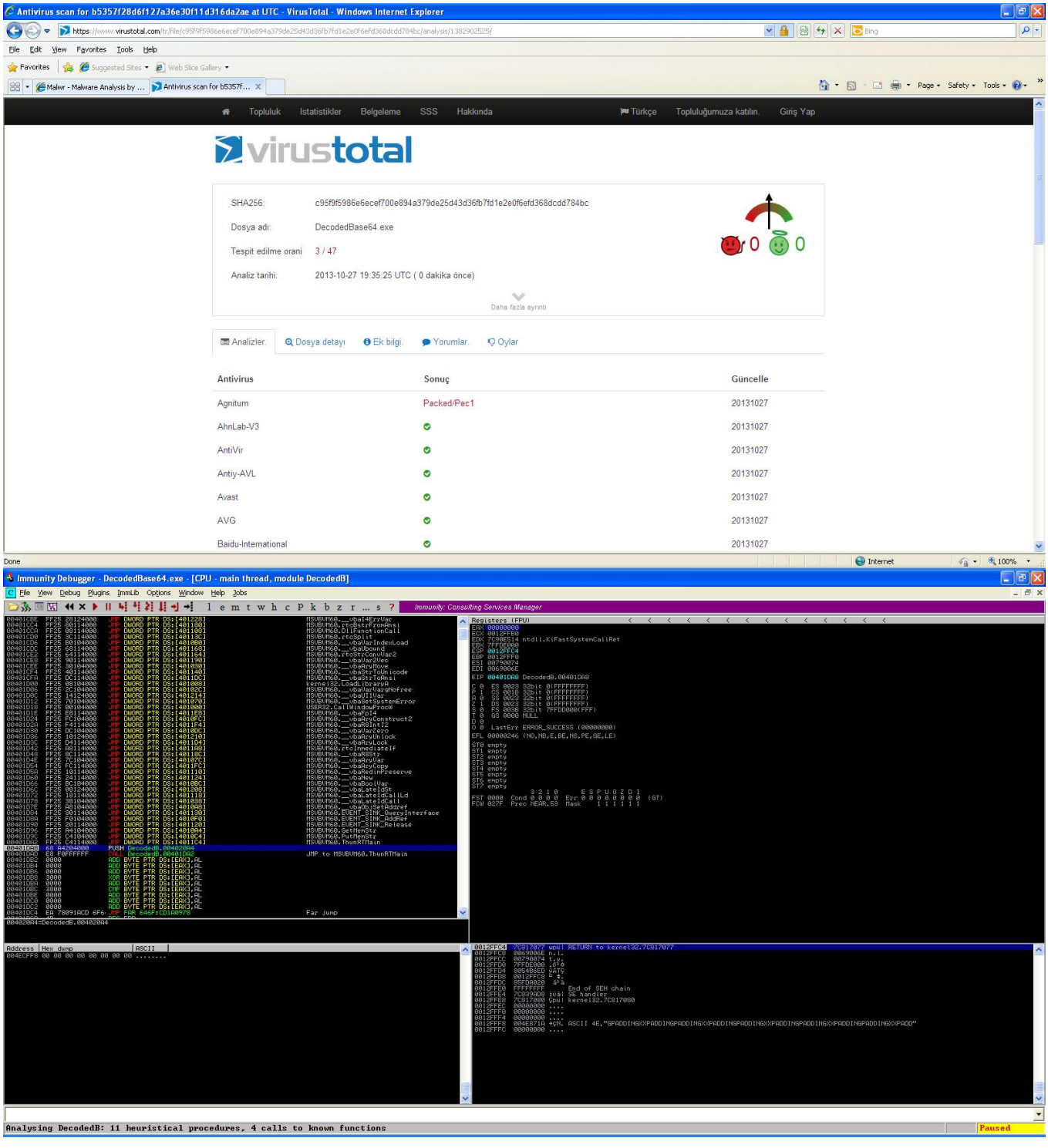


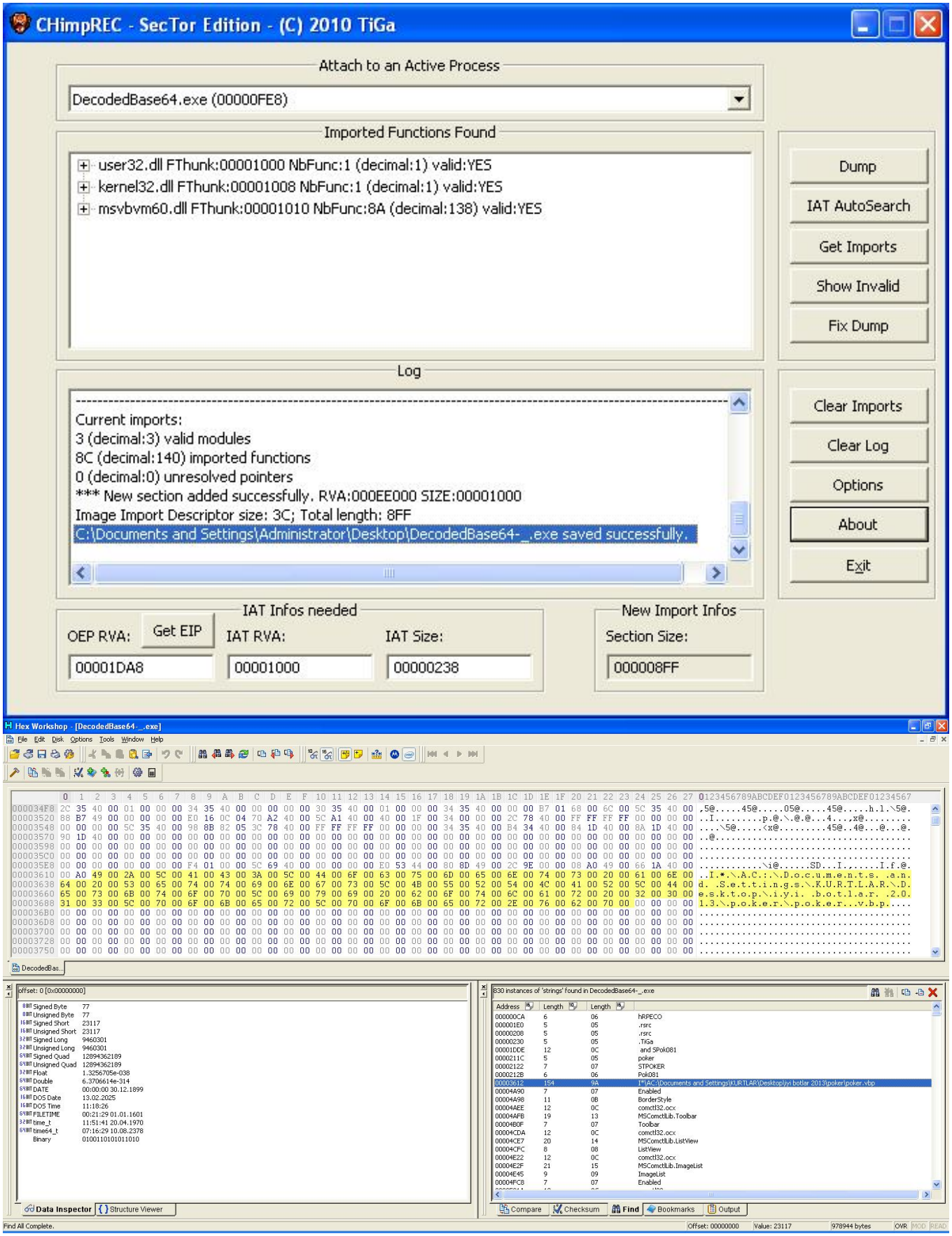
birlestirici.class dosyasını kaynak koduna çevirip analiz ettiğimde 777.exe ve POS Kontör İşlemleri Odeme_Listesi.xls dosyalarını BASE64 ile decode edip çalıştırdığını gördüm.



