Hack 4 Career - 2014

Merhabalar,

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

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

Yeni yazılarla görüşmek dileğiyle...

Saygılarımla,

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

Air6372SO Varsayılan Hesap Doğrulaması

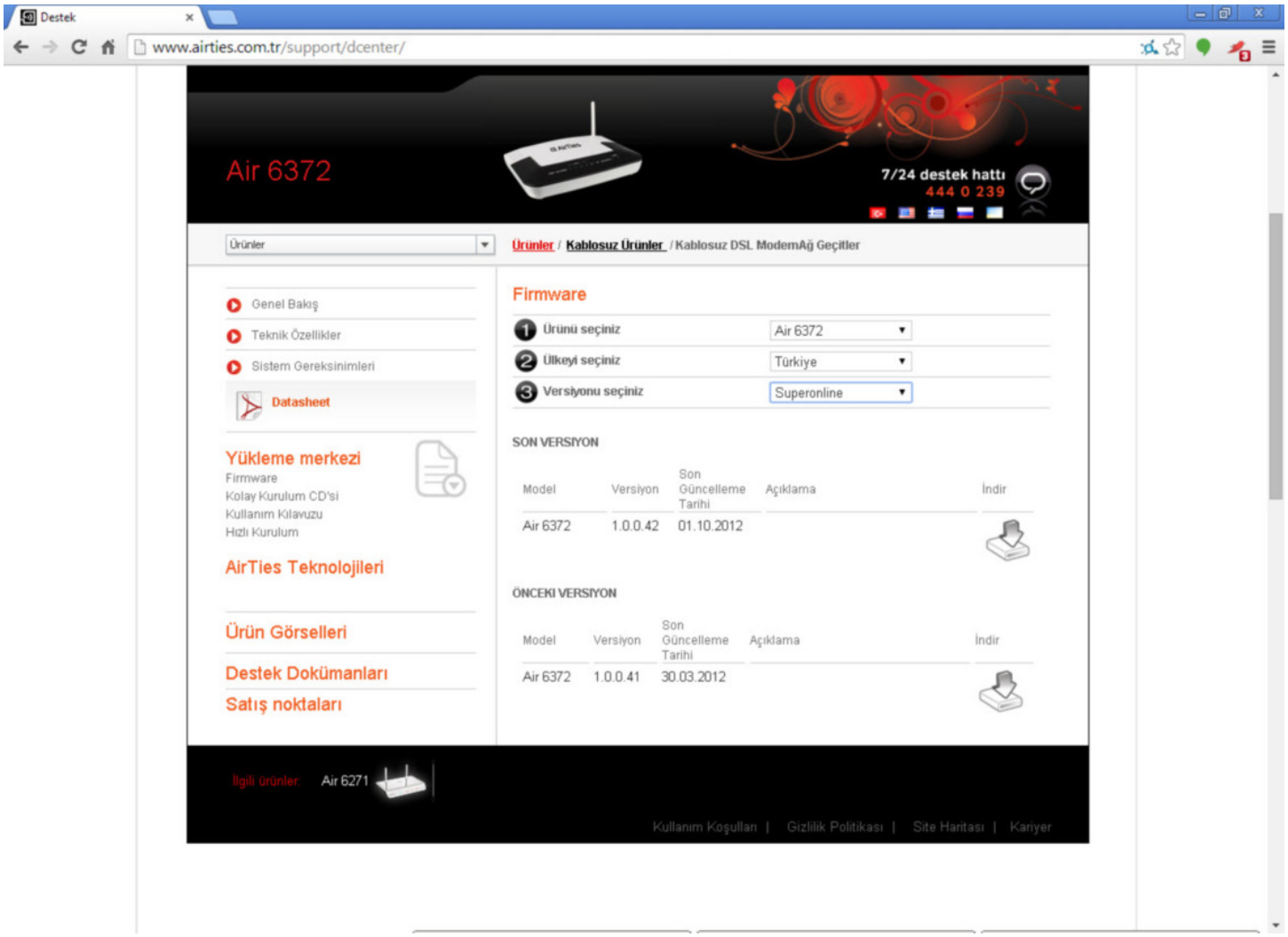
Source: https://www.mertsarica.com/air6372so-varsayilan-hesap-dogrulamasi/

