

# Basit Malware Analizi (Windows)

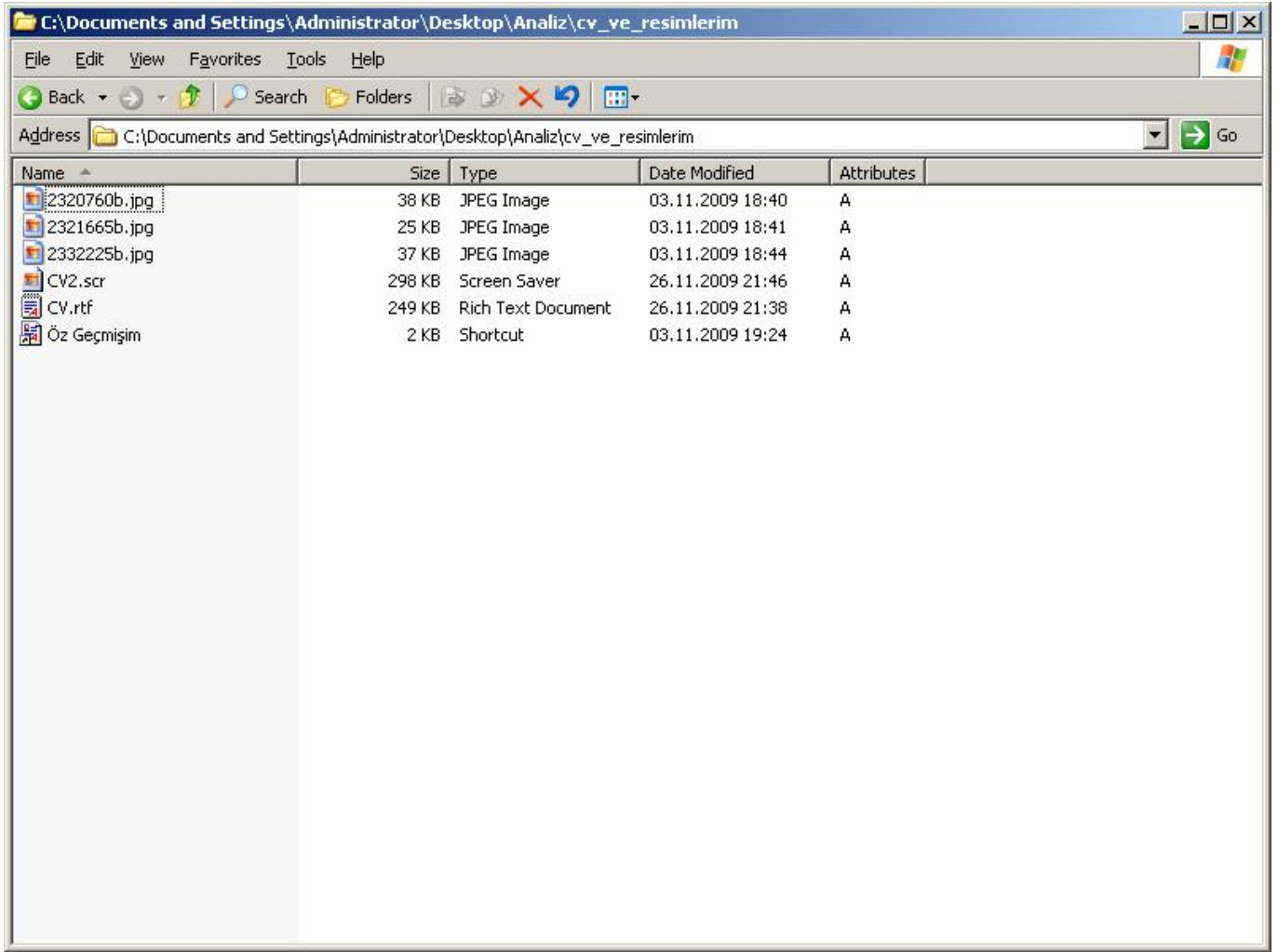
written by Mert SARICA | 9 February 2010

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

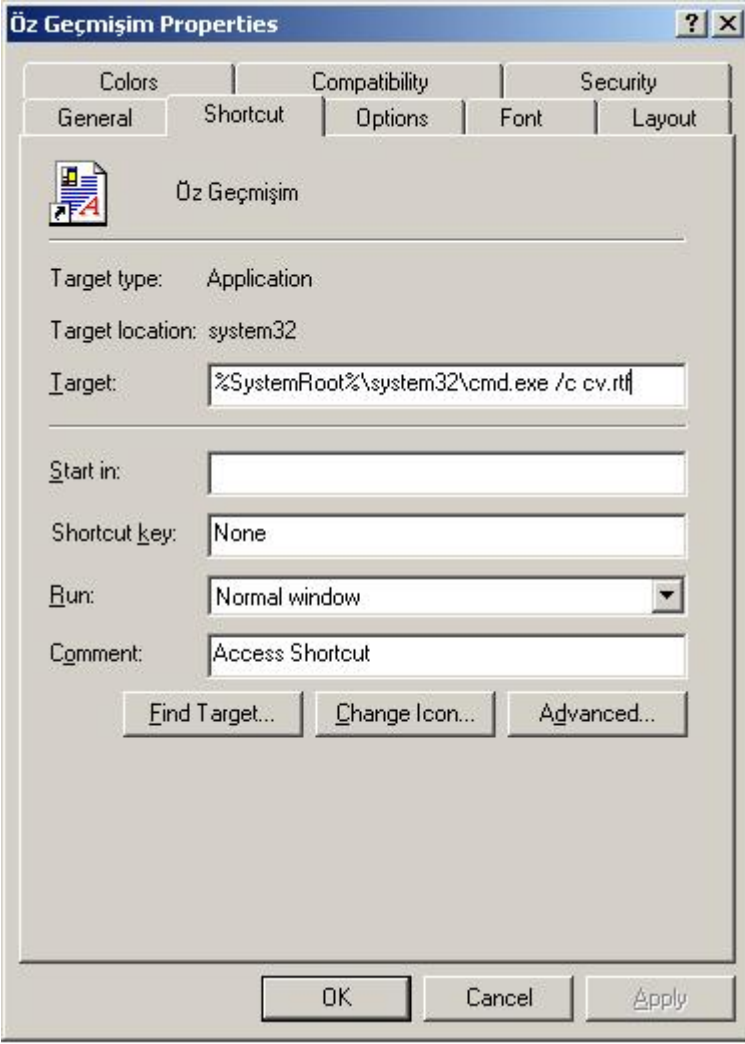
Bugünkü yazımın sizlere basitçe şüphelendiğiniz bir programın işletim sisteminizde ne işler çevirdiğini anlamanız için yol göstereceğini ümit ediyorum.

