Basit Malware Analizi (Windows)

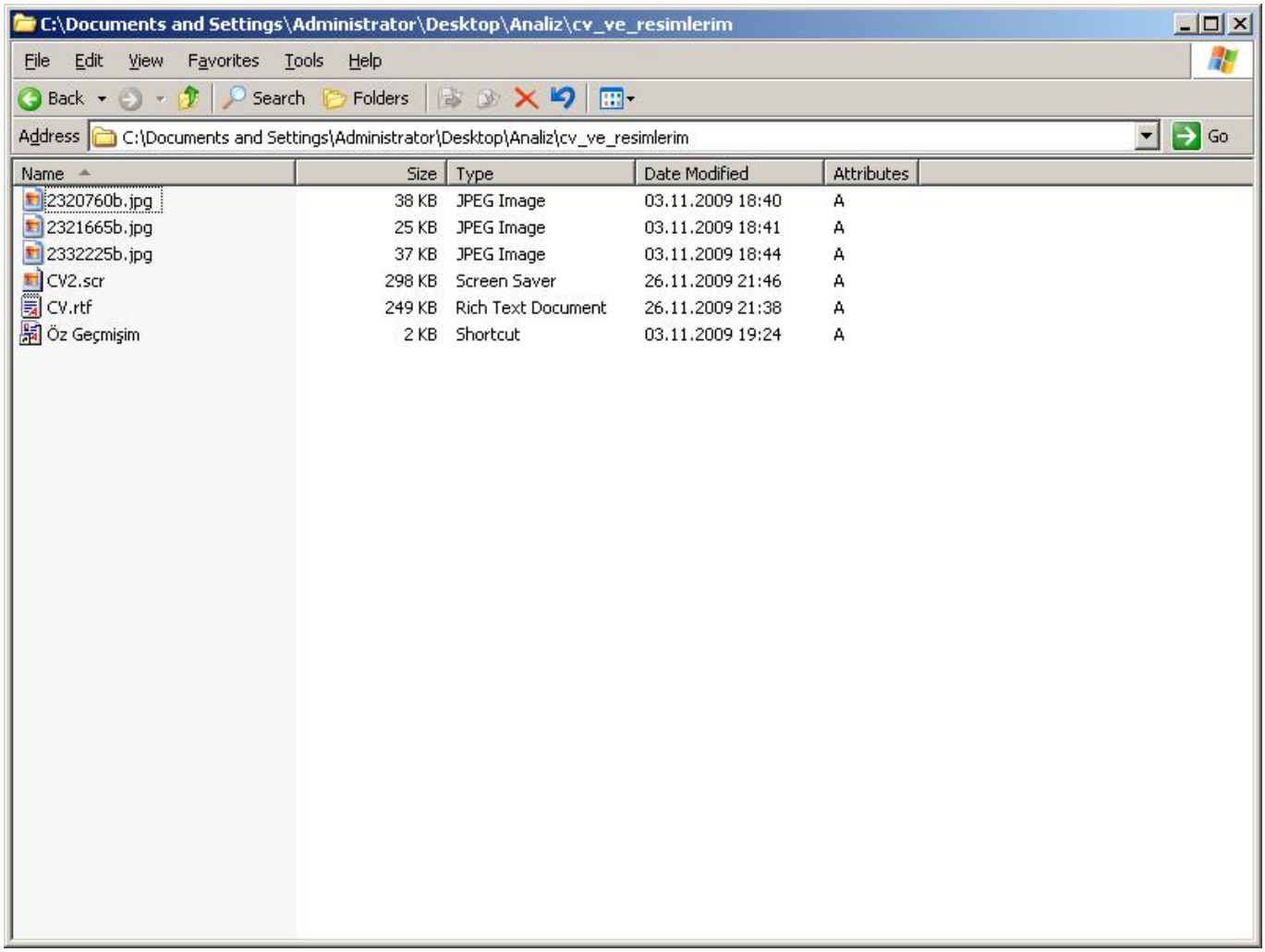
written by Mert SARICA | 9 February 2010

Hatırlarsanız Aralık ayında şans eseri bir arkadaşımın şüphelendiği bir e-postayı bana göndermesi ve incelememem sonrasında Türkiye'de internet bankacılığını kullanan müşterileri hedef alan ve çalıştığı işletim sistemi üzerindeki kullanıcının internet bankacılığına girişi esnasında kullanıcı adı ve sanal klavyeninin ekran görüntüsünü kayıt eden ve tuş bilgilerini çalan bir trojan keşfetmiştim. Trojanı nasıl keşfettiğim ile ilgili bir yazı karalayacağımı belirtmiştim ancak araya giren diğer işler nedeniyle bugüne kısmet oldu.

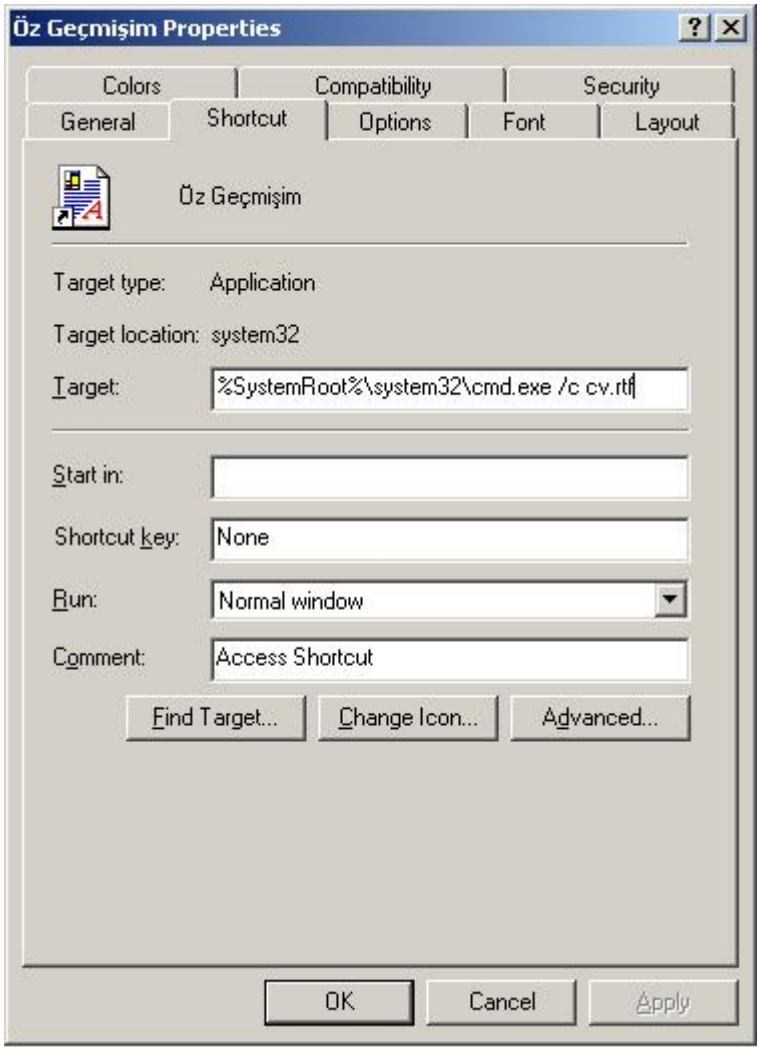
Bugünkü yazımın sizlere basitçe şüphelendiğiniz bir programın işletim sisteminizde ne işler çevirdiğini anlamanız için yol göstereceğini ümit ediyorum.

