

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.

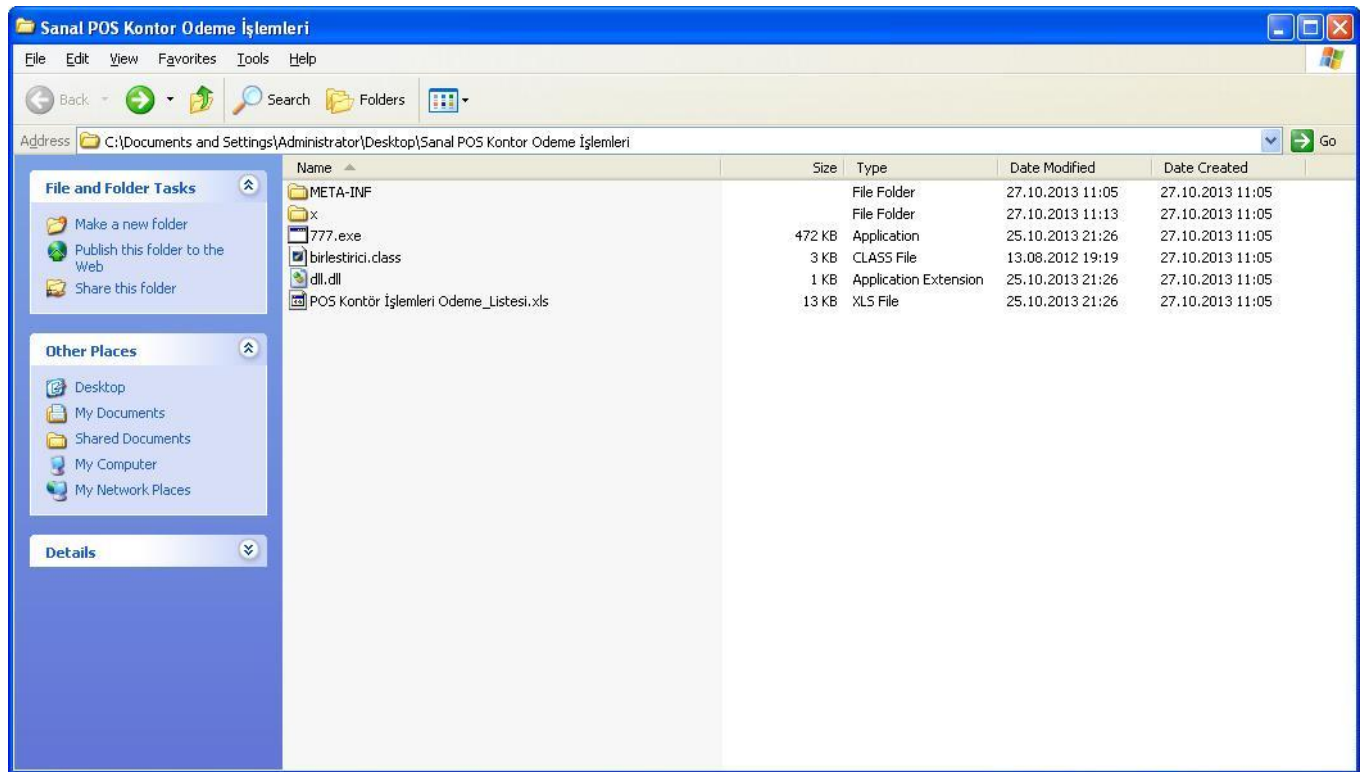
Sahte e-postanın ekinde Sanal POS Kontor Odeme İşlemleri.jar isimli bir dosya yer alıyordu.

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 Kontör 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 dosyalarının 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 screenshot 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 c95f95986e6ecf700e894a379de25d43d36fb7fd1e2e0fe6d368dcd784bc. The scan results show that the file is 'Packed/Pec1' and is detected by several antivirus engines, including Agnitum, AhnLab-V3, AntiVir, Antiy-AVL, Avast, AVG, and Baidu-International. The bottom screenshot is a screenshot of Immunity Debugger showing the execution of 'DecodedBase64.exe'. The CPU window shows the main thread at address 00401000, which is the entry point of the program. The registers window shows the EIP register at 00401000, which is the entry point of the program. The memory window shows the program's memory at address 00401000, which is the entry point of the program. The status bar at the bottom indicates that the program is 'Paused'.