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 takdirde 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.

VirusTotal. MDS: 08f4cdf468b18f8337416c791d4684dd TrojWare.Win32.TrojJan.Agent.Gen BackDoor.Pois - Windows Internet Explorer

http://www.virustotal.com/analysis/432f6429bb786315cae4f17bb1df61a95fd111d41af4ed5330de8ada4c03770-1259767972

File Edit View Favorites Tools Help

VirusTotal. MDS: 08f4cdf468b18f8337416c791d4684dd...

**VIRUS TOTAL**

VirusTotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

File **CV.rtf** received on **2009.12.02 15:32:52 (UTC)**  
Current status: **finished**  
Result: **3/41 (7.32%)**

[Compact](#) [Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.43	2009.12.02	-
AhnLab-V3	5.0.0.2	2009.12.02	-
AntiVir	7.9.1.92	2009.12.02	-
Antiy-AVL	2.0.3.7	2009.12.02	-
Authentium	5.2.0.5	2009.12.02	-
Avast	4.8.1351.0	2009.12.02	-
AVG	8.5.0.426	2009.12.02	-
BitDefender	7.2	2009.12.02	-
CAT-QuickHeal	10.00	2009.12.02	-
ClamAV	0.94.1	2009.12.02	-
Comodo	3103	2009.12.01	TrojWare.Win32.TrojJan.Agent.Gen
DrWeb	5.0.0.12182	2009.12.02	BackDoor.Poison.767

Internet 100%

VirusTotal. MDS: de49ad1512394a6975905de745b5dbb5 Heuristic.BehavestLike.Win32.Dropper.I TrojWar - Windows Internet Explorer

http://www.virustotal.com/analysis/49ddc2733ae2ba12b7c392f55c60a02c974e5372ede7c78fb151163ae8e9be65-1259850756

File Edit View Favorites Tools Help

VirusTotal. MDS: de49ad1512394a6975905de745b5dbb5...

**VIRUS TOTAL**

VirusTotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

File **CV2.scr** received on **2009.12.03 14:32:36 (UTC)**  
Current status: **finished**  
Result: **7/40 (17.50%)**

[Compact](#) [Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.43	2009.12.03	-
AhnLab-V3	5.0.0.2	2009.12.03	-
AntiVir	7.9.1.92	2009.12.03	-
Antiy-AVL	2.0.3.7	2009.12.03	-
Authentium	5.2.0.5	2009.12.02	-
Avast	4.8.1351.0	2009.12.03	-
AVG	8.5.0.426	2009.12.03	-
BitDefender	7.2	2009.12.03	-
CAT-QuickHeal	10.00	2009.12.03	-
ClamAV	0.94.1	2009.12.03	-
Comodo	3103	2009.12.01	TrojWare.Win32.TrojJan.Agent.Gen
DrWeb	5.0.0.12182	2009.12.03	BackDoor.Poison.767
eSafe	7.0.17.0	2009.12.02	-
eTrust-Vet	35.1.7155	2009.12.03	-
F-Prot	4.5.1.85	2009.12.02	-
F-Secure	9.0.15370.0	2009.12.03	-
Fortinet	4.0.14.0	2009.12.03	-

Internet 100%

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.





Hex Workshop - [malware.rar]