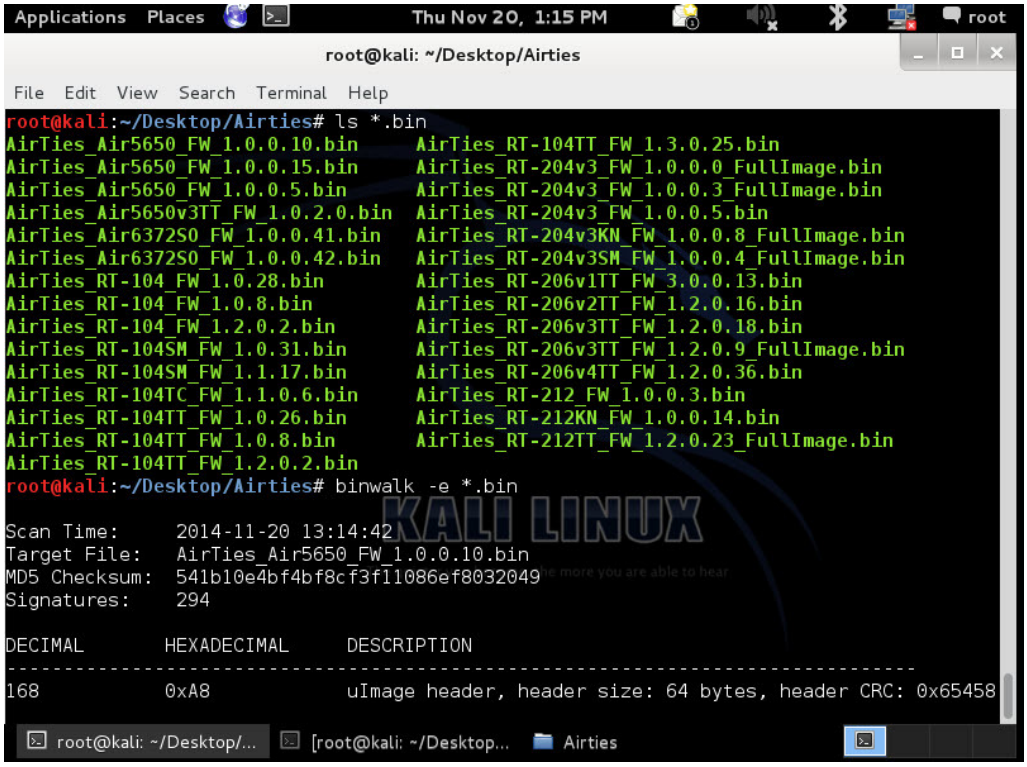
By M.S on December 1st, 2014

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

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

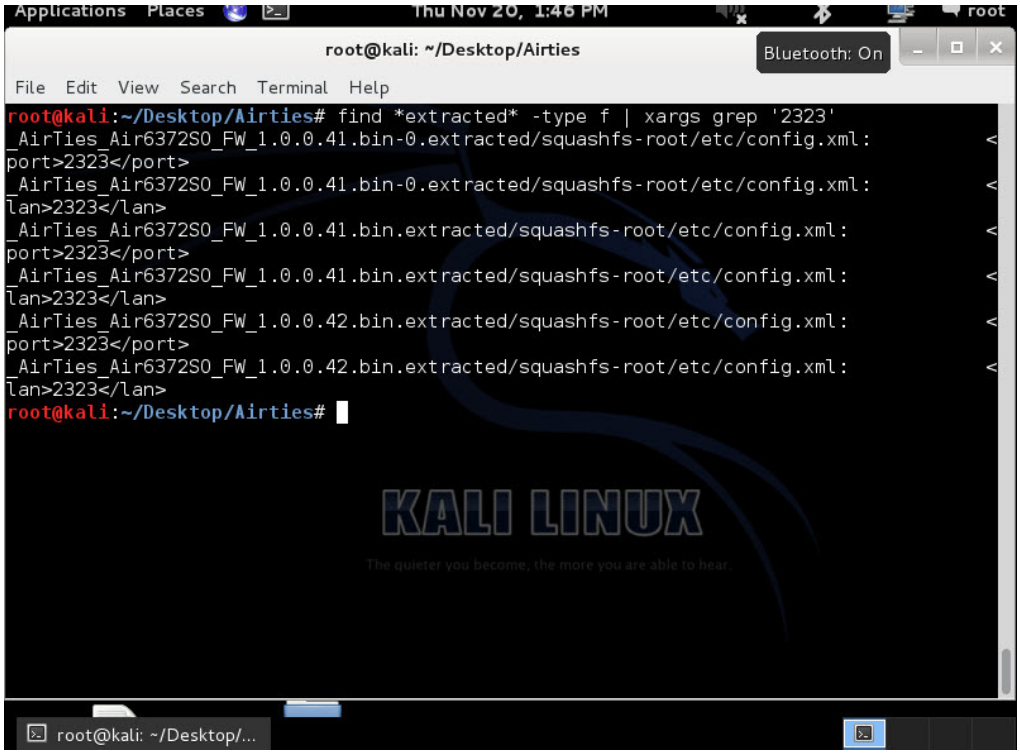
Airties'ın web sitesinde yer alan çoğu kablosuz modemin donanım yazılımını indirdikten sonra donanım yazılım analizi için biçilmiş kaftan olan ve Kali işletim sistemi ile gelen binwalk aracı ile donanım yazılımlarını bu araca toplu bir şekilde analiz ettirmeye başladım.





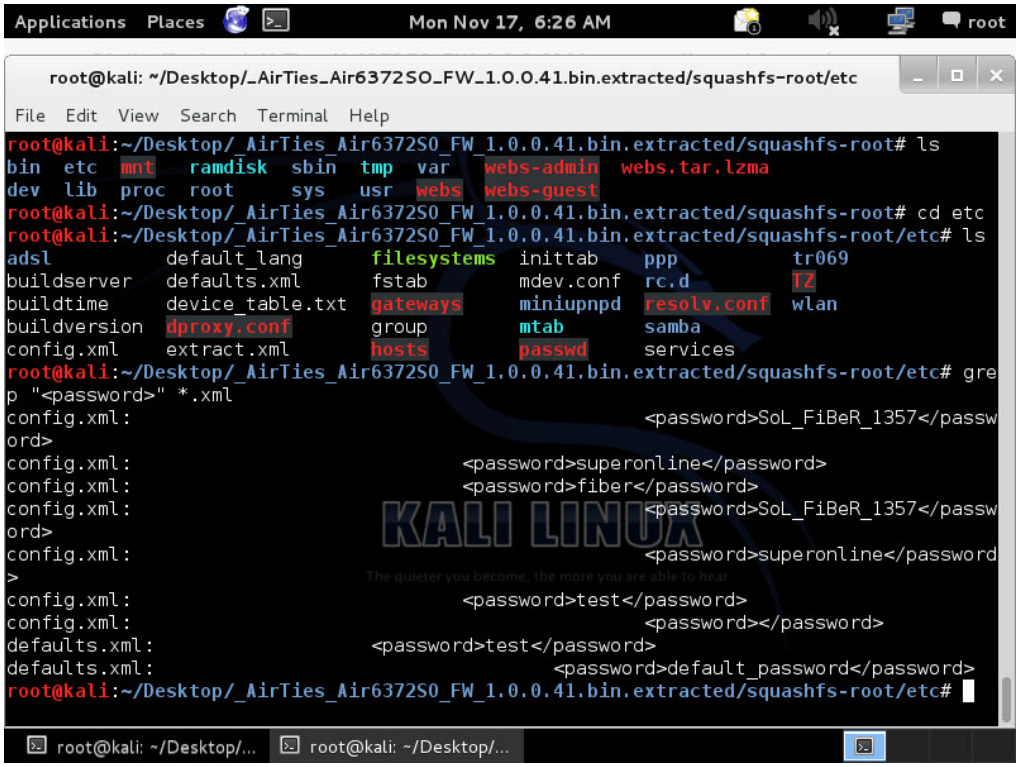
> *Bilmeyenler için binwalk aracından kısaca bahsetmek gerekirse, bu araç belirtilen donanım yazılımını otomatik olarak analiz ederek eğer sıkıştırılmış (compressed) ise öncelikle açarak içindeki dosyaları, dosya sistemi hiyerarşisine uygun olarak ilgili klasöre kopyalamaktadır. Siz de daha sonra kopyalanan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