Antivirus scan for b5357f728d6f127a36e30f11d316da2ae at UTC. VirusTotal. Windows Internet Explorer

File Edit View Favorites Tools Help

Malwr - Malware Analysis by ... Antivirus scan for b5357f... X

Topluluk İstatistikler Belgeleme SSS Hakkında Türkçe Topluluğumuza katılın. Giriş Yap

virustotal

SHA256: c95f95986e6ecf700e894a379de25d43d36fb7fd1e2e0fe6d368dcd784bc

Dosya adı: DecodedBase64.exe

Tespit edilme oranı: 3 / 47

Analiz tarihi: 2013-10-27 19:35:25 UTC (0 dakika önce)

Daha fazla ayrıntı

Analizler: Dosya detayı Ek bilgi Yorumlar Oylar

Antivirus	Sonuç	Güncelle
Agnitum	Packed/Pec1	20131027
AhnLab-V3	✓	20131027
AntiVir	✓	20131027
Antiy-AVL	✓	20131027
Avast	✓	20131027
AVG	✓	20131027
Baidu-International	✓	20131027

Done

Immunity Debugger - DecodedBase64.exe [CPU - main thread, module DecodedB]

File View Debug Plugins ImmLib Options Window Help Jobs

Immunity Consulting Services Manager

Registers (FPU)

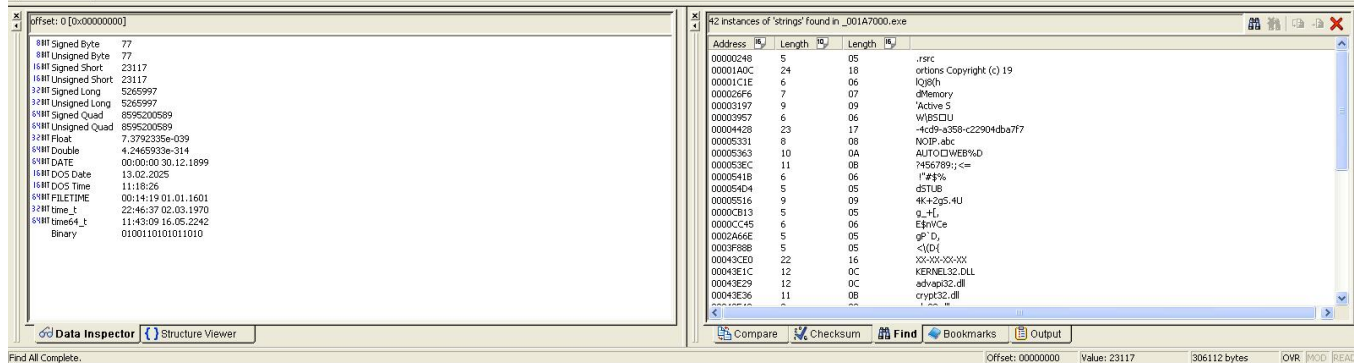
EAX 00000000
ECX 0012FF00
EDX 7C901F00
ESP 0012FF00
EBP 0012FF00
ESI 007A0074
EDI 0069006E
EIP 00401000 DecodedB.00401000

C 0 ES 0020 32b1 0FFFFFFF
P 1 ES 0018 32b1 0FFFFFFF
O 0 SS 0020 32b1 0FFFFFFF
C 1 DS 0020 32b1 0FFFFFFF
S 0 FS 0020 32b1 7F000000
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_SUCCESS (00000000)
EFL 00002040 (NO,IO,E,GE,NO,FE,GE,LE)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty

FPU Cond 0 0 0 0 Exp 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,S3 Rask 1 1 1 1 1 1 1 1