File Edit Disk Options Tools Window Help

0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 0123456789ABCDEF0123456789ABCDEF01

```

00000000 52 61 72 21 1A 07 00 CF 90 73 00 00 00 00 00 00 04 6F 7A 00 80 23 00 AA 00 00 00 01 00 Rar!.....s.....oz.#.....
00000022 00 02 10 59 8B 96 00 00 00 00 1D 33 03 00 01 00 00 00 43 4D 54 09 90 D5 10 BD 98 11 23 B5 07 83 BC 09 ..Y.....3.....CMT.....#.....
00000044 0C DC 99 A5 D0 ED 50 C3 01 DA 86 60 28 E3 F8 1F DF 63 78 6A 36 DD DE 5D FB C1 32 DF C7 0D BB 9E 95 3C .....P.....(....cxj6..).2.....<
00000066 4F 72 4A 21 5A 28 9A A7 C5 4E 19 9C 64 1D 06 11 A4 78 13 5E D8 2C 38 ED 3E AB D6 E2 7E 43 79 5E 25 B1 0rJlZ(...N..d...x.^..8>...~Cy^%.
00000088 BD 65 F6 A8 58 9B F4 1C 1D 03 28 D0 E9 BA AF AB 17 53 79 CA 94 9A 15 32 FD D9 2E AD D6 5F 6E FF 00 BE .e.X....(....Sy...2....._n...
000000AA CB 39 D1 0F A8 4E 7F 49 F0 90 E8 63 A9 DB F4 6D F0 F0 6A 9A 06 7F 6E E5 B8 9A B9 7E 4A A9 D8 E2 CE 83 .9...N.I..c...m..j...n...~J...
000000CC 8F CD 21 E6 95 65 A7 B4 BA 45 EB FF 0D 26 9A A5 7E E1 D2 CB CA 71 E2 74 40 90 2C 00 01 31 03 00 02 E0 .l..e...E...&...&.q.t@...1...
000000EE 03 00 02 0D 7E 60 F4 CE AC 7A 3B 1D 33 07 00 20 00 00 00 61 78 65 2E 65 78 65 00 B0 DE 39 1A 10 1D 91 .....z;.3.....axe.exe...9...
00000110 11 08 95 9D 98 11 C1 EF 03 0D AA 08 28 20 22 08 08 22 7E 0C A6 B4 13 42 20 2A 2A 08 09 B7 0D 8E 80 45 .....( ".....B **...E
00000132 44 41 D4 08 2A 3A 07 F0 21 14 11 51 51 51 50 51 07 40 20 2A 3A 81 45 41 45 07 48 A2 3A 30 33 DF 2E EF DA.*:..!..QQQPQ.@*:.EAE.H.:03...
00000154 31 4D 2D 5D E2 02 2F 39 CE FE F7 CF 30 8F B1 1E 44 37 85 E5 DD 4D 4D 4E BA 9A D1 78 0E 3F C8 D4 D7 55 1M-].../9...=.D7...MMN...x.?..U
00000176 35 D5 4D 75 53 5D 47 CF 93 35 B6 EF B3 23 B8 8E 73 99 95 FF CF 61 F0 26 0F E8 78 00 0A 3A 8E 97 80 CD 5.MuSjG.5...#...s...a.&...x...:..
00000198 20 C0 76 13 A4 17 84 BB 36 E9 F5 20 AD AC A2 74 0B AE 70 B6 48 A6 27 1F BB 80 06 EC B4 A8 46 A1 7D 82 .v...6...t...p.H...F...}.
000001BA 6D E4 B1 61 09 E0 85 A3 18 42 7F 01 85 60 30 FC BC 00 53 A7 54 C9 53 C4 9B 7E E3 9B FC 04 4A 4C 34 44 ..a...B...0...S.T.S...~.x...:..JL4D
000001DC 2B F4 43 CC 1A 4B D3 CC 24 24 2C 52 4E 65 F1 26 23 0C 58 93 01 F6 99 F2 0E 49 30 70 AF 6F 8A 67 C7 C7 +.C..K..$$.RNe.&#5...=7.I...o.g
000001FE 69 86 48 39 38 23 8F 07 BE 26 03 4D 7B CA 29 47 BD 35 98 3A B8 C0 3D 3F 8D 4C 2F F0 E1 C1 A0 C0 DA 4A i.H98#...&.M().G.5...=#.L...nr...
00000220 F3 94 06 43 D6 CB D0 75 A1 60 49 1E 12 37 14 A8 12 0D 45 9A 23 F1 52 F1 5A 65 59 33 4C 65 99 23 2B 93 ..C...u..I..7...E.#.R.ZeY3Le.#+.
00000242 13 ED 35 1C 3F 79 36 E5 4D 0C 49 F8 FF 9F 9E B7 DD 0B CE F2 A8 51 3C 7B 12 E4 95 B9 A0 5F FF DE 13 C0 .5.?y6.M.I...#...Q<{...
00000264 4C A4 99 36 9C 02 2F E8 A7 14 F9 9D 8A 15 9F A3 32 8E 2A 0C F5 31 88 08 1E 14 DE DE 62 9E 46 5F 67 97 L..6.../.....2.*..1...^..b.F_g
00000286 AB A3 1C 00 C2 E8 14 E2 22 62 1E 82 32 A0 F6 99 66 6B 7F A0 96 3D 0C B1 F8 25 FC DB 6E 72 C9 B2 E4 DB ..b...2...fk...%...%..nr...
000002A8 96 D5 54 D9 DB 5B 42 FE 7B 80 C3 0C 30 C3 0C 30 C3 0C 31 3E B3 D7 83 C8 44 F8 9A 99 22 4D 67 5B A2 6D .T.[B{...0..0..>...D...Mg[.m

```

CV2.scr malware.rar

Offset: 209429 [0x0033215]

8BIT Signed Byte  
8BIT Unsigned Byte  
16BIT Signed Short  
16BIT Unsigned Short  
32BIT Signed Long  
32BIT Unsigned Long  
64BIT Signed Quad  
64BIT Unsigned Quad  
32BIT Float

Data Inspector Structure Viewer

605 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	33D03
0001321E	5	05	gqgw
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 Sysinternals...

My Network Places WinHex

Recycle Bin Analz

Internet Explorer

Hex Workshop Hex Editor

Immunity Debugger

Wireshark

Applications

C:\Documents and Settings\Administrator\Desktop\Analz\cv\_ve\_resimlerim\malware

Address C:\Documents and Settings\Administrator\Desktop\Analz\cv\_ve\_resimlerim\malware

