

Hack 4 Career - 2014

Merhabalar,

2009 yılında "Bilgi güçtür ve paylaştıkça artar" mottosuyla oluşturduğum siber güvenlik bloguma (<https://www.mertsarica.com>) , bilgi güvenliği farkındalığını artırma adına çok sayıda teknik yaziya yer vermeye çalıştım. Yıllar içinde Türkiye'nin dört bir yanından aldığı olumlu geri dönüşler sonucunda, yazıları yollar bazında e-kitap olarak derlemeye ve meraklıları ile paylaşmaya karar verdim.

Emek, zaman ve kaynak ayıracak yapışığım araştırmalar sonucunda yazdığım bu yazıların, siber güvenlik alanında kendini geliştirmek isteyenler için umarm faydalı olur.

Yeni yazılarla görüşmek dileğinde...

Saygılarımla,

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

Air6372SO Varsayılan Hesap Doğrulaması

Source: <https://www.mertsarica.com/air6372so-varsayılan-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.

The screenshot shows a Twitter interface. At the top, there's a status bar with icons for signal strength, battery level (92%), and the time (17:14). Below that is the Twitter header with a back arrow, a Twitter logo, and the word 'Tweet'. To the right of the header are search and more options icons. The main content area shows a tweet from a user named 'Hacker Fantastic' (@hackerfantastic). The tweet's profile picture is a blue unicorn-like creature. The tweet text is: "Turkish friends, if you have a Airties DSL router - you can telnet to port 2323 and login with "root" / "dsl_2012_Air" ;-) Hack the planet." Below the tweet is the timestamp "01:24 · 15 Kas 14". At the bottom of the tweet card, there are engagement metrics: "28 RETWEET 27 FAVORİ". Below the tweet card are four small icons for interacting with the post: a reply arrow, a retweet arrow, a star, and a share symbol.

Bu iddiayı doğrulamak için, [IstSec](#) konferansında yaptığım donanım yazılımı analizi sunumuna hazırlamak için zamanında satın almış olduğum Airties RT-206v4 modeline hızlıca göz atmaya karar verdim. Nmap ile modem'in bağlantı noktalarını (1-65535) kontrol ettiğimde, modem'in 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 koyuldu.

Airties'in [web sitesinde](#) yer alan çoğu kablosuz modem'in 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 etmeye başladım.

The screenshot shows the AirTies website at www.airties.com.tr/support/dcenter/. The main header features the Air 6372 router and contact information: 7/24 destek hattı 444 0 239. The page title is 'Ürünler / Kablosuz Ürünler / Kablosuz DSL Modem Ağ Geçitleri'. On the left sidebar, there are links for 'Genel Bakış', 'Teknik Özellikler', 'Sistem Gereklilikleri', and a 'Datasheet' button. Below these are sections for 'Yükleme merkezi' (with links to 'Firmware', 'Kolay Kurulum CD'si', 'Kullanım Kılavuzu', and 'Hızlı Kurulum'), 'AirTies Teknolojileri', 'Ürün Görselleri', 'Destek Dokümanları', and 'Satış noktaları'. The right side contains a 'Firmware' section with dropdown menus for 'Ürünü seçiniz' (Air 6372), 'Ülkeyi seçiniz' (Türkiye), and 'Versiyonu seçiniz' (Superonline). Below this is a table for the 'SON VERSİYON' of Air 6372, showing Model: Air 6372, Versiyon: 1.0.0.42, Son Güncelleme Tarihi: 01.10.2012, and a download link. Another table for 'ÖNCEKİ VERSİYON' shows the same information for version 1.0.0.41 from 30.03.2012. At the bottom, it says 'İlgili ürünler: Air 6271'.

The terminal window shows the command `root@kali:~/Desktop/Airties# ls *.bin` followed by a list of AirTies firmware files. Then, the command `root@kali:~/Desktop/Airties# binwalk -e *.bin` is run, and the output of the binwalk tool is displayed. The output includes:

```

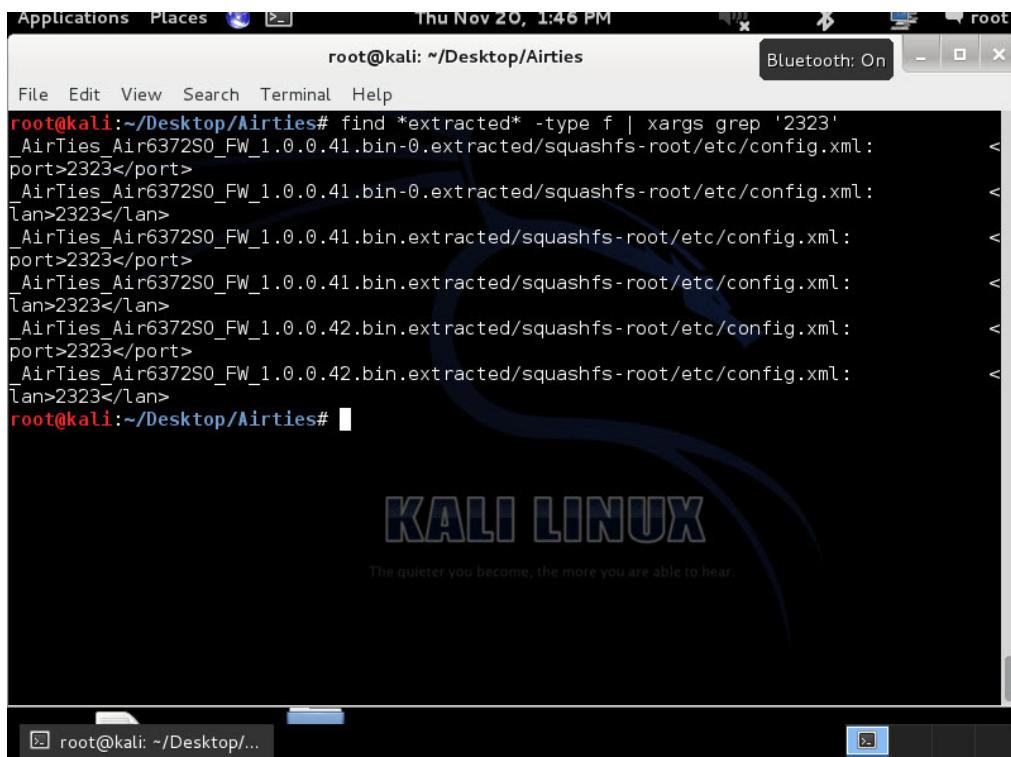
Scan Time: 2014-11-20 13:14:42
Target File: AirTies_Air5650_FW_1.0.0.10.bin
MD5 Checksum: 541b10e4bf4bf8cf3f11086ef8032049
Signatures: 294

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.

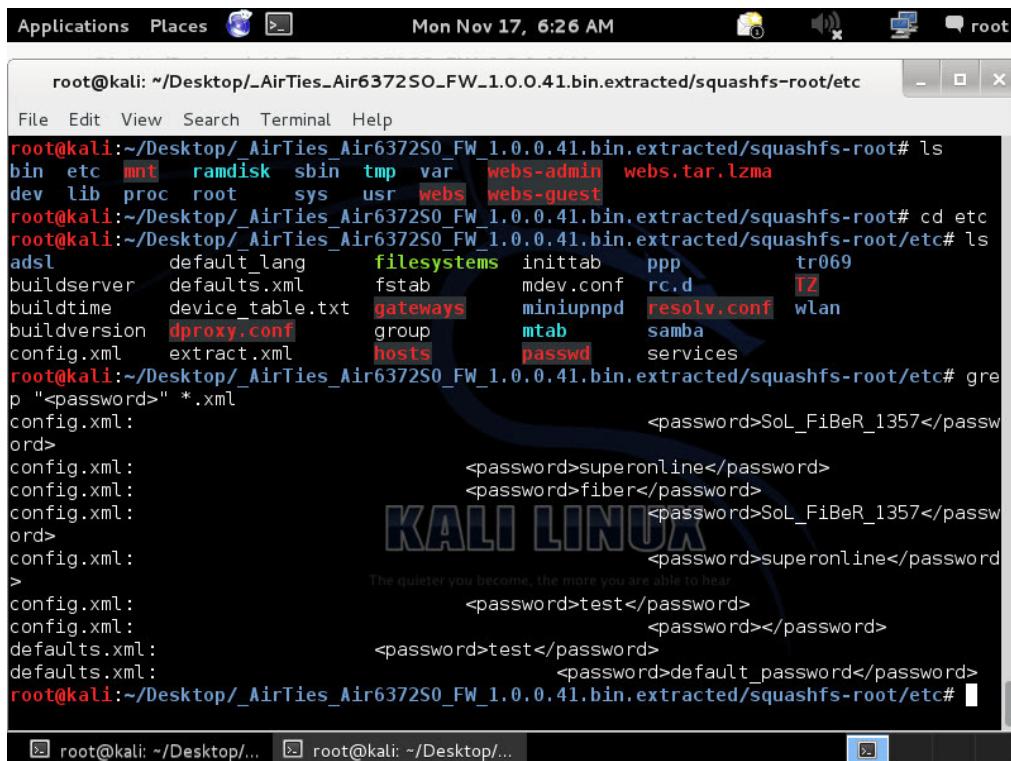
binwalk aracına -e parametresi ile tüm donanım yazılımlarını (*.bin) analiz ettirdikten sonra teker teker her bir açılan klasörün içine bilmek yerine 2323 bağlantı noktasını tüm *extracted* geçen (binwalk açtığı donanım yazılımlarını bu şekilde isimlendiriyor) klasör isimleri içinde grep aracı ile aramaya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



A screenshot of a Kali Linux desktop environment. The desktop background features the Kali Linux logo with the tagline "The quieter you become, the more you are able to hear." A terminal window titled "root@kali: ~/Desktop/Airties" is open, showing the output of a command to find files containing the string "2323". The terminal window has a dark theme with light-colored text. The desktop bar at the bottom shows icons for the terminal and file manager.

```
root@kali:~/Desktop/Airties# find *extracted* -type f | xargs grep '2323'
AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc/config.xml:
port>2323</port>
_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc/config.xml:
lan>2323</lan>
_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc/config.xml:
port>2323</port>
_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc/config.xml:
lan>2323</lan>
_AirTies_Air6372SO_FW_1.0.0.42.bin.extracted/squashfs-root/etc/config.xml:
port>2323</port>
_AirTies_Air6372SO_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 arattığında ise iddia edilenden farklı olan SoL_FiBeR_1357 şifresi hemen dikkatimi çekti. Bu dosyaya metin editörü ile baktığında 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)



A screenshot of a Kali Linux desktop environment. The desktop background features the Kali Linux logo with the tagline "The quieter you become, the more you are able to hear." A terminal window titled "root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc" is open, showing the output of commands to list files in the /etc directory and search for "password" in XML files. The terminal window has a dark theme with light-colored text. The desktop bar at the bottom shows icons for the terminal and file manager.

```
root@kali:~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc#
File Edit View Search Terminal Help
root@kali:~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc# 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_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc# cd etc
root@kali:~/Desktop/_AirTies_Air6372SO_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_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc# grep "<password>" *.xml
config.xml:                                     <password>SoL_FiBeR_1357</password>
config.xml:                                     <password>superonline</password>
config.xml:                                     <password>fiber</password>
config.xml:                                     <password>SoL_FiBeR_1357</password>
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_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc#
```

Applications Places Mon Nov 17, 6:27 AM root

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>
                <msg>you are able to hear</msg>
            </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

File Edit View Search Terminal Help

GNU nano 2.2.6 File: config.xml

```
<config version="1.0.1">
    <ddns>
        <ddns-0>
            <settings>
                <eco0146>1</eco0146>
            </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>
</config>
```

The quieter you become, the more you are heard.

^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/...

```

<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-0>
<static>
  <static-0>
    <log>
      <level>crit</level>
    </log>
  </static-0>
</static>

```

The terminal window title is "root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc". The status bar shows "Mon Nov 17, 6:32 AM" and "root". The bottom status bar also shows "root@kali: ~/Desktop/...".

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 bağlanılabilindiği bilgisi geldi.

Aslında bunun gibi uzaktan destek amacıyla modemlere, ağ cihazlarına tanımlanan hesaplara ara ara [rastlanmaktadır](#) ve güvenlik araştırmacıları tarafından bunlar ortaya çıkarılmaktadır. Bunların ortaya çıkarılmasının kullanıcılarından en önemli kısmı ise, kötüye kullanılabilecek bu şifrelerin en kısa sürede değiştirilebilmesi veya hesapların devre dışı bırakılabilmesidir. Bende bunun için iki şifre ile ilgili olarak hemen [Netsec e-posta listesine](#) konu ile ilgili [bir e-posta](#) göndermeye karar verdim. E-postayı gönderdiğimde 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 olarak ilgili donanım yazılımında hala bir düzeltme yapılmamıştı.

N. Ersen SİŞECİ via netsec.org
to liste

10:34 PM (15 hours ago)

Turkish ▾ 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, içerisinde çikartırmıştım. İkinci parolayı ise, Firmware Mod Kit ile çikartırmıştım. Her iki yönlü de SüperOnline'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 çikartılması diye sanırım) yedek alma özelliğini kapatıldı. Bu sürümde yedek alınamıyor. Bu sürüm ile sahadaki bir çok cihaz güncellendi ancak halen daha aynı parolalarla girilebiliyor. Sanırım şu an hala en güncel sürüm 1.0.0.52.

Defalarca SüperOnline ile mailléstim 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 ulaşılabilirsiniz.

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 arattığında ise modem sayısının hiç de azımsanmayacak kadar çok olduğunu (10000+) gördüm.

SHODAN - Computer Security 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			
Telnet (2323)	5,642	176.42.151.7	Air6372SO login:
SMB	58	Superonline ADSL	Added on 17.11.2014
NetBIOS	27		host-176-42-151-7.reverse.superonline.net

Top Countries			
Turkey	5,727	213.14.140.48	Air6372SO login:
		Vestel Elektronik Sanayi ve Ticaret A.S.	Added on 17.11.2014
			Sanayi
		host-213-14-140-48.reverse.superonline.net	

91.93.133.76		Air6372SO login:	
Global İletişim Hizmetleri A.S.			Added on 17.11.2014
			
host-91-93-133-76.reverse.superonline.net			

176.43.217.211		Air6372SO login:	
Superonline ADSL			Added on 17.11.2014
			Izmir
host-176-43-217-211.reverse.superonline.net			

78.189.155.33		Air6372SO login:	
Türk Telekom			Added on 17.11.2014
			
78.189.155.33.static.ttnet.com.tr			

88.250.19.200		Air6372SO login:	
Türk Telekom			



Celebrating 3 years of Shodan



Önlem olarak bu marka model modem kullanan kullanıcılar 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



Bildığınız gibi son 1.5 senedir vatandaşımız, Hesperbot adındaki ileri seviye internet bankacılığı zararlı yazılımı salğını (#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` aracı 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 bellegi taramasını sağlayabilirsiniz.

