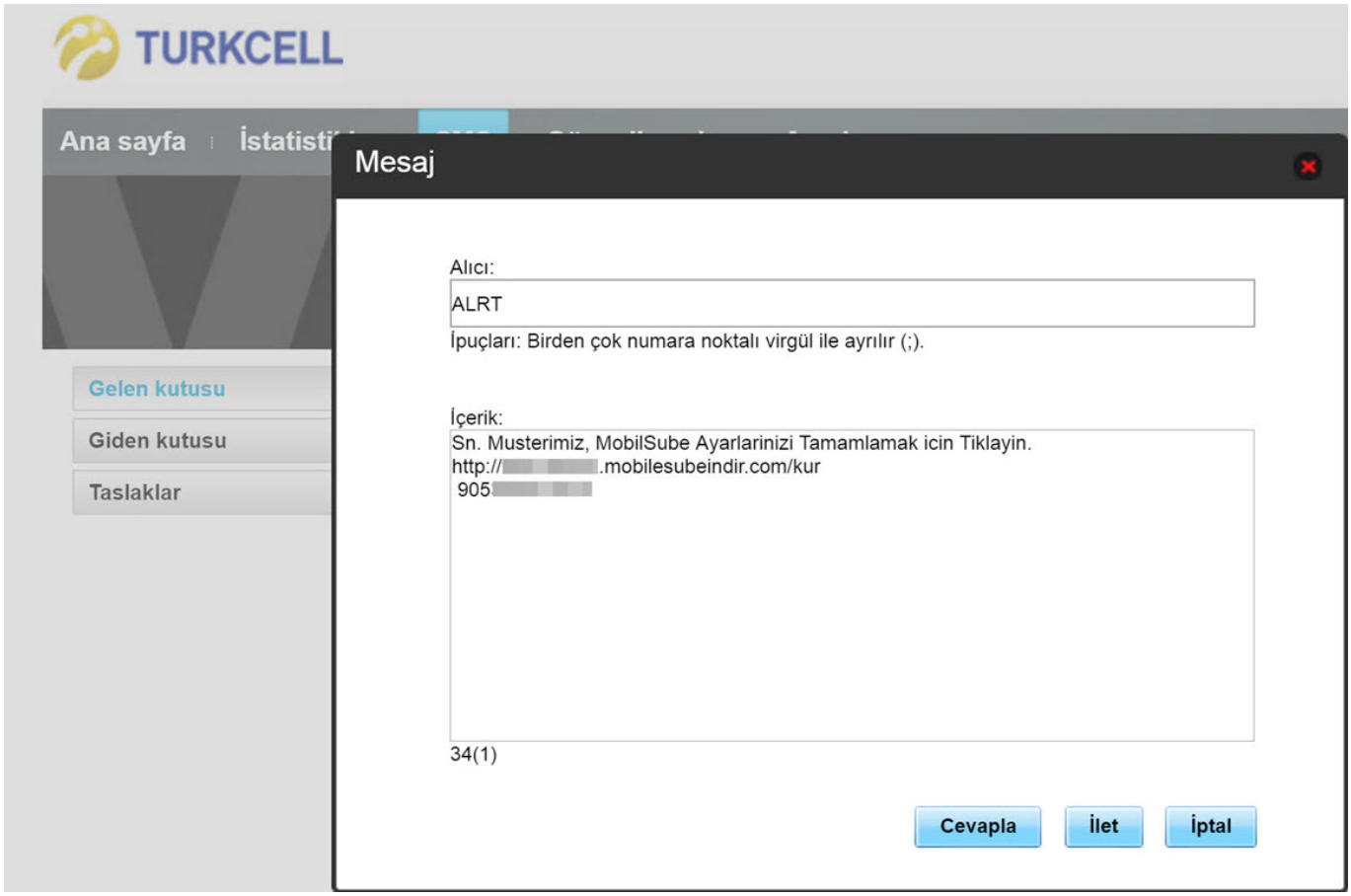
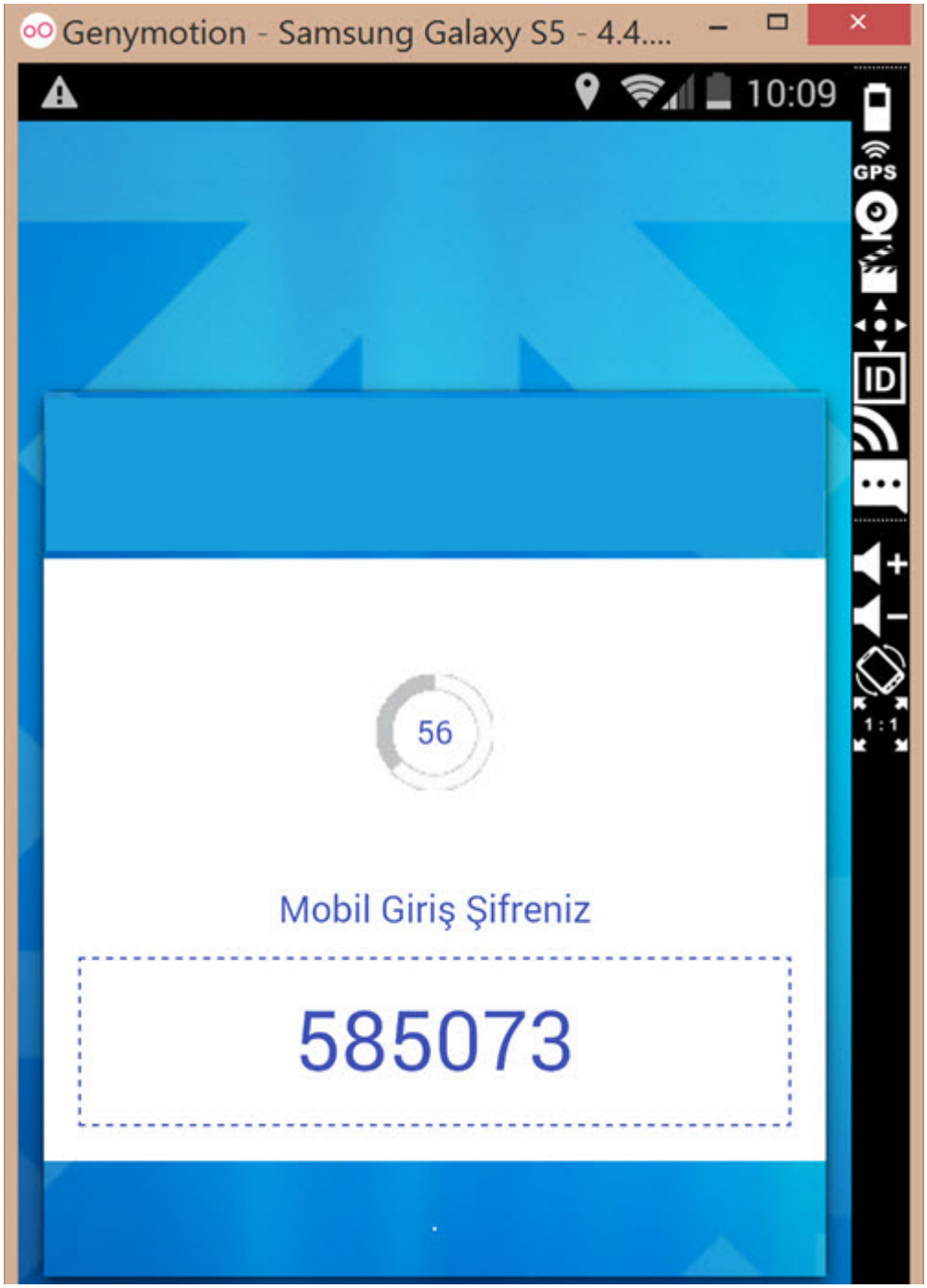
AutoIt Bankacılık Zararlı Yazılımı