Hemen konuya girecek olursam, şüpheli dosyamızın adı cv_ve_resimlerim.rar

Rar dosyasını açtıktan sonra içerisinden resim dosyası görünümüne bürünmüş SCR uzantılı bir dosya, RTF uzantılı başka bir dosya, bir kısa yol dosyası ve belden altı tüm dosyaları açmaya teşvik edecek 3 adet resim ile karşılaştım. (Hedef kitleyi tahmin edebildiniz mi :p)

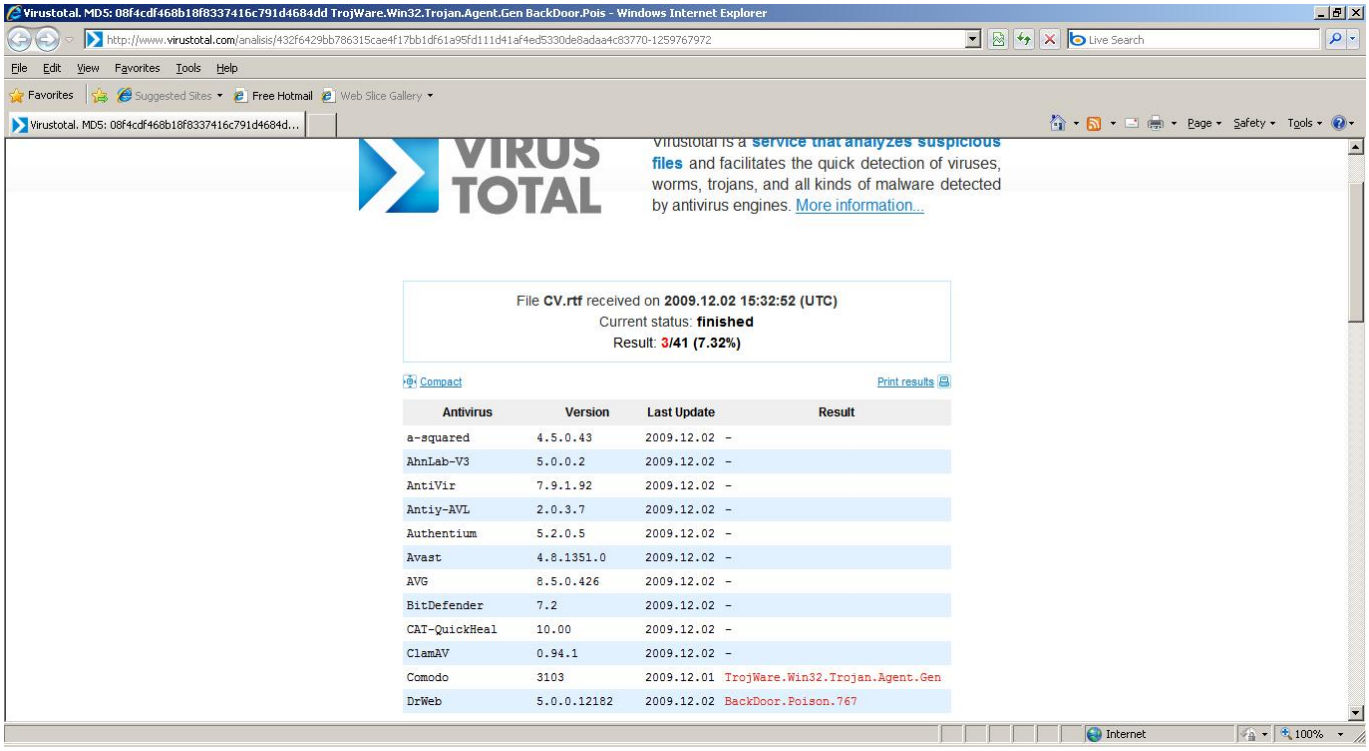


Kısa yol dosyasının özelliklerine baktığım zaman cv.rtf dosyasının SCR uzantılı diğer dosya gibi şüpheli olduğunu anlamam pek zor olmadı.



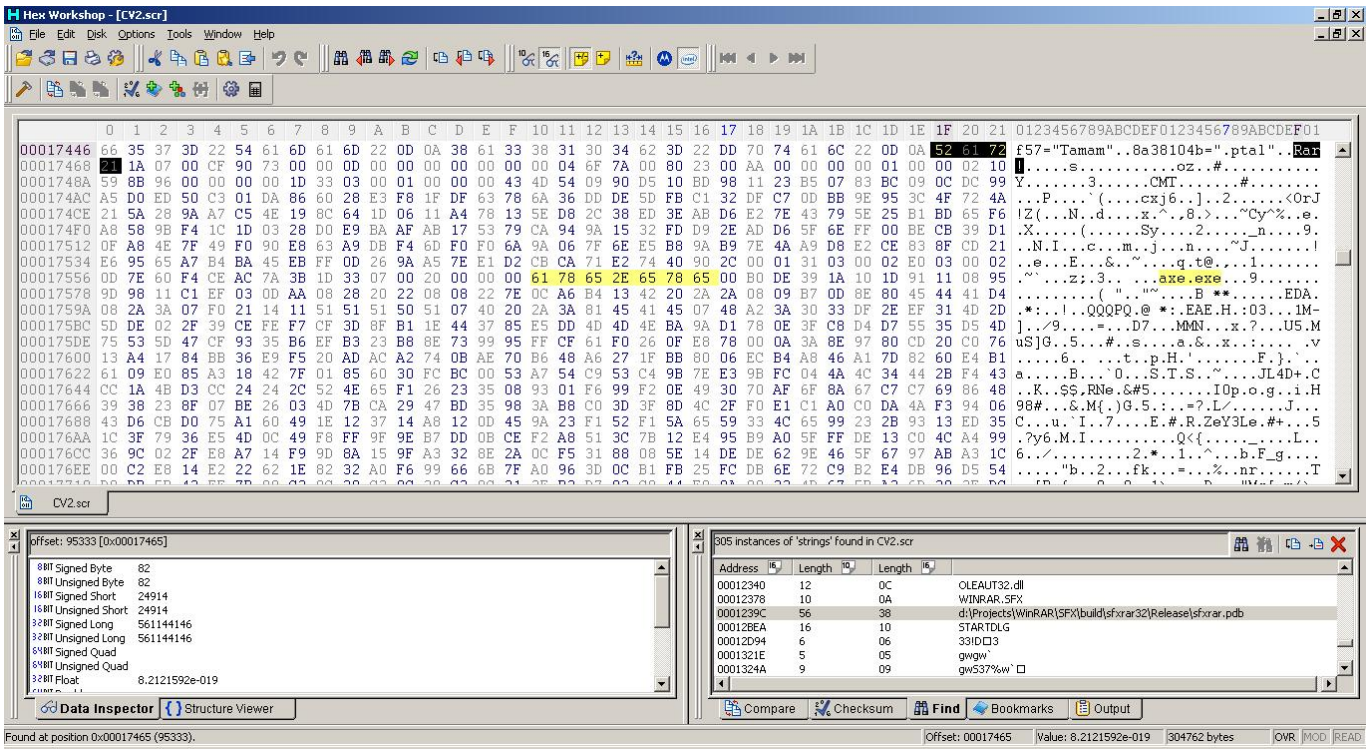
Bildiğiniz veya bilmediğiniz üzere uygulanabilir dosya başlığına sahip herhangi bir dosya, uzantısı farklı dahi olsa komut satırından çalıştırıldığı taktirde uygulanabilir program olarak çalışmaktadır. Örneğin calc.exe dosyasının uzantısını rtf olarak değiştirir ve calc.rtf olarak kaydeder ve komut satırından calc.rtf olarak çalıştırırsanız hesap makinası uygulaması karşınıza çıkacaktır. Bu yöntem oldukça basit ve eskidir ve hatırladığım kadarıyla rahmetli Bülent Tigin, CEH eğitiminin ilk veya ikinci dersinde bu yöntemden bahsetmişti. Bu konu ile ilgili detaylı bilgiye buradan ulaşabilirsiniz.