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

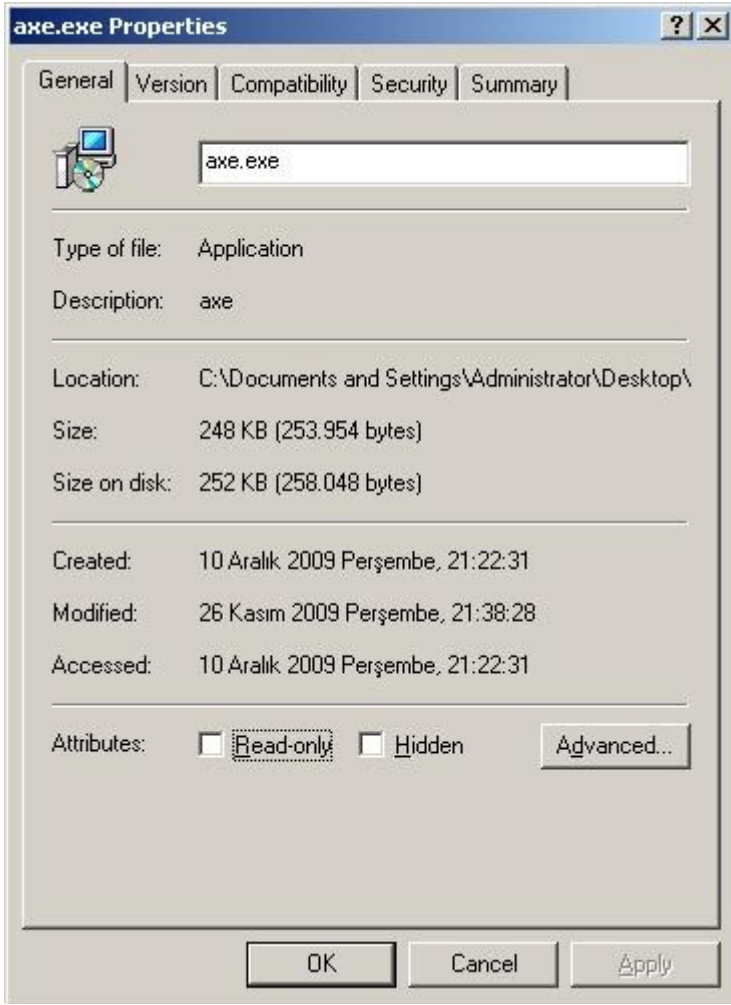
Type of file: Application  
Description: axe

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.



**Hex Workshop - [axe.exe]**

The hex dump shows the following data:

```

00001F58 C0 BA B4 53 40 00 68 B0 10 40 00 C3 B8 84 00 00 00 66 3D 33 C0 BA 54 D5 40 00 68 B0 10 40 00 C3 F4 01 ...S@.h.e.....f=3..T.@.h...@...
00001F7A 00 00 C4 24 40 00 00 00 00 00 00 90 D5 40 00 A0 E0 08 00 00 00 E0 40 00 98 10 40 00 00 00 00 00 00 ...@.....@.....@.....
00001F9C 2A 00 5C 00 41 00 43 00 3A 00 5C 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 61 00 ...\.A.C:...\D.o.c.u.m.e.n.t.s.\.a
00001FBE 6E 00 64 00 20 00 53 00 00 65 00 74 00 74 00 69 00 66 00 67 00 73 00 65 00 4F 00 77 00 6E 00 65 00 72 00 ...n.d.\.S.e.t.t.i.n.g.s.\.O.w.n.e.r.
00001FE0 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 42 00 6C 00 6F 00 77 00 66 00 69 00 73 00 68 00 ...\.D.e.s.k.t.o.p.\.B.l.o.w.f.i.s.h.
00002002 5C 00 50 00 72 00 6F 00 6A 00 64 00 63 00 74 00 51 00 2E 00 76 00 62 00 70 00 00 00 00 00 00 00 00 ...\.P.r.o.j.e.c.t.l...v.b.p.....
  
```

**114 instances of 'strings' found in axe.exe**

Address	Length	Length	String
00001F9C	128	80	*[AC:\Documents and Settings\Owner\Desktop\Blowfish\Project1.vbp
00002648	8	08	Project1
00002654	5	05	Form1
0000265C	6	06	Class1
00002664	5	05	clsBf
0000266C	5	05	Modul
00002674	7	07	asqasqa
0000267C	6	06	FSHSH
000026EC	53	35	C:\Program Files\Microsoft Visual Studio\VB98\VB6.OLB
00002828	5	05	Class
00002840	34	22	C:\WINDOWS\system32\msvbvm60.dll3
00002864	5	05	VBRUN
00002898	8	08	kernel32
000028A8	13	0D	RtlMoveMemory
000028EC	13	0D	DecryptString
000028FC	11	0B	DecryptByte
00002908	8	08	Progress
00002A80	12	0C	MSVBVM60.DLL
00002A94	14	0E	__vbaCopyBytes
00002AE4	12	0C	QURFKJLXAET
00002AF4	12	0C	HJGTAXPGHRFP
00002B04	12	0C	IPNELYVJQWKLJ
00002B14	12	0C	MUJPKWHLIYX
00002B24	12	0C	OISNDQWMGGT

Immunity debugger ile programı çalıştırdığımda da bu ihtimal iyice güçlenmişti.