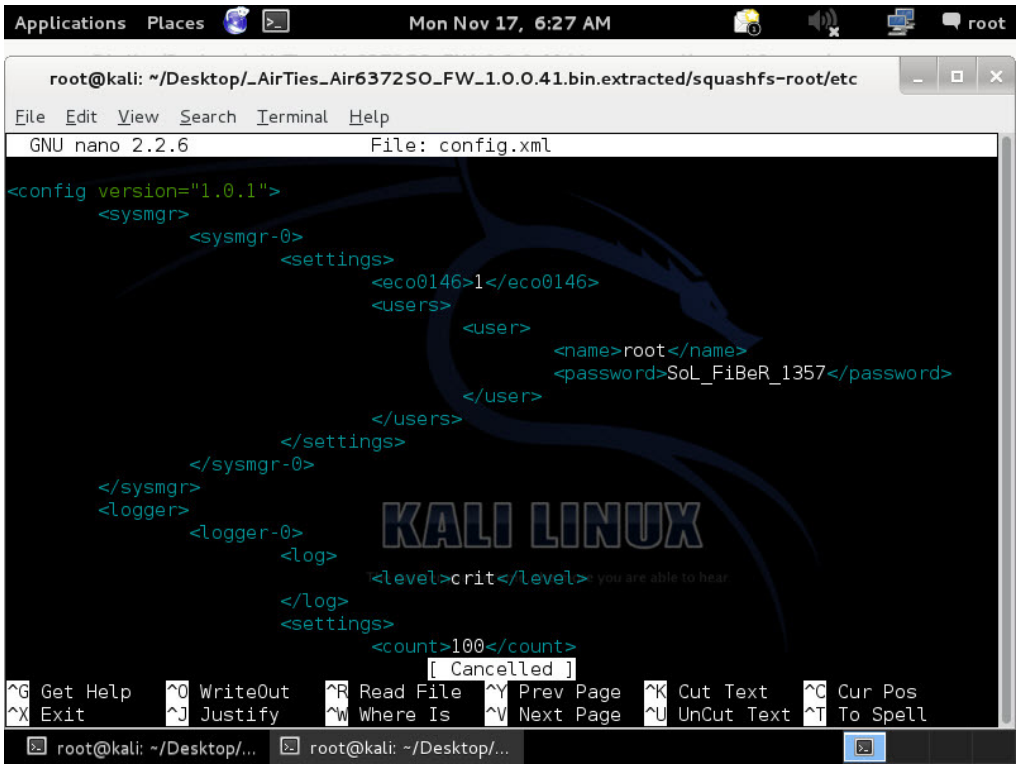
binkwalk aracına -e parametresi ile tüm donanim yazılımlarını (*.bin) analiz ettirdikten sonra teker teker her bir açılan klasörün içine bakmak yerine 2323 bağlantı noktasını tüm *extracted* geçen (binwalk açtığı donanım yazılımlarını bu şekilde isimlendiriyor) klasör isimleri içinde grep aracı ile aramaya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