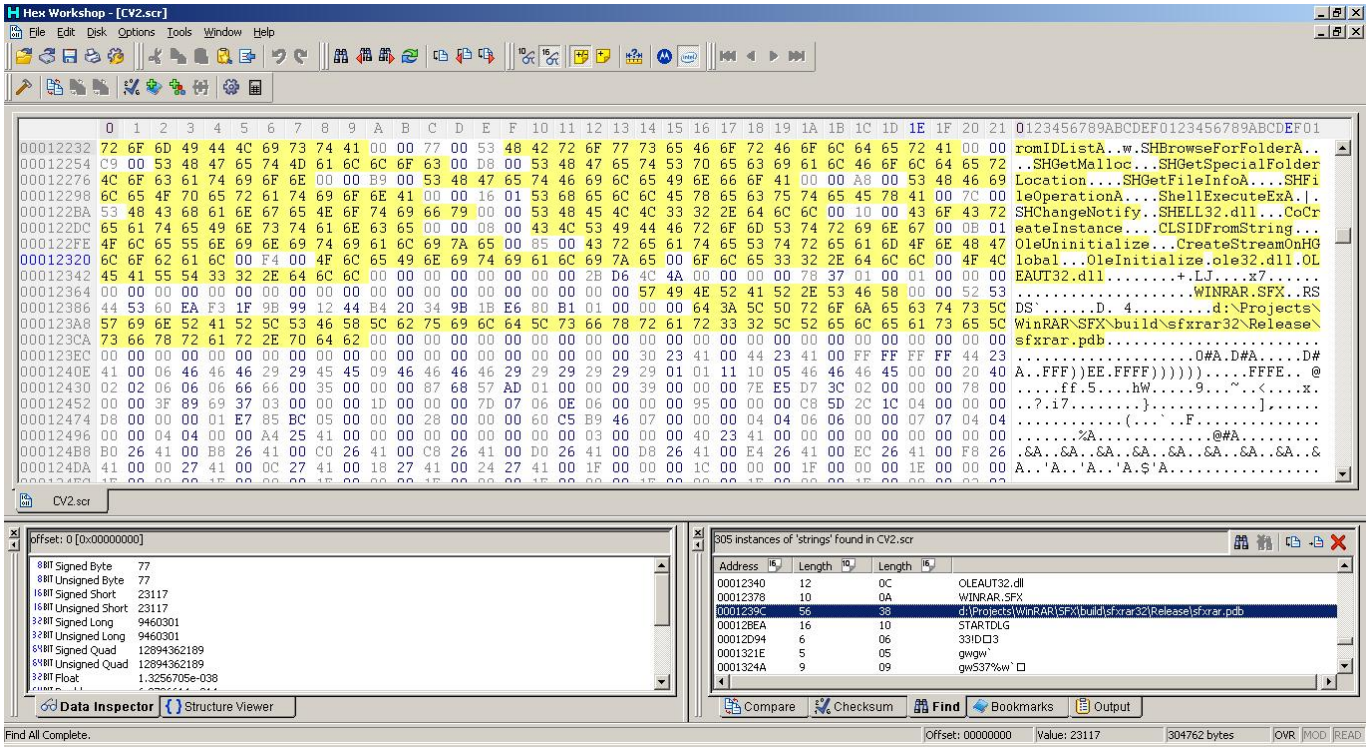
Genellikle şüphelendiğim dosyaları virustotal sitesine yüklemeyi görev edinmiş biri olarak yine ilk işim tüm dosyaları bu siteye yüklemek oldu. Virustotal sitesini bilmeyenler için ufak bir not düşeyim, bu site yolladığınız dosyayı yaklaşık 40 farklı antivirus motoru ile tarıyor ve sonucu hemen size gösteriyor.



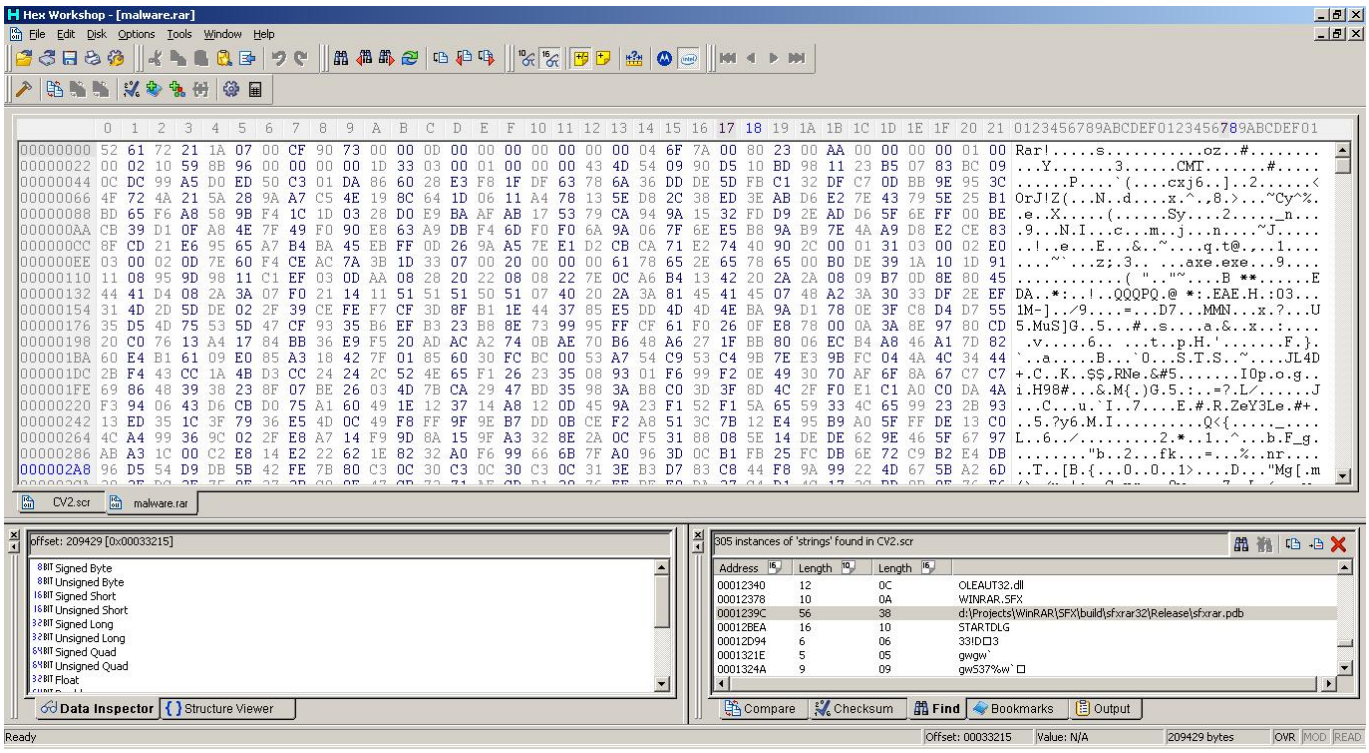
SCR ve RTF uzantılı iki dosyayı siteye yüklediğimde boş yere şüphelenmediğimi bir nevi teyit etmiş oldum.