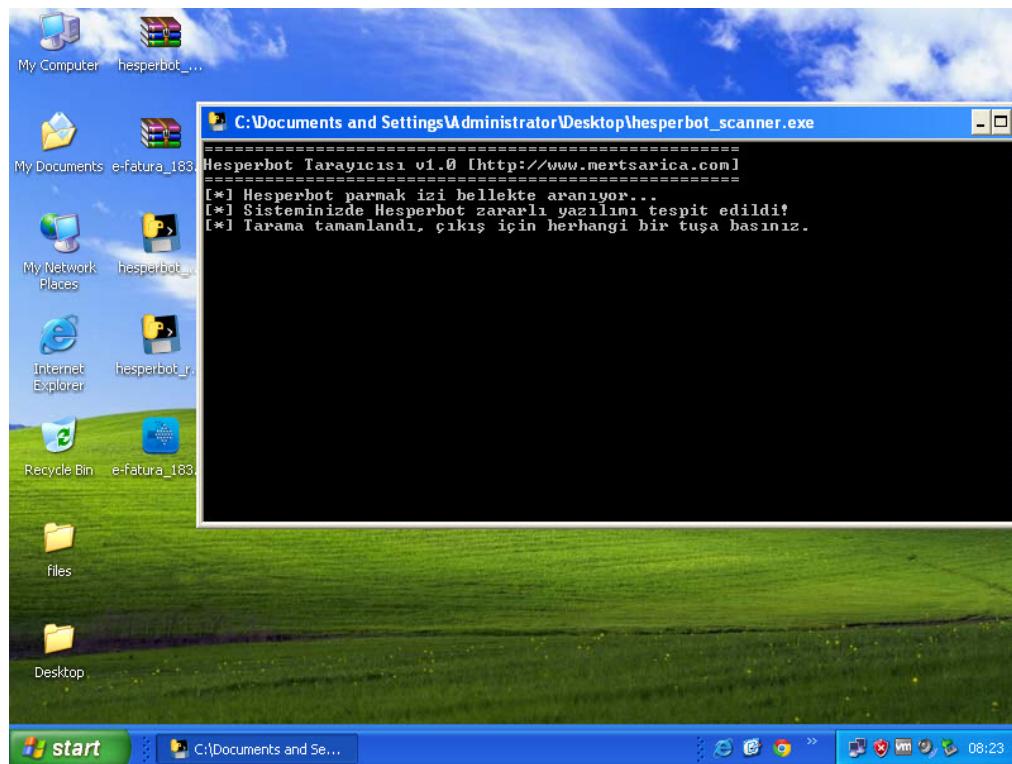
```
C:\Documents and Settings\Administrator\Desktop\hesperbot_scanner.exe
=====
Hesperbot Tarayıcı v1.0 [http://www.mertsarica.com]
=====
[*] Hesperbot parmak izi bellekte aranıyor...
[*] Sisteminizde Hesperbot zararlı yazılımı tespit edildi!
[*] Tarama tamamlandı, çıkış için herhangi bir tuşa basınız.
```

```
C:\WINDOWS\system32\cmd.exe - hesperbot_scanner.exe https://[REDACTED]
=====
Hesperbot Tarayıcı v1.0 [http://www.mertsarica.com]
=====
[*] Belirtilen adres ziyaret edilerek Hesperbot'un devreye girmesi bekleniyor:
  https://[REDACTED]
[*] 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 uğraşınlar :)) 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	HTTP	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.

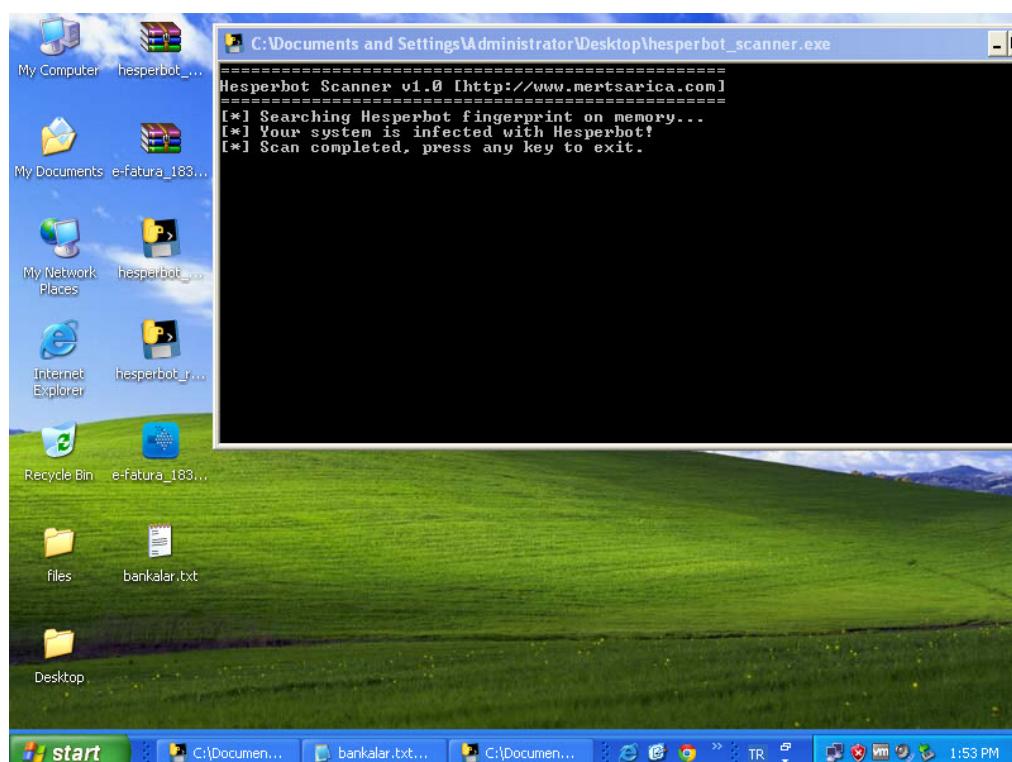
---- ENGLISH ----

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](#).)

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](#). 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](#) is pretty simple, just run it on the infected/suspected system and check the result.

[Click here to download Hesperbot Scanner](#)



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 yardım ile donanım yazılımı güncellemesi esnasında kullanılan komutları tespit etmişler. Daha sonra 2 aydan kısa bir süre içinde donanım yazılımını tersine mühendislik ile analiz ederek, orjinal 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](#) yazdığını ve yine hedef sistem üzerinde USB bağlantı noktasından takıldığı takdirde komut çalıştırma imkan tanıyor [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 itibarıyle yakalanma/tespit edilme olasılığı гореce 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.

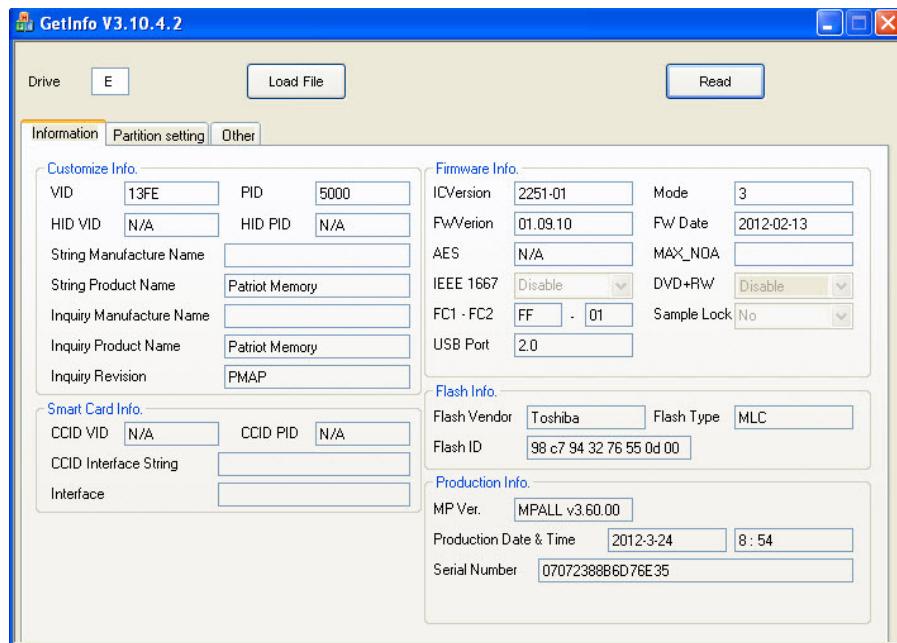
BadUSB ile ilgili çalışma yapan araştırmacıların [web sitesini](#) ziyaret edecek olursanız bu çalışmaya ait POC (proof-of-concept) kodlarını yayınlamadıklarını görebilirsiniz. Benim gibi ben de bir BadUSB oluşturmak istiyorum diyenlerin üzülmeye gerek yok çünkü Adam Caudill ve Brandon Wilson adındaki 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 çalışıklarını görebilirsiniz dolayısıyla geliştirmiş oldukları aracın çalışabilmesi için kullanılacak olan USB belleğin bu model mikrodenetçiye sahip olması gerekmektedir.

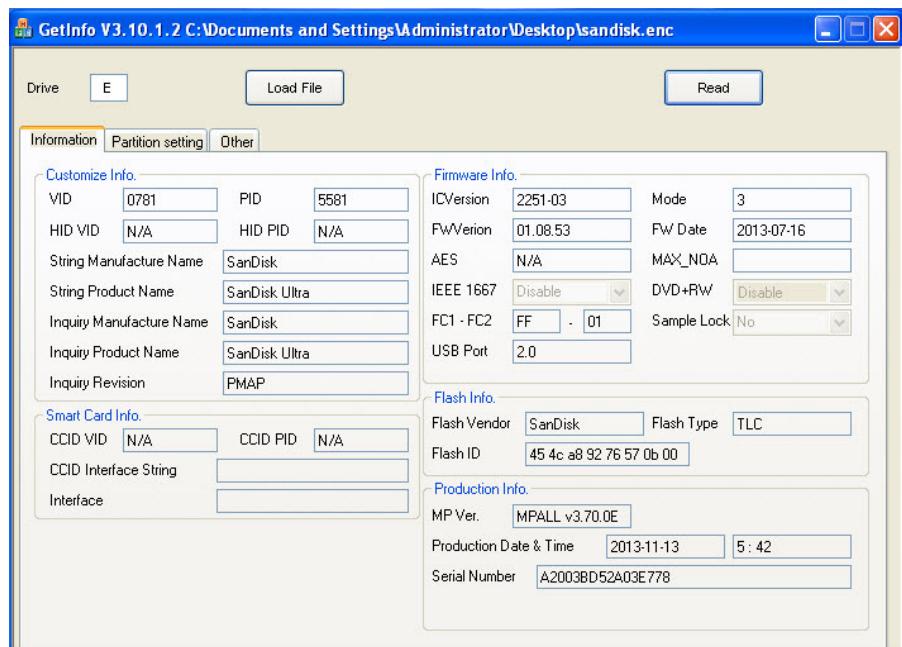
USB bellek geldikten sonra Phison'un modelini [GetInfo](#) aracı (veya [Chip Easy](#) aracını da kullanabilirsiniz) ile kontrol ettiğimde modelin farklı olması nedeniyle hısrana uğradım ve bu defa Phison marka PS2251-03 model USB bellek avına çıktım.





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.





Adımlardan birinde yaptığım dikkatsizlikten dolayı aldığım bu diski çöpe atmak zorunda kaldım :) Ardından bu defa biraz daha temkinli davranışarak 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](#) oluştururdum. ([ReadMe](#) dosyasında yer alan Running Demo 1 (HID Payload) başlığı altında yazılanları yaptım.)

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Mert>cd C:\BadUSB\Psychson-master\firmware
C:\BadUSB\Psychson-master\firmware>build.bat
*** Building main.c...
*** Building timers.c...
*** Building usb.c...
*** Building control.c...
control.c:7: warning 116: right shifting more than size of object changed to zero
control.c:15: warning 116: right shifting more than size of object changed to zero
*** Building sesi.c...
sesi.c:188: warning 85: in function HandleCDB unreferenced local variable : 'i'
*** Done.

```

Name	Date modified	Type	Size
control.lst	24.10.2014 21:45	MASM Listing	53 KB
control.rel	24.10.2014 21:45	REL File	10 KB
control.rst	24.10.2014 21:45	RST File	53 KB
control.sym	24.10.2014 21:45	SYM File	40 KB
fw.bin	24.10.2014 21:45	BIN File	201 KB
main.asm	24.10.2014 21:45	Assembler Source	107 KB
main.lst	24.10.2014 21:45	MASM Listing	460 KB
main.rel	24.10.2014 21:45	REL File	51 KB
main.rst	24.10.2014 21:45	RST File	460 KB
main.sym	24.10.2014 21:45	SYM File	41 KB
output.bin	24.10.2014 21:45	BIN File	13 KB

```
key.txt - Notepad
File Edit Format View Help
DELAY 3000
GUI r
DELAY 500
STRING notepad
DELAY 500
ENTER
DELAY 750
STRING Mert SARICA
ENTER

C:\Windows\system32\cmd.exe
C:\BadUSB\BadUSB\Encoder_2.6.3>DuckEncoder_2.6.3>java -jar encoder.jar -i key.txt -o inject.bin
Hak5 Duck Encoder 2.6.3
Loading File ..... [ OK ]
Loading Keyboard File ..... [ OK ]
Loading Language File ..... [ OK ]
Loading DuckyScript ..... [ OK ]
DuckyScript Complete..... [ OK ]
C:\BadUSB\BadUSB\Encoder_2.6.3>
```

Sonunda aşağıdaki tüm adımları başarıyla geçtikten sonra BadUSB oluşturmayı başardım :) 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.

```
C:\Windows\system32\cmd.exe
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=SetBootMode
Action specified: SetBootMode
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=SendExecutable /burner=BN03U104M.BIN
Action specified: SendExecutable
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=DumpFirmware /firmware=dump.bin
Action specified: DumpFirmware
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=GetInfo
Action specified: GetInfo
Gathering information...
Reported chip type: 2302
Reported chip ID: 45-4C-A8-92-76-57
Reported firmware version: 1.01.10
Mode: Burner
C:\BadUSB\Psychson-master\tools>EmbedPayload.exe inject.bin fw.bin
File updated.
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=SendFirmware /burner=BN03U104M.BIN /firmware=fw.bin
Action specified: SendFirmware
Gathering information...
Reported chip type: 2302
Reported chip ID: 45-4C-A8-92-76-57
Reported firmware version: 1.01.10
Mode: Burner
Rebooting...
Sending firmware...
Executing...
Mode: Firmware
```

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 ürünler 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

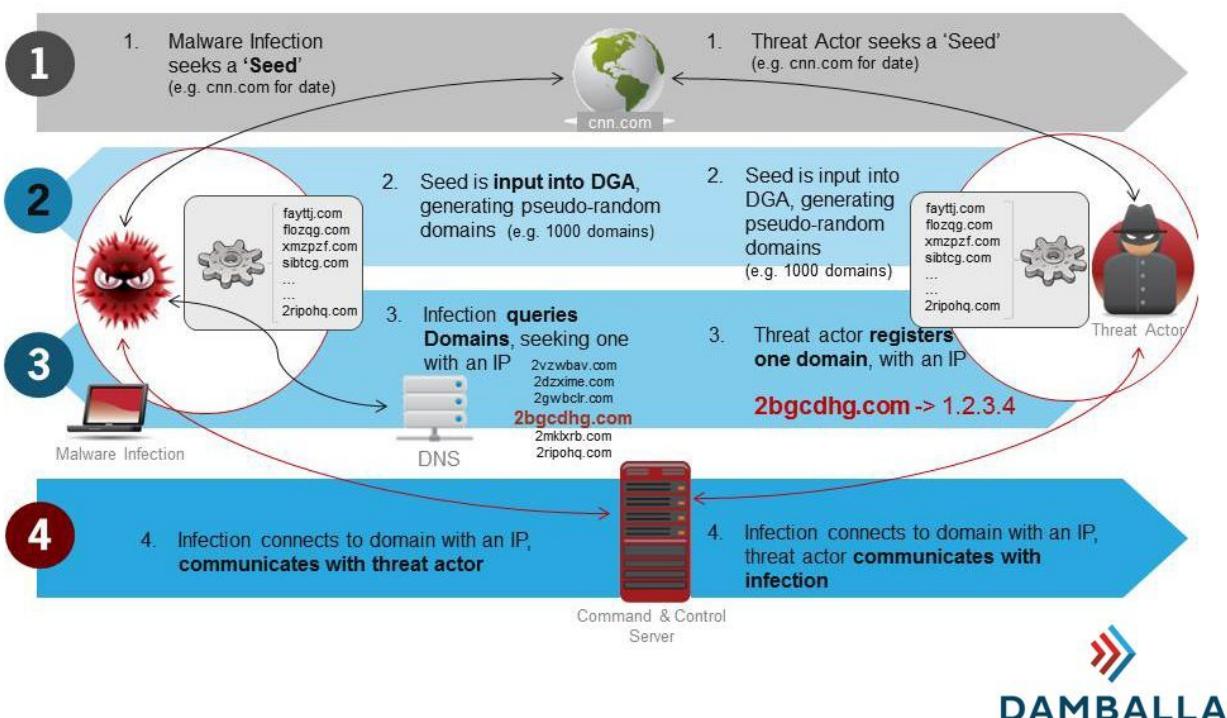
Source: <https://www.mertsarica.com/hesperbot-dga-analizi/>

By M.S on October 1st, 2014



Alan adı üretme algoritması (DGA), zararlı yazılımlar tarafından yeni bir alan adı üretmek amacıyla kullanılan algoritmalarıdır. 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)]								
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 0x0cf8	A kvbqxktzlhylzmonqwcqheov.net			
583	202.891744 127.0.0.2	127.0.0.1	DNS	72 Standard query 0x13e4	A swijdmjofmrskeohzgjnnr.ru			
351	178.726997 127.0.0.2	127.0.0.1	DNS	72 Standard query 0x17db	A abmciduijgjifuhqoknktw.info			
1227	272.201407 127.0.0.2	127.0.0.1	DNS	77 Standard query 0x1a9e	A upnkflbmkmzbpbhzxtrstdipjei.biz			
555	199.867395 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x1be9	A eahrkeuemlmzhainkjmbijy়ে.net			
751	221.037837 127.0.0.2	127.0.0.1	DNS	75 Standard query 0x1bf8	A qijdeqpkzhexyqctcuyxnjjgeso.ru			
485	192.306523 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x1eed	A vgkymfvshbjxbogatgldamknrydwp.com			
513	195.330872 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x21ee	A usfugqfbmmrskmfccykaivvrlzpr.com			
1423	293.231647 127.0.0.2	127.0.0.1	DNS	74 Standard query 0x2293	A aqwgqkukizoznaufmypkrkmb.ru			
1255	275.205727 127.0.0.2	127.0.0.1	DNS	70 Standard query 0x249f	A xozammrhcmtlhiznfxkh.ru			
863	233.115203 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x26f0	A hyvgusqscacqhyqcwkrrhmnrorp.info			
625	207.428267 127.0.0.2	127.0.0.1	DNS	77 Standard query 0x28e0	A ojyhqpnraqbaqcpeapfzdtucgu.org			
891	236.129538 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x2af2	A ugrcusdibddqquuehitwlrdwbi.net			
695	214.989139 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x2eff	A ivhpnjzlhutfedscxvwvovgq.info			
737	219.525663 127.0.0.2	127.0.0.1	DNS	77 Standard query 0x2fff	A obzpjbrojfhxivskfmvgjnsnvv.biz			
267	169.663965 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x32de	A gqeuibzfwswjzijinydlylxg.net			
457	189.282175 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x35d3	A hbeifydekzjbprwpisceikbop.biz			
1073	255.677647 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x3787	A hygpjusibxvhvghxxccunjjb.com			
989	246.664687 127.0.0.2	127.0.0.1	DNS	72 Standard query 0x3789	A vcithyrkdmdbmdlbc1vgexc.com			
1171	266.192767 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x3a9c	A aqdeufircjvfzejbtptzuovkdeazh.ru			
231	166.649631 127.0.0.2	127.0.0.1	DNS	75 Standard query 0x3adc	A xgficemkvwoxkptmjcyrcxwgt.ru			
1311	281.214367 127.0.0.2	127.0.0.1	DNS	80 Standard query 0x3c9b	A hahizprusxfwffqqcwczlydswmrphcu.info			
1395	290.227327 127.0.0.2	127.0.0.1	DNS	75 Standard query 0x3e92	A ffilsolnzhifzxrxkdicujbl.net			
597	204.403919 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x3ee6	A ypcifaxweaskfcisohxbmjtnbhy.biz			
653	210.452616 127.0.0.2	127.0.0.1	DNS	77 Standard query 0x42e3	A vgcqr1xgmvetcpvlbybzhtpjttx.com			
877	234.617363 127.0.0.2	127.0.0.1	DNS	72 Standard query 0x42f1	A twnjtsqsgxekzpcyptf.biz			
1339	284.218687 127.0.0.2	127.0.0.1	DNS	66 Standard query 0x4c96	A fdkhjkjbjreylznhr.ru			
253	168.161805 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x4ddd	A futjnitzortcllhizydifxgby.com			
611	205.916093 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x4fe7	A xkonfizpgpailjeaytamjnfykbtk.net			
541	198.355221 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x51e8	A jmrzgxreymovxozeurwaercp.org			
471	190.794349 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x51ed	A xgbukvukzdcmoncigbyuzpeujr.info			
1451	296.245981 127.0.0.2	127.0.0.1	DNS	71 Standard query 0x52ad	A tdpzpeulfxdmhlpvpjf.net			
527	196.843047 127.0.0.2	127.0.0.1	DNS	77 Standard query 0x53ef	A qoqcaekezxqoytuopbdixyojf.biz			
1437	294.733807 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x54ac	A hgqubujmbvczhhltngvcpbkv.biz			
1213	270.699247 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x569e	A ofypoxxppnduovdofaedydqdyuw.org			
779	224.062186 127.0.0.2	127.0.0.1	DNS	75 Standard query 0x57fb	A xojbqcjlzwcepnuwhaaeiiip.net			
147	157.576584 127.0.0.2	127.0.0.1	DNS	77 Standard query 0x59c7	A hqgkvkhwkscahoxoldtshylby.ru			
69	150.025727 127.0.0.2	127.0.0.1	DNS	77 Standard query 0x59ca	A xkbagejntccqamiжvoxrwknyld.com			
421	186.267840 127.0.0.2	127.0.0.1	DNS	75 Standard query 0x61d0	A vduiceqwmzhpozsvsorqcinrg.com			
1143	263.188447 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x6283	A hmeiaqprmojskhhyhikfmvdv.info			
295	172.688314 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x64d9	A guosadlfpnlnvcxxwirfmaqdnr.info			
1185	267.694927 127.0.0.2	127.0.0.1	DNS	74 Standard query 0x669d	A tzxosqsrtpyxdagauopfpvif.com			
835	230.090855 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x66f7	A amontwfqidinvsowxtodmsggagy.ru			
1199	269.197087 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x689e	A inqomfnvjbytgztovcidjvlcvg.info			
1269	276.707887 127.0.0.2	127.0.0.1	DNS	72 Standard query 0x6b98	A hulgtaqrzvldqbobjf.com			
919	239.143872 127.0.0.2	127.0.0.1	DNS	77 Standard query 0x738d	A fqcjfmampvnzpaurbzmyrdijai.ru			
681	213.476965 127.0.0.2	127.0.0.1	DNS	71 Standard query 0x73fd	A tohejnjrduofebubrggepp.com			
337	177.224837 127.0.0.2	127.0.0.1	DNS	75 Standard query 0x76db	A dergatdxctgqwuwlzxqjtsgpv.com			
1297	279.712207 127.0.0.2	127.0.0.1	DNS	73 Standard query 0x779a	A jcapcivrpgeqlzqsirweeid.biz			
203	163.625282 127.0.0.2	127.0.0.1	DNS	78 Standard query 0x7ac3	A ibhulbthbjbmnzndidqqjigtpcup.net			
365	180.239171 127.0.0.2	127.0.0.1	DNS	76 Standard query 0x80db	A pfdecapbpnlvuhcmheogfutgjn.org			
667	211.964791 127.0.0.2	127.0.0.1	DNS	72 Standard query 0x80fc	A hhmigegyvkeqsgfqswclkbj.ru			
1283	278.210047 127.0.0.2	127.0.0.1	DNS	79 Standard query 0x8498	A vxgcvzhhqhpipjyppnbllwctwqoc.net			
1381	288.725167 127.0.0.2	127.0.0.1	DNS	74 Standard query 0x8f91	A emsoxgcekzxhcmduylxiffud.org			
1353	285.720847 127.0.0.2	127.0.0.1	DNS	74 Standard query 0x9497	A uknjidjddatdaeytmilgadupvg.com			