written by Mert SARICA | 1 July 2016

2015 yılından bu yana Türkiye'de çok sayıda bankanın müşterilerinin hedef alındığı bir zararlı yazılım salgını olduğu bilinmekteydi. Kullanmış olduğu Windows işletim sistemi üzerinde bu yazıya konu olan bankacılık zararlı yazılımı çalışan banka müşterileri, ilgili bankaların internet şubelerine girişi esnasında, mobil şube uygulaması yükletme vaadiyle cep telefonu numarası isteyen bir pencere ile karşılaşıyorlardı. Pencerede yer alan görsellerin tasarımının bankanın tasarımıyla uyum içinde olması ise müşterileri cep telefonu numarası girmeye ikna eden önemli etkenlerden biriydi.

Bu pencereye girilen cep telefonu numarasından sonra müşterinin cep telefonuna bağlantı adresi (link) içeren (http://banka.mobilsubeindir.com/kur) bir SMS gönderilmekteydi. Bu bağlantı adresini ziyaret eden ve Android işletim sistemi yüklü akıllı cihaz kullanan müşterinin karşısına, SMS çalabilme yeteneğine de sahip olan Android zararlı yazılımının kurulmasına yönelik yönergeler çıktığı daha önce gerçekleştirilen analizlerden bilinmekteydi. (Bu Android zararlı yazılımı ile ilgili detaylı bilgi almak için Bakır EMRE'nin analiz yazısını inceleyebilirsiniz.) Ben de bu yazımda, Windows işletim sistemi üzerinde çalışan ve yukarıda bahsi geçen Android zararlı yazılımının ilk halkası olan Windows zararlı yazılımını kısaca inceledim.

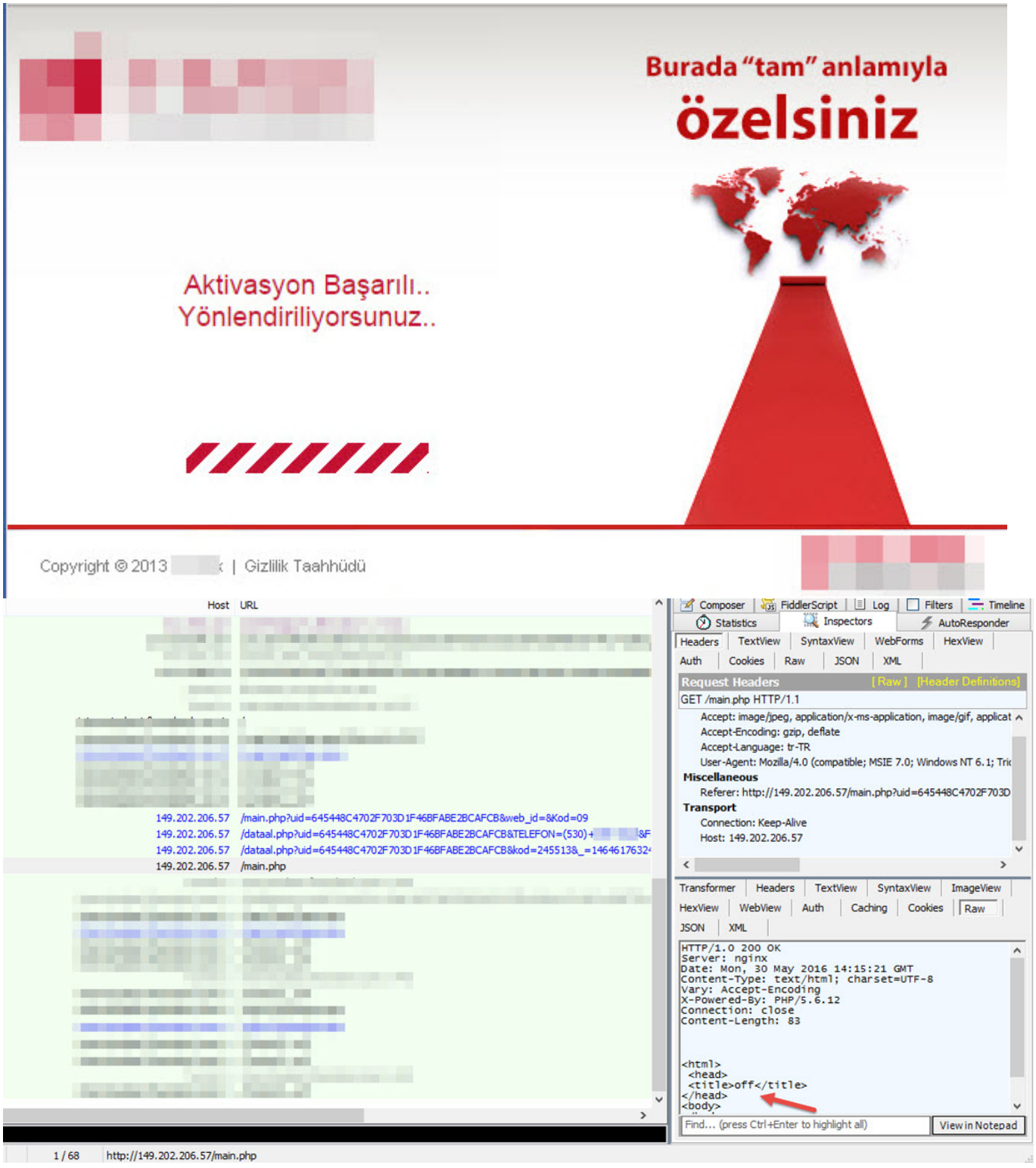

TURKCELL
Ana sayfa
İstatisti
Gelen kutusu
Giden kutusu
Taslaklar
Mesaj
Alıcı:
ALRT
İpuçları: Birden çok numara noktalı virgül ile ayrılır (;).
İçerik:
Sn. Musterimiz, MobilSube Ayarlarinizi Tamamlamak icin Tiklayin.
http://[redacted].mobilesubeindir.com/kur
905[redacted]
34(1)
Cevapla
İlet
İptal