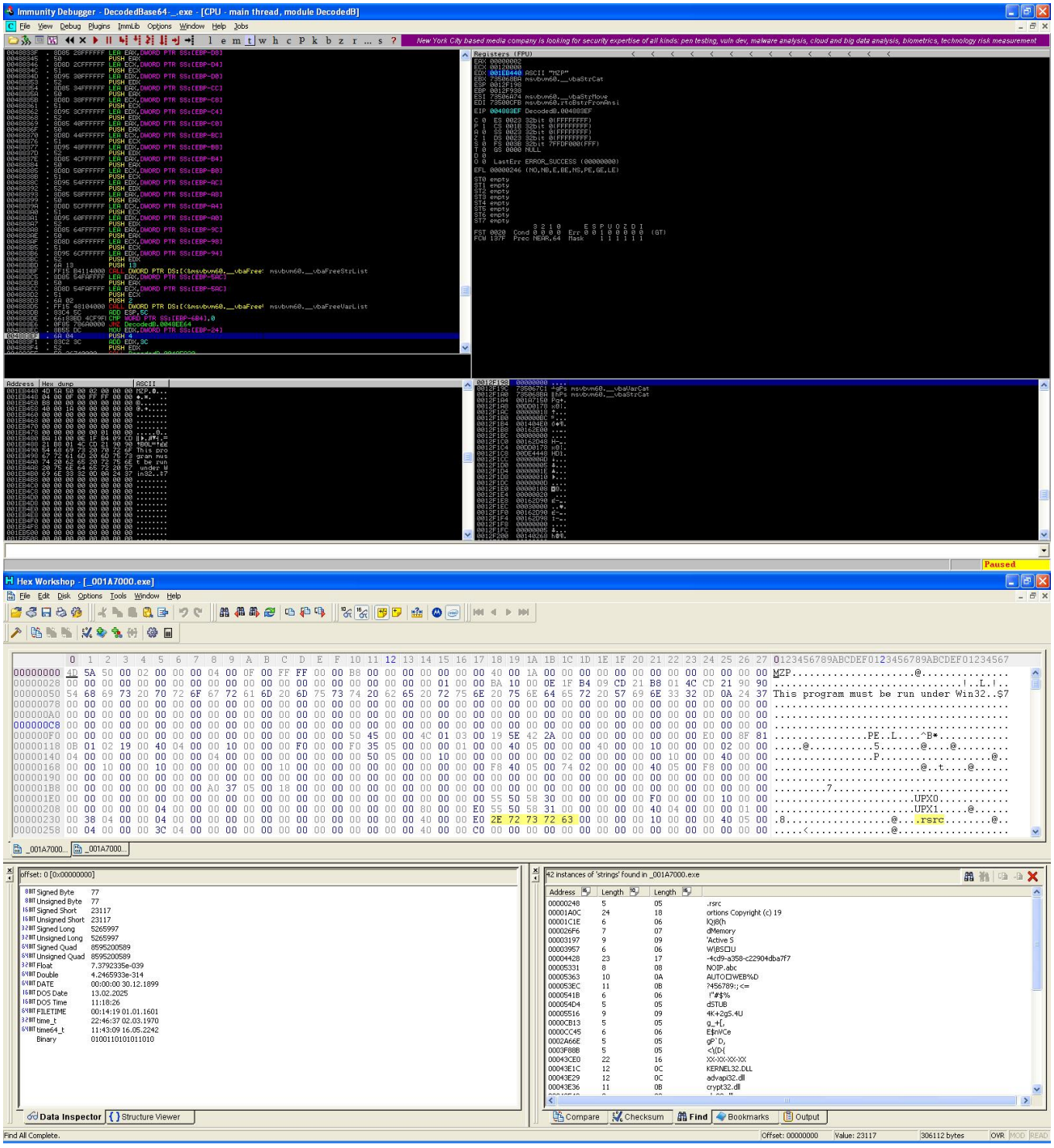
Zararsız excel dosyası bir kenara, 777.exe dosyasını BASE64 ile decode