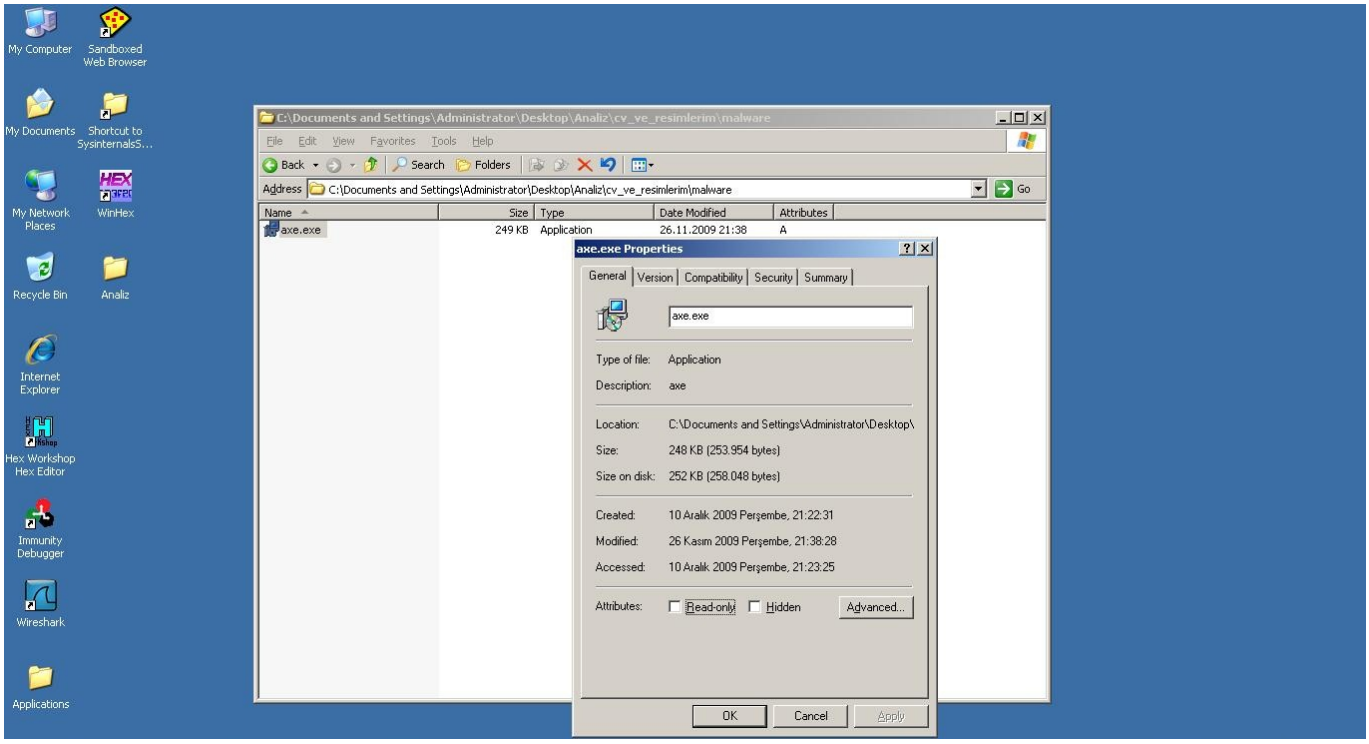
Biraz daha ileriye giderek CV2.scr dosyasını hex editor ile incelediğimde RAR başlığı ile karşılaştım. Bu durum şüpheli dosya içerisinde rar ile sıkıştırılmış başka bir dosyanın var olduğuna dair ufak bir işaretti.

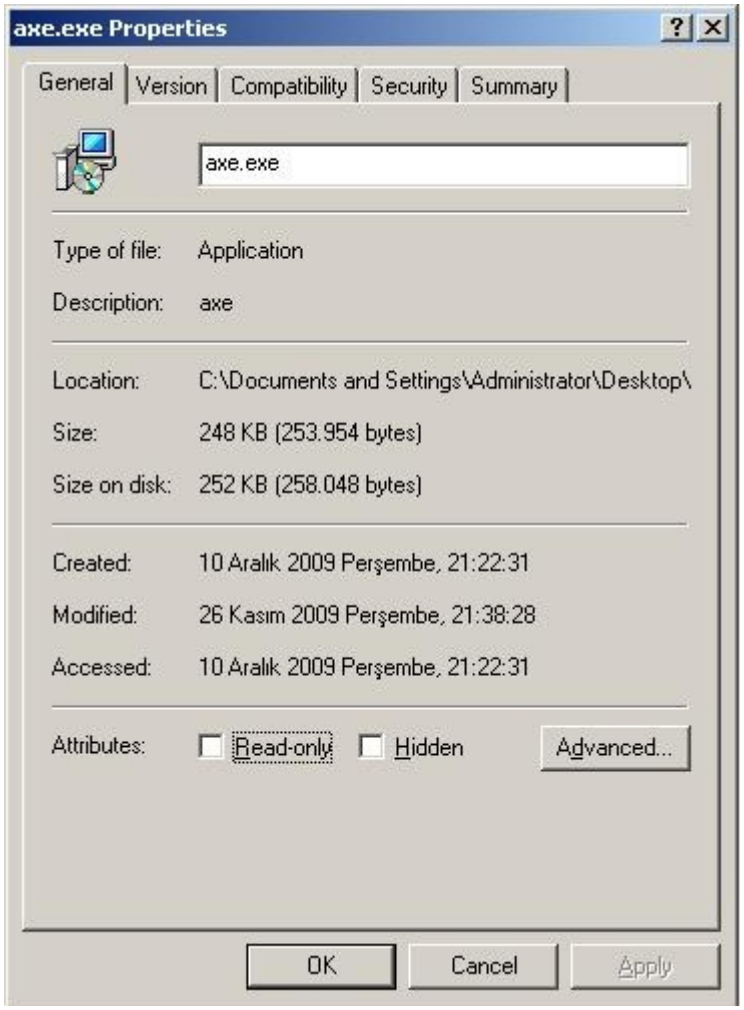




Tüm stringleri listeledikten Winrar ile ilgili başka stringler ile de karşılaşınca RAR başlığı ile başlayan kısımları SCR dosyasından çıkartmaya, malware.rar adı altında kaydetmeye ve daha sonrasında winrar uygulaması ile açmaya karar verdim.

