

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.

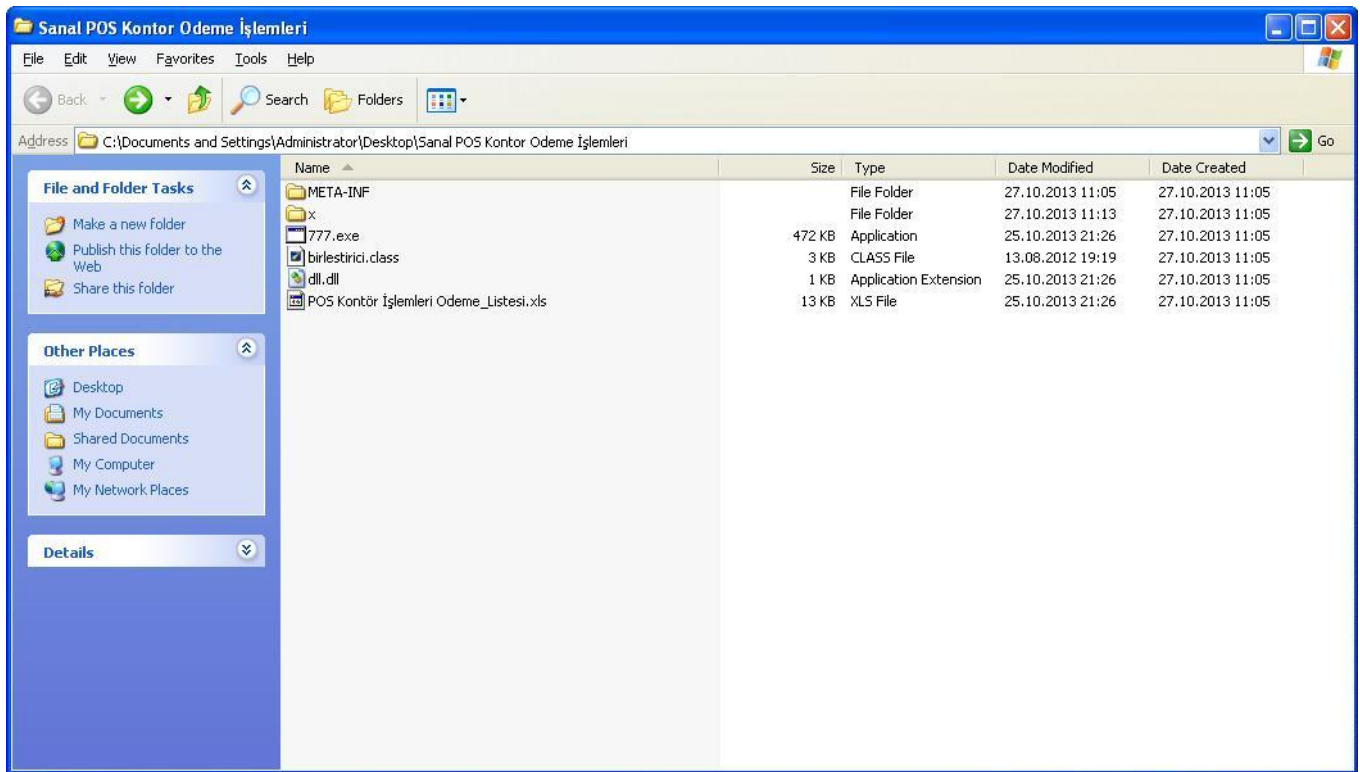
Sahte e-postanın ekinde Sanal POS Kontor Odeme İşlemleri.jar isimli bir dosya yer alıyordu.

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.