00401000 FF25 20124000 JFF DMOG PTR DS:[401200]
00401004 FF25 00114000 JFF DMOG PTR DS:[401100]
00401008 FF25 00114000 JFF DMOG PTR DS:[401100]
0040100C FF25 00114000 JFF DMOG PTR DS:[401100]
00401010 FF25 00114000 JFF DMOG PTR DS:[401100]
00401014 FF25 00114000 JFF DMOG PTR DS:[401100]
00401018 FF25 00114000 JFF DMOG PTR DS:[401100]
0040101C FF25 00114000 JFF DMOG PTR DS:[401100]
00401020 FF25 00114000 JFF DMOG PTR DS:[401100]
00401024 FF25 00114000 JFF DMOG PTR DS:[401100]
00401028 FF25 00114000 JFF DMOG PTR DS:[401100]
0040102C FF25 00114000 JFF DMOG PTR DS:[401100]
00401030 FF25 00114000 JFF DMOG PTR DS:[401100]
00401034 FF25 00114000 JFF DMOG PTR DS:[401100]
00401038 FF25 00114000 JFF DMOG PTR DS:[401100]
0040103C FF25 00114000 JFF DMOG PTR DS:[401100]
00401040 FF25 00114000 JFF DMOG PTR DS:[401100]
00401044 FF25 00114000 JFF DMOG PTR DS:[401100]
00401048 FF25 00114000 JFF DMOG PTR DS:[401100]
0040104C FF25 00114000 JFF DMOG PTR DS:[401100]
00401050 FF25 00114000 JFF DMOG PTR DS:[401100]
00401054 FF25 00114000 JFF DMOG PTR DS:[401100]
00401058 FF25 00114000 JFF DMOG PTR DS:[401100]
0040105C FF25 00114000 JFF DMOG PTR DS:[401100]
00401060 FF25 00114000 JFF DMOG PTR DS:[401100]
00401064 FF25 00114000 JFF DMOG PTR DS:[401100]
00401068 FF25 00114000 JFF DMOG PTR DS:[401100]
0040106C FF25 00114000 JFF DMOG PTR DS:[401100]
00401070 FF25 00114000 JFF DMOG PTR DS:[401100]
00401074 FF25 00114000 JFF DMOG PTR DS:[401100]
00401078 FF25 00114000 JFF DMOG PTR DS:[401100]
0040107C FF25 00114000 JFF DMOG PTR DS:[401100]
00401080 FF25 00114000 JFF DMOG PTR DS:[401100]
00401084 FF25 00114000 JFF DMOG PTR DS:[401100]
00401088 FF25 00114000 JFF DMOG PTR DS:[401100]
0040108C FF25 00114000 JFF DMOG PTR DS:[401100]
00401090 FF25 00114000 JFF DMOG PTR DS:[401100]
00401094 FF25 00114000 JFF DMOG PTR DS:[401100]
00401098 FF25 00114000 JFF DMOG PTR DS:[401100]
0040109C FF25 00114000 JFF DMOG PTR DS:[401100]
004010A0 FF25 00114000 JFF DMOG PTR DS:[401100]
004010A4 FF25 00114000 JFF DMOG PTR DS:[401100]
004010A8 FF25 00114000 JFF DMOG PTR DS:[401100]
004010AC FF25 00114000 JFF DMOG PTR DS:[401100]
004010B0 FF25 00114000 JFF DMOG PTR DS:[401100]
004010B4 FF25 00114000 JFF DMOG PTR DS:[401100]
004010B8 FF25 00114000 JFF DMOG PTR DS:[401100]
004010BC FF25 00114000 JFF DMOG PTR DS:[401100]
004010C0 FF25 00114000 JFF DMOG PTR DS:[401100]
004010C4 FF25 00114000 JFF DMOG PTR DS:[401100]
004010C8 FF25 00114000 JFF DMOG PTR DS:[401100]
004010CC FF25 00114000 JFF DMOG PTR DS:[401100]
004010D0 FF25 00114000 JFF DMOG PTR DS:[401100]
004010D4 FF25 00114000 JFF DMOG PTR DS:[401100]
004010D8 FF25 00114000 JFF DMOG PTR DS:[401100]
004010DC FF25 00114000 JFF DMOG PTR DS:[401100]
004010E0 FF25 00114000 JFF DMOG PTR DS:[401100]
004010E4 FF25 00114000 JFF DMOG PTR DS:[401100]
004010E8 FF25 00114000 JFF DMOG PTR DS:[401100]