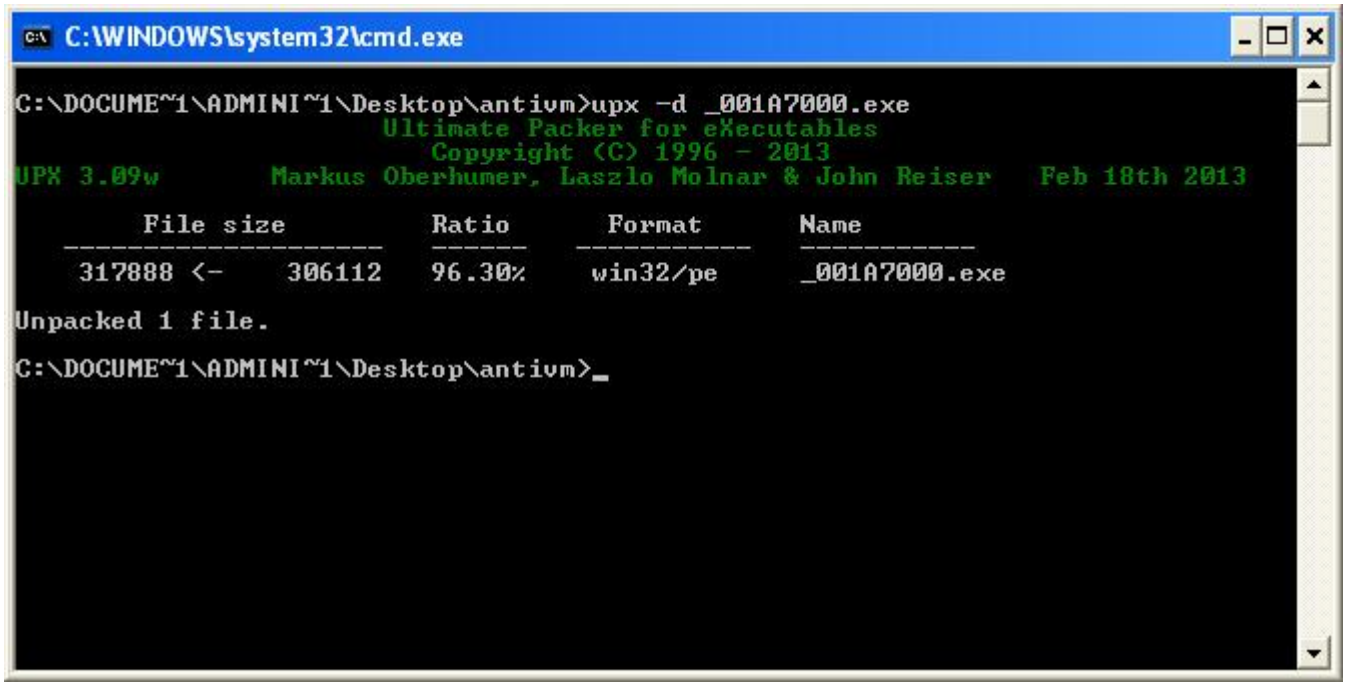
ettikten sonra (DecodedBase64.exe) Immunity Debugger hata ayıklama aracı (debugger) ile analiz etmeye başladım. Paketlenmiş olan bu dosyayı adım adım analiz ettikten sonra Visual Basic ile yazılmış başka bir yazılımı hafızada açtığını (unpack) gördüm. Statik analiz için OEP (original entry point) üzerinde programı hafızadan diske CHimpREC aracı ile DecodedBase64-_.exe adı altında kayıt (dump) ettim. Ardından bu yazılımı Malwr (cuckoo sandbox) sitesine yüklediğimde analizin başarısızlıkla sonuçlandığını gördüm.