File: "C:\Users\R Bashir\Downloads\mal...\ Packets: 1464 · Displayed: 204 (13.9%) · Load time: 0:00:044

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

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 çalışmıyor taktirde üçüncü yöntem olarak kullanmaktadır. DGA'nın birincil yöntem olarak kullanılmamasının temel sebebi, zararlı yazılım analistleri, siber güvenlik uzmanları tarafından kod analizi ile zararlı yazılımda tespit edilen DGA'nın yanı alan adlarının, yazılım geliştiricisinden önce kayıt edilebilmesine imkan tanımıştır. Bu sayede uzmanlar, Conficker örneğinde olduğu gibi zararlı yazılımlar ile ilgili çeşitli bilgileri toplayabilmekte, kimi zaman ise zararlı yazılımları kontrol altına alabilmektedirler.

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

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

5 Eylül tarihinde [INTELRAD](#) ekibi, Hesperbot'un hedef aldığı bankalara ait kural dosyasını ve ilave modüllerini indirmek için kullandığı alan adına (followtweertag.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.

THIS DOMAIN IS SEIZED BY MUTUAL COOPERATION BETWEEN

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 kurumları ve müşterilerini hedef alan genel kapsamlı bir siber dolandırıcılık operasyonu ile bağlantılı olduğunu tespit edimiz. Etik değerlerimiz gereğince, hedef alınan taraflara ugranalılmıştır. Zaraara da böbürlenmem adına PRODAFT Siber İstihbarat Ltd. Şti. bu alan adına el koymuş bulunmaktadır. Yürütmeceğimiz soruşturma perşevesinde, tüm yetkililerin kurumlara, siber-dolandırıcılık operasyonunu yürütür şahıslara ait IP ve diğer bağlayıcı veriler iletimi bulunmaktadır.

[RU] Данный домен и его владелец 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.

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

Seized domains:
 dicslogjimsiziridligqt.ru
 addmytweeter.com
 followtweetertag.com
 sdomainhelp.ru
 skonwyoyhost.ru
 zwebitedesign.ru
 zdomainstore.ru
 aidwvboqmbu.ru
 zdomainsupport.ru
 xwebsitehosting.ru
 xsolarenergy.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:EFH2B5jVGzF8R2tTLHZGsVhFz0shG_-IACVF03N
359	302	HTTP	cache.pack.google.com	/edgedi/update2/1.3.24.15/GoogleUpdateSetup.exe
360	502	HTTP		Tunnel to followtweetertag.com:443
361	302	HTTP	cache.pack.google.com	/edgedi/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	/edgedi/update2/1.3.24.15/GoogleUpdateSetup.exe
367	502	HTTP		Tunnel to followtweetertag.com:443
368	302	HTTP	cache.pack.google.com	/edgedi/update2/1.3.24.15/GoogleUpdateSetup.exe
369	302	HTTP	cache.pack.google.com	/edgedi/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	/edgedi/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=sq4JVJmFHsa08wfutGADA
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	/edgedi/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. 11617em1rcuykcsrn49lo1x9whsv.biz	<input type="checkbox"/>	<input type="checkbox"/>
2. 16m4ethimpjre119w61x1g5bgjy.biz	<input type="checkbox"/>	<input type="checkbox"/>
3. 190hi6jsut1qu0ezxxqxl9.biz	<input type="checkbox"/>	<input type="checkbox"/>
AND 53 other domains...		

Bildiğiniz gibi hem isim gereği hem de ilgi alanına 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 aramamadaki temel amaç en kısa sürede Hesperbot'un üreteceği alan adlarına ve hangilerinin Hesperbot geliştiricileri tarafından kayıt edildiği bilgisine en kısa sürede ulaşmakti. Fonksiyona ulaşmadığım taktirde izleyeceğim yol, Hesperbot'un öncelikle ilgili komuta kontrol merkezi adresine bağlanması 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 ayıklayıcısıdır.

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

```

C:\> 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 followtweetertag.com:443
4261	200	HTTP	Tunnel to iahapemwionkmti.ru:443
4262	200	HTTP	www.download.windowsupdate.com /msdownload/update/v3/static/trustedr/en/authrootseq.txt
4263	200	HTTP	www.download.windowsupdate.com /msdownload/update/v3/static/trustedr/en/authrootstl.cab
4264	200	HTTP	Tunnel to iahapemwionkmti.ru:443
4265	502	HTTP	Tunnel to dksqljglsmisizjrdllqjt.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 mvpwpppsujt.ru:443
4276	502	HTTP	Tunnel to qhereqyk.ru:443
4277	502	HTTP	Tunnel to wjikeymj.ru:443
4278	502	HTTP	Tunnel to agxqstwcoc.ru:443
4279	502	HTTP	Tunnel to trzxvhstbnthwccego.ru:443
4280	502	HTTP	Tunnel to oibldgaj.ru:443
4281	502	HTTP	Tunnel to hloqjbahr.ru:443
4282	502	HTTP	Tunnel to hkpfcp.ru:443
4283	502	HTTP	Tunnel to gstdidaxyepi.ru:443
4284	502	HTTP	Tunnel to rbmccpnyjjsmhg.ru:443
4285	502	HTTP	Tunnel to qfayqwzqxmvejjtwrmmsgsg.ru:443
4286	502	HTTP	Tunnel to ytigdmjnkhmaavjpyfimro.ru:443
4287	502	HTTP	Tunnel to uxzusbcu.ru:443
4288	502	HTTP	Tunnel to ejmlcqddjijxzfn.ru:443
4289	502	HTTP	Tunnel to difnjbmrlrexdkiwyhqnka.ru:443
4290	502	HTTP	Tunnel to qcncqjy.ru:443
4291	502	HTTP	Tunnel to phplstkpzvzxakyb.c:443
4292	502	HTTP	Tunnel to xcofeihllczdvsduugpj.l:443
4293	502	HTTP	Tunnel to luamnnbo.ru:443
4294	502	HTTP	Tunnel to jaxvaxwdfsdpzgsuprga.ru:443
4295	502	HTTP	Tunnel to yjubrrfpkjadsevaqz.ru:443
4296	502	HTTP	Tunnel to bgjmnsqg.ru:443
4297	502	HTTP	Tunnel to epztnxcjaldvqa.ru:443
4298	502	HTTP	Tunnel to rysialzkrikwyxhxlqjdnekd.ru:443
4299	502	HTTP	Tunnel to kivhkjgvsephj.ru:443
4300	502	HTTP	Tunnel to yvncijmgktr.ru:443
4301	502	HTTP	Tunnel to sykrqgfhekgtplpi.ru:443
4302	502	HTTP	Tunnel to mdfttmsx.ru:443

lahapemwionkmti.ru

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link), ...

Bilgi Tarihi: 22.08.2015
Oluşturulma Tarihi: 22.08.2014
NS Sunucu 1: ns1.reg.ru
NS Sunucu 2: ns2.reg.ru
IP Adresi: 94.126.178.17
Düzen Bilgisi: REGISTERED, DELEGATED, UNVERIFIED
.ru Uzantı Ülkesi: Rusya/Federasyonu
Registrar: REGRU-RU
Registry Whois Sunucusu: whois.ripe.net

Dksqlojgismsizjrrllgiqt.ru

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link), ...

Bilgi Tarihi: 28.08.2015
Oluşturulma Tarihi: 28.08.2014
NS Sunucu 1: ns1.reg.ru
NS Sunucu 2: ns2.reg.ru
IP Adresi: 179.43.160.25
Düzen Bilgisi: REGISTERED, DELEGATED, UNVERIFIED
.ru Uzantı Ülkesi: Rusya/Federasyonu
Registrar: REGRU-RU
Registry Whois Sunucusu: whois.ripe.net

Mqyuledcycic.ru

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link), ...

Bilgi Tarihi: 01.09.2015
Oluşturulma Tarihi: 01.09.2014
NS Sunucu 1: ns1.reg.ru
NS Sunucu 2: ns2.reg.ru
IP Adresi: 193.124.18.187
Düzen Bilgisi: REGISTERED, DELEGATED, UNVERIFIED
.ru Uzantı Ülkesi: Rusya/Federasyonu
Registrar: REGRU-RU
Registry Whois Sunucusu: whois.ripe.net

Obqpdmjn.ru

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link), ...

.ru Uzantı Ülkesi: Rusya Federasyonu
Registry Whois Sunucusu: whois.ripe.net

Jatpvjafbwptyag.ru

Alan Adı, IDN, IP, E-posta adresi, bağlantı (link), ...

.ru Uzantı Ülkesi: Rusya Federasyonu
Registry Whois Sunucusu: whois.ripe.net

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

Linux'te Zararlı Yazılım Analizi İçin Faydalı Araçlar

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

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, yazılımlara baktığınız zaman çoğunun sadece Windows işletim sistemi ile ilgili olduğunu görebilirsiniz. Her yıl yayınlanan siber güvenlik tehdit raporlarını incelerseniz 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 ettiğiniz zaman, Linux'e kıyasla çok daha fazla araç bulmanız da bu sebepten ötürü şartlısı 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 yazımı 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 disasemble edebilir hem de hata ayıklayıcı olarak kullanarak rahatlıkla analiz edebilirsiniz. [REMnux](#) ile birlikte gelen EDB'yi çalıştırma için komut satırında `edb` yazmanız yeterli.

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

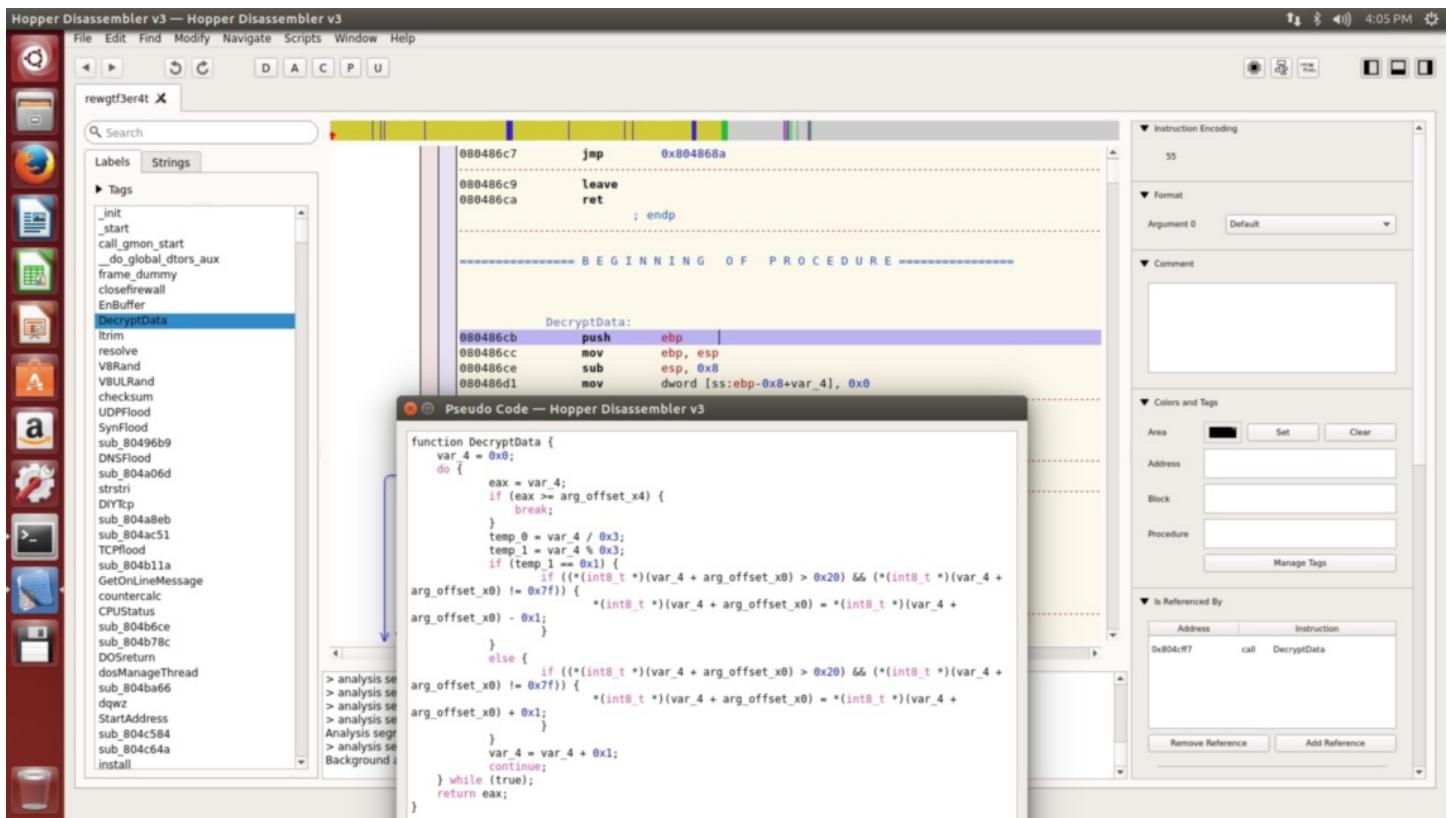
Araçlara kısaca göz atmak için örnek bir zararlı yazılım üzerinden hızlıca ilerleyelim. Elimizde komuta kontrol merkezi ile haberleşen bir zararlı yazılım var ve bu zararlı yazılım komuta kontrol merkezine ait olan adresi strings, disasembler gibi araçlardan gizlemek için üzerinde gizli (encoded) olarak 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 yiğina (stack) gizlenmiş veriyi (`kyipvm-k`bl41177/bnn`) kopyalandığını görebiliyoruz. DecryptData fonksiyonun içine girdiğimizde, sıradan disasembler 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) çeviriçi (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 görüntüleyebiliyoruz. Bundan sonrası ise programlama bilginize kalıyor.

The screenshot shows the Hopper Disassembler interface. The assembly window displays the following code for the `main` function:

```
0004cfbf push    ebp
0004fcf0 mov     esp, ebp
0004fcf2 sub     esp, 0x8
0004fcf5 and     esp, 0xffffffff0
0004fcf8 mov     eax, 0x0
0004fcf9 sub     esp, eax
0004fcfa push    esp, 0x8
0004fcfd push    0x1
0004fcf4 push    0xd
0004fcf6 call    signal
0004fcf8 add    esp, 0x10
0004fcf9 sub    esp, 0x8
0004fcfa sub    esp, 0x4
0004fcf4 push    0x800bc000
0004fcf5 call    strlen
0004fcf6 add    esp, 0x8
0004fcf7 push    eax
0004fcf8 push    0x800bc000
0004fcf9 call    DecryptData
0004fcf2 push    0x800bc000
0004fcf3 call    DecryptData
0004fcf4 add    esp, 0x10
0004fcf5 call    a
0004fcf6 install
0004fcf7 nodie
0004fcf8 push    0x0
0004fcf9 push    0x80481f0
0004fcf0 push    0x0
0004fcf1 push    eax, dword [ss:ebp-0x8+var_4]
```

The right panel shows the instruction encoding as `55` and the comment field contains `": \"kyipvm-k`bl41177/bnn\""`. The colors and tags section shows the `DecryptData` instruction highlighted in yellow.



The terminal window shows the command being run and the output:

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Mert>cd Desktop
C:\Users\Mert\Desktop>python dec.py
Encoded data: kyipvm-k`bl41177/bnn
Decoded data: lxjqun.jack52088.com
C:\Users\Mert\Desktop>

```

Disassemblers ve programlama ile uğraşmak istemiyorum, kısa yoldan OllyDbg'da olduğu gibi fonksiyonun (DecryptData) üzerinden hızlıca geçerek fonksiyonun gizlenmiş veriyi çözmeyi sağlayayım diyenler için ise EDB hemen imdadımıza yetiyor. EDB'ye zararlı yazılımı yükledikten sonra main fonksiyonuna gitmek için, Plugins menüsü altında SymbolViewer eklentisini çalıştırıldıkten 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 kısmında 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.