004010EC FF25 00114000 JFF DMOG PTR DS:[401100]
004010F0 FF25 00114000 JFF DMOG PTR DS:[401100]
004010F4 FF25 00114000 JFF DMOG PTR DS:[401100]
004010F8 FF25 00114000 JFF DMOG PTR DS:[401100]
004010FC FF25 00114000 JFF DMOG PTR DS:[401100]
00401100 FF25 00114000 JFF DMOG PTR DS:[401100]
00401104 FF25 00114000 JFF DMOG PTR DS:[401100]
00401108 FF25 00114000 JFF DMOG PTR DS:[401100]
0040110C FF25 00114000 JFF DMOG PTR DS:[401100]
00401110 FF25 00114000 JFF DMOG PTR DS:[401100]
00401114 FF25 00114000 JFF DMOG PTR DS:[401100]
00401118 FF25 00114000 JFF DMOG PTR DS:[401100]
0040111C FF25 00114000 JFF DMOG PTR DS:[401100]
00401120 FF25 00114000 JFF DMOG PTR DS:[401100]
00401124 FF25 00114000 JFF DMOG PTR DS:[401100]
00401128 FF25 00114000 JFF DMOG PTR DS:[401100]
0040112C FF25 00114000 JFF DMOG PTR DS:[401100]
00401130 FF25 00114000 JFF DMOG PTR DS:[401100]
00401134 FF25 00114000 JFF DMOG PTR DS:[401100]
00401138 FF25 00114000 JFF DMOG PTR DS:[401100]
0040113C FF25 00114000 JFF DMOG PTR DS:[401100]
00401140 FF25 00114000 JFF DMOG PTR DS:[401100]
00401144 FF25 00114000 JFF DMOG PTR DS:[401100]
00401148 FF25 00114000 JFF DMOG PTR DS:[401100]
0040114C FF25 00114000 JFF DMOG PTR DS:[401100]
00401150 FF25 00114000 JFF DMOG PTR DS:[401100]
00401154 FF25 00114000 JFF DMOG PTR DS:[401100]
00401158 FF25 00114000 JFF DMOG PTR DS:[401100]
0040115C FF25 00114000 JFF DMOG PTR DS:[401100]
00401160 FF25 00114000 JFF DMOG PTR DS:[401100]
00401164 FF25 00114000 JFF DMOG PTR DS:[401100]
00401168 FF25 00114000 JFF DMOG PTR DS:[401100]
0040116C FF25 00114000 JFF DMOG PTR DS:[401100]
00401170 FF25 00114000 JFF DMOG PTR DS:[401100]
00401174 FF25 00114000 JFF DMOG PTR DS:[401100]
00401178 FF25 00114000 JFF DMOG PTR DS:[401100]
0040117C FF25 00114000 JFF DMOG PTR DS:[401100]
00401180 FF25 00114000 JFF DMOG PTR DS:[401100]
00401184 FF25 00114000 JFF DMOG PTR DS:[401100]
00401188 FF25 00114000 JFF DMOG PTR DS:[401100]
0040118C FF25 00114000 JFF DMOG PTR DS:[401100]
00401190 FF25 00114000 JFF DMOG PTR DS:[401100]
00401194 FF25 00114000 JFF DMOG PTR DS:[401100]
00401198 FF25 00114000 JFF DMOG PTR DS:[401100]
0040119C FF25 00114000 JFF DMOG PTR DS:[401100]
004011A0 FF25 00114000 JFF DMOG PTR DS:[401100]
004011A4 FF25 00114000 JFF DMOG PTR DS:[401100]
004011A8 FF25 00114000 JFF DMOG PTR DS:[401100]
004011AC FF25 00114000 JFF DMOG PTR DS:[401100]
004011B0 FF25 00114000 JFF DMOG PTR DS:[401100]
004011B4 FF25 00114000 JFF DMOG PTR DS:[401100]
004011B8 FF25 00114000 JFF DMOG PTR DS:[401100]
004011BC FF25 00114000 JFF DMOG PTR DS:[401100]
004011C0 FF25 00114000 JFF DMOG PTR DS:[401100]
004011C4 FF25 00114000 JFF DMOG PTR DS:[401100]
004011C8 FF25 00114000 JFF DMOG PTR DS:[401100]
004011CC FF25 00114000 JFF DMOG PTR DS:[401100]
004011D0 FF25 00114000 JFF DMOG PTR DS:[401100]
004011D4 FF25 00114000 JFF DMOG PTR DS:[401100]