**Immunity Debugger - axe.exe - [CPU - main thread, module axe]**

The assembly view shows the following instructions:

```

004010C4 68 3C1E4888 PUSH eax,004010C8
004010C5 EB EF7F8000 JBE 004010C5
004010C6 90 ADD BYTE PTR DS:[EAX],AL
004010C7 90 ADD BYTE PTR DS:[EAX],AL
004010C8 90 ADD BYTE PTR DS:[EAX],AL
004010C9 90 ADD BYTE PTR DS:[EAX],AL
004010CA 90 ADD BYTE PTR DS:[EAX],AL
004010CB 90 ADD BYTE PTR DS:[EAX],AL
004010CC 90 ADD BYTE PTR DS:[EAX],AL
004010CD 90 ADD BYTE PTR DS:[EAX],AL
004010CE 90 ADD BYTE PTR DS:[EAX],AL
004010CF 90 ADD BYTE PTR DS:[EAX],AL
004010D0 90 ADD BYTE PTR DS:[EAX],AL
004010D1 90 ADD BYTE PTR DS:[EAX],AL
004010D2 90 ADD BYTE PTR DS:[EAX],AL
004010D3 90 ADD BYTE PTR DS:[EAX],AL
004010D4 90 ADD BYTE PTR DS:[EAX],AL
004010D5 90 ADD BYTE PTR DS:[EAX],AL
004010D6 90 ADD BYTE PTR DS:[EAX],AL
004010D7 90 ADD BYTE PTR DS:[EAX],AL
004010D8 90 ADD BYTE PTR DS:[EAX],AL
004010D9 90 ADD BYTE PTR DS:[EAX],AL
004010DA 90 ADD BYTE PTR DS:[EAX],AL
004010DB 90 ADD BYTE PTR DS:[EAX],AL
004010DC 90 ADD BYTE PTR DS:[EAX],AL
004010DD 90 ADD BYTE PTR DS:[EAX],AL
004010DE 90 ADD BYTE PTR DS:[EAX],AL
004010DF 90 ADD BYTE PTR DS:[EAX],AL
004010E0 90 ADD BYTE PTR DS:[EAX],AL
004010E1 90 ADD BYTE PTR DS:[EAX],AL
004010E2 90 ADD BYTE PTR DS:[EAX],AL
004010E3 90 ADD BYTE PTR DS:[EAX],AL
004010E4 90 ADD BYTE PTR DS:[EAX],AL
004010E5 90 ADD BYTE PTR DS:[EAX],AL
004010E6 90 ADD BYTE PTR DS:[EAX],AL
004010E7 90 ADD BYTE PTR DS:[EAX],AL
004010E8 90 ADD BYTE PTR DS:[EAX],AL
004010E9 90 ADD BYTE PTR DS:[EAX],AL
004010EA 90 ADD BYTE PTR DS:[EAX],AL
004010EB 90 ADD BYTE PTR DS:[EAX],AL
004010EC 90 ADD BYTE PTR DS:[EAX],AL
004010ED 90 ADD BYTE PTR DS:[EAX],AL
004010EE 90 ADD BYTE PTR DS:[EAX],AL
004010EF 90 ADD BYTE PTR DS:[EAX],AL
004010F0 90 ADD BYTE PTR DS:[EAX],AL
004010F1 90 ADD BYTE PTR DS:[EAX],AL
004010F2 90 ADD BYTE PTR DS:[EAX],AL
004010F3 90 ADD BYTE PTR DS:[EAX],AL
004010F4 90 ADD BYTE PTR DS:[EAX],AL
004010F5 90 ADD BYTE PTR DS:[EAX],AL
004010F6 90 ADD BYTE PTR DS:[EAX],AL
004010F7 90 ADD BYTE PTR DS:[EAX],AL
004010F8 90 ADD BYTE PTR DS:[EAX],AL
004010F9 90 ADD BYTE PTR DS:[EAX],AL
004010FA 90 ADD BYTE PTR DS:[EAX],AL
004010FB 90 ADD BYTE PTR DS:[EAX],AL
004010FC 90 ADD BYTE PTR DS:[EAX],AL
004010FD 90 ADD BYTE PTR DS:[EAX],AL
004010FE 90 ADD BYTE PTR DS:[EAX],AL
004010FF 90 ADD BYTE PTR DS:[EAX],AL
00401100 90 ADD BYTE PTR DS:[EAX],AL
00401101 90 ADD BYTE PTR DS:[EAX],AL
00401102 90 ADD BYTE PTR DS:[EAX],AL
00401103 90 ADD BYTE PTR DS:[EAX],AL
00401104 90 ADD BYTE PTR DS:[EAX],AL
00401105 90 ADD BYTE PTR DS:[EAX],AL
00401106 90 ADD BYTE PTR DS:[EAX],AL
00401107 90 ADD BYTE PTR DS:[EAX],AL
00401108 90 ADD BYTE PTR DS:[EAX],AL
00401109 90 ADD BYTE PTR DS:[EAX],AL
0040110A 90 ADD BYTE PTR DS:[EAX],AL
0040110B 90 ADD BYTE PTR DS:[EAX],AL
0040110C 90 ADD BYTE PTR DS:[EAX],AL
0040110D 90 ADD BYTE PTR DS:[EAX],AL
0040110E 90 ADD BYTE PTR DS:[EAX],AL
0040110F 90 ADD BYTE PTR DS:[EAX],AL
00401110 90 ADD BYTE PTR DS:[EAX],AL
00401111 90 ADD BYTE PTR DS:[EAX],AL
00401112 90 ADD BYTE PTR DS:[EAX],AL
00401113 90 ADD BYTE PTR DS:[EAX],AL
00401114 90 ADD BYTE PTR DS:[EAX],AL
00401115 90 ADD BYTE PTR DS:[EAX],AL
00401116 90 ADD BYTE PTR DS:[EAX],AL
00401117 90 ADD BYTE PTR DS:[EAX],AL
00401118 90 ADD BYTE PTR DS:[EAX],AL
00401119 90 ADD BYTE PTR DS:[EAX],AL
0040111A 90 ADD BYTE PTR DS:[EAX],AL
0040111B 90 ADD BYTE PTR DS:[EAX],AL
0040111C 90 ADD BYTE PTR DS:[EAX],AL
0040111D 90 ADD BYTE PTR DS:[EAX],AL
0040111E 90 ADD BYTE PTR DS:[EAX],AL
0040111F 90 ADD BYTE PTR DS:[EAX],AL
00401120 90 ADD BYTE PTR DS:[EAX],AL
00401121 90 ADD BYTE PTR DS:[EAX],AL
00401122 90 ADD BYTE PTR DS:[EAX],AL
00401123 90 ADD BYTE PTR DS:[EAX],AL
00401124 90 ADD BYTE PTR DS:[EAX],AL
00401125 90 ADD BYTE PTR DS:[EAX],AL
00401126 90 ADD BYTE PTR DS:[EAX],AL
00401127 90 ADD BYTE PTR DS:[EAX],AL
00401128 90 ADD BYTE PTR DS:[EAX],AL
00401129 90 ADD BYTE PTR DS:[EAX],AL
0040112A 90 ADD BYTE PTR DS:[EAX],AL
0040112B 90 ADD BYTE PTR DS:[EAX],AL
0040112C 90 ADD BYTE PTR DS:[EAX],AL
0040112D 90 ADD BYTE PTR DS:[EAX],AL
0040112E 90 ADD BYTE PTR DS:[EAX],AL
0040112F 90 ADD BYTE PTR DS:[EAX],AL
00401130 90 ADD BYTE PTR DS:[EAX],AL
00401131 90 ADD BYTE PTR DS:[EAX],AL
00401132 90 ADD BYTE PTR DS:[EAX],AL
00401133 90 ADD BYTE PTR DS:[EAX],AL
00401134 90 ADD BYTE PTR DS:[EAX],AL
00401135 90 ADD BYTE PTR DS:[EAX],AL
00401136 90 ADD BYTE PTR DS:[EAX],AL
00401137 90 ADD BYTE PTR DS:[EAX],AL
00401138 90 ADD BYTE PTR DS:[EAX],AL
00401139 90 ADD BYTE PTR DS:[EAX],AL
0040113A 90 ADD BYTE PTR DS:[EAX],AL
0040113B 90 ADD BYTE PTR DS:[EAX],AL
0040113C 90 ADD BYTE PTR DS:[EAX],AL
0040113D 90 ADD BYTE PTR DS:[EAX],AL
0040113E 90 ADD BYTE PTR DS:[EAX],AL
0040113F 90 ADD BYTE PTR DS:[EAX],AL
00401140 90 ADD BYTE PTR DS:[EAX],AL
00401141 90 ADD BYTE PTR DS:[EAX],AL
00401142 90 ADD BYTE PTR DS:[EAX],AL
00401143 90 ADD BYTE PTR DS:[EAX],AL
00401144 90 ADD BYTE PTR DS:[EAX],AL
00401145 90 ADD BYTE PTR DS:[EAX],AL
00401146 90 ADD BYTE PTR DS:[EAX],AL
00401147 90 ADD BYTE PTR DS:[EAX],AL
00401148 90 ADD BYTE PTR DS:[EAX],AL
00401149 90 ADD BYTE PTR DS:[EAX],AL
0040114A 90 ADD BYTE PTR DS:[EAX],AL
0040114B 90 ADD BYTE PTR DS:[EAX],AL
0040114C 90 ADD BYTE PTR DS:[EAX],AL
0040114D 90 ADD BYTE PTR DS:[EAX],AL
0040114E 90 ADD BYTE PTR DS:[EAX],AL
0040114F 90 ADD BYTE PTR DS:[EAX],AL
00401150 90 ADD BYTE PTR DS:[EAX],AL
  