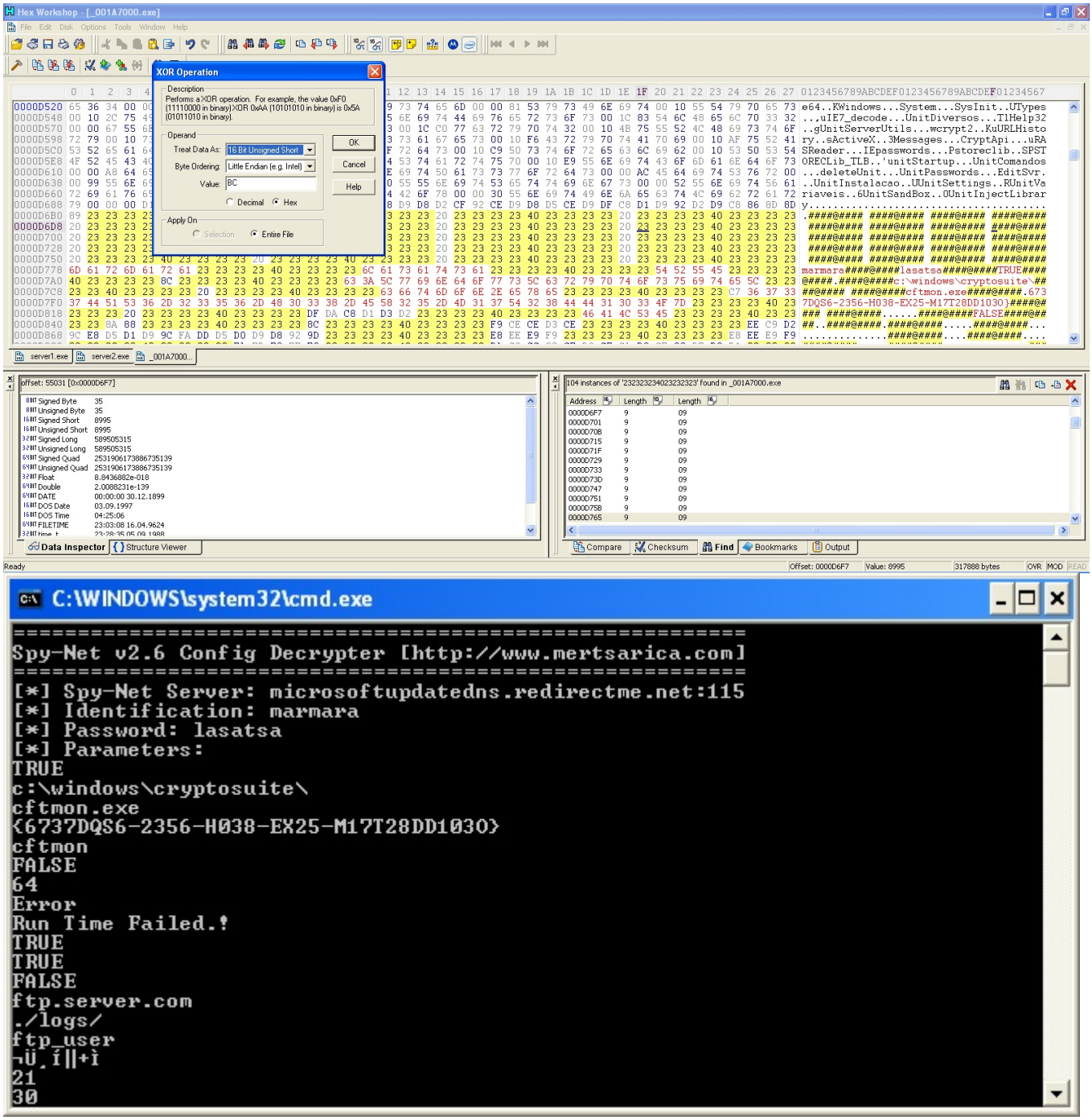


Ardından bu yazılımın da (DecodedBase64-_.exe), UPX ile derlenmiş başka bir yazılımı hafızaya açtığını gördüm ve bunu hafızadan, diske _001A7000.exe adı altında kayıt edip, UPX ile açtım (unpack).