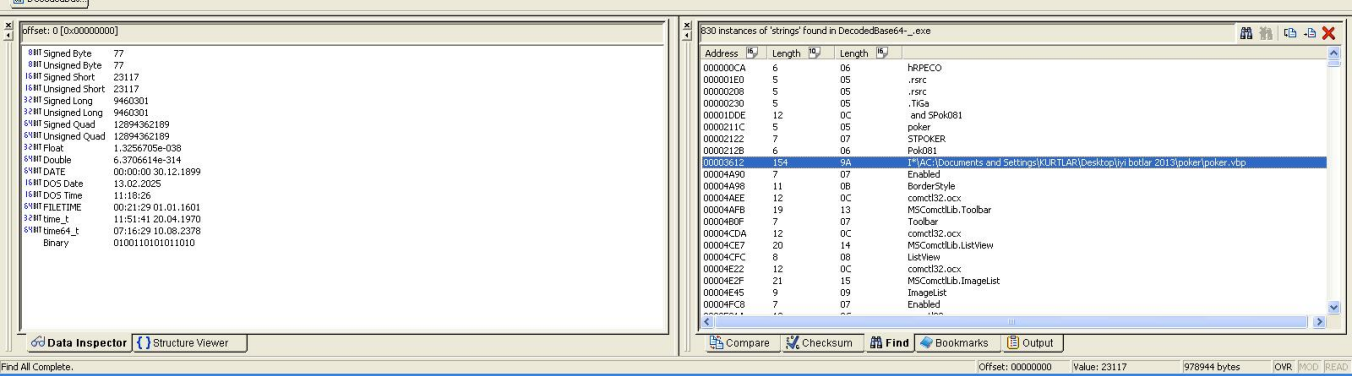
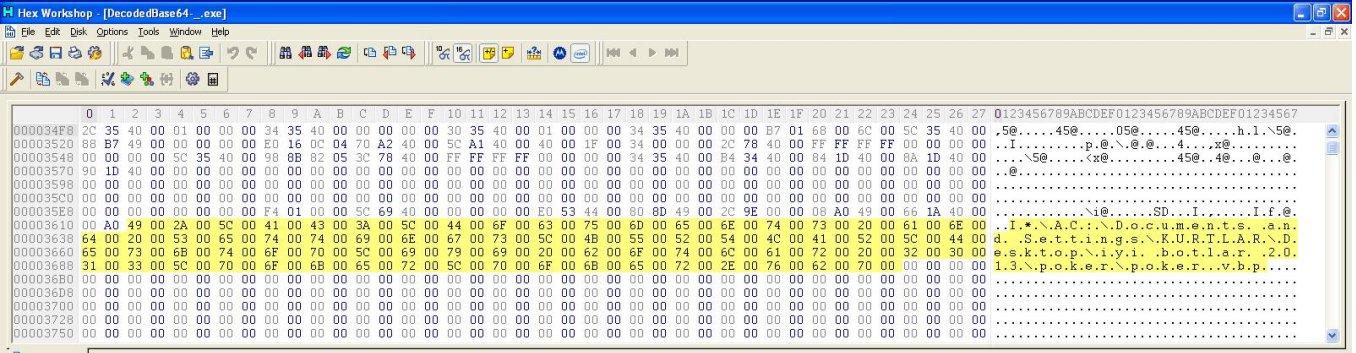
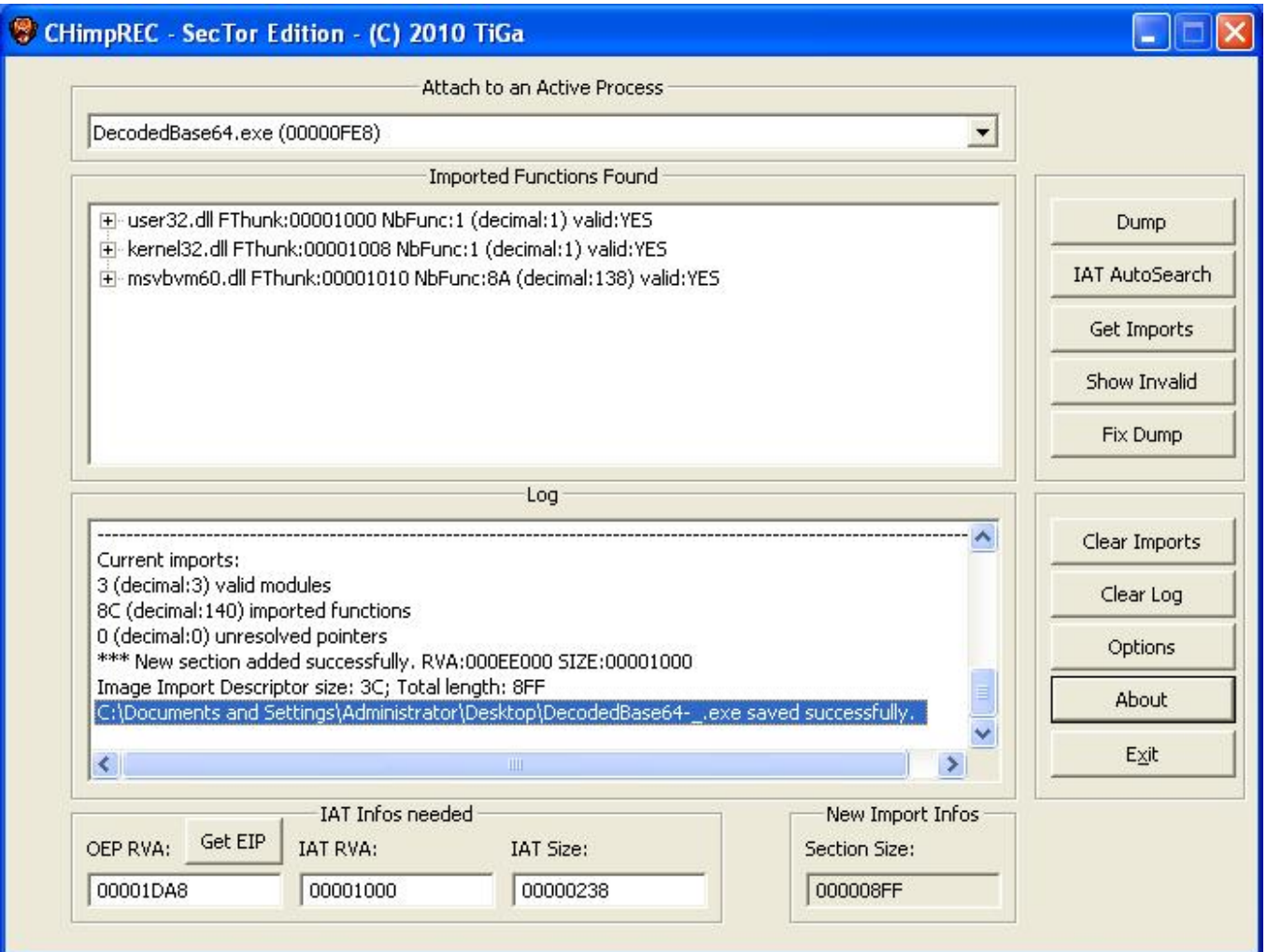