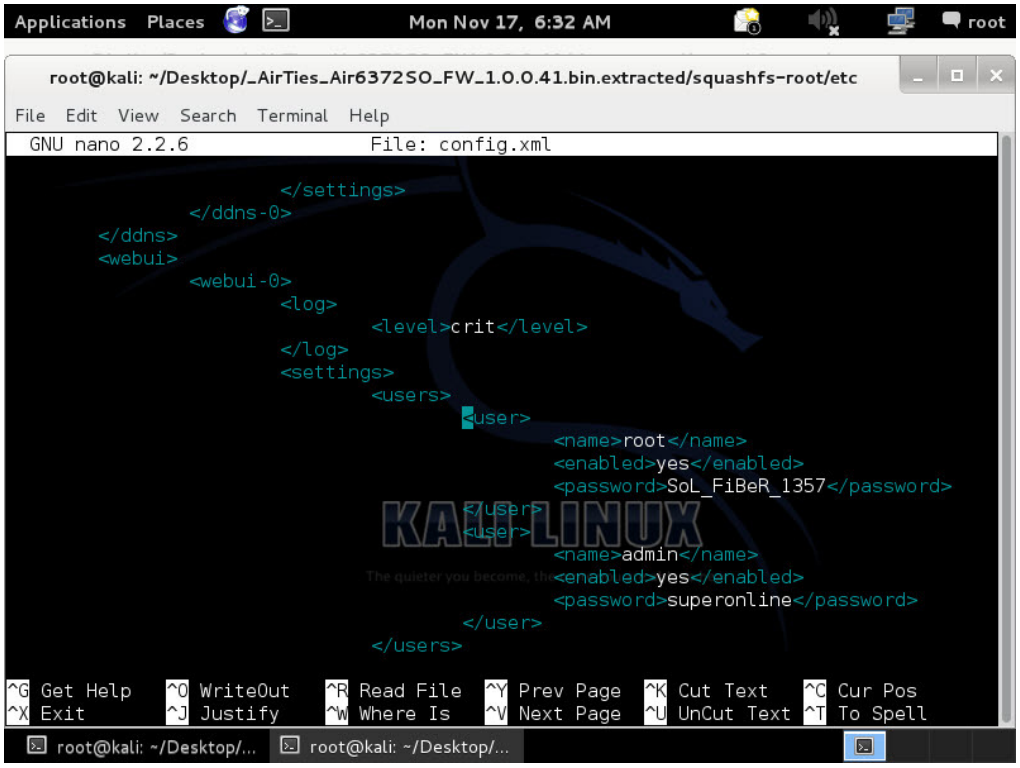


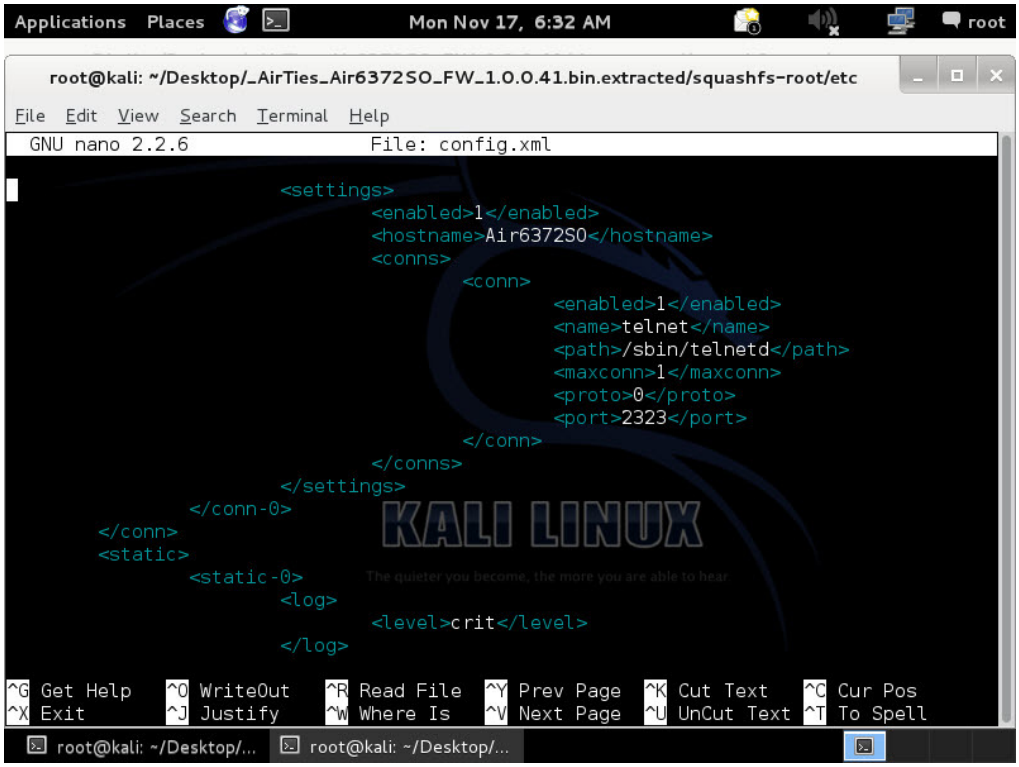
Grep aracının çıktısına göre bu varsayılan hesabın tek bir model için yani Air6372SO için geçerli olduğu olduğu görülüyordu.

config.xml dosyası içinde password kelimesini arattığımda ise iddia edilenden farklı olan SoL_FiBeR_1357 şifresi hemen dikkatimi çekti. Bu dosyaya metin editörü ile baktığımda ise bunun root şifresi olduğunu gördüm. (Airties'ın web sitesinde bu model için yer alan donanım yazılımı, Superonline için ayrıca geliştirildiği için muhtemelen şifre farklı)



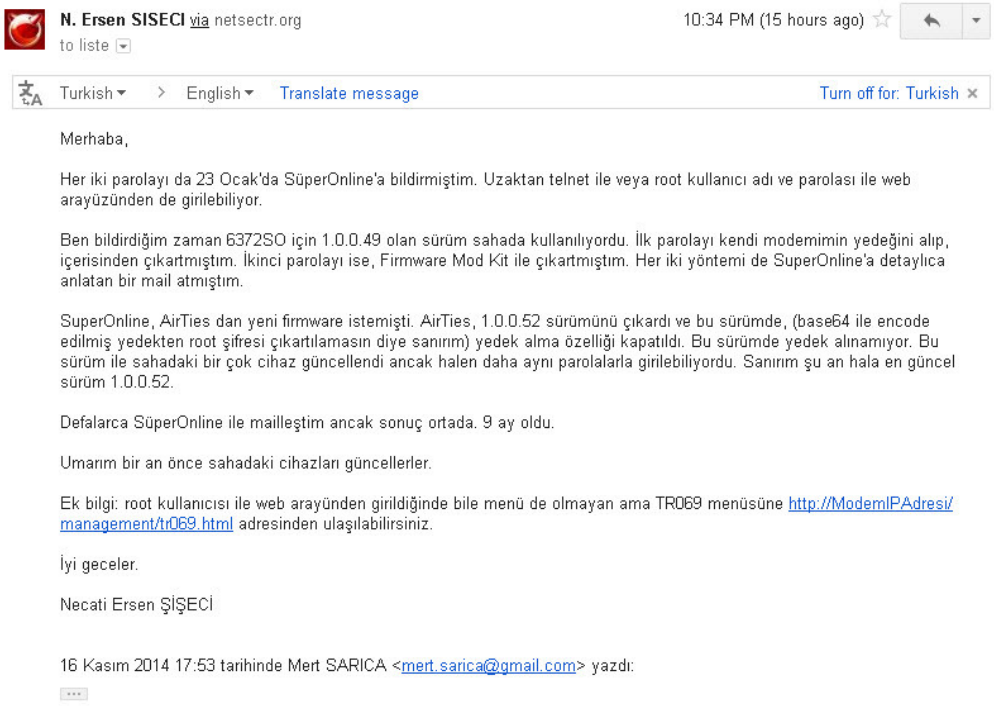

Applications Places Mon Nov 17, 6:27 AM root
root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc
File Edit View Search Terminal Help
GNU nano 2.2.6 File: config.xml
<config version="1.0.1">
<sysmgr>
<sysmgr-0>
<settings>
<eco0146>1</eco0146>
<users>
<user>
<name>root</name>
<password>SoL_FiBeR_1357</password>
</user>
</users>
</settings>
</sysmgr-0>
</sysmgr>
<logger>
<logger-0>
<log>
<level>crit</level>
</log>
<settings>
<count>100</count>
[Cancelled]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
root@kali: ~/Desktop/... root@kali: ~/Desktop/...