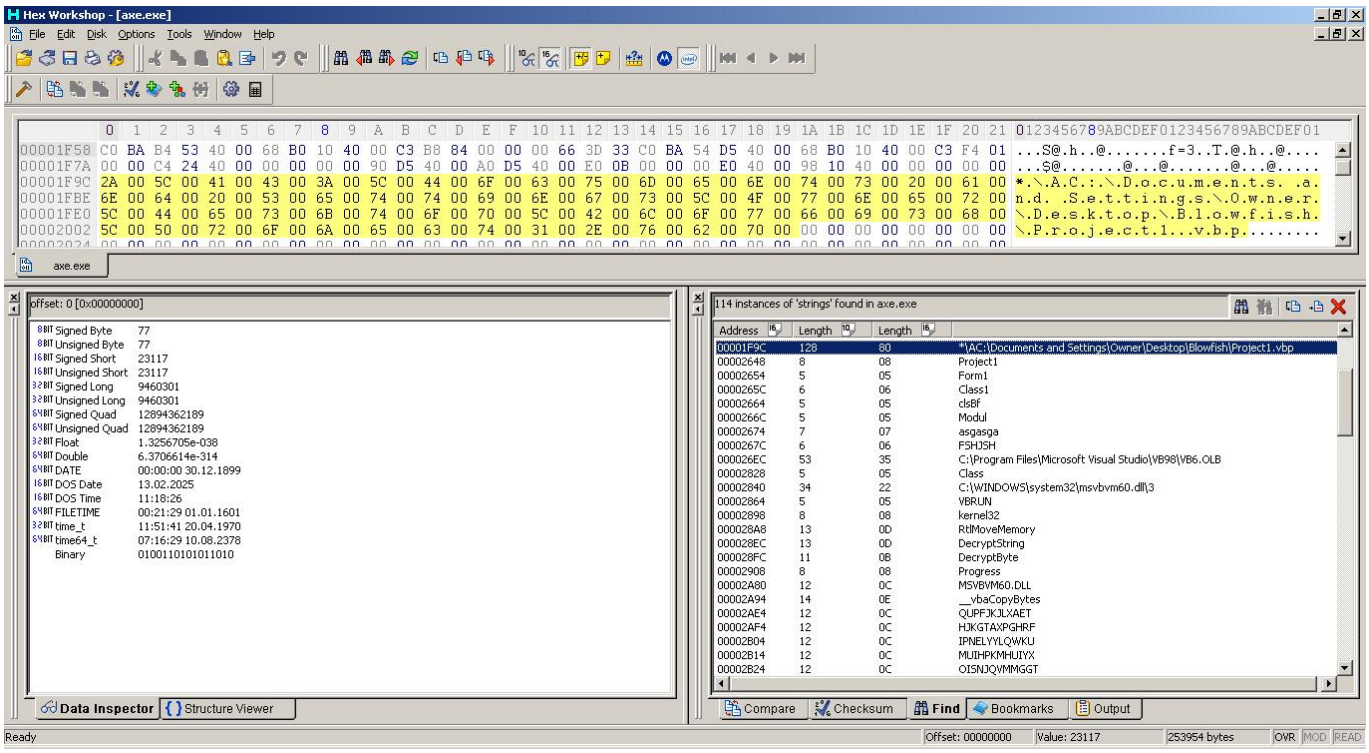

Hex Workshop - [malware.rar]
File Edit Disk Options Tools Window Help
CV2.scr
malware.rar
offset: 209429 [0x00033215]
8 BIT Signed Byte
8 BIT Unsigned Byte
16 BIT Signed Short
16 BIT Unsigned Short
32 BIT Signed Long
32 BIT Unsigned Long
64 BIT Signed Quad
64 BIT Unsigned Quad
32 BIT Float
Data Inspector
Structure Viewer
305 instances of 'strings' found in CV2.scr
Address
Length
Length
00012340 12 0C OLEAUT32.dll
00012378 10 0A WINRAR.SFX
0001239C 56 38 d:\Projects\WinRAR\SFX\build\sfxrar32\Release\sfxrar.pdb
00012BEA 16 10 STARTDLG
00012D94 6 06 33IDD3
0001321E 5 05 gwgw`
0001324A 9 09 gw537%w`□
Compare
Checksum
Find
Bookmarks
Output
Ready
Offset: 00033215
Value: N/A
209429 bytes
OVR
MOD
READ


My Computer
Sandboxed Web Browser
My Documents
Shortcut to SysinternalsS...
My Network Places
WinHex
Recycle Bin
Analiz
Internet Explorer
Hex Workshop Hex Editor
Immunity Debugger
Wireshark
Applications
C:\Documents and Settings\Administrator\Desktop\Analiz\cv_ve_resimlerim\malware
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\Administrator\Desktop\Analiz\cv_ve_resimlerim\malware
Go
Name Size Type Date Modified Attributes
axe.exe 249 KB Application 26.11.2009 21:38 A
axe.exe Properties
General Version Compatibility Security Summary
axe.exe
Type of file: Application
Description: axe
Location: C:\Documents and Settings\Administrator\Desktop\
Size: 248 KB (253.954 bytes)
Size on disk: 252 KB (258.048 bytes)
Created: 10 Aralık 2009 Perşembe, 21:22:31
Modified: 26 Kasım 2009 Perşembe, 21:38:28
Accessed: 10 Aralık 2009 Perşembe, 21:23:25
Attributes: Read-only Hidden Advanced...
OK
Cancel
Apply