birlestirici.class dosyasını kaynak koduna çevirip analiz ettiğimde 777.exe ve POS Kontör İşlemleri Odeme_Listesi.xls dosyalarını BASE64 ile decode edip çalıştırdığını gördüm.

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.

The image shows two screenshots. The top one is a VirusTotal scan result for a file named 'DecodedBase64.exe'. The scan was performed on 2013-10-27 at 19:35:25 UTC. The file's SHA256 hash is c95f95986e6ecf700e894a379de25d43d36fb7fd1e2e0f6fd368dcd784bc. The scan shows that Agnitum detected the file as 'Packed/Pec1', while all other antivirus engines (AhnLab-V3, AntiVir, Antiy-AVL, Avast, AVG, Baidu-International) reported the file as clean (green checkmarks).

The bottom screenshot shows the Immunity Debugger interface with the CPU registers (EIP, EAX, ECX, EDI, etc.) and the disassembled code of the 'DecodedBase64.exe' module. The EIP register is at address 00401D08, pointing to the instruction 'JMP to HSBWV60.ThunRtMain'. The disassembly shows various instructions including 'JMP', 'JMP to HSBWV60.ThunRtMain', 'JMP to HSBWV60.ThunRtMain', and 'Far Jump'.



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).


```
C:\WINDOWS\system32\cmd.exe

C:\DOCUMENTS\ADMINI~1\Desktop\antivm>upx -d _001A7000.exe
          Ultimate Packer for eXecutables
          Copyright (C) 1996 - 2013
UPX 3.09w      Markus Oberhumer, Laszlo Molnar & John Reiser   Feb 18th 2013

-----
File size      Ratio      Format      Name
-----
317888 <-    306112    96.30%    win32/pe    _001A7000.exe

Unpacked 1 file.

C:\DOCUMENTS\ADMINI~1\Desktop\antivm>_
```

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 kullanılacağı 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, çözebilir (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]

File Edit Disk Options Tools Window Help

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

Apply On: Selection Entire File

0 1 2 3 4

0000D520 65 36 34 00 00 9 73 74 65 6D 00 00 81 53 79 73 49 6E 69 74 00 10 55 54 79 70 65 73 e64..KWindows...System...SysInit...Types

0000D548 00 10 2C 75 45 5 6E 69 74 44 69 76 65 72 73 6F 73 00 1C 83 54 6C 48 65 6C 70 33 32 ..uIE7_decode...UnitDiversos...THelp32