004011D8 FF25 00114000 JFF DMOG PTR DS:[401100]
004011DC FF25 00114000 JFF DMOG PTR DS:[401100]
004011E0 FF25 00114000 JFF DMOG PTR DS:[401100]
004011E4 FF25 00114000 JFF DMOG PTR DS:[401100]
004011E8 FF25 00114000 JFF DMOG PTR DS:[401100]
004011EC FF25 00114000 JFF DMOG PTR DS:[401100]
004011F0 FF25 00114000 JFF DMOG PTR DS:[401100]
004011F4 FF25 00114000 JFF DMOG PTR DS:[401100]
004011F8 FF25 00114000 JFF DMOG PTR DS:[401100]
004011FC FF25 00114000 JFF DMOG PTR DS:[401100]
00401200 FF25 00114000 JFF DMOG PTR DS:[401100]
00401204 FF25 00114000 JFF DMOG PTR DS:[401100]
00401208 FF25 00114000 JFF DMOG PTR DS:[401100]
0040120C FF25 00114000 JFF DMOG PTR DS:[401100]
00401210 FF25 00114000 JFF DMOG PTR DS:[401100]
00401214 FF25 00114000 JFF DMOG PTR DS:[401100]
00401218 FF25 00114000 JFF DMOG PTR DS:[401100]
0040121C FF25 00114000 JFF DMOG PTR DS:[401100]
00401220 FF25 00114000 JFF DMOG PTR DS:[401100]
00401224 FF25 00114000 JFF DMOG PTR DS:[401100]
00401228 FF25 00114000 JFF DMOG PTR DS:[401100]
0040122C FF25 00114000 JFF DMOG PTR DS:[401100]
00401230 FF25 00114000 JFF DMOG PTR DS:[401100]
00401234 FF25 00114000 JFF DMOG PTR DS:[401100]
00401238 FF25 00114000 JFF DMOG PTR DS:[401100]
0040123C FF25 00114000 JFF DMOG PTR DS:[401100]
00401240 FF25 00114000 JFF DMOG PTR DS:[401100]
00401244 FF25 00114000 JFF DMOG PTR DS:[401100]
00401248 FF25 00114000 JFF DMOG PTR DS:[401100]
0040124C FF25 00114000 JFF DMOG PTR DS:[401100]
00401250 FF25 00114000 JFF DMOG PTR DS:[401100]
00401254 FF25 00114000 JFF DMOG PTR DS:[401100]
00401258 FF25 00114000 JFF DMOG PTR DS:[401100]
0040125C FF25 00114000 JFF DMOG PTR DS:[401100]
00401260 FF25 00114000 JFF DMOG PTR DS:[401100]
00401264 FF25 00114000 JFF DMOG PTR DS:[401100]
00401268 FF25 00114000 JFF DMOG PTR DS:[401100]
0040126C FF25 00114000 JFF DMOG PTR DS:[401100]
00401270 FF25 00114000 JFF DMOG PTR DS:[401100]
00401274 FF25 00114000 JFF DMOG PTR DS:[401100]
00401278 FF25 00114000 JFF DMOG PTR DS:[401100]
0040127C FF25 00114000 JFF DMOG PTR DS:[401100]
00401280 FF25 00114000 JFF DMOG PTR DS:[401100]
00401284 FF25 00114000 JFF DMOG PTR DS:[401100]
00401288 FF25 00114000 JFF DMOG PTR DS:[401100]
0040128C FF25 00114000 JFF DMOG PTR DS:[401100]
00401290 FF25 00114000 JFF DMOG PTR DS:[401100]
00401294 FF25 00114000 JFF DMOG PTR DS:[401100]
00401298 FF25 00114000 JFF DMOG PTR DS:[401100]
0040129C FF25 00114000 JFF DMOG PTR DS:[401100]
004012A0 FF25 00114000 JFF DMOG PTR DS:[401100]
004012A4 FF25 00114000 JFF DMOG PTR DS:[401100]
004012A8 FF25 00114000 JFF DMOG PTR DS:[401100]
004012AC FF25 00114000 JFF DMOG PTR DS:[401100]
004012B0 FF25 00114000 JFF DMOG PTR DS:[401100]
004012B4 FF25 00114000 JFF DMOG PTR DS:[401100]
004012B8 FF25 00114000 JFF DMOG PTR DS:[401100]
004012BC FF25 00114000 JFF DMOG PTR DS:[401100]