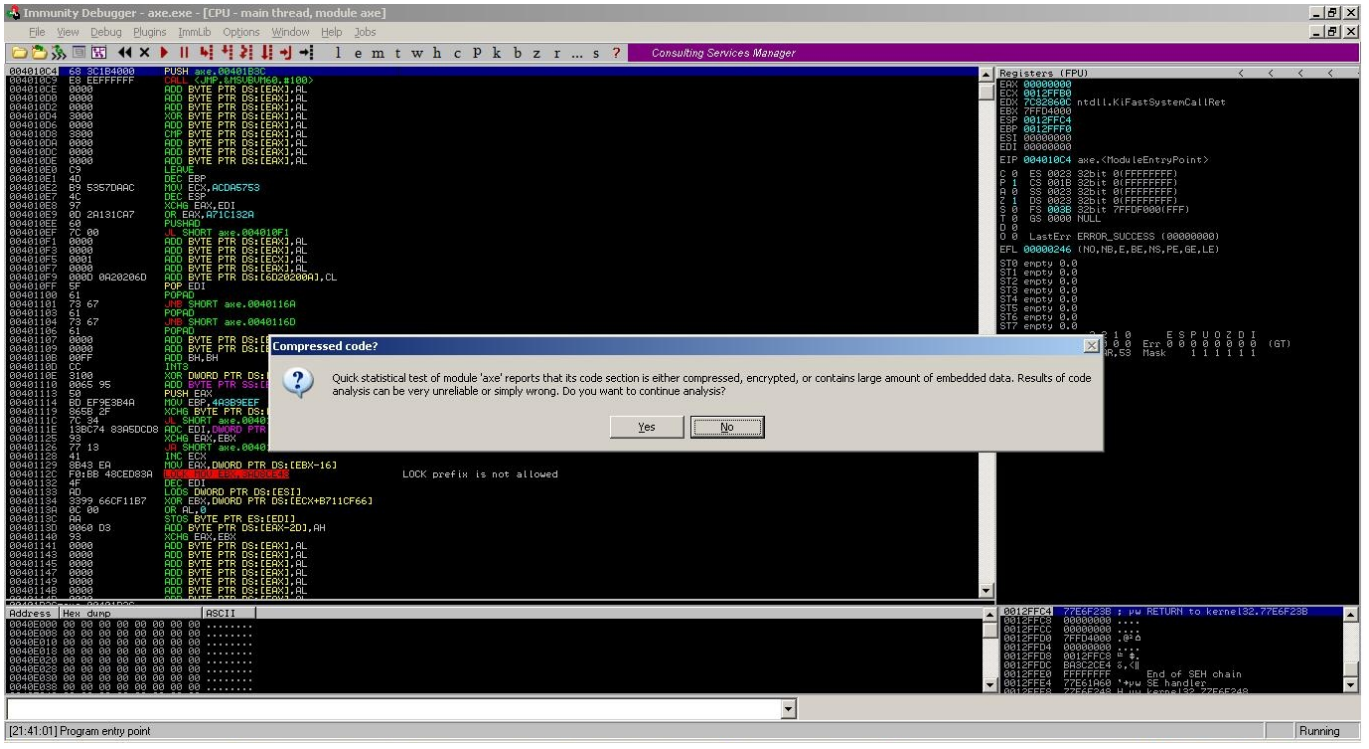


Bingo, axe.exe adında yeni bir dosya karşıma çıktı.

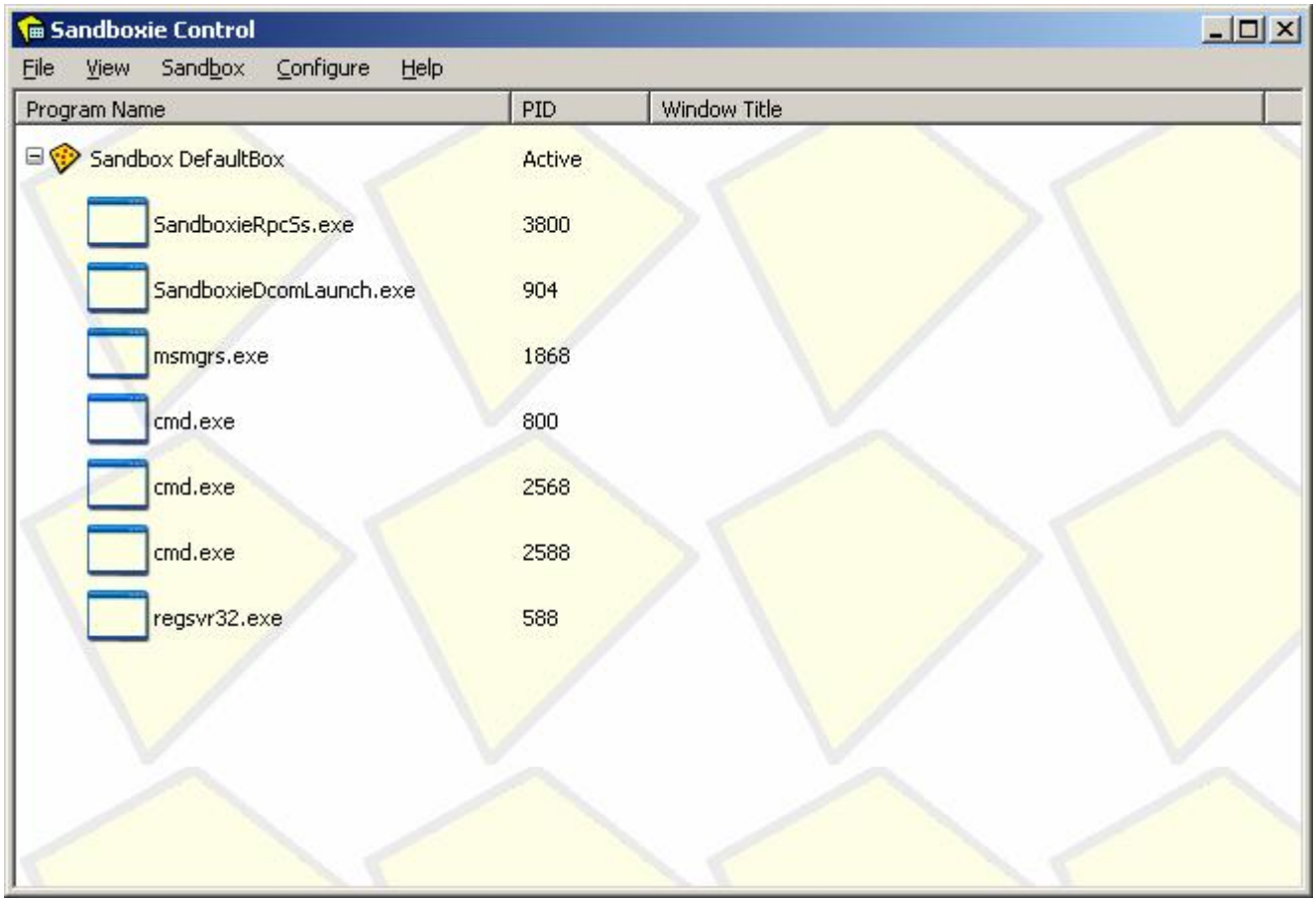
Bu dosyayı da hex editor ile incelediğimde decryptbyte, decryptstring fonksiyonları ile karşılaştım. Bu fonksiyonlar yazılımın bir şekilde encrypt edildiğini ve çalışma esnasında kendisini hafızada decrypt ettiği ihtimalini gündeme getirdi.