Immunity Debugger - DecodedBase64-_.exe - [CPU - main thread, module DecodedB]
File View Debug Plugins ImmLib Options Window Help Jobs
New York City based media company is looking for security expertise of all kinds: pen testing, vuln dev, malware analysis, cloud and big data analysis, biometrics, technology risk measurement
Registers (FPU)
Paused
Hex Workshop - [_001A7000.exe]
File Edit Disk Options Tools Window Help
_001A7000...
_001A7000...
offset: 0 [0x00000000]
Data Inspector
Structure Viewer
42 instances of 'strings' found in _001A7000.exe
Compare
Checksum
Find
Bookmarks
Output
Find All Complete.
Offset: 00000000
Value: 23117
306112 bytes
OVR
MOD
READ



Statik analiz ile yazılım üzerindeki dizilerden bunun Spy-Net RAT olabileceğini düşündüm. Spy-Net RAT'i genel olarak analiz ettiğimde, istemcinin bağlanacağı sunucu adresi, şifre, sistem üzerinde çalışırken kullanacağı dosya adı gibi çeşitli bilgileri, oluşturulurken (server.exe oluşturma), 0xBC ile XOR'layarak ####@#### dizileri arasına kaydettiğini tespit ettim. Ardından Python ile bu parametreleri tespit edip, çözebilrn (XOR), Spy-Net Config Decrypter adı altında ufak bir araç hazırladım. Bu aracı, Spy-Net istemcisi (_001A7000.exe (klasik server.exe)) üzerinde çalıştırdığımda bana, bağlanacağı ip adresinden (microsoftupdatedns.redirectme.net:115), şifresine, sistem üzerinde kendini gizlemek için kullandığı dosya adına (ctfmon.exe) kadar tüm bilgileri verdi. IP adresini (81.6.76.156) kontrol ettiğim de ise yine Vodafone IP bloğuna ait olduğunu gördüm.