Windows işletim sistemi üzerinde çalışan bu zararlı yazılımın kullanıcıların sistemlerine tam olarak hangi kaynaktan, nasıl bulaştığını tam olarak bilinmemekle birlikte, zararlı eklentiye sahip veya zararlı JAR dosyası bağlantı adresi içeren sahte sipariş e-postası kaynaklı olduğunu, bulaşmış olduğu sistemlerde Java ile geliştirilmiş başka bir zararlı yazılım olması nedeniyle tahmin etmekteyim.
(https://www.virustotal.com/en/file/0ba783b9cf1cee314c06f29b9ff629948a296257f1b1a19b09ba2a2369da3d0e/analysis/)

Cep telefonu numarasının girilmesini isteyen pencereye kullanıcı tarafından cep telefonu numarası girildiğinde, ilgili pencerede cep telefonu numarasına

SMS gönderildiği belirtilmekteydi. Android akıllı cihaza kurulan bu uygulama (zararlı yazılım) çalıştırıldığında da, ekranda yer alan 6 haneli sayının bu pencereye girilmesi istenmekteydi. Bu sayı girildikten sonra mobil zararlı yazılım ile pencere çıkaran zararlı yazılımın eşleştiği arka planda komuta kontrol merkezine (http://149.202.206.57) bildirilerek, Windows işletim sistemi üzerinde çalışan zararlı yazılımın artık internet şubeye girişte kullanıcıya pencere çıkartmayacak şekilde komuta kontrol merkezinden komut aldığı (off) görülüyordu.



Pencere çıkaran zararlı yazılım sisteme bulaştıktan sonra işletim sistemi yeniden başlatıldığında C:\Users\kullanıcı adı\AppData\Roaming\Apple_Updater\ klasörü altında lsasss.exe adı altında, aynı klasörde bulunan safe dosyasını yükleyerek çalışmaktaydı.

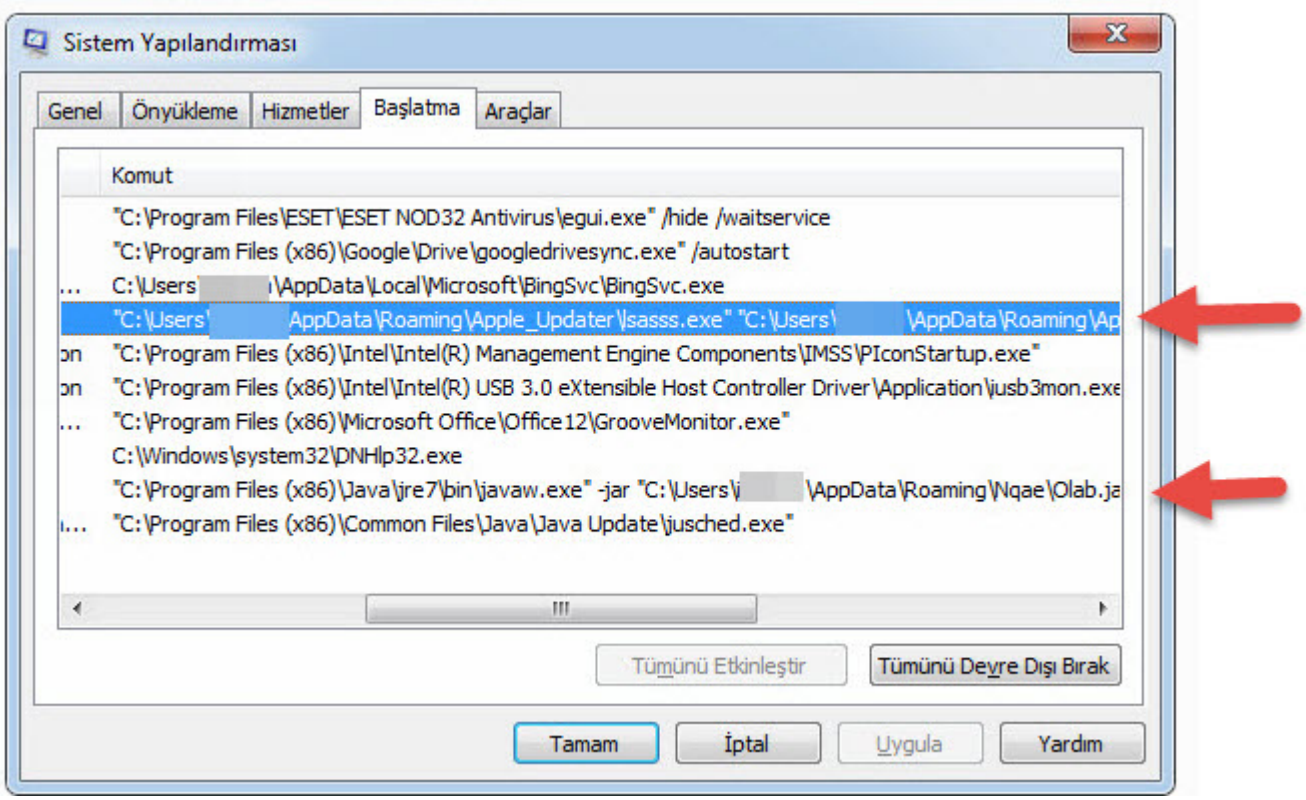
lsass.exe
MD5: 6A93A4071CC7C22628AF40A4D872F49B
SHA-1: BA916E686AA0CAE19AB907BDAB94924ADA92B5F4
SHA-256: 8465F3FCBCCCE3EA12495EDBB0BD09C3B066E3DF891613CE3180F9BB38B37B01