Applications Places Mon Nov 17, 6:32 AM root
root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc
File Edit View Search Terminal Help
GNU nano 2.2.6 File: config.xml
</settings>
</ddns-0>
</ddns>
<webui>
<webui-0>
<log>
<level>crit</level>
</log>
<settings>
<users>
<user>
<name>root</name>
<enabled>yes</enabled>
<password>SoL_FiBeR_1357</password>
</user>
<user>
<name>admin</name>
<enabled>yes</enabled>
<password>superonline</password>
</user>
</users>
^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/...



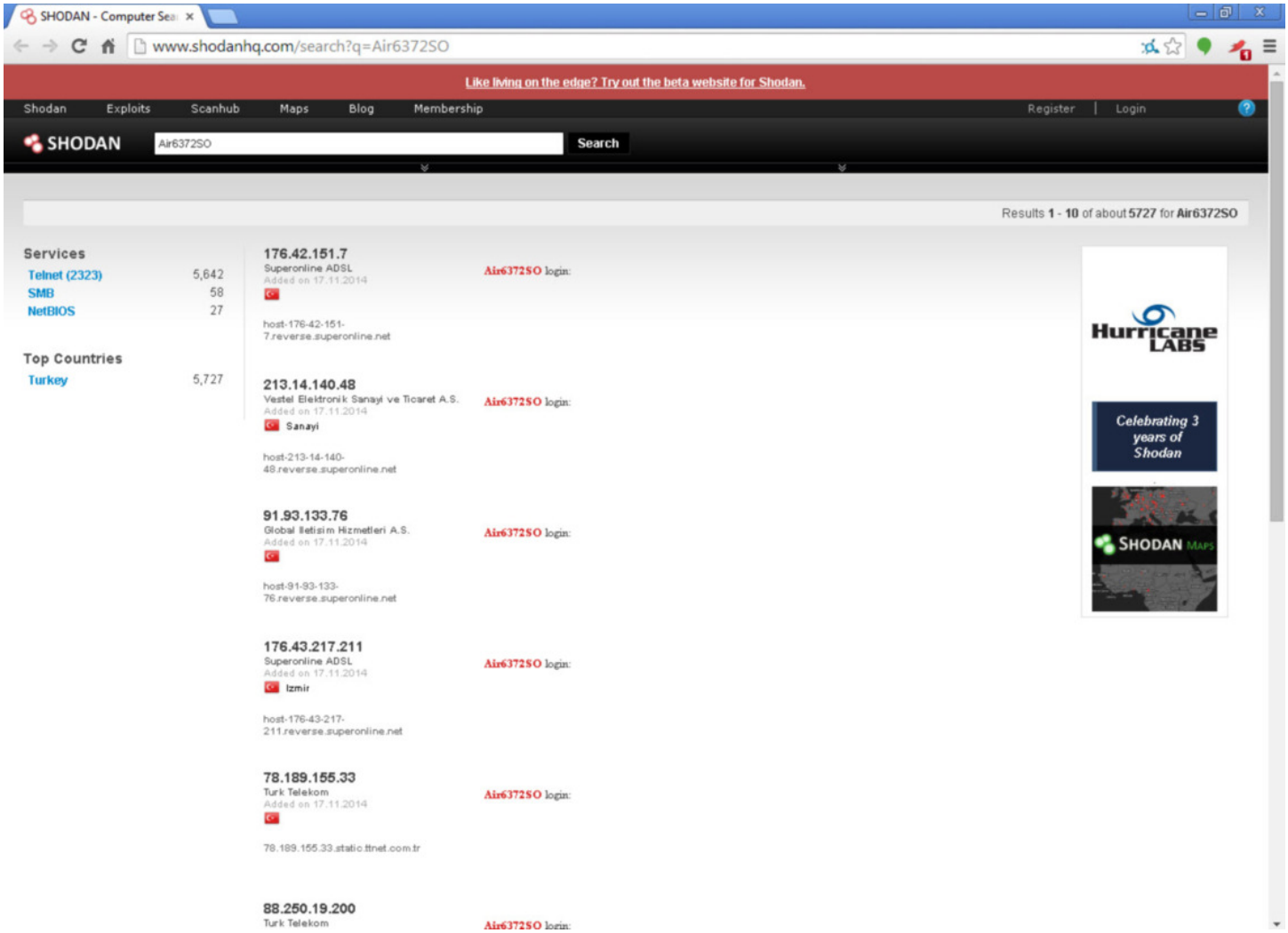
Tabii bende bu marka ve model modem olmadığı için bu kullanıcı adı ve şifrenin doğru olup olmadığını teyit etmek için hemen bir tweet göndererek takipçilerimden yardım istedim ve çok geçmeden hard_ress Twitter hesabından bu kullanıcı adı ve şifre ile modeme telnet üzerinden bağlanılabilindiği bilgisi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