The screenshot shows the edb debugger interface with the following details:

- Assembly View:** Displays assembly code from address 0x0804:cfb0 to 0x0804:d017. The code includes calls to `<rewgtf3er4t::ssignal>`, `<rewgtf3er4t::strlen>`, and `<rewgtf3er4t::DecryptData>`. A red arrow points to the instruction at address 0x0804:cfb0.
- Registers View:** Shows the state of general purpose registers:
 - EAX: 00000014
 - EBX: 00000000
 - ECX: ffffffea
 - EDX: 00000000
 - EBP: bfabd6b8
 - ESP: bfabd6a0
 - ESI: 00000000
 - EDI: 0804f7ac
 - EIP: 0804cff7 <rewgtf3er4t::...
- Stack View:** Shows the stack dump starting at address 0x08048000-0x080bc000. It lists memory locations with their addresses and values, including ASCII strings like "kyipvm-k\bl41177/bnn".
- Data Dump View:** Shows the data dump starting at address 0x08048000-0x080bc000. It lists memory locations with their addresses and values, including ASCII strings like "kyipvm-k\bl41177/bnn".
- Bookmarks View:** An empty table for managing bookmarks.

The screenshot shows the Remnux debugger interface with the following panes:

- Assembly pane:** Displays assembly code starting at address 0x0804:cfcf. The code includes pushes to the stack, calls to functions like `ssignal`, `DecryptData`, and `install`, and pushes of 0x00. A green arrow points to the instruction at address 0x0804:cfcf.
- Registers pane:** Shows the CPU register state. The EIP register is highlighted with the value 0x0804fcfc.
- Stack pane:** Shows the current stack dump, which includes the string "lxjqun.jack52088.com".
- Data Dump pane:** Shows memory dump data from address 0x08048000 to 0x080bc000, containing ASCII strings and binary data.

Linux üzerinde tersine mühendislik ve zararlı yazılım analizi ile ilgilenmek isteyenler için faydalı bir yazı olduğunu ümit ederek bir sonraki yazda 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 duymıştır, "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 kemeri takmasam olur mu? Rekabetçi bir ortamda zaman zaman geliştirilmesi talep edilen güvenlik kontrolleri, alınması gereken güvenlik önlemleri, iş birimleri tarafından mal yet ve süre artıran adımlar olarak görülebilmektedir. Kimi zaman ise mevcut güvenlik kontrolleri, müşteri memnuniyetini ve kullanım kolaylığını artırmaya adımları isteyerek veya istemeden zayıflatılabilmektedir. Özellikle bu tür zayıf noktalara şifremi hatırla, şifremi unuttum gibi sayfalarda rastlanabilmektedir.

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

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

The screenshot shows a web browser window with multiple tabs open, all related to 'Web Tabanlı Yapılandırmacı'. The main content area displays a warning page with the following text:

KULLANICI ADI VE ŞİFRE UYARI SAYFASI

Değerli [REDACTED] müşterimiz,

ADSL kullanıcı adı veya şifre hatası nedeniyle internete bağlanamayorsunuz. Modeminiz sistem tarafından desteklenen bir model ise, bu sayfaya birlikte yüklenenek [REDACTED].exe bileseni modeminizde olması gereken ADSL kullanıcı adı ve şifreyi ayarlayacaktır.

Bu bilesen;

- Kesinlikle herhangi bir kişisel bilgi toplamamaktadır.
- Modem yönetim paneli erişim şifrenizi değiştirdiğiniz sistem bu şifreyi sizden talep edecektir.
- Ayarlarınız başarılı bir şekilde yapılarak bağlantı sağlandığında sayfa siz otomatik olarak [REDACTED] Pratik Çözüm uygulamasına yönlendirilecektir.
- Bu işlem 3-5 dakika sürebilir, ekrandaki yönereleri takip ederek bekleyiniz.

[REDACTED]_exe'yi yükleyebilmek için tarayıcınızda çıkan uyarı kutucuğundaki "Onay" butonuna tıkmanız gerekmektedir.

Exe uygulaması kurulacak, onaylıyor musunuz?

ADSL kullanıcı adı veya şifrenizi doğru girdiğinizden emin olun!

ADSL kota sorgulama sayfasından veya başka bir kanaldan ADSL kullanıcı adınızı ve şifrenizi değiştirdiğiniz, bu değişikliği modem arayüzünde de yapmalısınız. Bu güncelleme modem arayüzünde yapmazsanız, herhangi bir web sitesine erişmeyi denediğinizde otomatik olarak bu sayfaya ("Kullanıcı adı ve şifre uyarın sayfası") yönlendirilirsiniz.

Yazının başında da belirttiğim gibi bu tür otomatik şifre hatırlama, şifre girme gibi kullanıcı dostu araçlar, güvenli tasarılanmadığı takdirde güvenlik zayıflıklarına 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.xxxxxx.com.tr sunucusu ile haberleştiğini ve bu sunucudan şifreli bir içerik aldığı 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.



Charles 3.9.2

File Edit View Proxy Tools Window Help

Structure Sequence

Overview Request Response Summary Chart Notes

GET http://bilgi[REDACTED].com.tr/hatali_kullanici_adi_sifre/GetConfigFile.ashx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate,sdch
Pragma: no-cache
AuthKey: 93142ECA27180F39AF3970E11C6B4E5D5C9DCF4C90FCE6525CDBD9D55C95327C
Version: 2
CallType: 1
User-Agent: [REDACTED]
Host: bilgi[REDACTED].com.tr

POST http://bilgi[REDACTED].com.tr/hatali_kullanici_adi_sifre/ReportData.aashx?ConfigID=0&Status=7

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 şifremi nasıl indirdiğini ve bu bilginin bu şifreli dosya içinde yer alıp olmadığını 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 adimin ve şifremin, uygulama tarafından çağrılan GetConfigFile.ashx sayfasına, sunucu tarafından dönülen yanitta yer alan ParamHeader başlığında şifreli olarak yer aldığınoticedim. 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 şifremi sunucudan alıyordu. Bu durumu, PİN/Şifre koruması devrede olmayan cep telefonunuzu çaldığınızda, art niyetli kişinin cep telefonunuzdan bankanızın çağrı merkezini arayıp herhangi bir doğrulama adımdan geçmeden kredi kartı veya bankamatik kartının PİN'ini öğrenebilmesine benzettim.

Sistemime bulaşmış bir zararlı yazılımın, şifreli ADSL kullanıcı adı ve şifremin açık/şifresiz haline ulaşmasının ne kadar kolay olup olamayacağını 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 izleyebileceğim 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 aldığı ve bunu configdata.xml dosyasına kaydettiğini bildiği için şifresi çözülen bu bilgileri configdata.xml dosyasına yazan fonksiyona yönlendirdim ve uygulamayı bu haliyle diske kaydettim. Yamalanmış uygulamayı çalıştırıldığında artık uygulama şifreli bilgileri sunucudan alıyor ve diske kaydediyordu.

The screenshots show the Immunity Debugger interface with two windows open. The left window displays assembly code for a module named 'Exe'. The right window shows the memory dump of the same module. In the assembly code, several instructions are highlighted in red, indicating they are part of the exploit payload. The memory dump shows the raw bytes of the assembly code, with specific memory locations highlighted in red. The bottom part of the image shows a Windows file explorer window displaying the 'configdata.xml' file, which contains the extracted user and password information.

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?

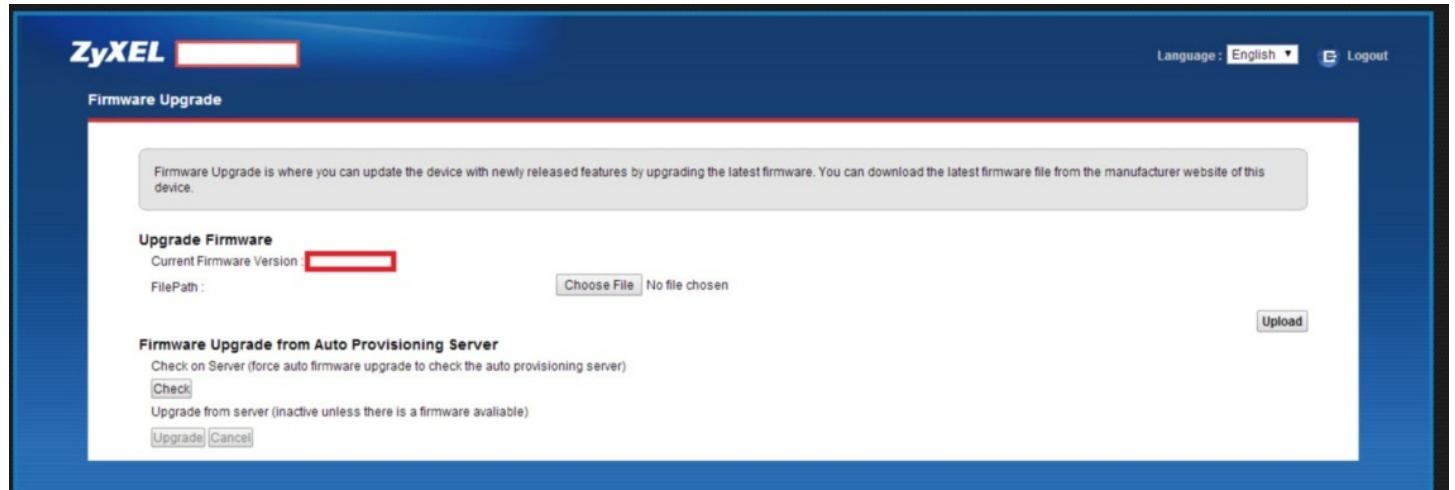
Source: <https://www.mertsarica.com/hediye-modemler/>

By M.S on July 1st, 2014



Bir öğle vakti iş arkadaşlarımla yürüken, internet servis sağlayıcılarının (ISS) müşterilerine dağıtıltığı modemlere ISS çalışanlarının uzaktan bağlanabileceğii 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 yerlestirdiği](#), devletimin ISSler üzerinden [SSL trafiğin araya girilmesini](#) planladığı şu günlerde, ISSler verdiği modemleri kullanmak ister istemez insanın aklında soru işaretlerine yol açıyordu. Bu zamana dek ISS'in hediye ettiği modemini 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 modem'in tüm trafiğini izleyecektim (sniff) ve ipucu elde etmeye çalışacaktım ya da modem'in arabirimini (console) üzerinden komutlar ile bunu öğrenecektim. Kolay yoldan ilermeye karar vererek modeme telnet ile eriştim ve desteklediği komutları teker teker incelemeye başladım.

Sızmaya testi uzmanı olarak switch ve routerlar ile az çok hazır 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 çalıştırıldım ve ardından modem'in o esnada iletişim kurduğu tüm adresleri görebildim.

```
Telnet 192.168.1.1
[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> show
ZySH> show
arp        hosts      interfaces      ip      memory      processes
version

ZySH> show hosts
Host          Address          Flags
Expires
twitter.com  199.16.156.38   4F
4294967266
twitter.com  199.16.156.70   4F
4294967266
twitter.com  199.16.156.230  4F
4294967266
twitter.com  199.16.156.6    4F
```

Amacım güncel cihaz yazılımının nereden kontrol edildiği bilgisini öğrenmek olduğu için, modem'in web arayüzünden cihaz yazılımını kontrol et butonuna bastım ve ardından telnet arabirimini üzerinden show hosts komutunu çalıştırarak, cihaz yazılımının kontrol edildiği sunucuya aramaya başladım. Çok geçmeden ftp.xxxxxx.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- Trafığınızı 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 modemin 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 autowup komutunun FTP sunucusuna bağlanmak için gerekli bilgileri (kullanıcı adı: zyxeluser) gösterdiğimizi buldum.

Modem - SecureCRT

File Edit View Options Transfer Script Tools Window Help

Enter host <Alt+R>

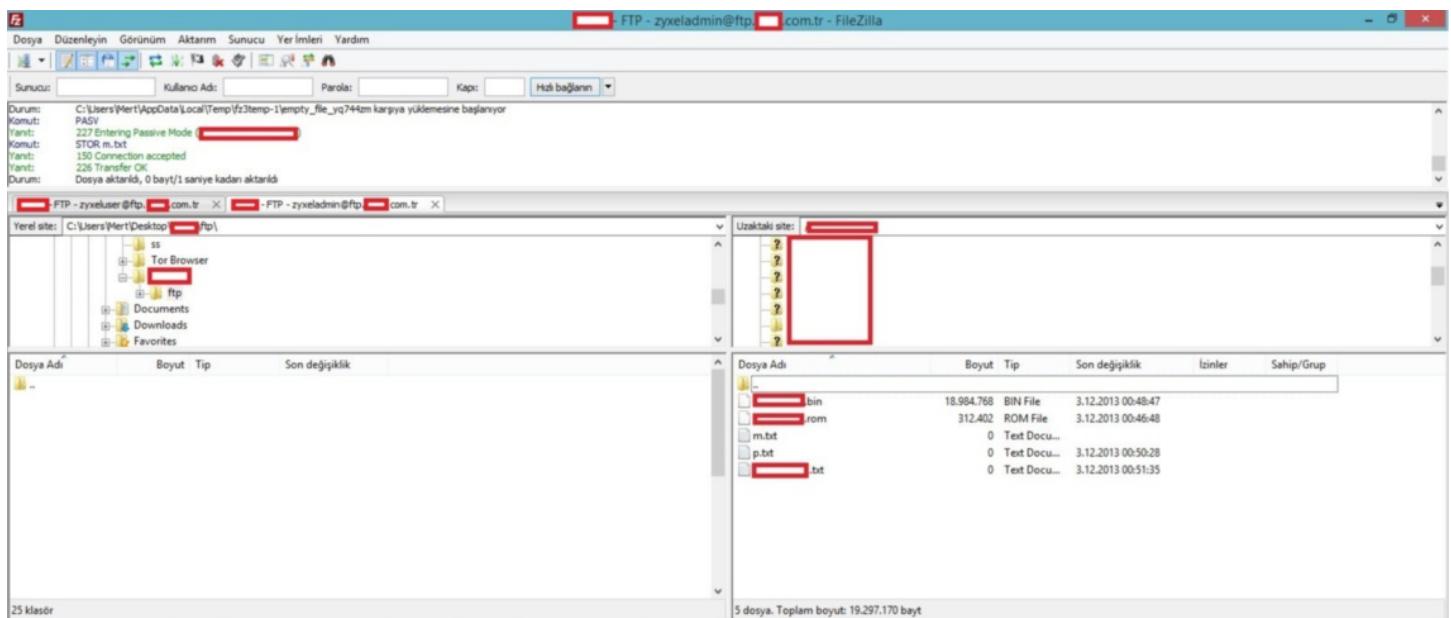
Modem X Kali

```

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# autowup
<CR> |
config# autowup
autowup#show
autowup#show
autowup#show config
Active:
ServerAddr: 1 ftp.[REDACTED].com.tr
Username: zyxeluser
Password: [REDACTED]
Directory: [REDACTED]
Filename: [REDACTED].txt
Interval: 720
Notification: 1
=====
autowup#

```

Modemime verilen yetki dahilinde, bu kullanıcı adı ve şifre ile FTP sunucusuna bağlandığında, 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 klasörlerle göz attığında, bazı dosyalar içinde modemlerin yönetici yetkisi (kullanıcı adı: zyxeladmin) 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 yükleyebildiği 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, modemin olası bir değişikliğe karşı (muhtemelen cihaz yazılımları geliştirici tarafından imzalanıyor) yazılımı yüklemeden önce kontrol ettiği bilgi paylaşılmıştı. (Kendilerine hem hızlı geri dönüş yaptıkları hem de aksiyon aldıkları için teşekkür etmeyi ihmäl 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 gönderilirse 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 mu?
- 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 yazda 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 saatı 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 yapmak için kullandığı web sitesini aşağıda görebilirsiniz.

Sahte Fatura E-postası:

The screenshot shows an Outlook inbox with an email from turkcell@turkcell-e-fatura.net. The subject of the email is '2581787267 Turkcell E-Fatura Servisi'. The message body contains a Turkcell e-fatura invoice for March 2014, amounting to 258.27 TL, due by 18.03.2014. It includes links for viewing details and paying the bill. The message is identified as Read-Only.

Sahte Fatura Web Sitesi:



[ESET'in Hesperbot raporu](#) incelendiğinde, zararlı yazılımin hedef sistemden e-posta adreslerini çaldığı ve uzaktaki sunucuya bu bilgileri传递 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 fırsatı olduğu için bunu sizlerle de paylaşmak istedim.