004012C0 FF25 00114000 JFF DMOG PTR DS:[401100]
004012C4 FF25 00114000 JFF DMOG PTR DS:[401100]
004012C8 FF25 00114000 JFF DMOG PTR DS:[401100]
004012CC FF25 00114000 JFF DMOG PTR DS:[401100]
004012D0 FF25 00114000 JFF DMOG PTR DS:[401100]
004012D4 FF25 00114000 JFF DMOG PTR DS:[401100]
004012D8 FF25 00114000 JFF DMOG PTR DS:[401100]
004012DC FF25 00114000 JFF DMOG PTR DS:[401100]
004012E0 FF25 00114000 JFF DMOG PTR DS:[401100]
004012E4 FF25 00114000 JFF DMOG PTR DS:[401100]
004012E8 FF25 00114000 JFF DMOG PTR DS:[401100]
004012EC FF25 00114000 JFF DMOG PTR DS:[401100]
004012F0 FF25 00114000 JFF DMOG PTR DS:[401100]
004012F4 FF25 00114000 JFF DMOG PTR DS:[401100]
004012F8 FF25 00114000 JFF DMOG PTR DS:[401100]
004012FC FF25 00114000 JFF DMOG PTR DS:[401100]
00401300 FF25 00114000 JFF DMOG PTR DS:[401100]
00401304 FF25 00114000 JFF DMOG PTR DS:[401100]
00401308 FF25 00114000 JFF DMOG PTR DS:[401100]
0040130C FF25 00114000 JFF DMOG PTR DS:[401100]
00401310 FF25 00114000 JFF DMOG PTR DS:[401100]
00401314 FF25 00114000 JFF DMOG PTR DS:[401100]
00401318 FF25 00114000 JFF DMOG PTR DS:[401100]
0040131C FF25 00114000 JFF DMOG PTR DS:[401100]
00401320 FF25 00114000 JFF DMOG PTR DS:[401100]
00401324 FF25 00114000 JFF DMOG PTR DS:[401100]
00401328 FF25 00114000 JFF DMOG PTR DS:[401100]
0040132C FF25 00114000 JFF DMOG PTR DS:[401100]
00401330 FF25 00114000 JFF DMOG PTR DS:[401100]
00401334 FF25 00114000 JFF DMOG PTR DS:[401100]
00401338 FF25 00114000 JFF DMOG PTR DS:[401100]
0040133C FF25 00114000 JFF DMOG PTR DS:[401100]
00401340 FF25 00114000 JFF DMOG PTR DS:[401100]
00401344 FF25 00114000 JFF DMOG PTR DS:[401100]
00401348 FF25 00114000 JFF DMOG PTR DS:[401100]
0040134C FF25 00114000 JFF DMOG PTR DS:[401100]
00401350 FF25 00114000 JFF DMOG PTR DS:[401100]
00401354 FF25 00114000 JFF DMOG PTR DS:[401100]
00401358 FF25 00114000 JFF DMOG PTR DS:[401100]
0040135C FF25 00114000 JFF DMOG PTR DS:[401100]
00401360 FF25 00114000 JFF DMOG PTR DS:[401100]
00401364 FF25 00114000 JFF DMOG PTR DS:[401100]
00401368 FF25 00114000 JFF DMOG PTR DS:[401100]
0040136C FF25 00114000 JFF DMOG PTR DS:[401100]
00401370 FF25 00114000 JFF DMOG PTR DS:[401100]
00401374 FF25 00114000 JFF DMOG PTR DS:[401100]
00401378 FF25 00114000 JFF DMOG PTR DS:[401100]
0040137C FF25 00114000 JFF DMOG PTR DS:[401100]
00401380 FF25 00114000 JFF DMOG PTR DS:[401100]
00401384 FF25 00114000 JFF DMOG PTR DS:[401100]
00401388 FF25 00114000 JFF DMOG PTR DS:[401100]
0040138C FF25 00114000 JFF DMOG PTR DS:[401100]
00401390 FF25 00114000 JFF DMOG PTR DS:[401100]
00401394 FF25 00114000 JFF DMOG PTR DS:[401100]
00401398 FF25 00114000 JFF DMOG PTR DS:[401100]
0040139C FF25 00114000 JFF DMOG PTR DS:[401100]
004013A0 FF25 00114000 JFF DMOG PTR DS:[401100]
004013A4 FF25 00114000 JFF DMOG PTR DS:[401100]
004013A8 FF25 00114000 JFF DMOG PTR DS:[401100]