```

The registers window shows the following values:

```

EAX 00000000
ECX 0012FF80
EDX 783280A1 rdt1.KiFastSystemCallRet
EBX 7FFD4000
ESP 0012FFC4
EBP 0012FF00
ESI 00000000
EDI 00000000
EIP 004010C4 axe.(ModuleEntryPoint)
  
```

A dialog box titled "Compressed code?" is displayed with the following text:

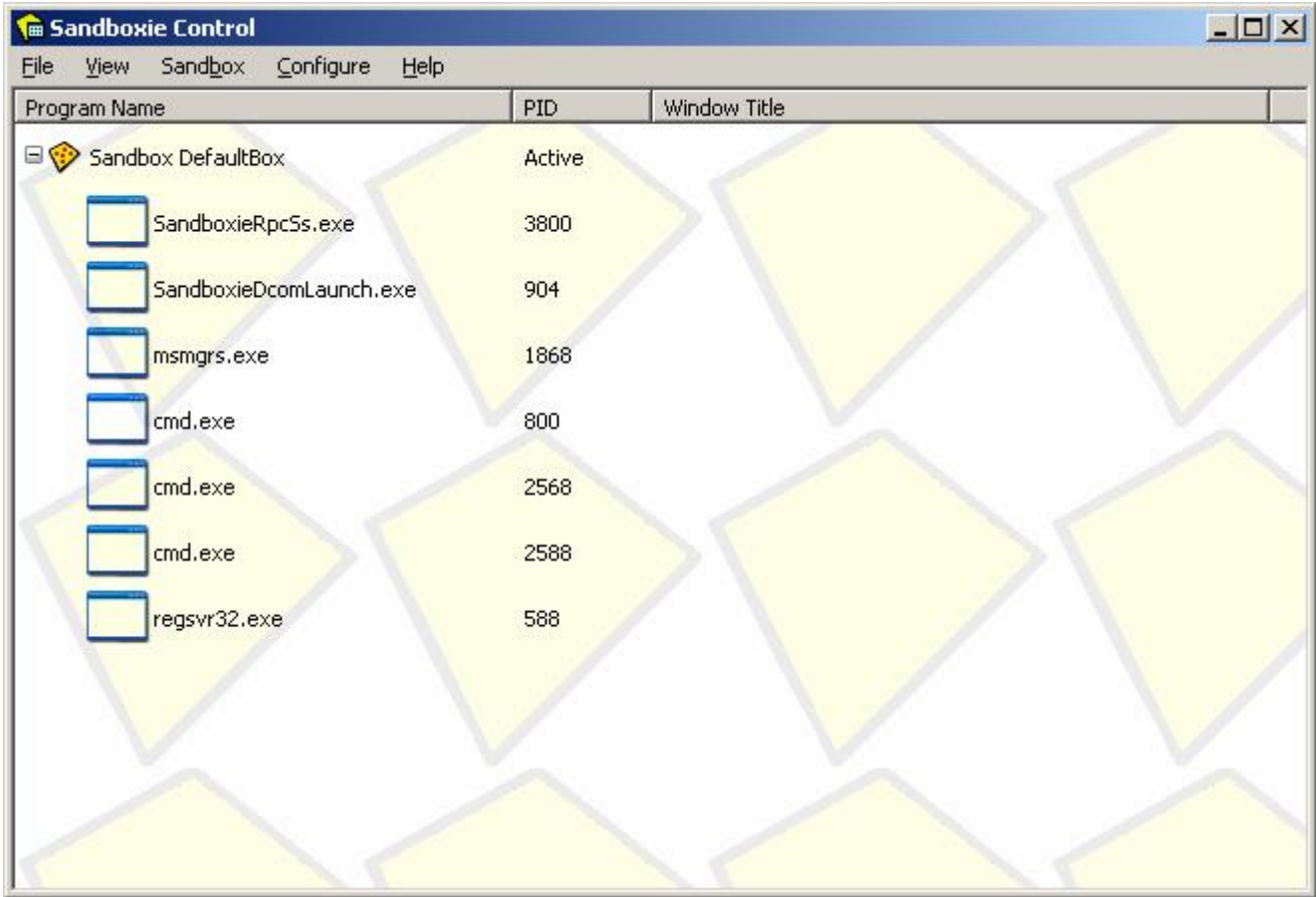
```

Quick statistical test of module 'axe' reports that its code section is either compressed, encrypted, or contains large amount of embedded data. Results of code analysis can be very unreliable or simply wrong. Do you want to continue analysis?
  