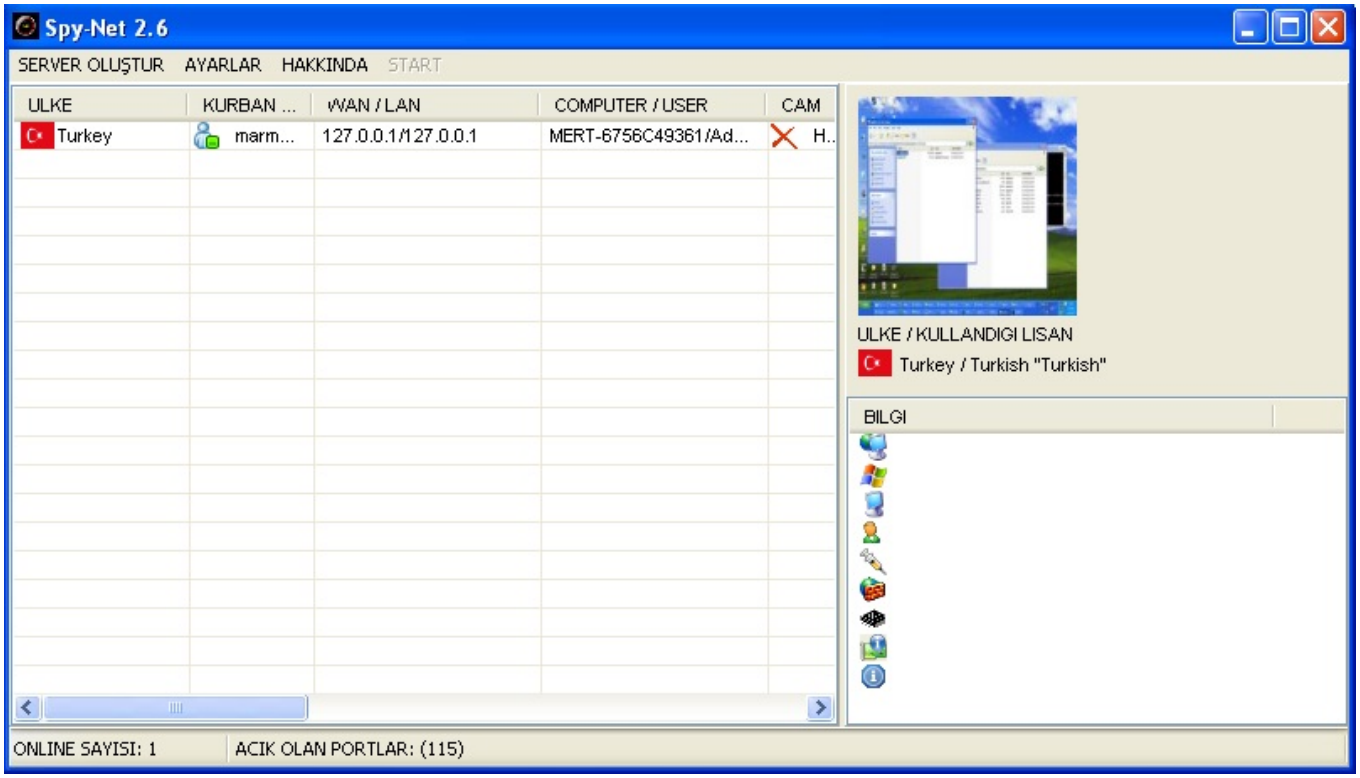

Hex Workshop - [_001A7000.exe]
XOR Operation
Description
Performs a XOR operation. For example, the value 0xF0 (11110000 in binary) XOR 0xAA (10101010 in binary) is 0x5A (01011010 in binary).
Operand
Treat Data As: 16 Bit Unsigned Short
Byte Ordering: Little Endian (e.g. Intel)
Value: BC
Decimal
Hex
Apply On
Selection
Entire File
OK
Cancel
Help
server1.exe
server2.exe
_001A7000...
Data Inspector
Structure Viewer
Compare
Checksum
Find
Bookmarks
Output
Ready

C:\WINDOWS\system32\cmd.exe
Spy-Net v2.6 Config Decrypter [http://www.mertsarica.com]
[*] Spy-Net Server: microsoftupdatedns.redirectme.net:115
[*] Identification: marmara
[*] Password: lasatsa
[*] Parameters:
TRUE
c:\windows\cryptosuite\
cftmon.exe
{6737DQS6-2356-H038-EX25-M17T28DD1030}
cftmon
FALSE
64
Error
Run Time Failed.!
TRUE
TRUE
FALSE
ftp.server.com
./logs/
ftp_user
21
30

81.6.76.156 domaininin (sitesinin) whois bilgileri :

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '81.6.64.0 - 81.6.95.255'

inetnum:        81.6.64.0 - 81.6.95.255
netname:        Vodafone-Turkey-Customer-IP-Pools
descr:          Vodafone Turkey GPRS address pool
country:        TR
admin-c:        VT1712-RIPE
tech-c:         VT1712-RIPE
status:         ASSIGNED PA
mnt-by:         RTNET-MNT
mnt-lower:      RTNET-MNT
mnt-routes:     RTNET-MNT
source:         RIPE # Filtered

person:         VODAFONE TURKEY
address:        Vodafone Telekomunikasyon A.S.
address:        Vodafone Plaza Buyukdere Cad. No:251
address:        34398 Maslak, Istanbul
address:        TURKEY
phone:          +90 212 3670000
fax-no:         +90 212 3670010
nic-hdl:        VT1712-RIPE
abuse-mailbox:  abuse-tr@vodafone.com
remarks:        Vodafone Turkey IP Management Team
source:         RIPE # Filtered
mnt-by:         RTNET-MNT