004013AC FF25 00114000 JFF DMOG PTR DS:[401100]
004013B0 FF25 00114000 JFF DMOG PTR DS:[401100]
004013B4 FF25 00114000 JFF DMOG PTR DS:[401100]
004013B8 FF25 00114000 JFF DMOG PTR DS:[401100]
004013BC FF25 00114000 JFF DMOG PTR DS:[401100]
004013C0 FF25 00114000 JFF DMOG PTR DS:[401100]
004013C4 FF25 00114000 JFF DMOG PTR DS:[401100]
004013C8 FF25 00114000 JFF DMOG PTR DS:[401100]
004013CC FF25 00114000 JFF DMOG PTR DS:[401100]
004013D0 FF25 00114000 JFF DMOG PTR DS:[401100]
004013D4 FF25 00114000 JFF DMOG PTR DS:[401100]
004013D8 FF25 00114000 JFF DMOG PTR DS:[401100]
004013DC FF25 00114000 JFF DMOG PTR DS:[401100]
004013E0 FF25 00114000 JFF DMOG PTR DS:[401100]
004013E4 FF25 00114000 JFF DMOG PTR DS:[401100]
004013E8 FF25 00114000 JFF DMOG PTR DS:[401100]
004013EC FF25 00114000 JFF DMOG PTR DS:[401100]
004013F0 FF25 00114000 JFF DMOG PTR DS:[401100]
004013F4 FF25 00114000 JFF DMOG PTR DS:[401100]
004013F8 FF25 00114000 JFF DMOG PTR DS:[401100]
004013FC FF25 00114000 JFF DMOG PTR DS:[401100]
00401400 FF25 00114000 JFF DMOG PTR DS:[401100]
00401404 FF25 00114000 JFF DMOG PTR DS:[401100]
00401408 FF25 00114000 JFF DMOG PTR DS:[401100]
0040140C FF25 00114000 JFF DMOG PTR DS:[401100]
00401410 FF25 00114000 JFF DMOG PTR DS:[401100]
00401414 FF25 00114000 JFF DMOG PTR DS:[401100]
00401418 FF25 00114000 JFF DMOG PTR DS:[401100]
0040141C FF25 00114000 JFF DMOG PTR DS:[401100]
00401420 FF25 00114000 JFF DMOG PTR DS:[401100]
00401424 FF25 00114000 JFF DMOG PTR DS:[401100]
00401428 FF25 00114000 JFF DMOG PTR DS:[401100]
0040142C FF25 00114000 JFF DMOG PTR DS:[401100]
00401430 FF25 00114000 JFF DMOG PTR DS:[401100]
00401434 FF25 00114000 JFF DMOG PTR DS:[401100]
00401438 FF25 00114000 JFF DMOG PTR DS:[401100]
0040143C FF25 00114000 JFF DMOG PTR DS:[401100]
00401440 FF25 00114000 JFF DMOG PTR DS:[401100]
00401444 FF25 00114000 JFF DMOG PTR DS:[401100]
00401448 FF25 00114000 JFF DMOG PTR DS:[401100]
0040144C FF25 00114000 JFF DMOG PTR DS:[401100]
00401450 FF25 00114000 JFF DMOG PTR DS:[401100]
00401454 FF25 00114000 JFF DMOG PTR DS:[401100]
00401458 FF25 00114000 JFF DMOG PTR DS:[401100]
0040145C FF25 00114000 JFF DMOG PTR DS:[401100]
00401460 FF25 00114000 JFF DMOG PTR DS:[401100]
00401464 FF25 00114000 JFF DMOG PTR DS:[401100]
00401468 FF25 00114000 JFF DMOG PTR DS:[401100]
0040146C FF25 00114000 JFF DMOG PTR DS:[401100]
00401470 FF25 00114000 JFF DMOG PTR DS:[401100]
00401474 FF25 00114000 JFF DMOG PTR DS:[401100]
00401478 FF25 00114000 JFF DMOG PTR DS:[401100]
0040147C FF25 00114000 JFF DMOG PTR DS:[401100]
00401480 FF25 00114000 JFF DMOG PTR DS:[401100]
00401484 FF25 00114000 JFF DMOG PTR DS:[401100]
00401488 FF25 00114000 JFF DMOG PTR DS:[401100]
0040148C FF25 00114000 JFF DMOG PTR DS:[401100]
00401490 FF25 00114000 JFF DMOG PTR DS:[401100]
00401494 FF25 00114000 JFF DMOG PTR DS:[401100]
0040