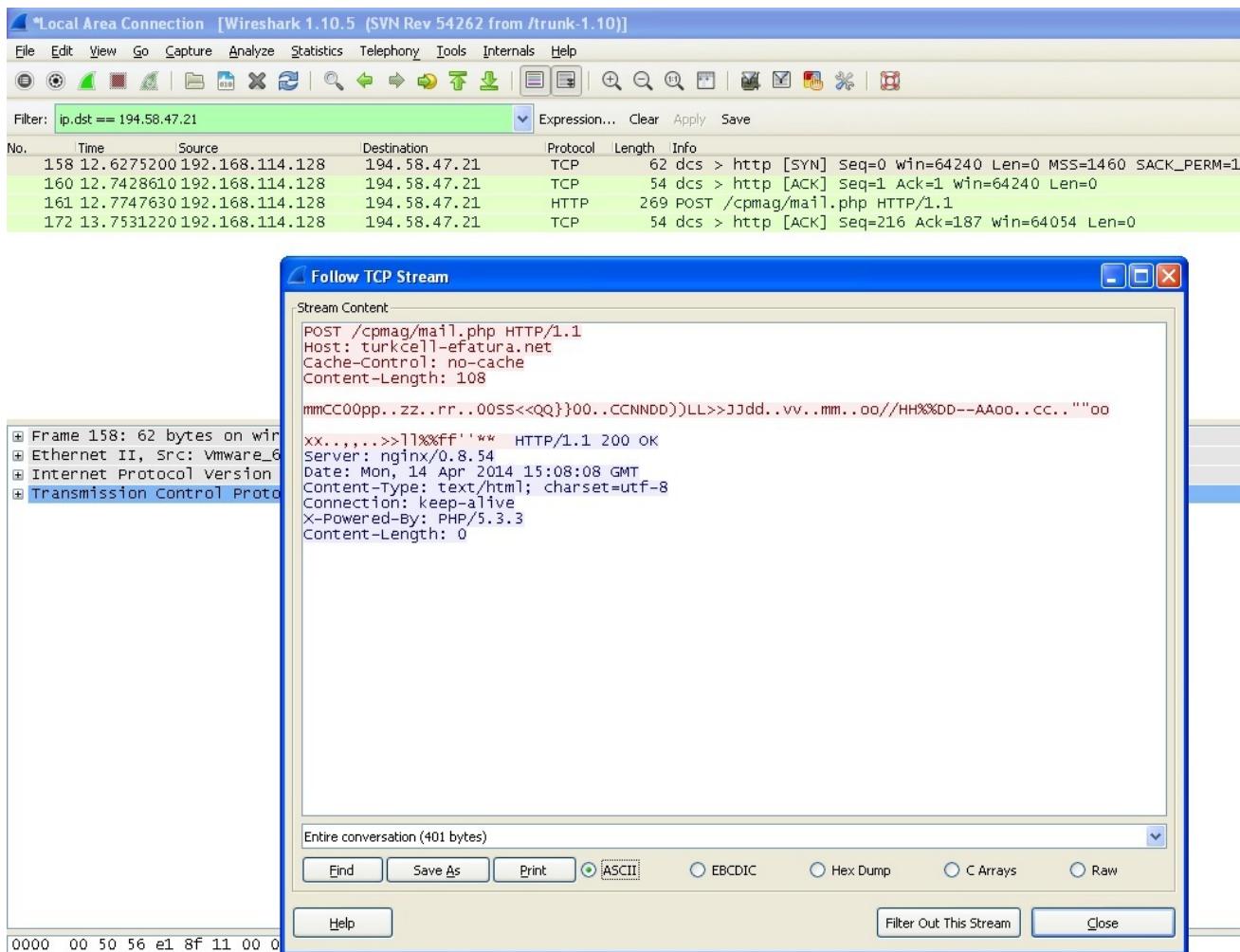
Hesperbot'un hedef sisteme bulaştıktan bir zaman sonra zararlı yazılımı yaymak amacıyla kullanmış olduğu sunucudan [ege.xe](#) adında bir yazılım indirdiğini tespit ettim. Paketlenmiş (packed) olan bu yazılımin uzantısını .exe olarak değiştirip her zamanki gibi Immunity Debugger aracı ile incelemeye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

Immunity Debugger - _014E0000.exe - [Text strings referenced in _014E000:.text]

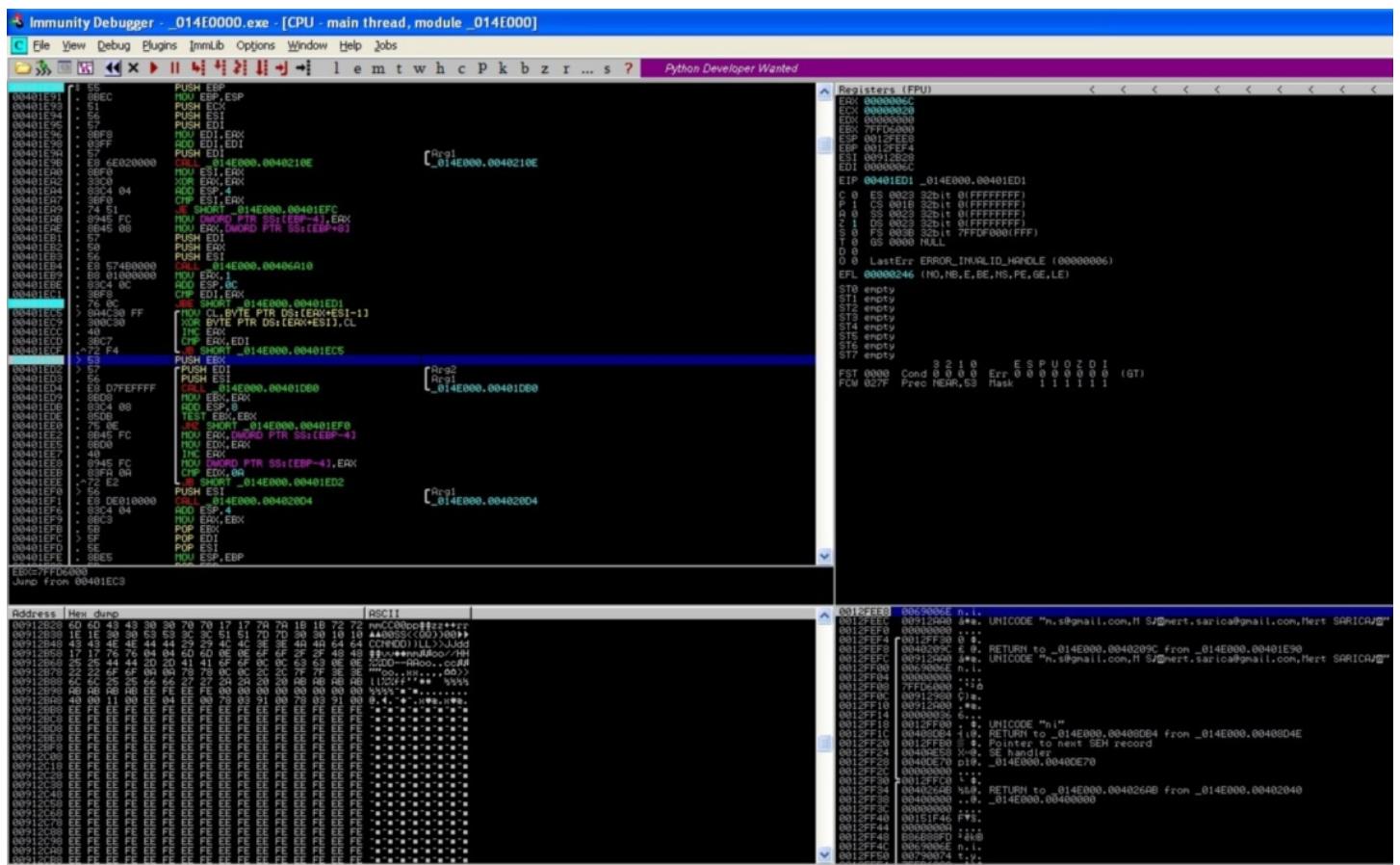
Address	Disassembly	Text String
004018D7	RETN	(Initial CPU selection)
00401563	PUSH _014E0000.0040D908	UNICODE "Common Files\System\wab32.dll"
00401589	PUSH _014E0000.0040DA0C	ASCII "WABOpen"
00401626	PUSH _014E0000.0040D914	UNICODE "/*,*"
00401642	PUSH _014E0000.0040D940	ASCII "/*,*"
00401648	PUSH _014E0000.0040D944	ASCII "/*\$*\$"
0040165F	PUSH _014E0000.0040D94C	ASCII "(*\$*"
00401748	PUSH _014E0000.0040D950	ASCII "/*\$*\$"
00401765	PUSH _014E0000.0040D958	ASCII "/*\$*\$"
00401800	PUSH _014E0000.0040D964	ASCII "/*\$*\$"
004018F1	PUSH _014E0000.0040D964	ASCII "/*\$*\$"
0040190B	PUSH _014E0000.0040D96C	ASCII "/*\$*\$"
0040191C	PUSH _014E0000.0040D91C	ASCII "/*\$*\$"
004019E2	MOV EDI,_014E0000.0040D974	ASCII "/*\$*\$"
004019E3	MOV EDI,_014E0000.0040D984	ASCII "/*\$*\$"
004019D0	PUSH _014E0000.0040D9A4	UNICODE "history.nab"
00401B07	PUSH _014E0000.0040D9A4	UNICODE "Thunderbird\Profiles\"
00401C49	PUSH _014E0000.0040D98C	UNICODE "...
00401CD3	MOV ECX,_014E0000.0040D9E0	ASCII "turkcell-eftura.net"
00401DDF	PUSH _014E0000.0040D9E0	ASCII "index.php"
00401E00	PUSH _014E0000.0040D9E0	ASCII "POST"
00401E03	PUSH _014E0000.0040D9F4	UNICODE "JB"
00401F2	PUSH _014E0000.0040D928	UNICODE "mscoree.dll"
004027B6	PUSH _014E0000.0040C190	ASCII "CorExitProcess"
004027C5	PUSH _014E0000.0040C190	ASCII "Runtime Error!@Program:"
00402800	PUSH _014E0000.0040CB3C	UNICODE "Program name unknown!"
0040280E	PUSH _014E0000.0040CB34	UNICODE "BP"
00402BC3	PUSH _014E0000.0040CB2C	UNICODE "Microsoft Visual C++ Runtime Library"
00402BC4	PUSH _014E0000.0040CE00	ASCII "C:\Documents and Settings\Administrator\Desktop\unpacked_hesperbot_addressbook_steler_014E0000.exe"
00402DCF	PUSH _014E0000.0040CB2C	UNICODE "KERNEL32.DLL"
00402E03	PUSH _014E0000.0040CB2C	UNICODE "KERNEL32.DLL"
00402E05	PUSH _014E0000.0040CF88	ASCII "FIsAlloc"
00402E06	PUSH _014E0000.0040CEC0	ASCII "FIsGetValue"
00402E07	PUSH _014E0000.0040CEC0	ASCII "FIsSetValue"
00402E08	PUSH _014E0000.0040CEC0	ASCII "FIsFree"
00402E52	PUSH _014E0000.0040D658	UNICODE "USER32.DLL"
00402E60	PUSH _014E0000.0040CD5C	ASCII "MessageBoxW"
00402E66	PUSH _014E0000.0040D4C4	ASCII "GetActiveWindow"
00402E68	PUSH _014E0000.0040CD58	ASCII "GetLastActivePopUp"
00402E69	PUSH _014E0000.0040CD50	ASCII "GetUserObjectInformation"
00402E70	PUSH _014E0000.0040CD54	ASCII "GetProcessWindowStation"
00402E7E	PUSH _014E0000.0040D900	UNICODE "CONOUT\$"

[WABOpen](#) fonksiyonundan bunun adres defterinde yer alan e-posta adres bilgilerini çaldığını tahmin etmem pek güç olmadı. Immunity Debugger ile yazılımı çalıştırıldığında 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 yazılımin koduna geçiş yaptım. Sistem üzerinde yüklü olan Outlook üzerinde geçerli bir profil olmadığı için çağrılan [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.

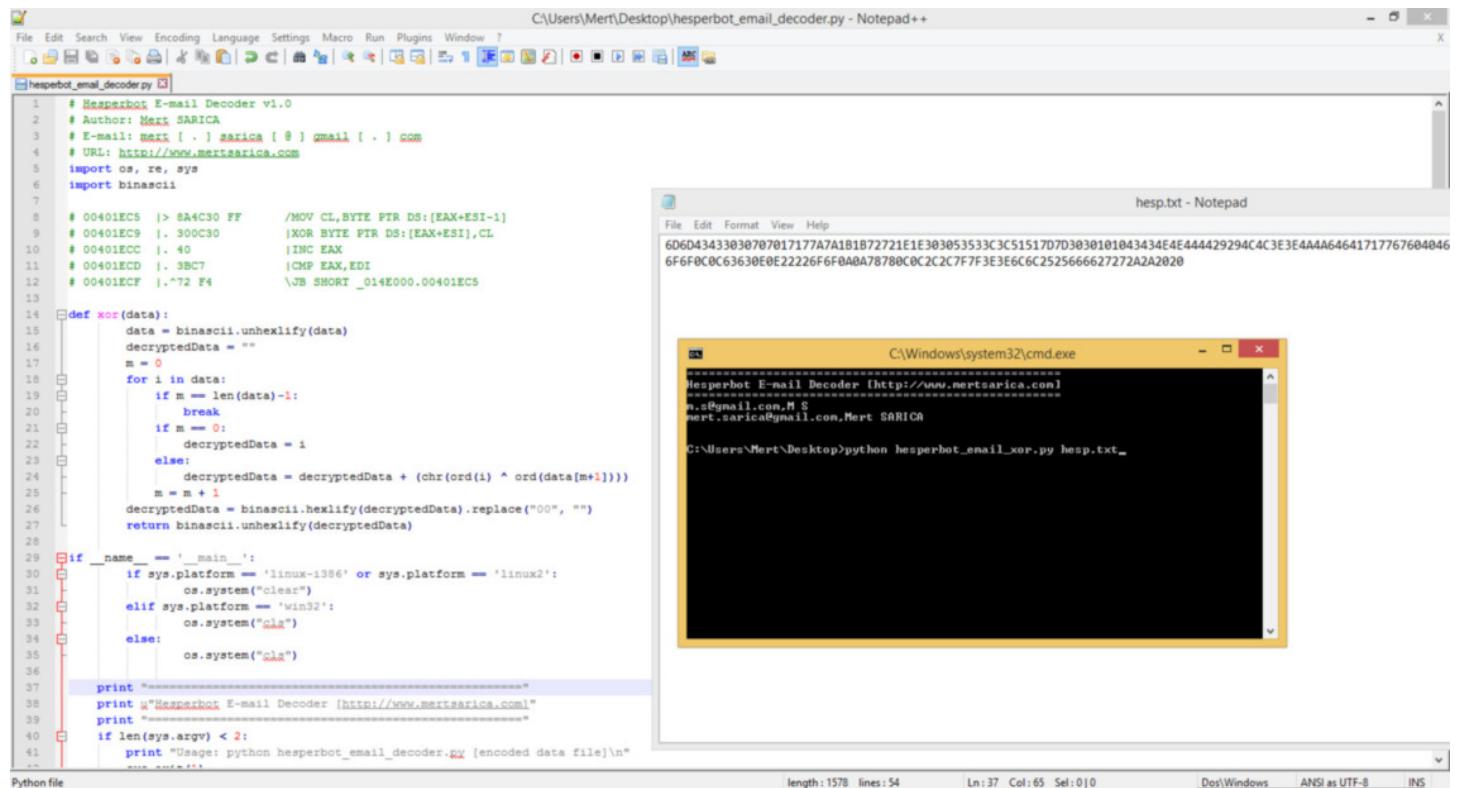
Yazılım son sürat çalıştırıldığınmdan sonra oluşan trafiği Wireshark ile izlediğimde, uzaktaki sunucuya (<http://turkcell-efatura.net/cpmag/mail.php>) gönderilen e-posta bilgilerinin okunamaz halde (encoded) gönderildiğini gördüm ve bu fonksiyonu bulmaya karar verdim.



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.



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



The screenshot shows two windows. On the left is Notepad++ displaying the Python script 'hesperbot_email_decoder.py'. The script contains comments about the author (Mert SARICA) and his email (mert.sarica@gmail.com). It includes imports for os, re, and binascii, and defines a xor function for XORing data. It also handles command-line arguments and prints usage information. On the right is a hex editor window titled 'hesp.txt - Notepad' showing a hex dump of an encoded email message. Below these is a command prompt window titled 'C:\Windows\system32\cmd.exe' running under 'Hesperbot E-mail Decoder [http://www.mertsarica.com]'. It shows the command 'python hesperbot_email_decoder.py hesp.txt' being run, followed by the output of the decoded email message which includes the recipient's email address (m.s@gmail.com) and name (M.S).

```
1 # Hesperbot E-mail Decoder v1.0
2 # Author: Mert SARICA
3 # E-mail: mert [ . ] sarica [ @ ] gmail [ . ] com
4 # URL: http://www.mertsarica.com
5 import os, re, sys
6 import binascii
7
8 # 00401EC5 1> 8A4C30 FF      /MOV CL,BYTE PTR DS:[EAX+ESI-1]
9 # 00401EC9 1. 300C30      |XOR BYTE PTR DS:[EAX+ESI],CL
10 # 00401ECC 1. .40        |INC EAX
11 # 00401ECD 1. 3BC7      |CMP EAX,EDI
12 # 00401ECF 1. ^72 F4     \JB SHORT _014E000.00401ECS
13
14 def xor(data):
15     data = binascii.unhexlify(data)
16     decryptedData = ""
17     m = 0
18     for i in data:
19         if m == len(data)-1:
20             break
21         if m == 0:
22             decryptedData = i
23         else:
24             decryptedData = decryptedData + (chr(ord(i) ^ ord(data[m+1])))
25         m = m + 1
26     decryptedData = binascii.hexlify(decryptedData).replace("00", "")
27     return binascii.unhexlify(decryptedData)
28
29 if __name__ == '__main__':
30     if sys.platform == 'linux-i386' or sys.platform == 'linux2':
31         os.system("clear")
32     elif sys.platform == 'win32':
33         os.system("cls")
34     else:
35         os.system("cls")
36
37 print "*****"
38 print u"Hesperbot E-mail Decoder [http://www.mertsarica.com]"
39 print "*****"
40 if len(sys.argv) < 2:
41     print "Usage: python hesperbot_email_decoder.py [encoded data file]\n"
42     exit(1)
```

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 atlatılacağı anlaşıldı. Hatta bazı haber kanalları canlı yayında DNS değişikliğinin nasıl yapılabileceğini adım adım gösterdi. Canlı yayını kaçırılanlar 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 faydalananmak) biri izlenebilirdi. Cihazı rootlamak beraberinde ilave güvenlik riskleri getireceğinden ötürü cihazımı rootlamaya hiçbir zaman sıcak baktım, Twitter yasağı nedeniyle de rootlamayı tercih etmedim. Ücretsiz bir VPN uygulaması ile VPN hizmetinden faydalama 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 atlatlıyor 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 eşleştirme 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 Freedome](#) VPN uygulamasını mı kullansam derken aklıma aylardır evde kuzu gibi yatan ve üzerinde [Kali](#) yüklü olan 2. [Raspberry PI](#) geldi. Kali üzerinde [OpenVPN](#) sunucusu kurmak tam da gözümde büyürken [Gökhan POYRAZ](#)'in attığı [bir tweet](#) imdadıma yetti. Gökhan'ın [blogunda](#) yer alan [strongSwan](#) VPN uygulaması kurulum adımlarından hızla geçtikten sonra Kali üzerinde başarıyla strongSwan'i kurdum. (GMP ve libgmp3c2_4.3.2+dfsg-1_armel.deb paketlerini ayrıca kurmam gerekti.)