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



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

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



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

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

Hesperbot Tarayıcısı

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

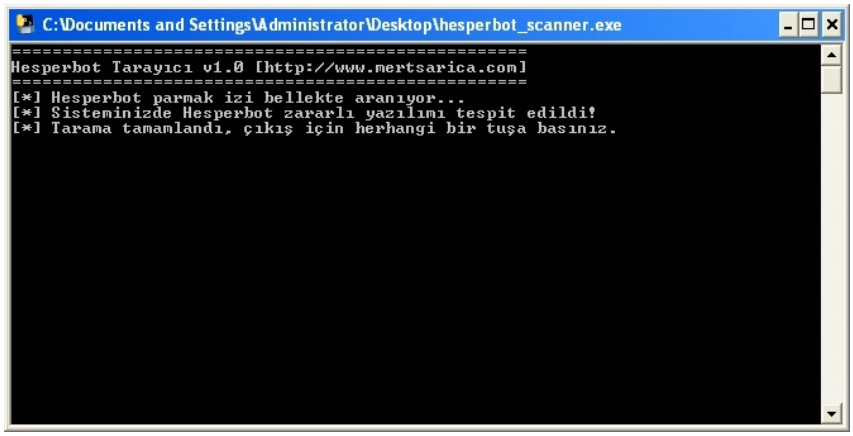
By M.S on November 7th, 2014

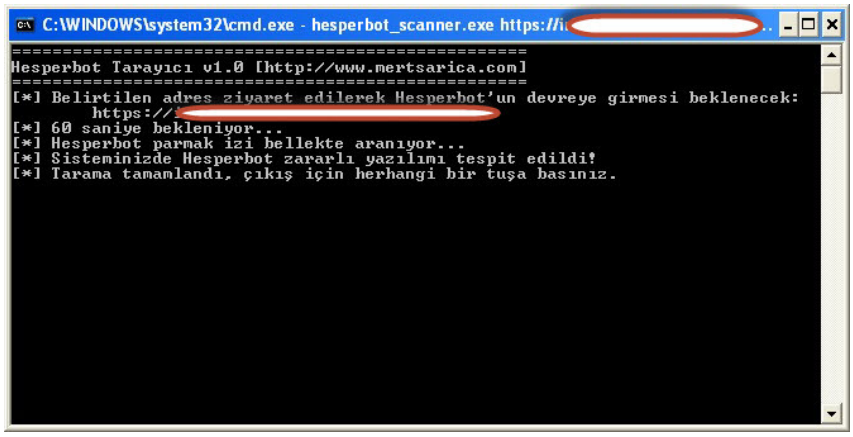
Bildiğiniz gibi son 1.5 senedir vatandaşımız, Hesperbot adındaki ileri seviye internet bankacılığı zararlı yazılımı salgını (#1, #2, #3) ile boğuşmaktadır. Özellikle her yeni salgında siber dolandırıcıların, Hesperbot zararlı yazılımının imza tabanlı antivirüs ve benzer güvenlik yazılımları ve teknolojileri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

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

Aracı iki şekilde kullanabilirsiniz;
1. hesperbot_scanner.exe aracını Hesperbot zararlı yazılımının bulaştığından şüphe ettiğiniz sistem üzerinde çalıştırabilirsiniz.

2. hesperbot_scanner.exe [internet bankacılığı adresi] şeklinde çalıştırarak aracın belirttiğiniz bankanın internet bankacılığı web sayfasını otomatik olarak açmasını, Hesperbot devreye girene kadar bir dakika boyunca beklemesini (devreye girmeme ihtimaline karşı) ve ardından belleği taramasını sağlayabilirsiniz.

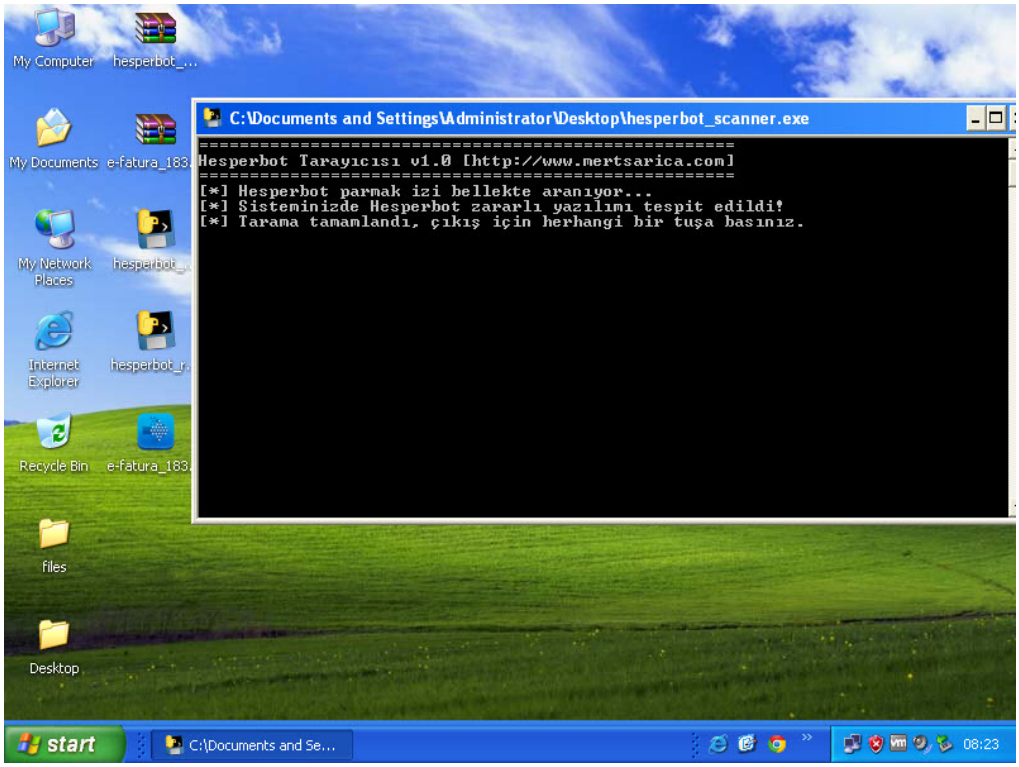




Hesperbot geliştiricilerinin ekmeğine yağ sürmemek için (biraz da onlar uğraşsınlar :)) kaynak kodunu paylaşmadığım Hesperbot Tarayıcısını buradan indirebilirsiniz.