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

C:\DOCUMENT~1\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:\DOCUMENT~1\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 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, 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.

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'

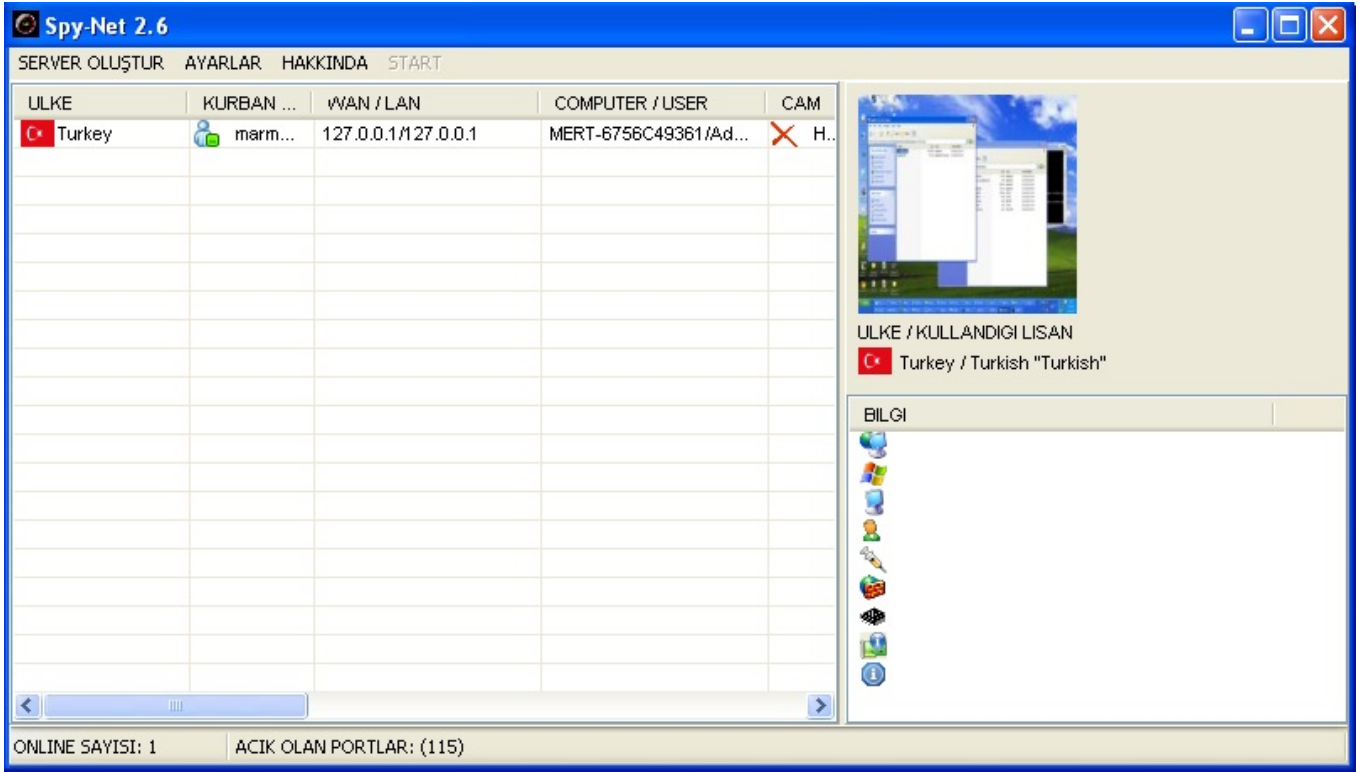
inetnum:        81.6.64.0 - 81.6.95.255
netname:        Vodafone-Turkey-Customer-IP-Pools
descr:          Vodafone Turkey GPRS address pool
country:        TR
admin-c:         VT1712-RIPE
tech-c:         VT1712-RIPE
status:         ASSIGNED PA
mnt-by:         RTNET-MNT
mnt-lower:       RTNET-MNT
mnt-routes:     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 çocuklarınıza 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, güvenliğiniz açısından önem arz etmektedir.

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

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