safe

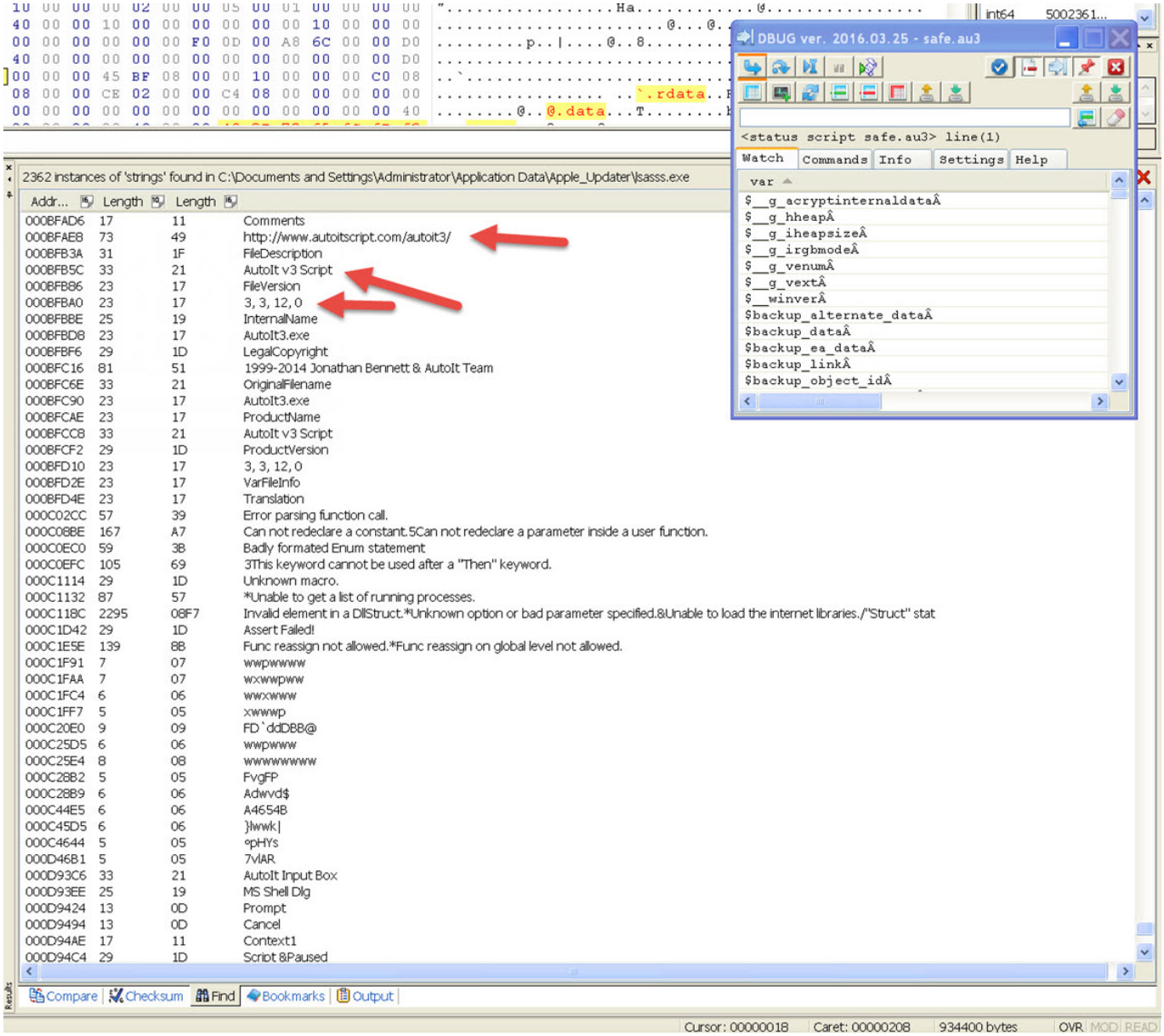
MD5: A77D3D8060DC0096AF6F2F24AFD57EF7

SHA-1: B22068203898FB5643E5060AC72A29FD3D35DECE

SHA-256: 02E8EACE1A4FB827BB78BA1F5A40D9E54E98AED7E555093B37C0243AF6B05D99

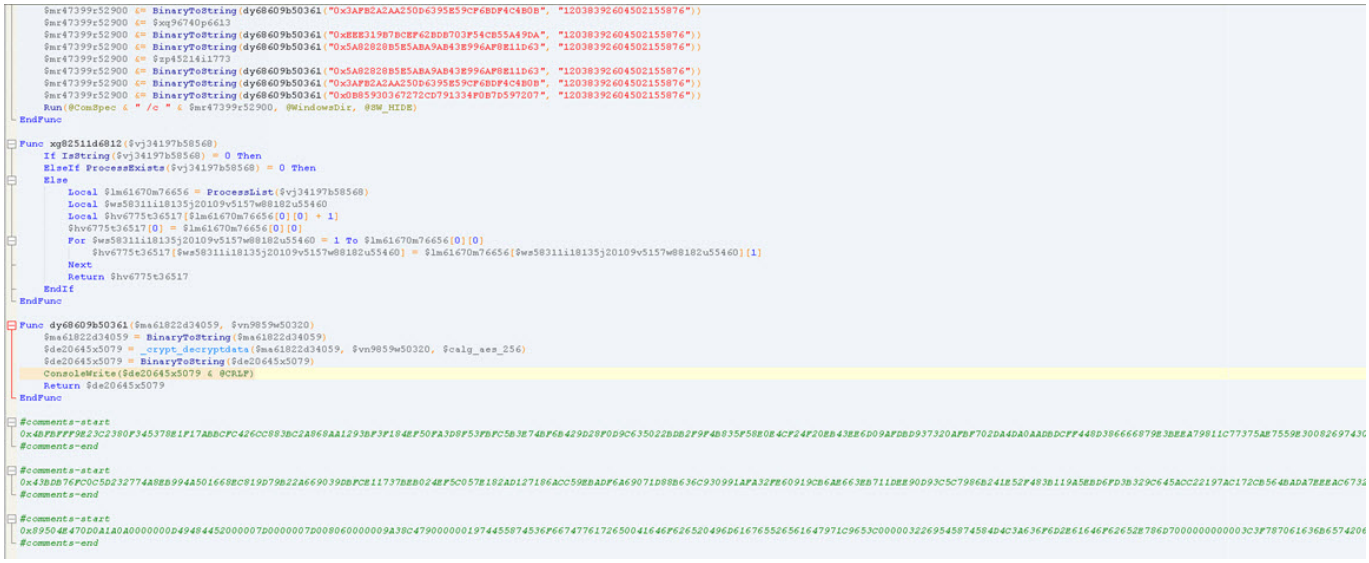


Kısa bir araştırmadan sonra, lsasss.exe programının AutoIt v3.3.12 programının (https://www.autoitscript.com/site/autoit/) adının değiştirilmiş hali (rename) olduğu, safe dosyasının ise AutoIt betiği (script) olduğunu tespit ettim.