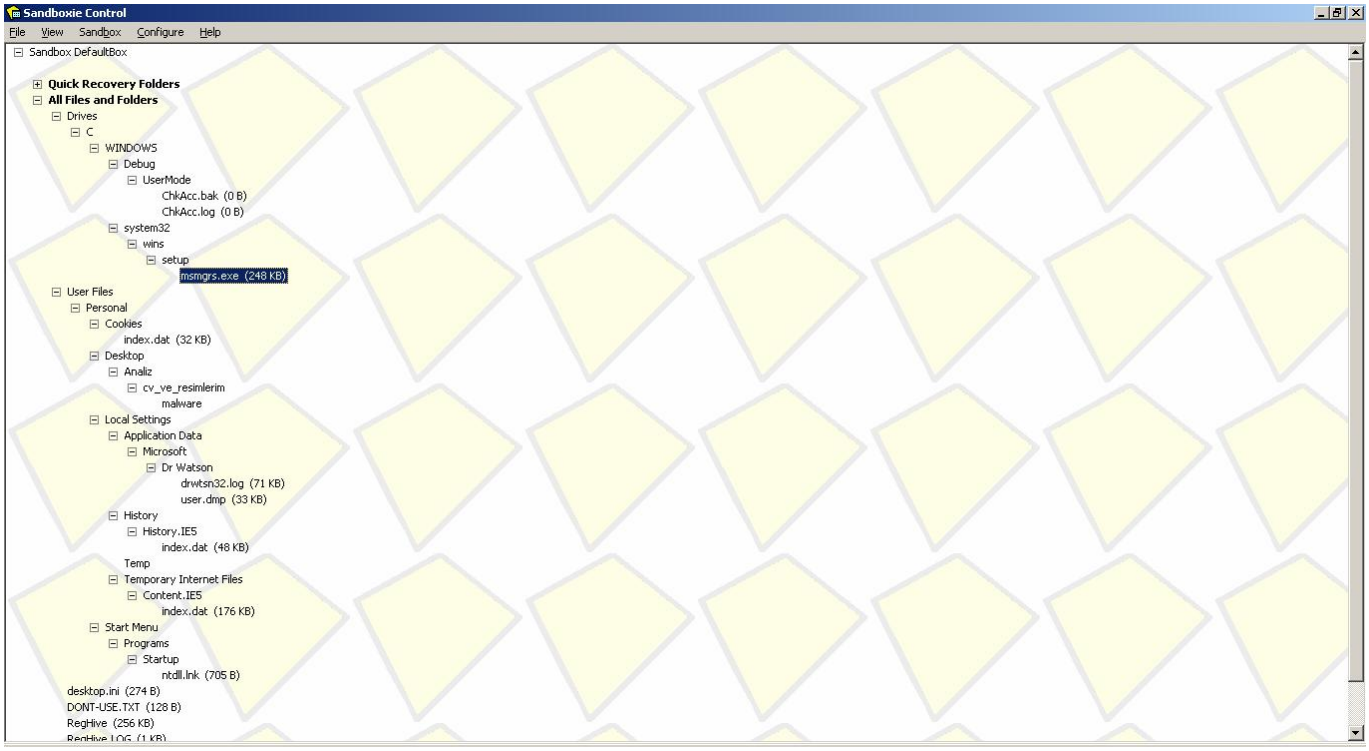


Immunity debugger ile programı çalıştırdığımda da bu ihtimal iyice güçlenmişti.



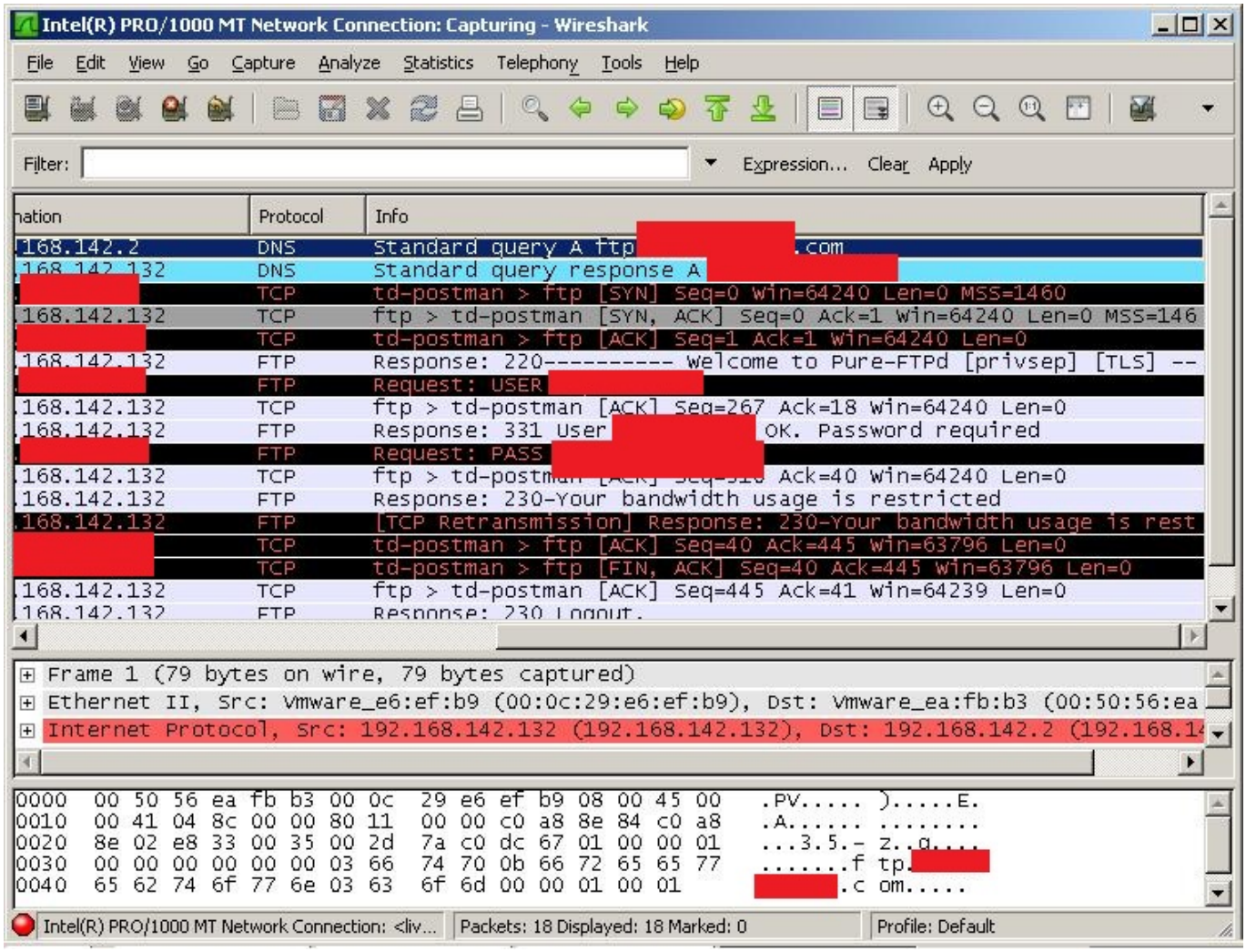
Trojanı sandboxta çalıştırdığımda kendisini msmgrs.exe adı altında system32\wins\setup klasörü altına kopyaladığını gördüm.