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

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



Aracın kullanımı için aşağıdaki videoyu aşağıdan izleyebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

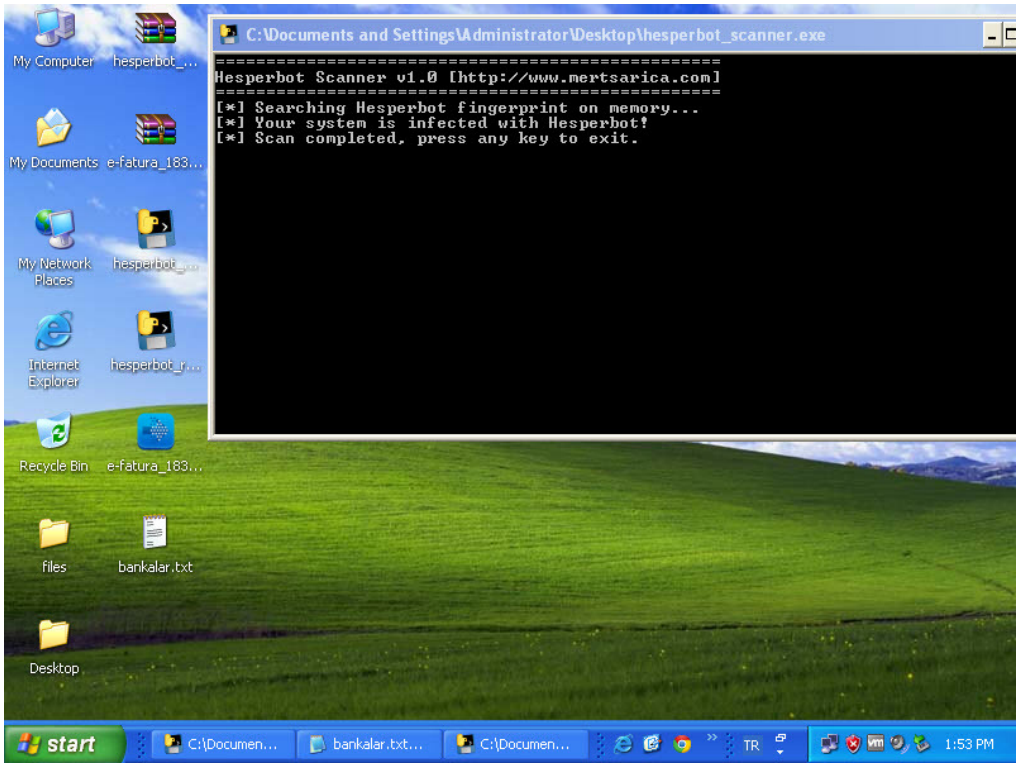
---- ENGLISH ----

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

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 yardımı ile donanım yazılımı güncellemesi esnasında kullanılan komutları tespit etmişler. Daha sonra 2 aydan kısa bir süre içinde donanım yazılımını tersine mühendislik ile analiz ederek, 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.

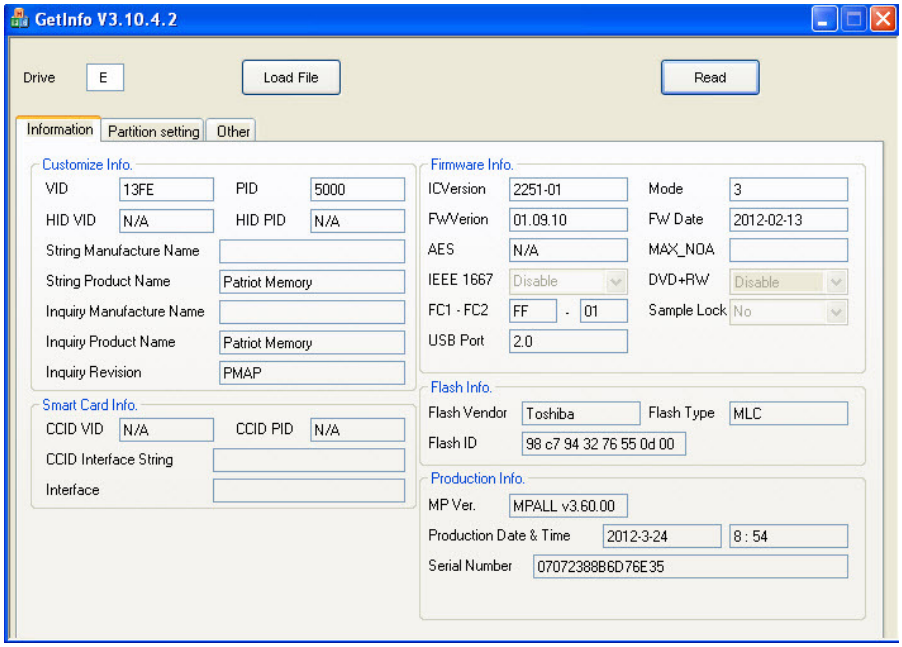
Peki bunun daha önce üzerine yazı yazdığım ve yine hedef sistem üzerinde USB bağlantı noktasından takıldığı taktirde komut çalıştırmaya imkan tanıyan Teensy'den veya USB Rubber Ducky'den ne farkı var ? Pratikte pek bir farkı bulunmuyor. BadUSB ile gerçekleştirilen sosyal mühendislik testlerinde diğerlerine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

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

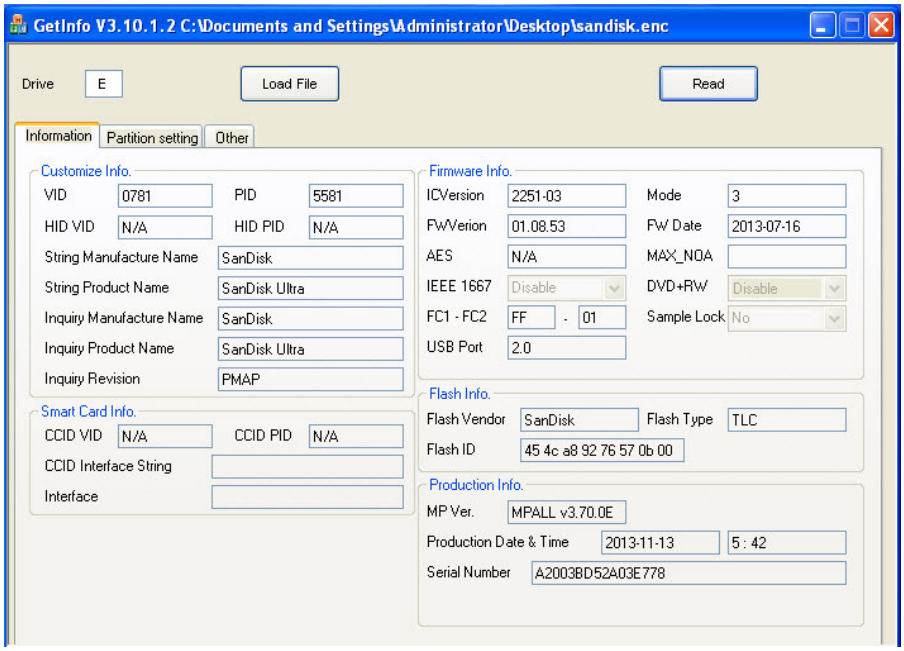
Sunum dosyasına ve kodlara baktıktan sonra ben de bir BadUSB oluşturmak için işe koyuldum. Araştırmacıların kullandığı Phison marka mikrodenetleyiciye sahip Patriot marka Xpress model USB bellek Türkiye'de olmadığı için Amazon'dan sipariş ettim.