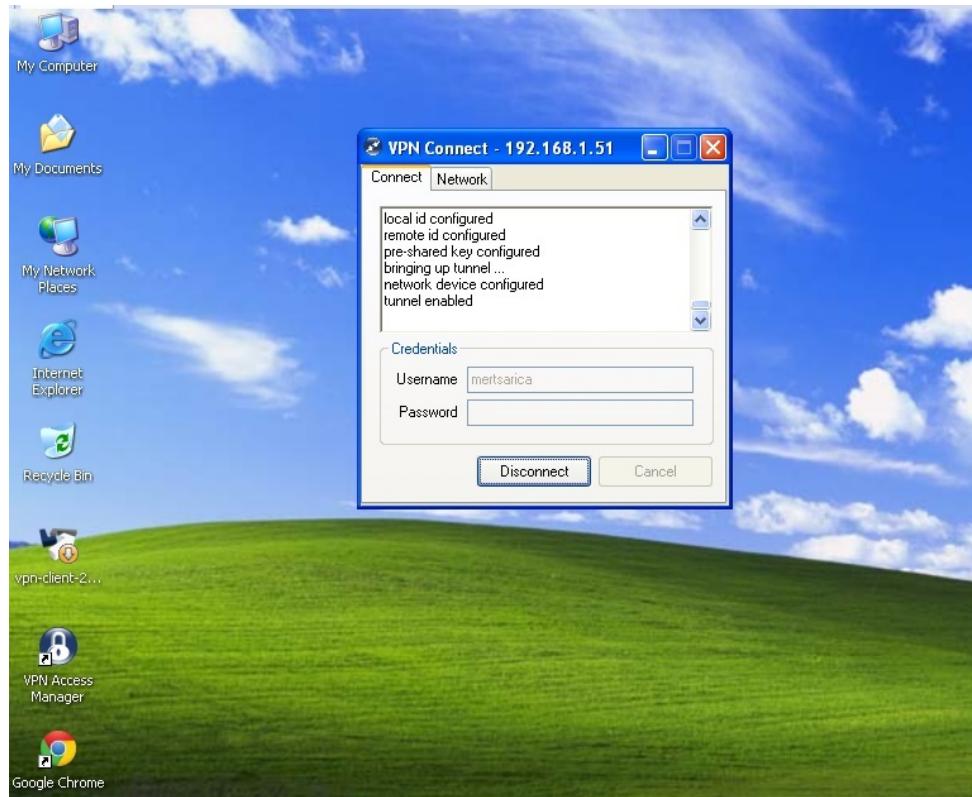
Herkesin elinin altında benim gibi VPN uygulaması kuracak hazır bir sistemi olmadığı için çoğu kimsenin ücretsiz VPN hizmetlerinden faydalandığını farkettim. Özellikle yakın çevremden gelen, hangi VPN uygulamasını yüklemeliyim ? Hangisi daha güvenli ? gibi sorular karşısında VPN kullanımının halk arasında 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 kitesine anlatmak çok kolay olmadı.

Twitter yasağı nedeniyle VPN kullanımımı arttıktan sonra güvenilir olmayan VPN sunucuları üzerinden şifrelerin çalıldığı 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 yazmadığım konusunda eleştiri oklarını bir bir üzerine atmaya başladı. Ben de hazır Kali üzerinde VPN uygulaması kurmuşken, art niyetli kişilerce yönetilen bir VPN sunucusunun nasıl kullanıcıların internet bankacılığı şifrelerini çalabileceğini arkadaşımı göstermeye ve eleştirilerine bu yazı ile karşılık vermeye karar verdim.

Simülasyon için sanal makinede yüklü olan Windows XP işletim sistemi üzerinde 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 çalıştırıldım.



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.

```

Raspberry Kali
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'in 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) arattığında 40 tane sonuç ile karşılaştım.

```

1<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2<html>
3<head>
4    <meta http-equiv="content-type" content="text/html; charset=UTF-8"/>
5    <meta name="keywords" content="student loans, business banking, commercial banking, auto loans, Checkings, Chase bank, provides credit cards, mortgage, investing and retirement planning"/>
6    <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!"/>
7    <link rel="canonical" href="https://www.chase.com"/>
8        <title>CHASE Bank - Credit Cards, Mortgage, Personal & Commercial Banking, Auto Loans, Investing, Retirement Planning, Checking, and Business Banking</title>
9        <link rel="stylesheet" href="/c/040614/etc/designs/chasecomhomepage/clientlibs.css" type="text/css"/>
10       <link rel="shortcut icon" href="/etc/designs/chasecom/images/favicon.ico" type="image/vnd.microsoft.icon"/>
11       <link rel="icon" href="/etc/designs/chasecom/images/favicon.ico" type="image/vnd.microsoft.icon"/>
12
13<script>
14    var tagManagerConfig = {
15        tagServer: "https://www.chase.com"
16    };
17</script>
18<script type="text/javascript" src="/c/040614/apps/chase/clientlibs/foundation/scripts/Reporting.js"></script>
19<script id="ipmcjs-script" data-base="true" src="/c/040614/apps/chase/clientlibs/foundation/ipmcjs/js/ipmc.js"
20 type="text/javascript"></script>
21<script>
22 // Register contentJS and siteJS paths
23 require.config( {
24     paths: {
25         "content": tagManagerConfig.tagServer+"/apps/chase/clientlibs/foundation/contentjs/js/content",
26         "site": tagManagerConfig.tagServer+"/apps/chase/clientlibs/foundation/sitejs/js/site",
27         "content/conf/appsconfig": tagManagerConfig.tagServer+"/etc/chase/appsconfig"
28     }
29 });
30</script>
31<script id="homepage-po-script" src="/c/040614/apps/chase/clientlibs/foundation/publishoptimized/homepage-po-min.js"
32 type="text/javascript"></script>

```

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

The screenshot shows the Chase Bank homepage. At the top, there are tabs for Personal, Business, and Commercial. On the right, links for Find a Branch or ATM, Contact Us, and En Español are available. The Chase logo is prominently displayed. Below the logo, there are navigation links for Products & Services, Why Chase?, Log In or Enroll, and a search bar. A large banner in the center says "INTRODUCING THE QUICK AND SIMPLE CARD FINDER" and "IN JUST 3 STEPS, FIND THE CARD THAT FITS YOUR NEEDS." It features four sample credit cards: United MileagePlus, Chase Sapphire Preferred, and Chase Freedom. A green "Get Started" button is visible. To the right, a blue sidebar titled "Welcome" asks for a User ID and Password, with a "Forgot User ID/Password?" link. It includes a "Log In to Accounts" button and a "Remember Me" checkbox. At the bottom, there are promotional sections for business cards, accepting credit cards, and the Chase liquid card.

```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2 <html>
3 <head>
4     <meta http-equiv="content-type" content="text/html; charset=UTF-8"/>
5     <meta name="keywords" content="student loans, business banking, commercial banking, auto loans, Checkings, Chase
bank, provides credit cards, mortgage, investing and retirement planning"/>
6     <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!"/>
7     <link rel="canonical" href="http://www.chase.com"/>
8     <title>CHASE Bank - Credit Cards, Mortgage, Personal & Commercial Banking, Auto Loans, Investing, Retirement
Planning, Checking, and Business Banking</title>
9     <link rel="stylesheet" href="/c/040614/etc/designs/chasecomhomepage/clientlibs.css" type="text/css"/>
10    <link rel="shortcut icon" href="/etc/designs/chasecom/images/favicon.ico" type="image/vnd.microsoft.icon"/>
11    <link rel="icon" href="/etc/designs/chasecom/images/favicon.ico" type="image/vnd.microsoft.icon"/>
12
13 <script>
14     var tagManagerConfig = {
15         tagServer: "http://www.chase.com"
16     };
17 </script>
18 <script type="text/javascript" src="/c/040614/apps/chase/clientlibs/foundation/scripts/Reporting.js"></script>
19 <script id="jpmcjs-script" data-base="true" src="/c/040614/apps/chase/clientlibs/foundation/jpmcjs/js/jpmc.js"
type="text/javascript"></script>
20 <script>
21 // Register contentJS and siteJS paths
22 require.config( {
23     paths: {
24         "content": tagManagerConfig.tagServer+"/apps/chase/clientlibs/foundation/contentjs/js/content",
25         "site": tagManagerConfig.tagServer+"/apps/chase/clientlibs/foundation/sitejs/js/site",
26         "content/conf/appsconfig": tagManagerConfig.tagServer+"/etc/chase/appsconfig"
27     }
28 });
29
30 </script>
31 <script id="homepage-po-script" src="/c/040614/apps/chase/clientlibs/foundation/publishoptimized/homepage-po-min.js"
type="text/javascript"></script>
```

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

Bir sonraki yazda 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 sıkılıkla 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'in 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: Exploit.Kit.Neutrino			
Direction	Command	User-Agent	Host
GET	/breykipybegin?fugtpceqhi=4352018 HTTP/1.1	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	cot5seed.reservenone.com:8000
Others	Accept: text/html,application/xhtml+xml,*/* Referer: http://reklam.milliyet.com.tr/reklam/www/delivery/sfr.php?zoneid=2&cb=INSERT_RANDOM_NUMBER_HERE Accept-Language: en-US Accept-Encoding: gzip, deflate, peerdist X-P2P-PeerData: Version=1.0		

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 çöktan art niyetli kişilerin kontrolü altına girmiş olabilir. Zararlı yazılım analizi ile ilgilenen biri seniz de analiz için çoğu zaman zararlı yazılıma/koda erişmeniz bu uyarılarla karşılaşınca sunucuya/koda erişimin yasaklanması/kaldırılması nedeniyle pek mümkün olamayabiliyor.

Bildığınız 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 konumlandırdım. Internet tarayıcısı ile kullanıcı herhangi bir siteye bağlanmaya çalıştığı zaman bu araç kullanıcının bağlanmaya çalıştığı adresi paralelle olarak 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.

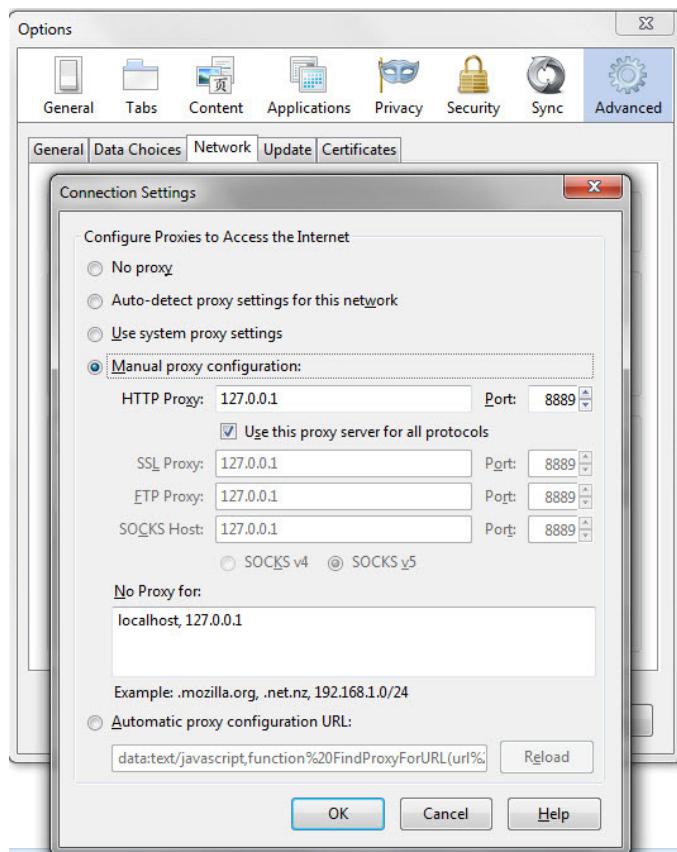
Aracın kullanımına geçmeden önce, sistem üzerinde mutlaka bir proxy aracının çalışması gerekiyor. Bunun için kendi sistemim üzerine açık kaynak kodlu [CNTLM](#) proxy aracını kurdum ve tüm trafik için proxy vazifesi görebilmesi adına ayar dosyasındaki (cntlm.ini) NoProxy ayarını * olarak değiştirdim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