```

The bottom status bar shows: [21:41:01] Program entry point Running

Trojani 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 nereden haberleştiğini tespit etmek oldu ve bir bingo daha program yurt dışında bir ftp sunucusuna bağlanıyordu.

Intel(R) PRO/1000 MT Network Connection: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.142.2	192.168.142.132	DNS	Standard query A ftp. [REDACTED].com
2	0.000000	192.168.142.132	192.168.142.2	DNS	Standard query response A [REDACTED].com
3	0.000000	[REDACTED]	192.168.142.132	TCP	td-postman > ftp [SYN] Seq=0 win=64240 Len=0 MSS=1460
4	0.000000	192.168.142.132	[REDACTED]	TCP	ftp > td-postman [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
5	0.000000	[REDACTED]	192.168.142.132	TCP	td-postman > ftp [ACK] Seq=1 Ack=1 win=64240 Len=0
6	0.000000	192.168.142.132	[REDACTED]	FTP	Response: 220----- welcome to Pure-FTPd [privsep] [TLS] --
7	0.000000	[REDACTED]	192.168.142.132	FTP	Request: USER [REDACTED]
8	0.000000	192.168.142.132	[REDACTED]	TCP	ftp > td-postman [ACK] Seq=267 Ack=18 win=64240 Len=0
9	0.000000	192.168.142.132	[REDACTED]	FTP	Response: 331 User [REDACTED] OK. Password required
10	0.000000	[REDACTED]	192.168.142.132	FTP	Request: PASS [REDACTED]
11	0.000000	192.168.142.132	[REDACTED]	TCP	ftp > td-postman [ACK] Seq=310 Ack=40 win=64240 Len=0
12	0.000000	192.168.142.132	[REDACTED]	FTP	Response: 230-Your bandwidth usage is restricted
13	0.000000	192.168.142.132	[REDACTED]	FTP	[TCP Retransmission] Response: 230-Your bandwidth usage is rest
14	0.000000	[REDACTED]	192.168.142.132	TCP	td-postman > ftp [ACK] Seq=40 Ack=445 win=63796 Len=0
15	0.000000	[REDACTED]	192.168.142.132	TCP	td-postman > ftp [FIN, ACK] Seq=40 Ack=445 win=63796 Len=0
16	0.000000	192.168.142.132	[REDACTED]	TCP	ftp > td-postman [ACK] Seq=445 Ack=41 win=64239 Len=0
17	0.000000	192.168.142.132	[REDACTED]	FTP	Response: 230 Logout.

Frame 1 (79 bytes on wire, 79 bytes captured)

Ethernet II, Src: Vmware\_e6:ef:b9 (00:0c:29:e6:ef:b9), Dst: Vmware\_ea:fb:b3 (00:50:56:ea:fb:b3)

Internet Protocol, Src: 192.168.142.132 (192.168.142.132), Dst: 192.168.142.2 (192.168.142.2)