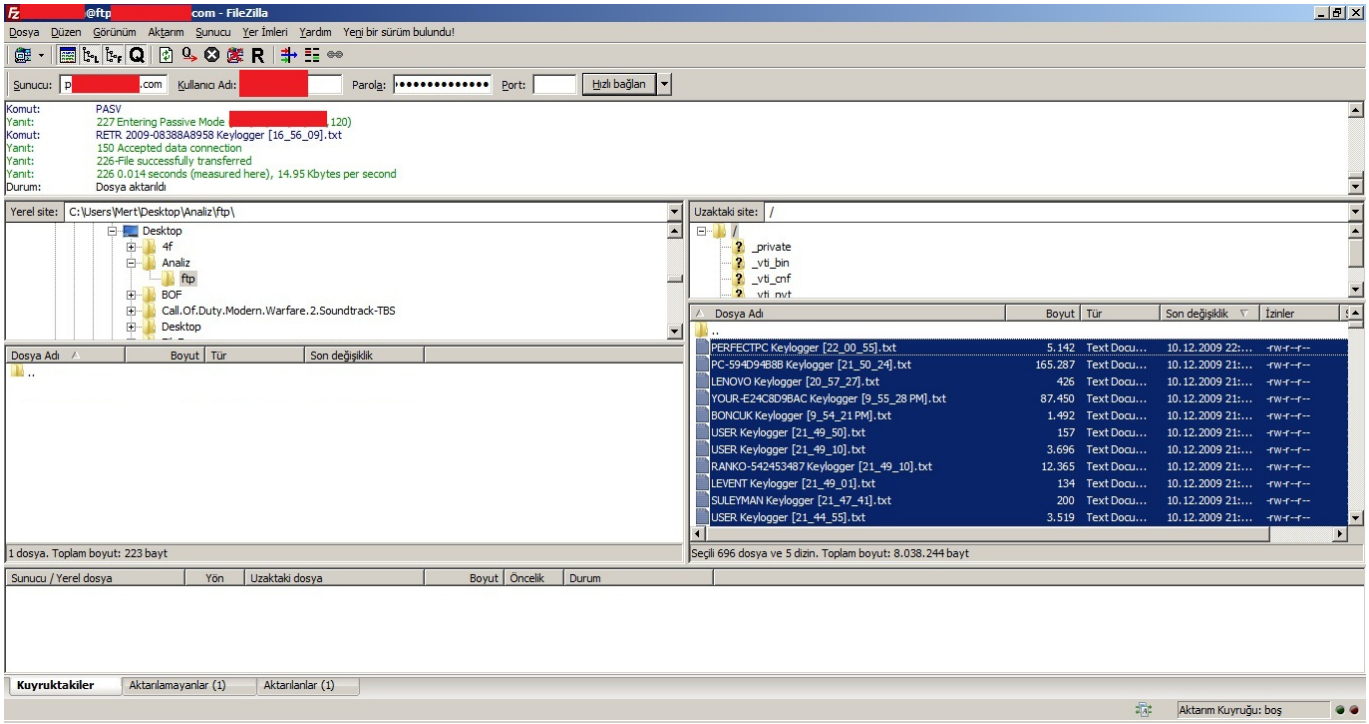


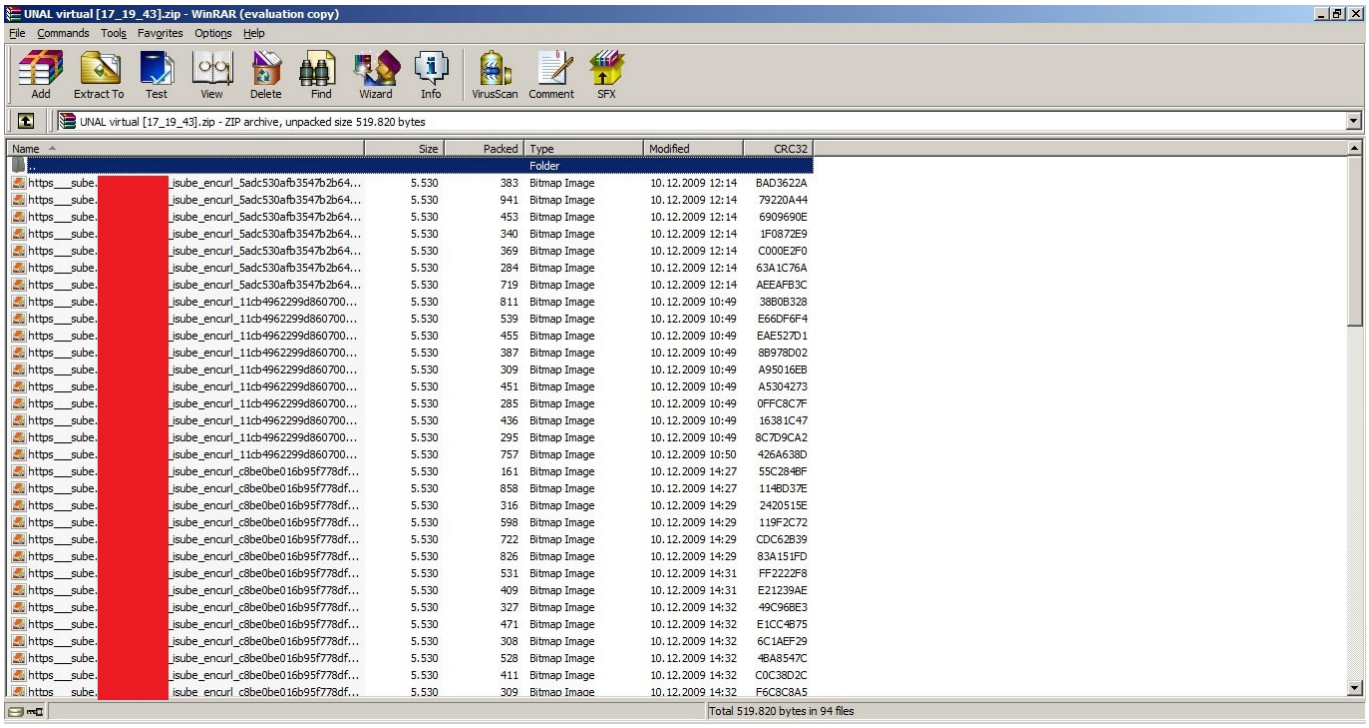
Sıra en can alıcı noktaya gelmişti, peki bu program çalıştıktan sonra ne yapıyordu ?

İlk yaptığım iş wireshark sniffer programını çalıştırmak ve programın nereyle haberleştiğini tespit etmek oldu ve bir bingo daha program yurt dışında bir ftp sunucusuna bağlanıyordu.



Malum ftp protokolü şifresiz haberleştiği için kullanıcı adını ve şifreyi tespit etmem hiçte zor olmadı. Bende aynı kullanıcı adı ve şifre ile ftp sunucusuna bağlandığımda yaklaşık 696 tane kullanıcıya ait olan tuş kayıtları ve internet bankacılığına girişte kayıt edilmiş olan ekran görüntüleri ile karşılaştım.





Daha da ileriye giderek trojanı decompile etmek ve memory’den decrypt edilmiş halini capture ederek incelemek istesemde bir türlü fırsat bulamadım.

That’s all folks…