```
# 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  
# SOCKSSUser and make authentication mandatory. SOCKSSUser  
# 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 kaçırınan zararlı kod tespit ederse sesli alarm üretmesi gerektiğini belirtiyorsunuz. (-a 2 ile 2 tane kaynak zararlı kod tespit ederse sesli alarm ver gibi)

```
c:\> 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 kaç tane zararlı kod tespit ettiğini, rapor adresleri ile birlikte kayıt altına alacaktır.



Haberler, Güncel Haberler, Gazete Haber... +

www.milliyet.com.tr

Most Visited Getting Started Suggested Sites Web Slice Gallery

Milliyet.com.tr SON DAKİKA 30 Mart gecesi seçim sonuçlarını Türkiye'ye milliyet.com.tr duyuracak...

Detaylı bilgi ve rezervasyon için; 444 0 329 www.touristica.com.tr touristica tatil aşkına

Bugünüz Gazete Milliyet Emlak Milliyet Heryerde Milliyet Arşiv Favorilerime ekle Ana sayfam yap Kütüye Kampanyalar

28 Mart 2014, Cuma Bizi izleyin: CANLI BÖRS BIST 68.438 2,07 EURO 3,0080 -0,08 USD 2,1910 0,23 ALTIN 91,3900 0,64

Türkiye'nin lider haber sitesi kelime ya da haber Ara ADAYINIZI DESTEKLEMEK İÇİN

Milliyet.com.tr BASINDA GÜVEN Son Dakika Yazarlar Siyaset Ekonomi Finans Spor SKORER Dünya Gündem Magazin Cadde MILLİYET.TV SKORER TV Tümü

FLASH

Connecting to: http://www.milliyet.com.tr
 Connecting to: http://www.milliyet.com.tr
 Connecting to: http://stats.g.doubleclick.net
 Connecting to: http://stats.g.doubleclick.net
 Connecting to: http://pagead2.googlesyndication.com
 Connecting to: http://pagead2.googlesyndication.com
 Connecting to: http://pagead2.googlesyndication.com
 Connecting to: http://pagead2.googlesyndication.com
 Connecting to: http://pubads.g.doubleclick.net
 Connecting to: http://www.milliyet.com.tr
 Connecting to: http://www.milliyet.com.tr
 Connecting to: http://www.milliyet.com.tr
 Connecting to: http://www.milliyet.com.tr
 Date: 28-3-2014 14:38:18 Domain: http://pubads.g.doubleclick.net Detection Ratio: 0 / 52 Report URL: https://www.virustotal.com/en/url/submit/?force=1&url=http://pubads.g.doubleclick.net/&token=3102333978c58aaa6cb1d1dc64ea0e0?f074da619hb7hd3539be1624253ff
 Date: 28-3-2014 14:38:18 Domain: http://i.milliyet.com.tr Detection Ratio: 0 / 52 Report URL: https://www.virustotal.com/en/url/submit/?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4afdcchfcF448757561hf9c6a370ab5215d
 Date: 28-3-2014 14:38:18 Domain: http://cdn.tccdn.com Detection Ratio: 0 / 52 Report URL: https://www.virustotal.com/en/url/submit/?force=1&url=http://cdn.tccdn.com/&token=3102333978c58aaa6cb1d1dc64ea0e0?f074da619hb7hd3539be1624253ff

İKA... SON DAKİKA... SON DAKİKA... G.Saray'a nester! 5 isim yolcu...

28-3-2014 14:36:44	http://i.milliyet.com.tr/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4afdcbbfcf448757561bf
28-3-2014 14:36:45	http://www.adobe.com/	1 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://www.adobe.com/&token=2711885954d1ebcbf941fe72d6a9dc66ecaa67275665e056e91778848e52
28-3-2014 14:36:45	http://www.googletagservices.com/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://www.googletagservices.com/&token=bef218cb27983674a82025a641d0f0492
28-3-2014 14:36:45	https://ssl.google-analytics.com/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=https://ssl.google-analytics.com/&token=a9b5574e0653d3c0c732736a401fc576bb
28-3-2014 14:36:45	http://stats.g.doubleclick.net/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://stats.g.doubleclick.net/&token=a563a8d723a2fae01cf56e919b1778848e52
28-3-2014 14:36:46	http://icube.milliyet.com.tr/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://icube.milliyet.com.tr/&token=1d56082a746427d140db9c4023a6470caaa5fa965
28-3-2014 14:36:47	https://sb.scorecardresearch.com/	1 / 52	https://www.virustotal.com/en/url/submit?force=1&url=https://sb.scorecardresearch.com/&token=e497eebdc853f81a9c9b2dd13bf2903361
28-3-2014 14:36:45	http://www.milliyet.com.tr/	2 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://www.milliyet.com.tr/&token=l2de7e2dd2f299b59a0e0dd424b4fd60bea5be63b554
28-3-2014 14:36:46	http://partner.googleadservices.com/	2 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://partner.googleadservices.com/&token=fe489cb9a13a9338736879ea8f0
28-3-2014 14:36:48	http://icdcube.milliyetemlak.com/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://icdcube.milliyetemlak.com/&token=l200741e97d127eeadabde6cd599ef40f
28-3-2014 14:38:18	http://pubads.g.doubleclick.net/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://pubads.g.doubleclick.net/&token=3102333978c58aa6ccb1d11dc64ea0e7f0
28-3-2014 14:38:18	http://i.milliyet.com.tr/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4afdcbbfcf448757561bf
28-3-2014 14:38:18	http://cdn.tcocdn.com/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://cdn.tcocdn.com/&token=c7731c5d28ff9d59ab392fb2a1e95969bacl549df6df247d6d7921
28-3-2014 14:38:18	https://sb.scorecardresearch.com/	1 / 52	https://www.virustotal.com/en/url/submit?force=1&url=https://sb.scorecardresearch.com/&token=e497eebdc853f81a9c9b2dd13bf2903361
28-3-2014 14:38:19	http://subi.milliyet.com.tr/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://subi.milliyet.com.tr/&token=418609e31e43ff0ba4f762c2f4ea703473c2459a0d67
28-3-2014 14:38:19	http://live.sporx.com/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://live.sporx.com/&token=2167a5c8fc51a8c422cbfa7be5516bc5b39e7412d3f3f41af2e169
28-3-2014 14:38:19	http://pagead2.googlesyndication.com/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://pagead2.googlesyndication.com/&token=e0c64f4b169d05b0bd59ef790
28-3-2014 14:38:18	http://www.milliyet.com.tr/	2 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://www.milliyet.com.tr/&token=l2de7e2dd2f299b59a0e0dd424b4fd60bea5be63b554
28-3-2014 14:41:20	http://icdcube.milliyetemlak.com/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://icdcube.milliyetemlak.com/&token=l200741e97d127eeadabde6cd599ef40f
28-3-2014 14:41:20	http://csi.gstatic.com/	0 / 52	https://www.virustotal.com/en/url/submit?force=1&url=http://csi.gstatic.com/&token=3466e7ec9094b2789ff436f10f18b9e5234c39999d4d065deb10e4

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

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

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

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

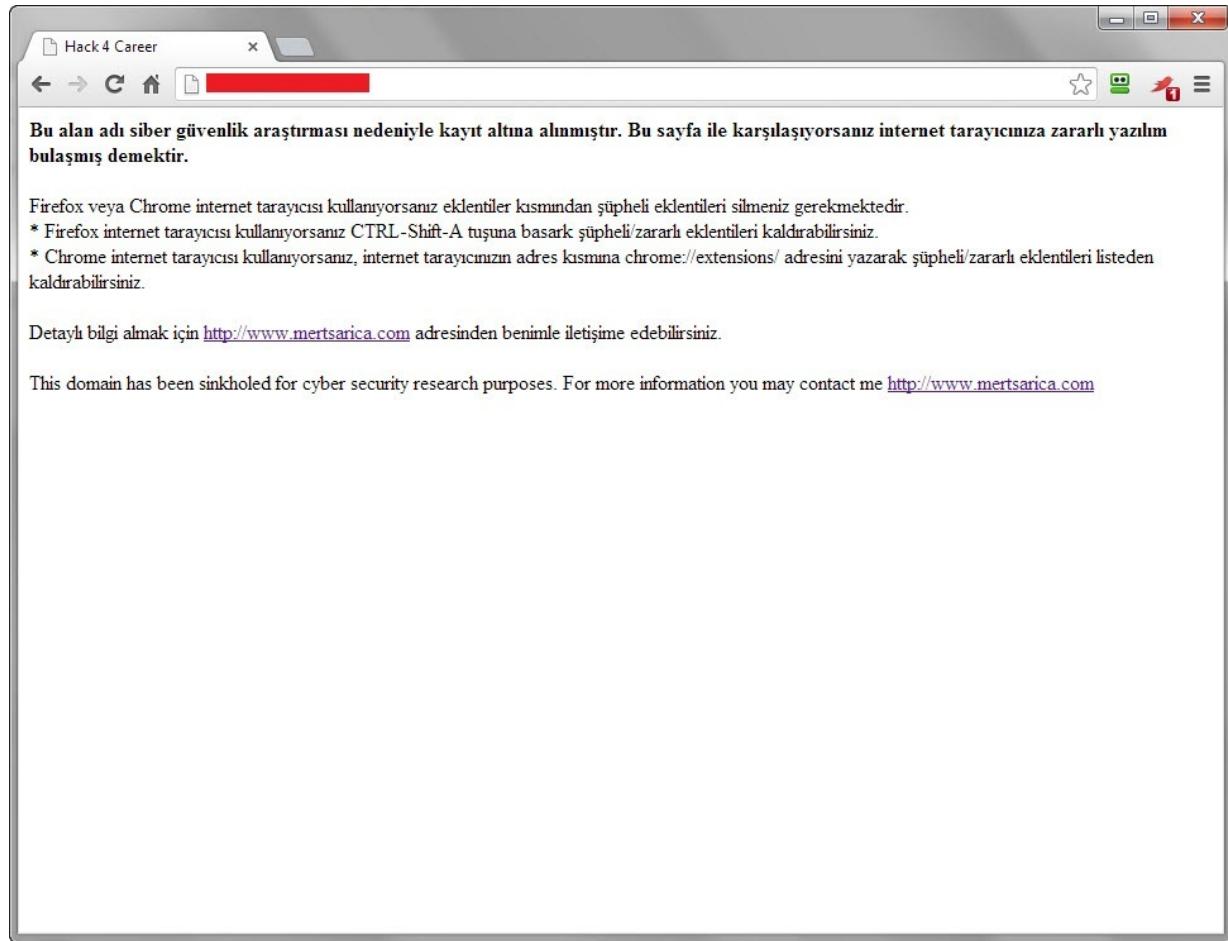


Obruk, yatay veya yataya yakın tabakalı kireçtaşlarında bulunan yeraltı nehirlerinin veya aktif mağara tavanlarının çökmesi sonucu oluşmuş baca veya kuyu görüntüsü veren derin çukurluklardır. Sanal obruk (sinkhole) ise zararlı yazılımlarla yapılan mücadelede, zararlı yazılım salgını (özellikle solucanlar) 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 sunucu 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 alınarakta trafik analiz edilebilmektedir.

2013 yılında, [sahte, zararlı Flash Player uygulaması](#) ile insanları kandıracak internet tarayıcılarına bulaşan ve sosyal medya hesaplarını ele geçirip reklam ve dolandırıcılık yapmaya çalışan çok sayıda zararlı yazılım ile karşılaşık 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 olmuştu. 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.



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

```
Raspberry - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
Raspberry x Raspberry (1) | Raspberry (2)
root@raspberrypi:/var/log/nginx# ls -al error.log
-rw-r--r-- 1 www-data adm 133898 Nov 26 20:04 error.log
root@raspberrypi:/var/log/nginx# ls -al error.log
-rw-r--r-- 1 www-data adm 145062 Nov 26 20:05 error.log
root@raspberrypi:/var/log/nginx# ls -al error.log
-rw-r--r-- 1 www-data adm 185345 Nov 26 20:06 error.log
root@raspberrypi:/var/log/nginx# ls -al error.log
-rw-r--r-- 1 www-data adm 224467 Nov 26 20:09 error.log
root@raspberrypi:/var/log/nginx# ls -al error.log
-rw-r--r-- 1 www-data adm 358830 Nov 26 20:19 error.log
root@raspberrypi:/var/log/nginx# ls -al error.log
-rw-r--r-- 1 www-data adm 582863 Nov 26 20:38 error.log
root@raspberrypi:/var/log/nginx#
```

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 aldığıni 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 ulaşmış olduğu da dikkatimden kaçmadı. (Yetkililer dilerlerse ilgili IP adresleri hakkında bilgi almak için benimle iletişime gecebilirler.)

```
C:\Windows\system32\cmd.exe - whois_desc.py
=====
Whois Desc Tool [http://www.mertsarica.com]
=====
IP: 109.160.100.133 Desc: DC-UAE-Pool1
IP: 141.111.111.111 Desc: Ankara GPRS <2G-3G>-MGB
IP: 141.111.111.116 Desc: Ankara GPRS <2G-3G>-MGB
IP: 151.101.101.101 Desc: TELLCOM ILETISIM HIZMETLERİ A.S.
IP: 151.101.101.105 Desc: TELLCOM ILETISIM HIZMETLERİ A.S.
IP: 151.101.101.109 Desc: TELLCOM ILETISIM HIZMETLERİ A.S.
IP: 176.101.101.101 Desc: TURKCELL INTERNET
IP: 176.101.101.102 Desc: TURKCELL INTERNET
IP: 176.101.101.103 Desc: Telcom Esentepe ADSL Pool
IP: 176.101.101.104 Desc: Telcom Ankara ADSL Pool
IP: 176.101.101.105 Desc: Telcom Ankara Fiber Dynamic
IP: 176.101.101.106 Desc: Telcom Ankara Fiber Dynamic
IP: 176.101.101.107 Desc: Telcom Bornova ADSL Pool
IP: 176.101.101.108 Desc: Telcom KARIAL Fttx Fiber
IP: 176.101.101.109 Desc: Telcom Adana Fttx Fiber
IP: 176.101.101.110 Desc: Telcom Adana Fiber Dynamic
IP: 176.101.101.111 Desc: Telcom Fiber Dynamic
IP: 176.101.101.112 Desc: Telcom KARIAL Fttx Fiber
IP: 176.101.101.113 Desc: Telcom KARIAL Fttx Fiber
```

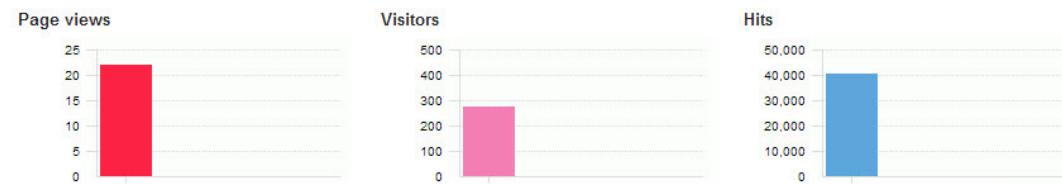
```
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\Desktop2\Sinkhole>cat desc.txt | cut -d ":" -f 2 | sort |
uniq | egrep -vi "ADSL"
70 Okullar Yolu, No 1 Kucuk Kaymakli, Lefkosa, Kibris
Ankara GPRS (2G-3G)-MGB
AVEA Iletisim Hizmetleri A.S.
Celal Bayar Universitesi
DC-UAE-Pool1
Devlet karayolu Uzeri Uzunkum/TRABZON
Global Iletisim Hizmetleri A.S.
Koc.Net DSL Corlu
Konak Mah. Izmiryolu Cad.
MALIYE BAKANLIGI
Mecidiyekoy Buyukdere Cad. 1. Imar Is Hanisi No
Oztiryakiler Madeni Esya 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 ILETISIM HIZMETLERİ A.S.
Tellcom KARTAL Fttx Fiber
Tellcom UAE Ist-Anadolu Dynamic
Tellcom YAPTA Istanbul Anadolu Dinamik - 1
Turk Telekom Tinet national backbone
Turk Telekomunikasyon Anonim Sirketi
TURKCELL INTERNET
TURKIYE BUYUK MILLET MECLISI (TBMM)
Turksat Uydu-Net Internet
Turksat Uydu Haberlesme Kablo TV ve Isletme A.S.
UAE-MARMARA?
YENIGUN INS.SAN.TIC.A.S.
C:\Users\Mert\Desktop\Desktop2\Sinkhole>
```

Zararlı yazılım, Javascript dosyası çağrırdığı 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 çağıracak şekilde programlandığı için ziyaret edilen her siteye ait kayıtlar, komuta kontrol merkezinde de yer almaktaydı dolayısıyla referrers kayıtları, sisteminde zararlı yazılım bulunanların ziyaret ettiği siteleri gösteriyordu.

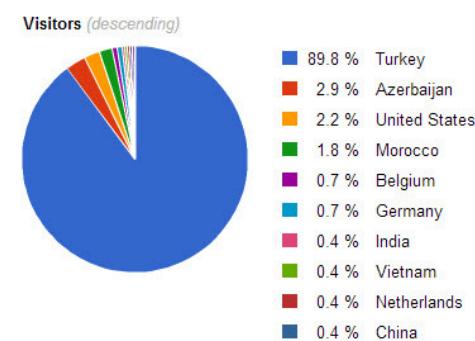
Overview

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 —

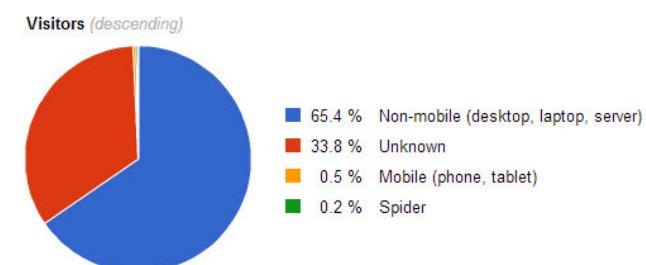
Traffic



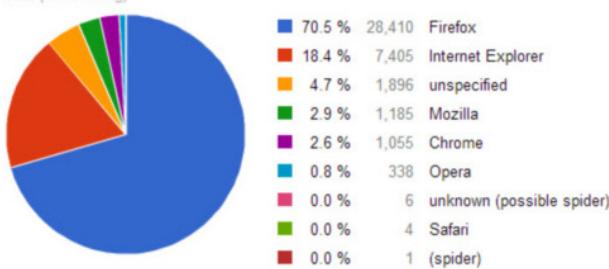
Country



Device Category



Hits (descending)



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%

Göründüğü 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 sisteme 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 ihtiyimali asla göz ardı edilmemelidir.

Zararlı yazılım ihtimaline karşı belli aralıklarda internet tarayıcınızın eklentilerini kontrol etmenizi önerir, bir sonraki yazda görüşmek dileğimle 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 yazmıştım. 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 üretебilen 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 taraflan 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 üremeye karar versem de, özelleştirilebilen daha esnek bir çözümün daha fazla zafiyet tarayıcısını ve zafiyet arayan botları engellemeye kullalabileceğini düşünerek farklı çözümler üzerinde düşünmeye başladım.

İşte 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 geçmişte öteye gidemeyen niyeti bozuk kişileri ve/veya botları bezdirmek için yeterli olacaktır. Örneğin aşağıdaki iki ekran görüntüsüne bakacak olursanız burada Netsparker'in USER-AGENT alanında imzasına yer verdiğiini 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(0x0002BF)/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(0x0002B4)/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/doxygen.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

Bezdirmeye 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 karşılaşmasını zannederek her sayfayı, bu sayfada bulunan formu ve ilgili alanları, test edilecek sayfalar kuyruğuna alarak kısır döngüye girmesini ve/veya sisteme üzerinde performans sorununa yol açmasını sağlamaktı.

```

antiscanner.php
1 <?php
2     function randString($length, $charset='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789')
3     {
4         $str = '';
5         $count = strlen($charset);
6         while ($length--) {
7             $str .= $charset[mt_rand(0, $count-1)];
8         }
9         return $str;
10    }
11   ?>
12   <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
13   <html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
14   <head profile="http://gmpg.org/xfn/11">
15     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
16     <title>Hack 4 Career - http://www.mertsarica.com</title>
17     <link rel="stylesheet" href="http://www.<?php echo randString(50);?>.com/<?php echo randString(50);?>.css" type="text/css" media="screen" />
18     <link rel="stylesheet" href="http://www.<?php echo randString(50);?>.com/<?php echo randString(50);?>.css" type="text/css" media="screen" />
19     <link rel="alternate" type="application/rss+xml" title="Hack 4 Career RSS Feed" href="http://www.<?php echo randString(50);?>.com/feed/" />
20     <link rel="alternate" type="application/atom+xml" title="Hack 4 Career Atom Feed" href="http://www.<?php echo randString(50);?>.com/feed/atom/" />
21     <link rel="pingback" href="http://www.<?php echo randString(50);?>.com/xmlrpc.php" />
22
23   <form action="<?php echo randString(50);?>.php" method="post">
24     <p><?php echo randString(50);?>: <input type="text" name="<?php echo randString(50); ?>" /></p>
25     <p><?php echo randString(50);?>: <input type="text" name="<?php echo randString(50); ?>" /></p>
26     <p><input type="submit" /></p>
27   </form>
28
29   function antiscanner($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 kısırlaşdırıcı kodu 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 faydalananmaya 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 sınızsız sayıda kural ve her kural için de sınırsız sayıda koşul destekler. URL değişiklikleri çeşitli sinamalara bağlı olabilir: sunucu değişkenleri, HTTP başlıklar, ortam değişkenleri, zaman damgaları, çeşitli biçimlerde harici veritabanı sorguları.

Tabii yanıtlanması gereken ufak bir soru daha vardı o da mod_rewrite ile tarayıcıyı kısırlaşdırıcı kodu 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'in (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 sürümde 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 çağrılığında sayfanın normal halini görüntüleyebildim.