% Information related to '81.6.64.0/19AS15897'

route:          81.6.64.0/19
descr:          Vodafone Turkey 3G Pool
origin:         AS15897
mnt-by:         RTNET-MNT
source:         RIPE # Filtered
```

Sıra bunun gerçekten Spy-Net RAT olup olmadığını teyit etmeye geldiğinde, sanal makineme 115. bağlantı noktasını dinleyen Spy-Net v2.6 sunucusu kurup, hosts dosyasına 127.0.0.1 microsoftupdatedns.redirectme.net satırını ekledim. Son olarak _001A7000.exe dosyasını çalıştırdığımda ise Spy-Net arabirimi üzerinden bağlantının başarıyla gerçekleştiğini gördüm ve bu sayede bunun Spy-Net zararlı yazılımı olduğunu teyit etmiş oldum.

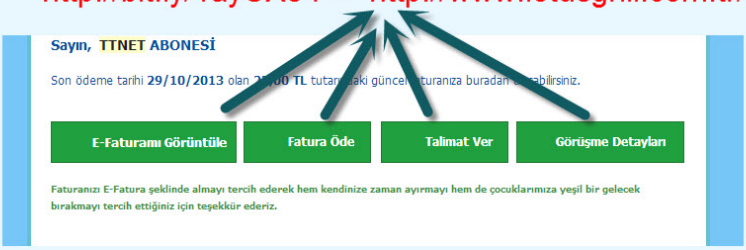


Umarım herkes için faydalı bir analiz yazısı olmuştur. Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Güncelleme: Art niyetli kişiler, 29.10.2013 tarihi itibariyle “ADSL fatura Son ödeme tarihi 29/10/2013 olan 23,00 TL tutarındaki güncel faturanız” başlıklı sahte e-posta gönderiyorlar. Bu e-postada yer alan bağlantı adresi (link) ziyaret edildiği takdirde www.lotusgrill.com.tr/tt.net.jar adresinden yukarıda analiz ettiğim benzer bir zararlı JAR dosyasını indiriliyor ve ardından microsoftupdatedns.redirectme.net adresine 112. bağlantı noktasından bağlanıyor.

From: info@ttnet.com.tr
Subject: ADSL fatura Son ödeme tarihi 29/10/2013 olan 23,00 TL tutarındaki güncel faturanız
Date: Tue, 29 Oct 2013 05:47:31 +0200

http://bit.ly/1ayCX54 -> http://www.lotusgrill.com.tr/tt.net.jar



E-FATURA (ELEKTRONİK FATURA)

KULLANIMINDA DİKKAT EDİLECEK HUSUSLAR

Türkiye genelinde e-fatura, Maliye Bakanlığı tarafından sadece elektronik fatura gönderme konusunda izin alan mükellefler tarafından gönderilebilir.

E-fatura gönderimine izin verilen mükellefler, Gelir İdaresi Başkanlığı tarafından http://www.efatura.gov.tr/ adresinde yayımlanmaktadır.

Faturada bulunan bilgilerin değiştirilmesini önlemek ve faturanın geldiği kaynağı doğrulamak amacıyla güvenli elektronik imza ile imzalanmış olması zorunluluğu bulunmaktadır. Bu nedenle, tarafınıza iletilen e-faturaların üzerinde yer alan elektronik imzanın doğrulanması, güvenliğiniz açısından önem arz etmektedir.

Adres: © Türk Telekomünikasyon A.Ş. Turgut Özal Bulvarı 06103 Aydınlıkevler, ANKARA

Faks: 0312 324 53 11