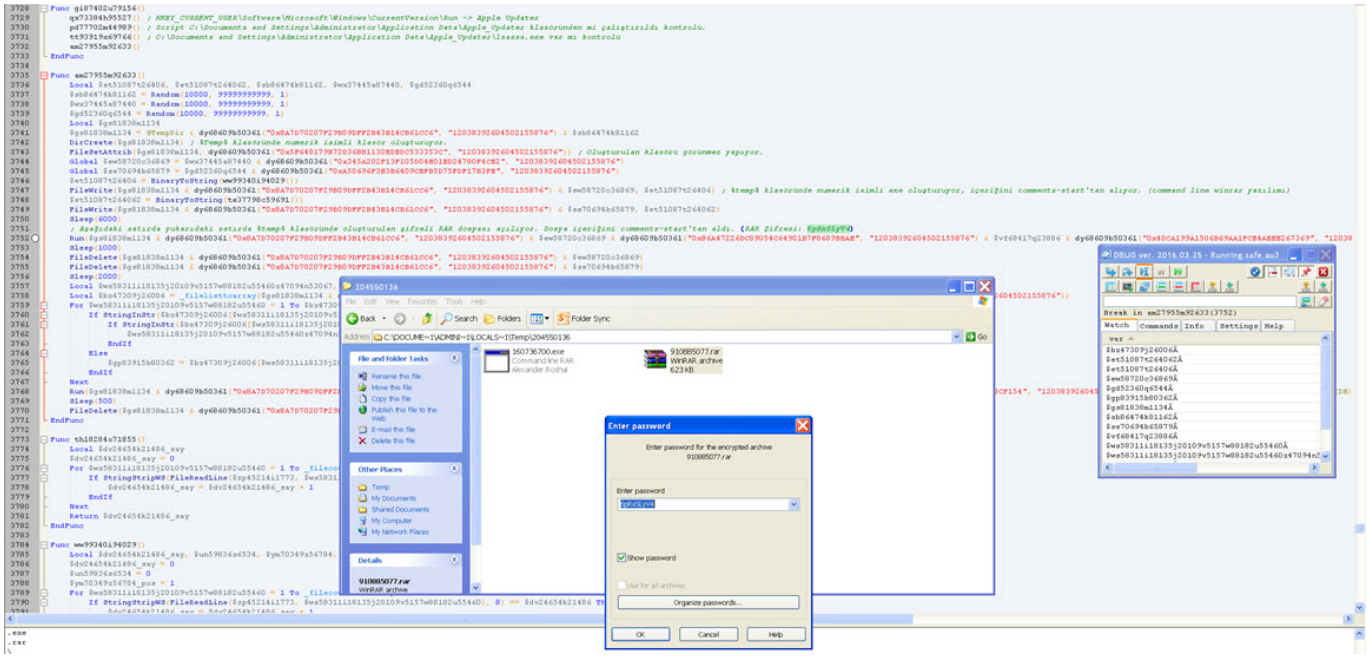


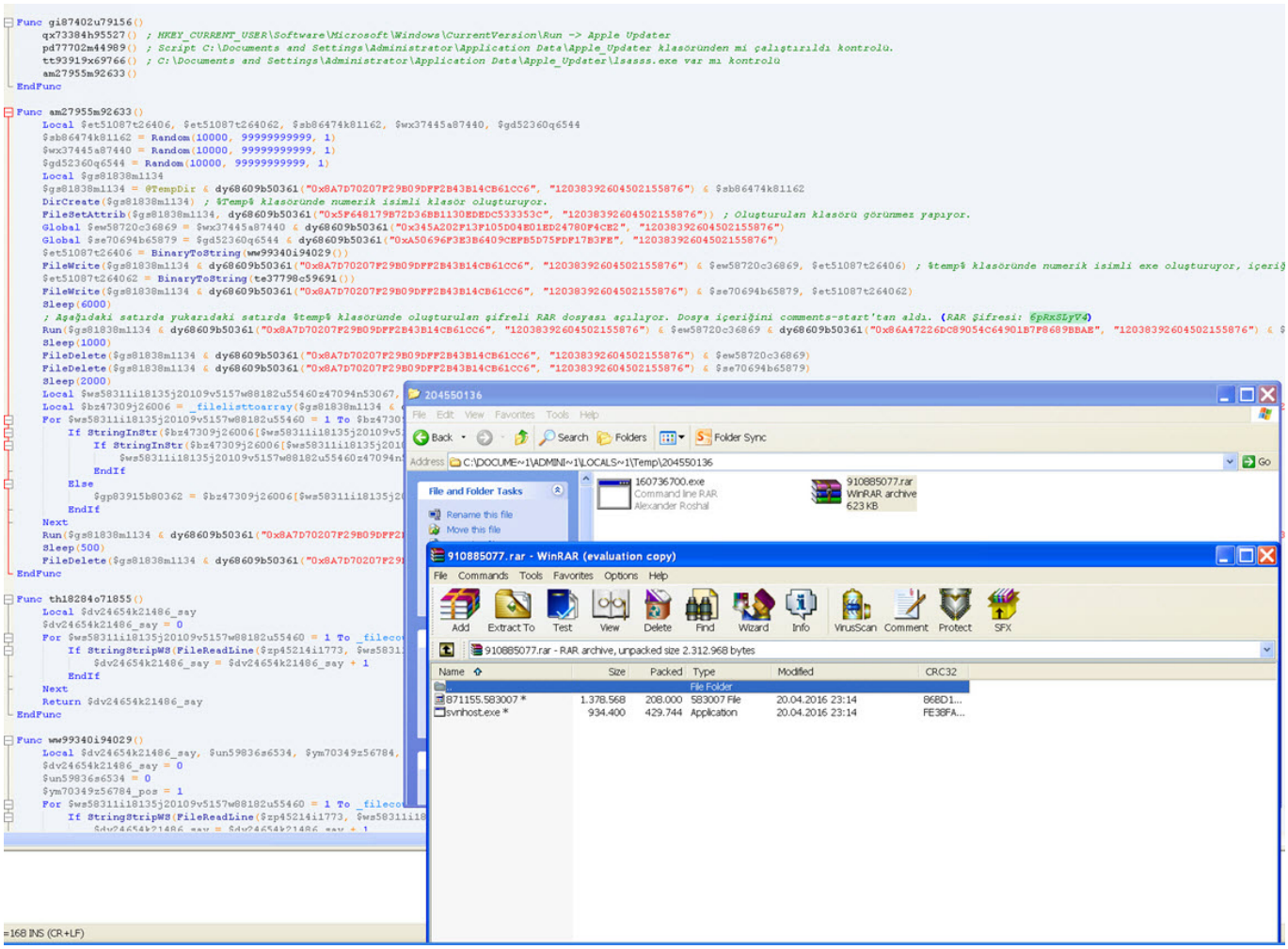
AutoIt betiğini OllyDbg gibi bir hata ayıklama programı ile analiz etmek için https://www.autoitscript.com/wiki/FAQ#How_can_I_debug_my_script.3F sayfasında yer alan araçları kullanabilirsiniz.

safe dosyasını incelendiğimde bu dosyada yer alan değişken isimlerinin karmaşıklaştırılmış olduğu, şifrelenmiş verilerin yer aldığı (#comments-start #comments-end), şifreleme amacıyla kullanılan fonksiyonlar olduğunu gördüm.