0000D570 00 00 67 55 65 3 00 1C 00 77 53 72 79 70 74 32 00 10 4B 75 55 52 4C 48 69 73 74 6F ..gUnitServerUtils...wcrypt2..KuURLHisto

0000D5C0 53 52 65 61 64 9 73 61 67 65 73 00 10 F6 43 72 79 70 74 41 70 69 00 10 AF 75 52 41 ry...ActiveX...3Messages...CryptApi...uRA

0000D5E8 4F 52 45 43 40 4 F 72 64 73 00 10 C9 50 73 74 6F 72 65 63 6C 69 62 00 10 53 50 53 54 SReader...IPasswords...PstocrcLib...SPST

0000D610 00 00 A8 64 69 4 53 74 61 72 74 75 70 00 10 E9 55 6E 69 74 43 6F 6D 61 6E 64 6F 73 ORECLib.TLB.'unitStartup...UnitComandos

0000D638 00 99 55 6E 65 0 55 55 6E 69 74 53 65 74 74 69 6E 67 73 00 00 52 55 6E 69 74 56 61 ..deleteUnit...UnitPasswords...EditSvr.

0000D660 72 69 61 76 65 4 42 6F 78 00 00 30 55 6E 69 74 49 6E 6A 65 63 74 4C 69 62 72 61 72 y.....

0000D688 75 00 00 00 0 8 D9 D8 D2 CF 92 CE D9 D8 D5 CE D9 DF 09 D1 D9 92 D2 D9 D8 06 0D 8D #####

0000D6B0 89 23 23 23 23 3 23 23 20 23 23 23 40 23 23 23 20 23 23 23 23 40 23 23 23 23 #####

0000D6D8 20 23 23 23 23 3 23 23 20 23 23 23 40 23 23 23 20 23 23 23 23 40 23 23 23 23 #####

0000D700 20 23 23 23 23 3 23 23 20 23 23 23 40 23 23 23 20 23 23 23 23 40 23 23 23 23 #####

0000D728 20 23 23 23 23 3 23 23 20 23 23 23 40 23 23 23 20 23 23 23 23 40 23 23 23 23 #####

0000D750 20 23 23 23 23 40 23 23 23 23 20 23 23 23 23 40 23 23 23 23 23 23 23 23 23 #####

0000D778 6D 61 72 6D 61 72 61 23 23 23 40 23 23 23 23 23 6C 61 73 61 74 73 61 23 23 23 40 23 23 23 54 52 55 45 23 23 23 23 marmara#####lasatsa#####IRUE###

0000D7A0 40 23 23 23 23 8C 23 23 23 23 40 23 23 23 23 63 38 5C 77 69 6E 64 6F 77 73 5C 63 72 79 70 74 6F 73 75 69 74 65 5C 23 23 8####.#####:windows\cryptosuite##

0000D7C8 23 23 40 23 23 23 20 23 23 23 23 40 23 23 23 23 63 66 74 6D 6F 6E 2E 65 78 65 23 23 23 40 23 23 23 07 36 37 33 #####.#####cftmon.exe#####673

0000D7F0 37 44 51 53 36 2D 32 33 35 36 2D 48 30 33 38 2D 45 58 32 35 2D 40 31 37 54 32 38 44 44 31 30 33 4F 7D 23 23 23 40 23 7DQSG-2356-H038-EX25-M17T28DD1030#####

0000D818 23 23 23 20 23 23 23 23 40 23 23 23 23 DF DA C8 D1 D3 D2 23 23 23 40 23 23 23 23 46 41 4C 53 45 23 23 23 40 23 23 23 23 #####

0000D840 23 23 BA 88 23 23 23 23 40 23 23 23 23 8C 23 23 23 23 40 23 23 23 23 CE C9 D2 ########FALSE#####

0000D868 9C E8 D5 D1 D9 9C FA DD D5 D0 D9 D8 92 9D 23 23 23 23 40 23 23 23 23 E8 E9 F9 #####

Ready Offset: 0000D6F7 Value: 8995 317888 bytes OVR MOD READ

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
{6737DQSG-2356-H038-EX25-M17T28DD1030}
cftmon
FALSE
64
Error
Run Time Failed.!
TRUE
TRUE
FALSE
ftp.server.com
./logs/
ftp_user
-Ü_î||+i
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'