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



```
function antiscanner($antiscanner)
{
    return $antiscanner;
}
"/usr/local/r3DTNPv2DijiGQUneenWCWsblG1BSigU4GDa6xhqGA5bjACtfT3"
"c/wHc216fs5oI6O5GbJkg3464kNGXufIMVoD0ktFdDVl3Z9ONo15"
define('DB_NAME', 'database');
define('DB_USER', 'www.mertsarica.com');
define('DB_PASSWORD', 'antiscanner');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8');
J07NrgQvoBhl0BLLMs cmd1Iqvff8idM8IkOIIGLouszHN2KYU@mabYEJPzNgBdv3yFn3YJwVaJp8KSIgP0i5NDmRY3li8qd79TM.com
```



```
function antiscanner($antiscanner)
{
    return $antiscanner;
}
"/usr/local/aF79V6teJWnFYRwfR9G2uw7GL2G5OXlaiRGOqr9aDTbIT1DkN"
"c/ha4CtMkL4KoaOkTbUBEr6qvO8avJslhc6mVlyneQ7FCyetw2V"
define('DB_NAME', 'database');
define('DB_USER', 'www.mertsarica.com');
define('DB_PASSWORD', 'antiscanner');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8');
ZEw33Ui7Rr3qlpBMXa3KM6vd0AxWjcdQp7Z3j9S8iOCgRKmqn@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)
- UqPAIw70vMR0mqyYBG5jEjm7B0z1zmLJtgMvyRq..
- i3oCXP48Emf5E1tp1B1U017vh3qljvmsExQZC..
- hpr2CborDWhalbw16VachMj268eB7p8AVvsDwH1..
- MY4CXChl616yaFdWDpUc7zfBK653jGx6W7cU..
- WUJyErz4dINMBqqdkNv1ILzLgcpZ1f0qz3C8N4..
- tDEBmMoc3COxNypck8srzWGVJr2Dx2Jceh0gMg..
- nNhjDeeKn6lsuIMACEfyVcrsGT2xVpsskV0a..
- uhjw54fyareuyKTrxTGUhr5Plsj0ao6yMgA1ct..
- 2AB052oxtr3v9syPy7mNGw47ZST7K1S5spax..
- te54bkpxObDpbu7tew84G871esU8K1yeYJQ8J19r..
- 1Q2df4pUmhxDzTJvkfZ2FSk6koW25hmlLlG..
- IkrXMyWCHMfhIRWxQkQezBqttd18VfPreVEbiX2R..

Crawling & Attacking (2/3)...

81%

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

Crawl & Attack phase started.

Windows Task Manager

File Options View Shut Down Help

Applications Processes Performance Networking Users

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
httpd.exe	Administrator	03	12,564 K
explorer.exe	Administrator	00	9,144 K
svchost.exe	SYSTEM	00	8,836 K
mcsshield.exe	SYSTEM	00	8,800 K
msiexec.exe	Administrator	00	6,868 K
taskmgr.exe	Administrator	00	4,564 K
httpd.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

Show processes from all users

End Process

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)

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.

Group Issues by

Vulnerability Type

Severity

Confirmation

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(0x0003E..

- [Possible] Internal Path Disclosure (Win..)
- [Possible] Internal Path Disclosure (*nix)
- Hobcj0q2N8JsggRSMeFJc7PuxRlxz2wqJ8FTx..
- [Possible] Internal Path Disclosure (Win..)
- [Possible] Internal Path Disclosure (*nix)
- Hobcj0q2N8JsggRSMeFJc7PuxRlxz2wqJ8FTx..
- [Possible] Internal Path Disclosure (Win..)
- [Possible] Internal Path Disclosure (*nix)
- F0nnPRCMgJq@NjdQjcgbE6y3CTUeqEDl9v9NS..
- NCoHtrEaeTrxQE1WhEs2DEUjcClloLSREETkQDU..

 - style%3E%3C
 - scRipt%3E%3CscRipt%3Enetsparker(0x0004..
 - scRipt%3E
 - [Possible] Internal Path Disclosure (Win..)
 - [Possible] Internal Path Disclosure (*nix)

Crawling & Attacking (2/3)...

97%

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

File Options View Shut Down Help

Applications Processes Performance Networking Users

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
httpd.exe	Administrator	05	12,128 K
explorer.exe	Administrator	00	11,616 K
svchost.exe	SYSTEM	00	11,048 K
mcsshield.exe	SYSTEM	00	9,276 K
chrome.exe	Administrator	00	8,676 K
httpd.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

Show processes from all users

End Process

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)

Logs (8)

Group Issues by

Vulnerability Type

Severity

Confirmation

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

Acunetix Web Vulnerability Scanner (Consultant Edition)

File Actions Tools Configuration Help

New Scan | Report | Start URL: http://127.0.0.1:80/ Profile: Default Stop Pause

Tools Explorer

- Web Vulnerability Scanner
- Web Scanner
- Tools
 - Site Crawler
 - Target Finder
 - Subdomain Scanner
 - Blind SQL Injector
 - HTTP Editor
 - HTTP Sniffer
 - HTTP Fuzzer
 - Authentication Tester
 - Compare Results
- Web Services
- Configuration
 - Application Settings
 - Scan Settings
 - Scanning Profiles
- General
 - Program Updates
 - Version Information
 - Licensing
 - Support Center
 - Purchase
 - User Manual
 - AcuSensor

Scan Results

Scan Thread 1 (http://127.0.0.1:80/) Status: Scanning

Responsive: true
Web server banner: Apache
Operating system: Unknown
Web server: Apache
Technologies:

Web Alerts (153)

- Slow HTTP Denial of Service Attack (1)
- HTML form without CSRF protection (150)
- Clickjacking: X-Frame-Options header missing (1)
- TRACE method is enabled (1)

Knowledge Base

Site Structure

/

- 132czGX8Gj4cr979pMQiiA4wdXo2KNONGh... OK
- 1cJHPVvb8NXDofb1siQD7wTh2k686R6g4U... OK
- 1v2ojh2OjkPOP2yfDTH3W5s5FIDtMBzwmM8... OK
- 2ekq4Ah7UwTM6t6BEjUtnrPVIrZ7XUnjk... OK
- 3vgV7xd0GFKpgJlNs7l9qDvk7JH0qMHO... OK
- 49Rfpf16dxA3l6lQx6df0ACmyIPaeNIXQuz... OK
- 4vUFpG4WvIrdwZHQQDCnjlHELYL9CxL26XJ... OK
- 5R1fAVtPgC5Kcy54EpnQRUHmB1xpF8j02yU... OK
- 7tFxoQSiWhJUUbE9cfzc8RVWtGUQQ2mnWF... OK
- 988mt6JR2sjlquD2nNSBOBFUfD9mUpmlLN... OK
- 9cJel8L52KneMtvpDirchBtwSxaMULMqwb... OK
- 9Ej2y5KmWpB5hBBpPNEUy17kKHQXXtvz9... OK
- a7sJhRCluXDiCubd91wFkpxvpbJlFIAEM48... OK
- abgh1xf2E5mpvF7gMza5W4RFVGOS5AG3g... OK
- Ac7LefvvCKlh7dV53mZxb1iau8cW0TumaS... OK

Activity Window

12.24 14:10:28, [Warning] Unable to download update information. Please review your settings or try later.
 12.24 14:10:28, [Error] Cannot connect. [00020004]
 Error while connecting to web server
12.24 14:18:34, [Error] Scan "Scan Thread 1" was aborted by user.

Application Log | Error Log

Web Scanner | Scanning 1 website(s) ... | Number of websites left to scan : 1

Acunetix Web Vulnerability Scanner (Consultant Edition)

File Actions Tools Configuration Help

New Scan | Report | Start URL: http://127.0.0.1:80/ Profile: Default Stop Pause

Tools Explorer

- Web Vulnerability Scanner
- Web Scanner
- Tools
 - Site Crawler
 - Target Finder
 - Subdomain Scanner
 - Blind SQL Injector
 - HTTP Editor
 - HTTP Sniffer
 - HTTP Fuzzer
 - Authentication Tester
 - Compare Results
- Web Services
- Configuration
 - Application Settings
 - Scan Settings
 - Scanning Profiles
- General
 - Program Updates
 - Version Information
 - Licensing
 - Support Center
 - Purchase
 - User Manual
 - AcuSensor

Scan Results

Scan Thread 1 (http://127.0.0.1:80/) Status: Scanning

Responsive: true
Web server banner: Apache
Operating system: Unknown
Web server: Apache
Technologies:

Target information: http://127.0.0.1:80/ Alerts summary: 153 alerts

Scan time: 1 hours, 44 minutes
Number of requests: 78069
Average response time: 0,91 milliseconds
Scan iteration: 1

Response time history:



Statistics: 78069 requests
Progress: 59,19%

Activity Window

12.24 14:10:28, [Warning] Unable to download update information. Please review your settings or try later.
 12.24 14:10:28, [Error] Cannot connect. [00020004]
 Error while connecting to web server
12.24 14:18:34, [Error] Scan "Scan Thread 1" was aborted by user.

Application Log | Error Log

Web Scanner | Scanning 1 website(s) ... | Number of websites left to scan : 1

Kıssadan hisse, mod_rewrite ve ufak bir PHP uygulaması ile script kiddie'ler'in taramalarını yavaşlatacak bir yöntem geliştirmiş oldum. Evet baklığınız 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 gazetedede [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 sizme testi uzmanlarına talep daha da arttı. Bugüne kadar başımıza ne geldi, 10 işi yapıyor sun, sizme 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 sizme testi uzmanlarına talep daha da arttı. Fakat buradan siber güvenlik uzmanlarını, sizme 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 siz 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 vermiyorlarsa görüşmeye gönül rahatlığıyla devam edebilirsiniz :)

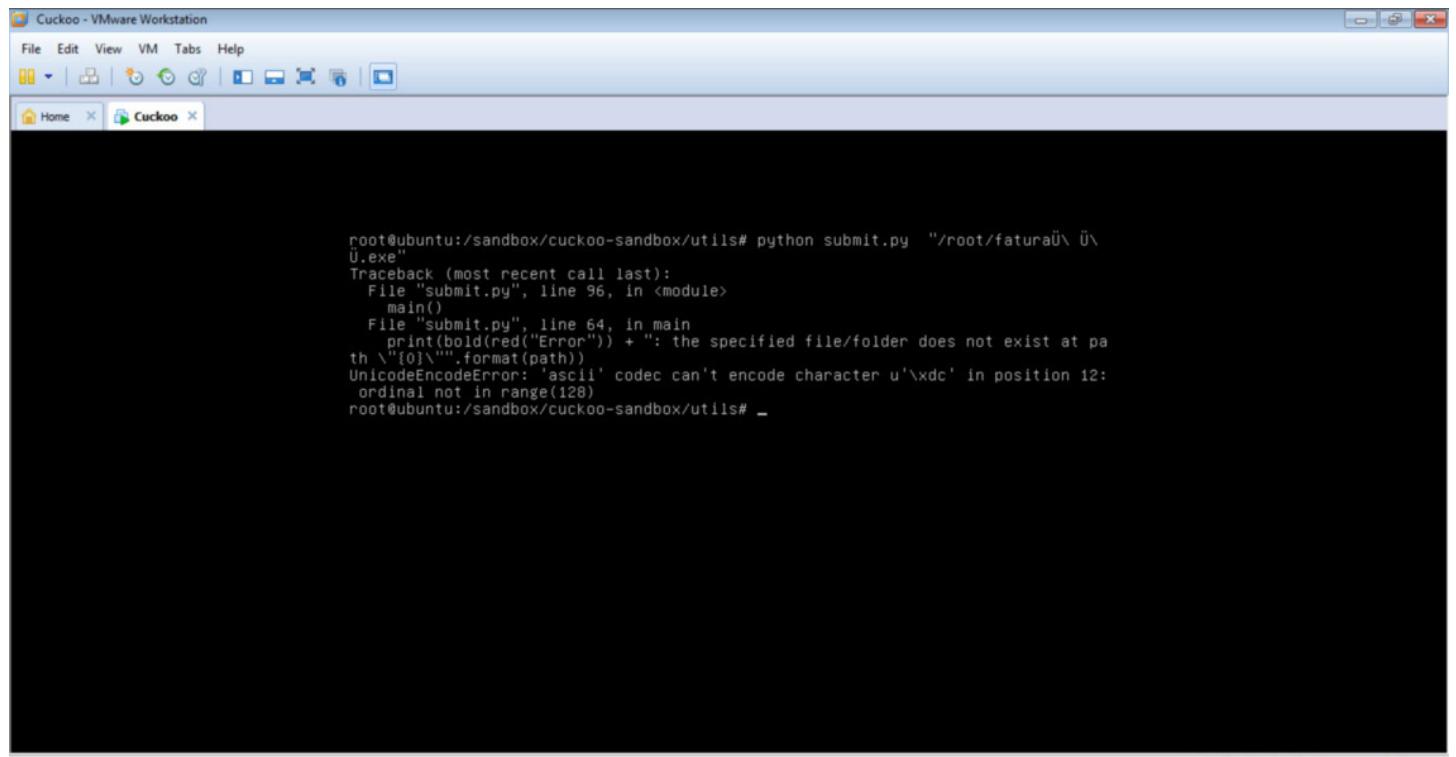
2013 yılı benim için bol bol sizme testi, zararlı yazılım analizi, blog yazısı, sunum, teknik çalışma ve [Güvenlik TV](#) ile geçti. Hacking haberleri sayesinde sizme testinin kurumlar için önemine dikkat çekmenin artık anlamsız olduğu şu günlerde, zararlı yazılım analizinin kurumlar için (özellikle 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 yazılarından aldığı olumlu geri dönüşler sayesinde motivasyonumu yüksek tutabildim ve her ay en az 1 yazı yazmaya özen gösterdim. [Halil ÖZTÜRKÇİ](#) ile gerçekleştirdiğimiz, birbirinden değerli konuklarım ile güvenlik dünyasında olup bitene yer verdığımız Güvenlik TV ile bir yılı geride bıraktım. Üniversitelerden gelen konuşturma 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-postaları 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 itibarıyle) 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 faydalananız. Dinamik analizde kum havuzları (sandbox), analizin olmazsa olmazlarından. Özellikle açık kaynak kodlu [Cuckoo Sandbox](#), (çevrimiçi sürümü ile [Malwr](#)) bu analizin vazgeçilmezidir. Ancak her zaman söylenilmiş 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 artttırmaya yardımcı olabilmek adına malwr.com'da hizmet veren Cuckoo Sandbox ile biraz oynamaya başladım. Güvenlik testlerinden bugüne dek tecrübe ettiğim kadariyla çoğulukla çevrimiçi, çevrimdışı olsun, dışarıdan dosya kabul eden benzer uygulamalar, sistemler, Türkçe karakter içeren dosya isimlerini çözümlemeye (parse) sıkıntı yaşayabiliyorlar. Hesperbot salgından elde ettiğim örnek zararlı yazılımın adını değiştirdip (fatura.exe dosyasının adını faturaÜ Ü Ü.exe olarak değiştirdim) malwr.com'a göndermeye başladıkten 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.

A screenshot of a web browser window displaying the Malwr - Malware Analysis website. The URL in the address bar is https://malwr.com/submission/status/NDFIYzY4NGJhZTk5NGRIZWiwyzu4ZjU5YTmNDgyMWY/. The page features the Malwr logo with a stylized beetle icon. A teal banner at the top left says "Hang on..." followed by the text "The analysis is still pending or under processing. This page will refresh every 30 seconds." Below this is a large blue progress bar with diagonal stripes. At the bottom of the page, there's a "Back to the top" link, a copyright notice about Creative Commons license, and a logo for shadowserver.



To direct input to this VM, click inside or press Ctrl+G.

Tabii diyeceksiniz ki adını fatura.exe yapıp yollasam analiz başarıyla tamamlanmayacak mı ? Tamamlanacak fakat zararlı yazılım çalıştırıldığın sonunda hangi isim altında çalışıp ona göre zararlı fonksiyonları çağırırsa şeikhde 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 karşılaşış karşılaşılmayacağıma bakmak istedim. 2 dosyayı da ayrı ayrı VirusTotal'a gönderip rapora baktığında, fatura_normal.zip (36/49) ile fatura_bypass.zip (35/49) için üretilen raporlarda, Comodo antivirus yazılımın farklı sonuç ürettiğini gördüm. fatura_normal.zip dosyasını zararlı olarak tespit edebiliyorken, fatura_bypass.zip için dosyanın güvenli olduğunu raporluyordu.

Antivirus scan for bc125e

<https://www.virustotal.com/en/file/07e8e66b1af6538f4cfc16fc8ae05ce76a3eefed9b1c3bad33f2db2703b349b/analysis/1387960134/>

Community Statistics Documentation FAQ About English Join our community Sign in

SHA256: 07e8e66b1af6538f4cfc16fc8ae05ce76a3eefed9b1c3bad33f2db2703b349b
 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.WelsofRtpDgIgf6w0	20131224
AhnLab-V3	Trojan.Win32.Zbot	20131224
AntiVir	TR/Spy.ZBot.8581754	20131224
Anti-AVL	Backdoor.Win32.Pushdo	20131224
Avast	Win32.Crypt-QH!I [Tr]	20131225
AVG	Downloader.Agent2.BR!XW	20131224
Baidu-International	Trojan.Win32.Wheelsof.aB	20131213
BitDefender	Trojan.GenericKD.1437245	20131225
Bkav	✓	20131225
ByteHero	✓	20130613
CAT-QuickHeal	✓	20131222
ClamAV	✓	20131225
CMC	✓	20131224
Commtouch	✓	20131225
Comodo	TrojWare.Win32.Injector.ASD	20131225

Antivirus scan for 441d3b

<https://www.virustotal.com/en/file/d26e74506fec76e3e68559b751f405032606553e17d0501a764481d1aa96df9b/analysis/1387960245/>

Community Statistics Documentation FAQ About English Join our community Sign in

SHA256: d26e74506fec76e3e68559b751f405032606553e17d0501a764481d1aa96df9b
 File name: fatura_bypass.zip
 Detection ratio: 36 / 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.WelsofRtpDgIgf6w0	20131224
AhnLab-V3	Trojan.Win32.Zbot	20131224
AntiVir	TR/Spy.ZBot.8581754	20131224
Anti-AVL	Backdoor.Win32.Pushdo	20131224
Avast	Win32.Crypt-QH!I [Tr]	20131225
AVG	Downloader.Agent2.BR!XW	20131224
Baidu-International	Trojan.Win32.Wheelsof.aB	20131213
BitDefender	Trojan.GenericKD.1437245	20131225
Bkav	✓	20131225
ByteHero	✓	20130613
CAT-QuickHeal	✓	20131222
ClamAV	✓	20131225
CMC	✓	20131224
Commtouch	✓	20131225
Comodo	✓	20131225

Kıssadan hisse, zararlı yazılım analizi için sistemsel, 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 :)