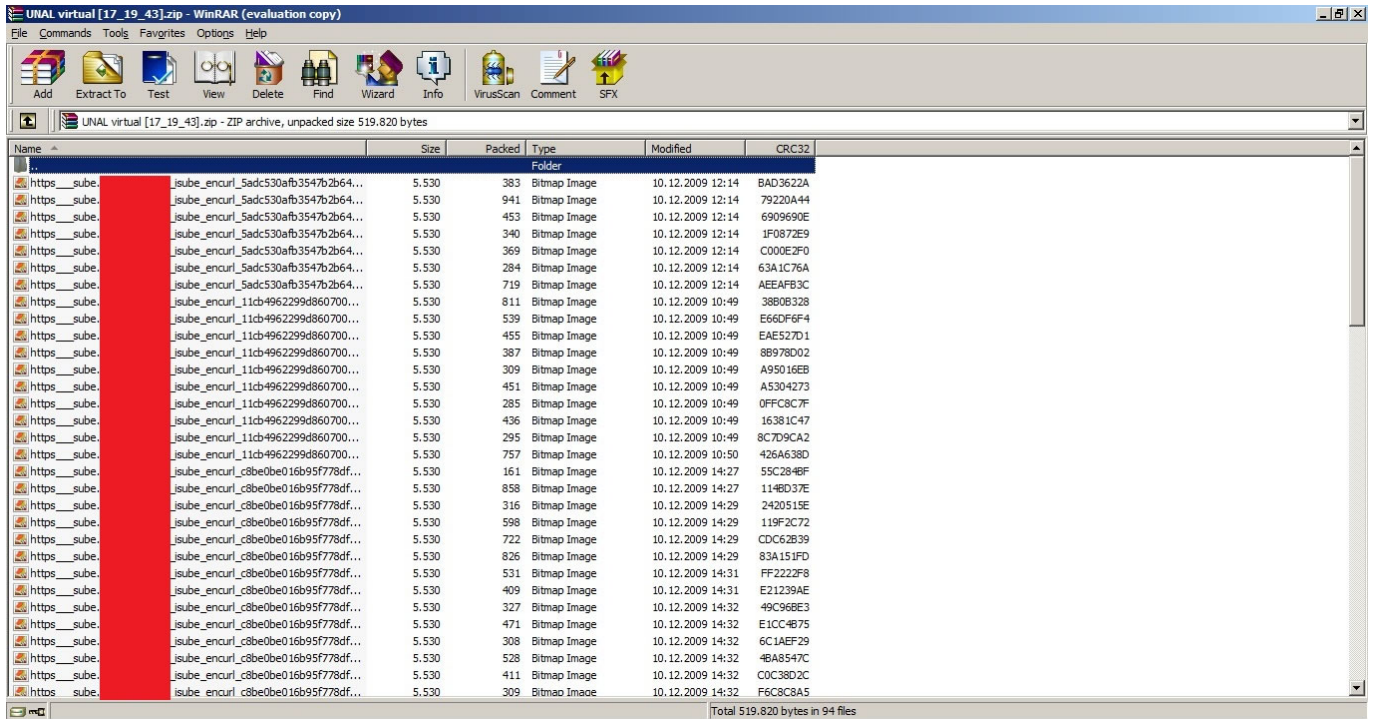
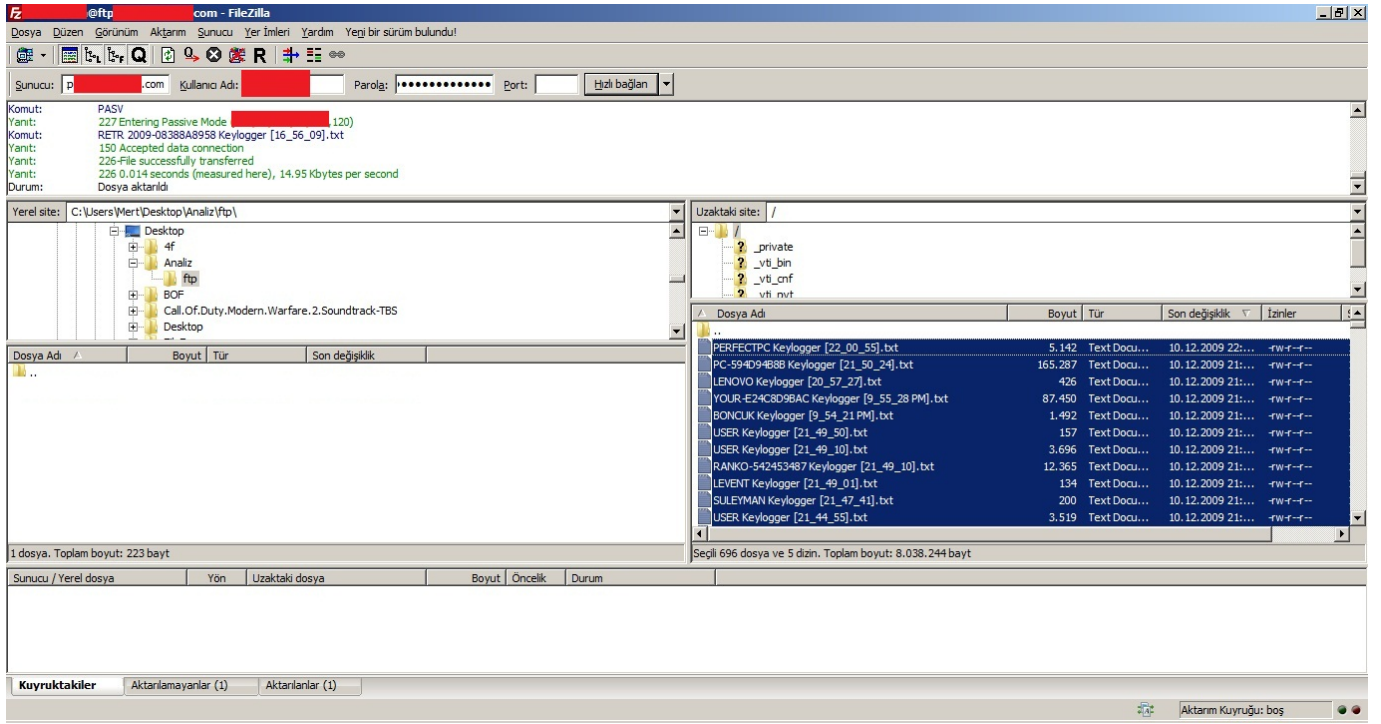
```

0000  00 50 56 ea fb b3 00 0c 29 e6 ef b9 08 00 45 00  .PV.....).....E.
0010  00 41 04 8c 00 00 80 11 00 00 c0 a8 8e 84 c0 a8  .A.....
0020  8e 02 e8 33 00 35 00 2d 7a c0 dc 67 01 00 00 01  ...3.5.-z..d....
0030  00 00 00 00 00 00 03 66 74 70 0b 66 72 65 65 77  .....f tp.[REDACTED]
0040  65 62 74 6f 77 6e 03 63 6f 6d 00 00 01 00 01  [REDACTED].com.....

```

Intel(R) PRO/1000 MT Network Connection: <liv... Packets: 18 Displayed: 18 Marked: 0 Profile: Default

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...