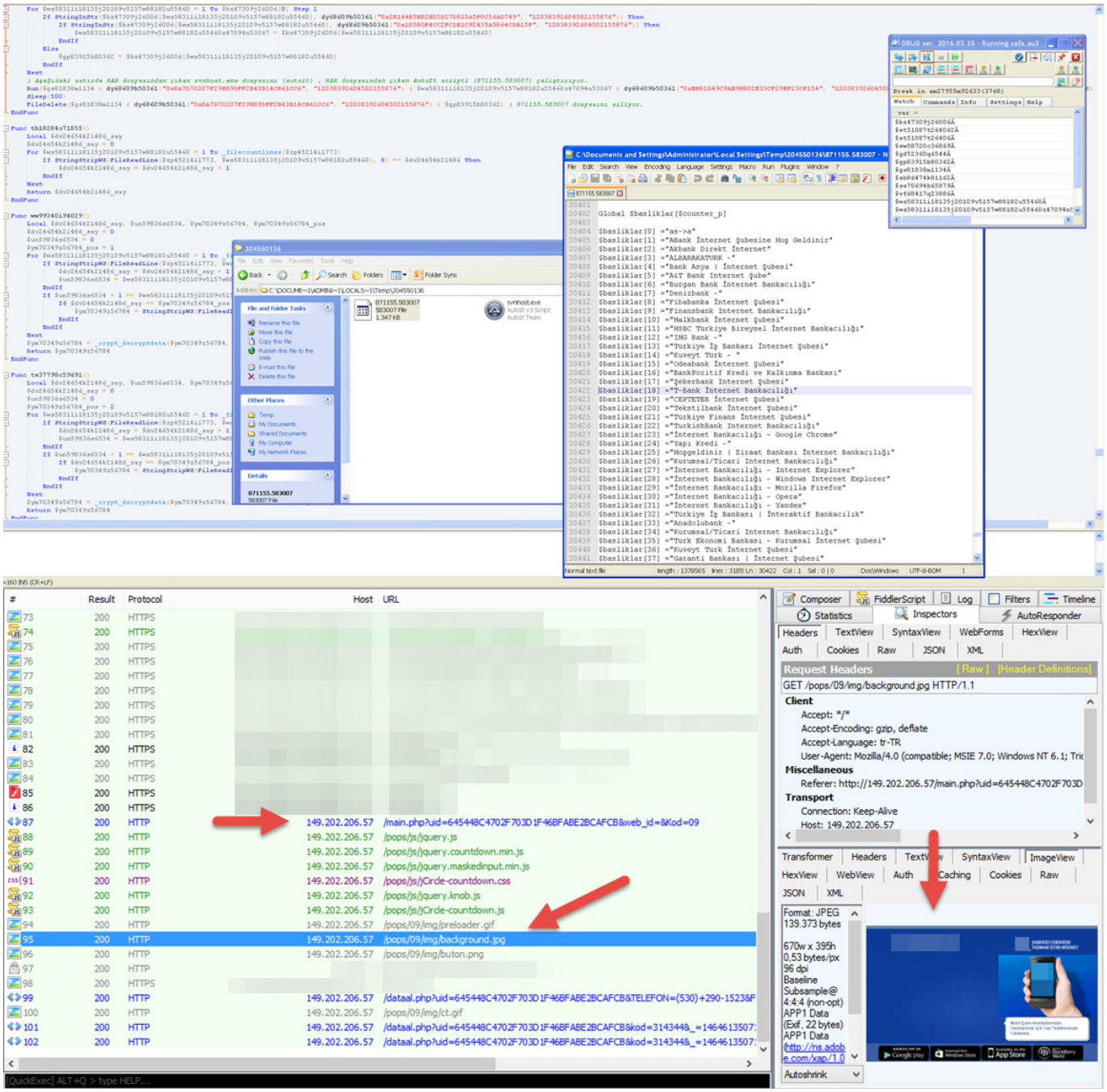
lsasss.exe programı çalıştırıldıktan sonra safe dosyası içinde yer alan şifrelenmiş verileri (1 adet EXE uzantılı dosya (command line winrar programı) ve 1 adet şifrelenmiş (şifre: 6pRxSLyV4) RAR uzantılı dosya) C:\Users\kullanıcı adı\AppData\Local\Temp\ klasörü altında rastgele oluşturduğu sayılardan oluşan isme sahip bir klasöre açmakta ve bu klasörü gizlemekteydi. (hidden)



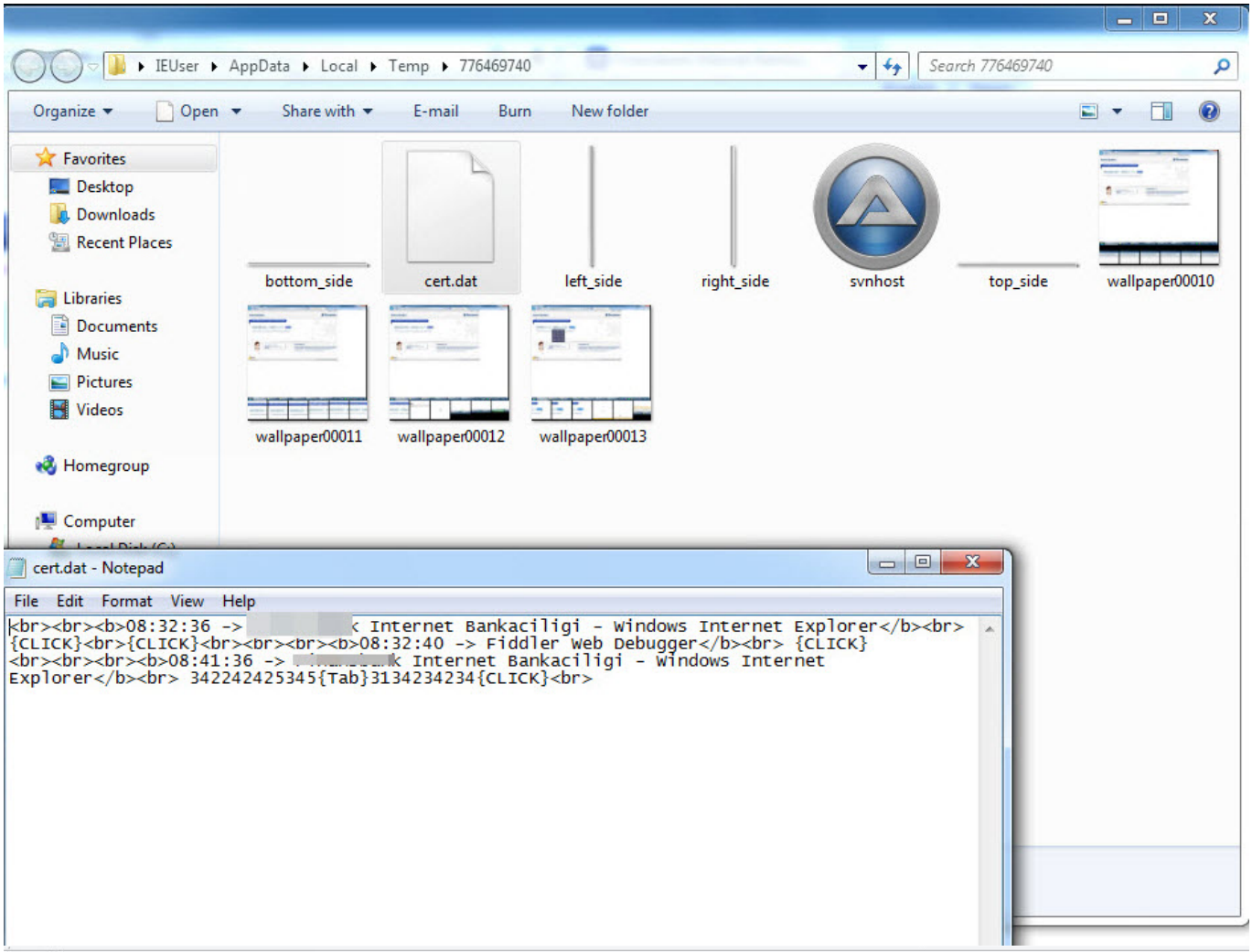


lsasss.exe programı, Winrar programı ile şifrelenmiş RAR dosyasını gizlenmiş klasöre açtıktan sonra, içinden çıkan svnhost.exe isimli programı (AutoIt programı) 871155.583007 (AutoIt betiği) dosyası ile çalıştırmakta ve 871155.583007 dosyasını silerek, sistem üzerinde svnhost.exe adı altında çalışmaktaydı.