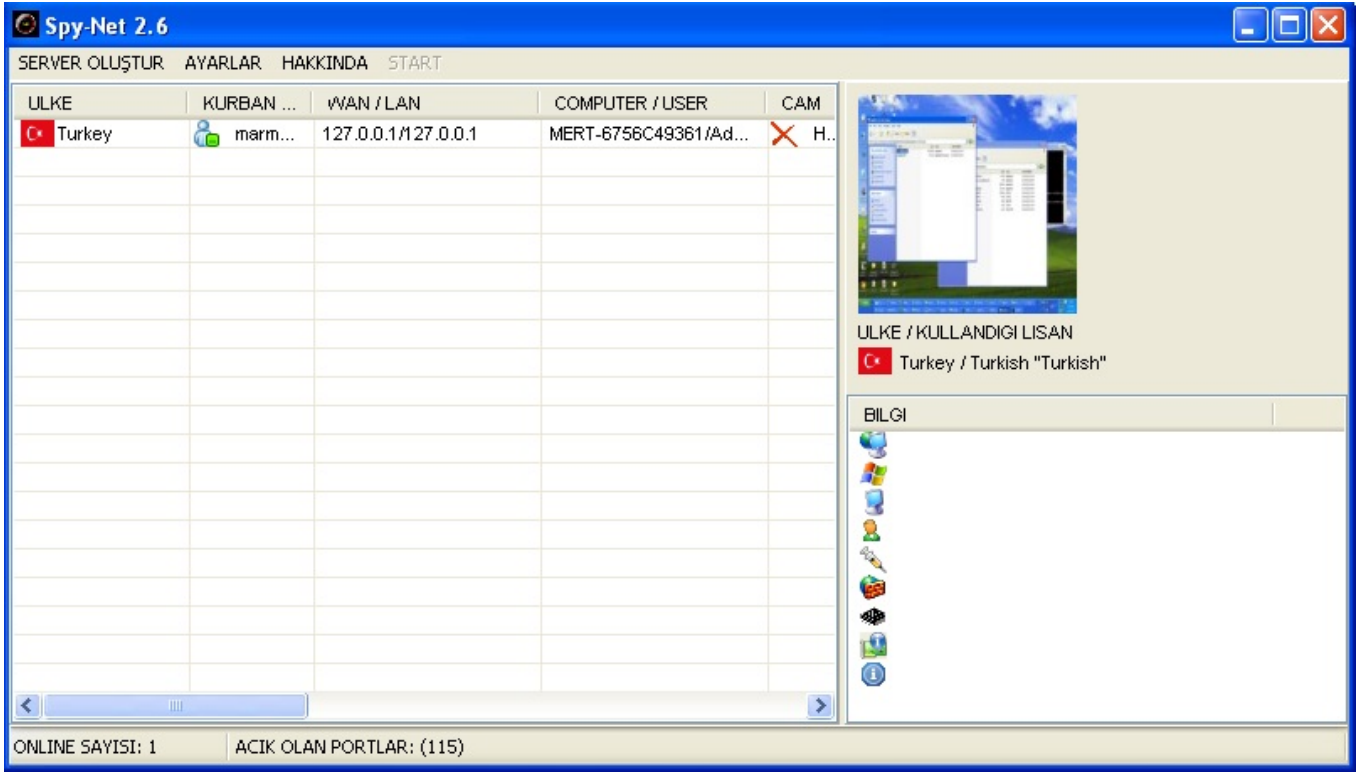
inetnum:        81.6.64.0 - 81.6.95.255
netname:        Vodafone-Turkey-Customer-IP-Pools
descr:          Vodafone Turkey GPRS address pool
country:        TR
admin-c:        VT1712-RIPE
tech-c:         VT1712-RIPE
status:         ASSIGNED PA
mnt-by:         RTNET-MNT
mnt-lower:      RTNET-MNT
mnt-routes: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

Sayın, **TTNET ABONESİ**

Son ödeme tarihi **29/10/2013** olan **23,00 TL** tutarındaki güncel faturanıza buradan ulaşabilirsiniz.

E-Faturamı Görüntüle

Fatura Öde

Talimat Ver

Görüşme Detayları

Faturanızı E-Fatura şeklinde almayı tercih ederek hem kendinize zaman ayırmayı hem de çocuklarımızı yeşil bir gelecek bırakmayı tercih ettiğiniz için teşekkür ederiz.

E-FATURA (ELEKTRONİK FATURA)

KULLANIMINDA DİKKAT EDİLECEK HUSUSLAR

Türkiye genelinde e-fatura, Maliye Bakanlığı tarafından sadece elektronik fatura göndeme 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, güvenliğinizi açısından önem arz etmektedir.

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

Faks: [0312 324 53 11](tel:03123245311)