871155.583007 dosyasını incelendiğimde ise sistemde açık olan pencerelerin başlık (title) bilgilerini izleyerek (Örnek kod: $basliklar[22] =”TurkishBank Internet Bankacılığı”), pencerede yer alacak bankanın görsellerini komuta kontrol merkezinden alarak 30’a yakın bankanın müşterisini ve internet şubesini hedef aldığını gördüm.

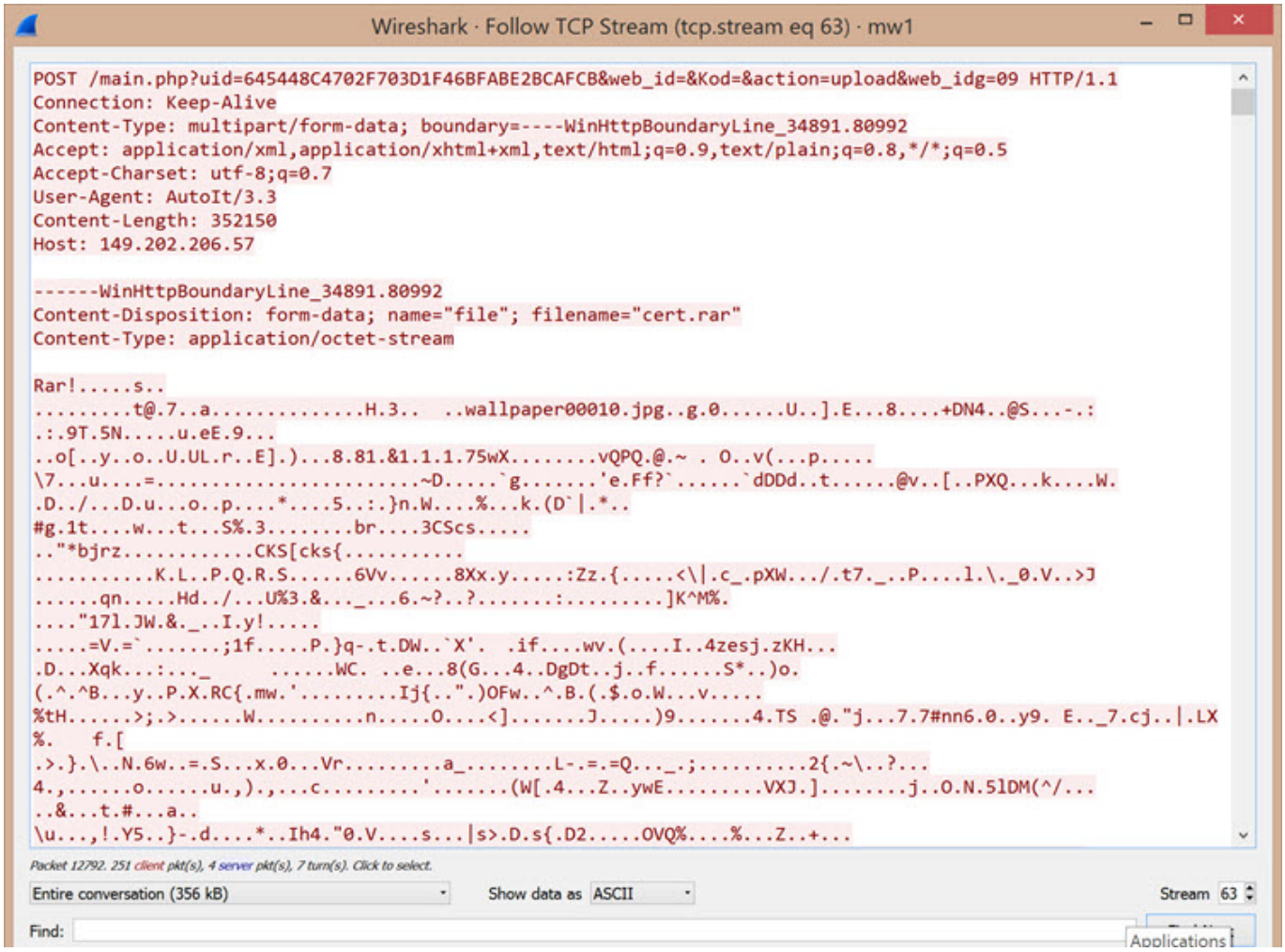


871155.583007 dosyasını incelendiğimde ayrıca bu zararlı yazılımının izlediği başlık bilgisini tespit ettiği anda tuş bilgisi kaydı yaptığını ve bu bilgileri cert.dat dosyasına kayıt ettiğini, ekran görüntüsü aldığını ve bunları da C:\Users\kullanıcı adı\AppData\Local\Temp\ klasörü altında rastgele oluşturduğu sayılardan oluşan ada sahip klasörde sakladığını gördüm. İlgili pencere kapatıldığı anda ise ilgili klasörde yer alan ekran görüntülerini RAR işleminden geçirdikten sonra cert.rar adı altında cert.dat (tuş bilgileri içeren dosya) dosyası ile birlikte komuta kontrol merkezine (http://149.202.206.57) göndermekteydi.



cert - Copy.rar - RAR archive, unpacked size 1.053.282 bytes

Name	Size	Packed	Type
..			File folder
wallpaper00010.jpg	106.802	73.109	JPEG image
wallpaper00011.jpg	136.953	89.021	JPEG image
wallpaper00012.jpg	138.322	93.712	JPEG image
wallpaper00013.jpg	136.456	94.868	JPEG image
wallpaper00014.jpg	124.163	84.669	JPEG image
wallpaper00015.jpg	146.919	94.909	JPEG image
wallpaper00016.jpg	125.371	86.047	JPEG image
wallpaper00017.jpg	138.296	92.723	JPEG image



871155.583007 dosyasında yer alan fonksiyon (Örnek: Func yazkizim($krctr)) ve değişken (Örnek: $sayac) isimlerinin Türkçe olması, bu zararlı yazılımın Türkçe bilen kişilerce geliştirildiği ihtimaline dikkat çekiyordu.

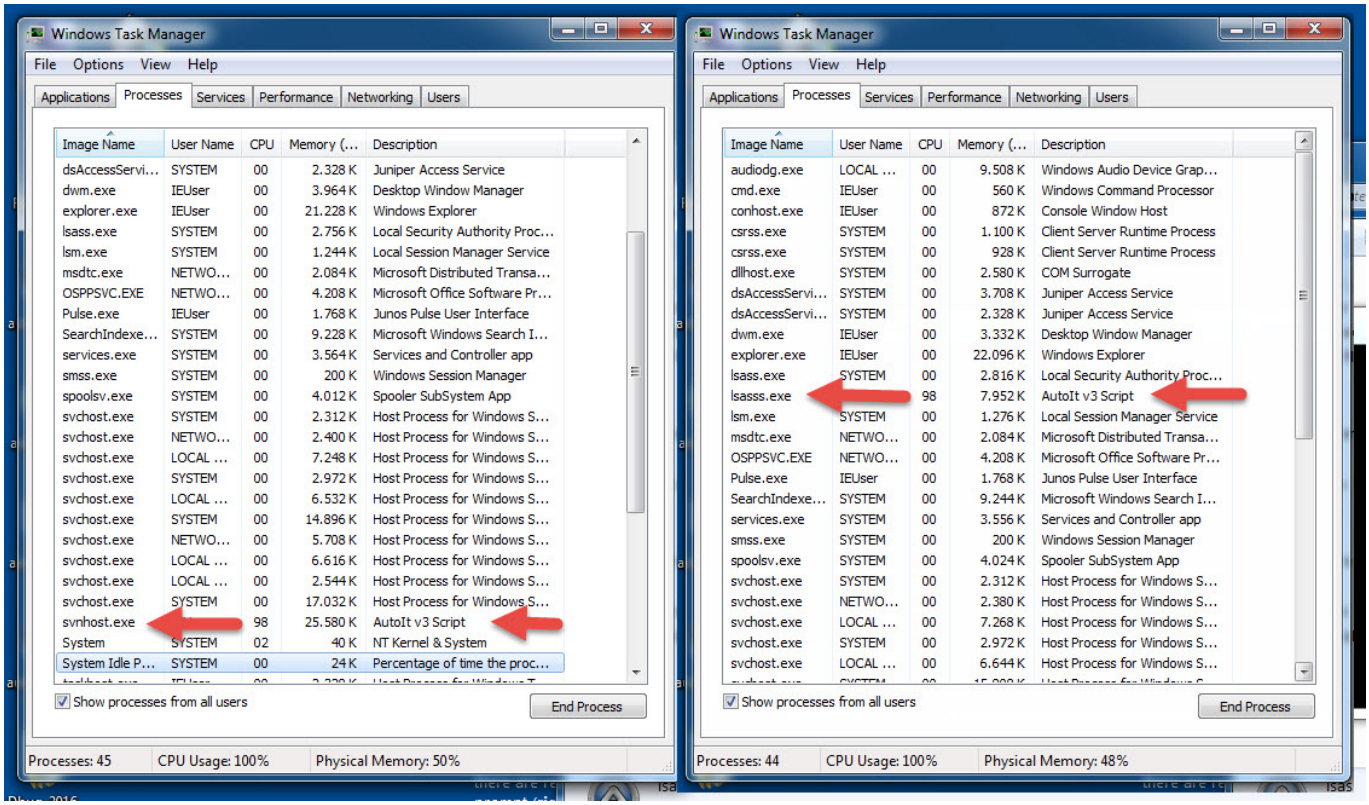
Ayrıca yine bu dosya içinde zararlı yazılımın çalıştıktan sonra kendisini silecek fonksiyonları barındırması ancak kullanmaması ve $cert_avi değişkenine sahip olması, zararlı yazılımın ilerleyen sürümlerinde bu özellikleri kullanma ihtimali olduğunu göstermekteydi.

```
; ============================================================
; ============================================================

Func _SelfDelete($iDelay = 0)
   Local $sCmdFile
   FileDelete(@TempDir & "\scratch.bat")
   $sCmdFile = 'ping -n ' & $iDelay & '127.0.0.1 > nul' & @CRLF _
         & ':loop' & @CRLF _
         & 'rd "' & @ScriptDir & "' /q /s ' & @CRLF _
         & 'if exist "' & @ScriptDir & "' goto loop' & @CRLF _
         & 'del ' & @TempDir & '\scratch.bat'
   FileWrite(@TempDir & "\scratch.bat", $sCmdFile)
   Run(@TempDir & "\scratch.bat", @TempDir, @SW_HIDE)
 EndFunc

; ============================================================
; ============================================================

Func _cikis()

  Sleep(500)
  Run( $anadosya & " " & "safe", @AppDataDir & "\Apple_Updater\", @SW_HIDE )
  Sleep(1000)
  _SelfDelete(10)

EndFunc
```

```
Global $increase_file    = @AppDataDir & "\Apple_Updater\" & "safe"          ; // Surum Yukseltme Dosyas
Global $version_file     = "ver.dat"                                                                  ; // Version Kontrol Dosyasi
Global $cert_file                = "cert.dat"                                                                  ; // cert.dat
Global $cert_rar                 = "cert.rar"                                                                  ; //  cert.rar
Global $cert_avi                 = "cert.avi"                                                                  ; // cert.avi
Global $wrar_file                = "wrar521.exe"                                                                  ; // wrar521.exe
Global $wfile                                = "\wrar521.exe /S"                                                          ; //  \wrar521.exe /S
```

Sonuç olarak internet bankacılığı müşterilerinin her daim bu ve benzeri zararlı yazılımlara karşı tetikte olması ve internet şubelere girişte ve/veya sonrasında karşılaştıkları olası şüpheli durumlarda mutlaka ama mutlaka bankalalarına haber vermeleri gerekmektedir. Zararlı yazılım analizi becerine sahip bankalar (ehem ehem :)) bu ve benzeri zararlı yazılımları analiz ederek sizlerin daha güvenli bankacılık yapabilmeniz adına imkanları dahilinde ellerinden gelenin en iyisini yapacaklardır.

Bu zararlı yazılımın sisteminizde çalışıp, çalışmadığından emin olmak için çalışan programlarda (görev yöneticisi) lsasss.exe ve/veya svnhost.exe olup olmadığını kontrol edebilirsiniz.



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Notlar:

1. Zararlı yazılımı temizlemek için Start -> Run -> Msconfig yazdıktan sonra Startup sekmesinde, Apple_Updater satırını bulup, sildikten/devre dışı bıraktıktan sonra sisteminizi yeniden başlatabilirsiniz.
2. 20’ye yakın bankanın yetkilileri ile bu bilgiler, siz bu yazıyı okumadan günler öncesinde paylaşılmıştır.
3. Bu yazı, 6. Pi Hediyem Var oyununun çözüm yolunu da içermektedir.