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

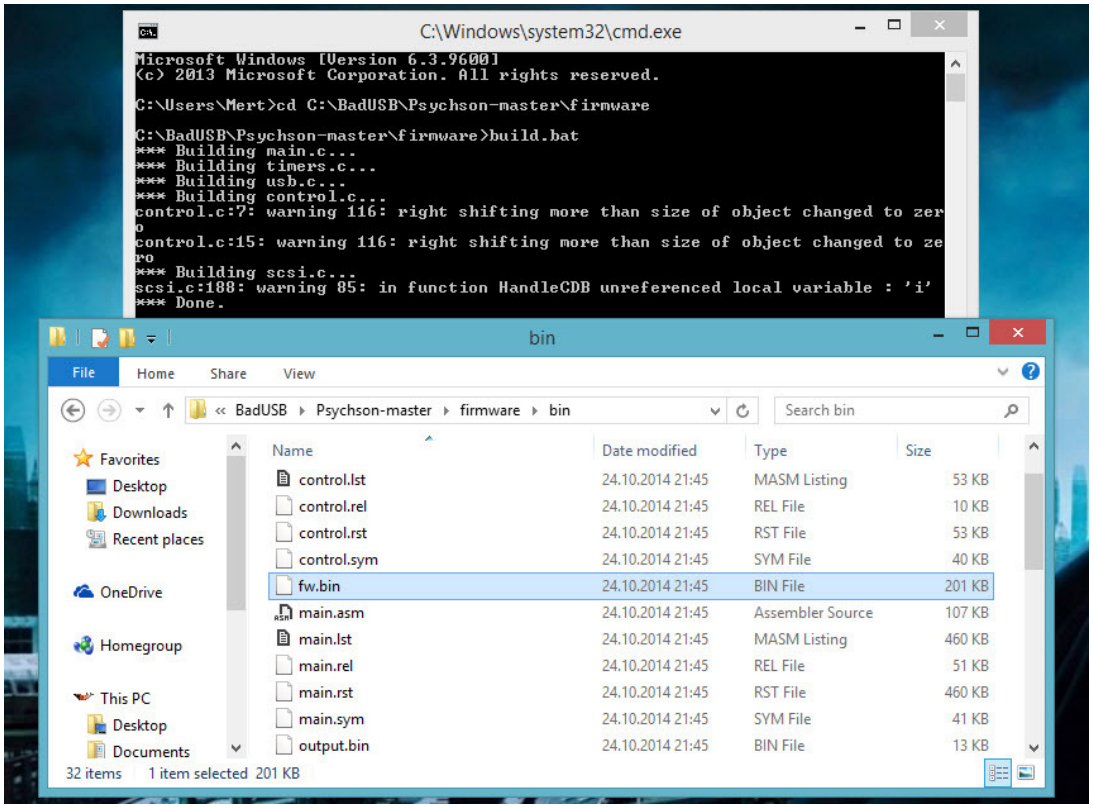
USB bellek geldikten sonra Phison'un modelini GetInfo aracı (veya Chip Easy aracını da kullanabilirsiniz) ile kontrol ettiğimde modelin farklı olması nedeniyle hüsrana uğradım ve bu defa Phison marka PS2251-03 model USB bellek avına çıktım.

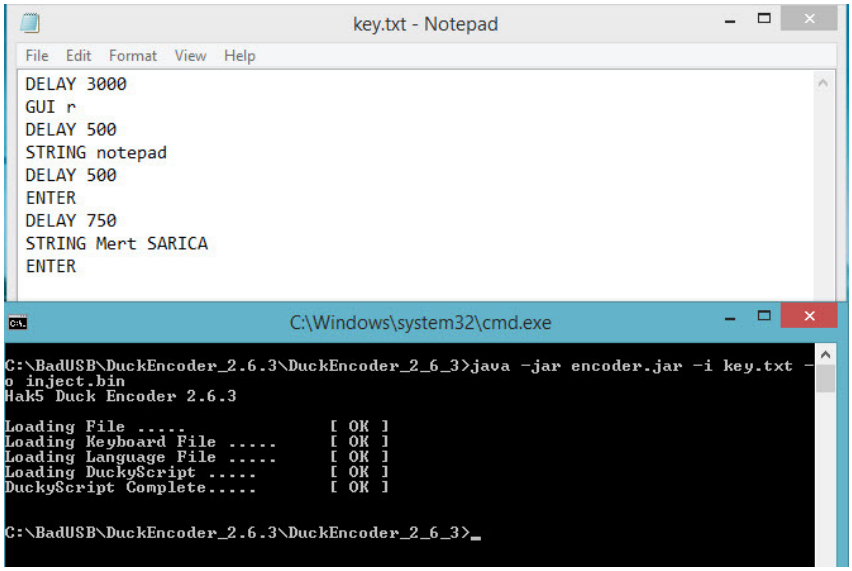


Benim gibi dünyada birçok kullanıcının ava çıkması ve araştırmacılara geri bildirimde bulunmaları sayesinde araştırmacılar, BadUSB olma potansiyeline sahip USB bellekleri bir listede toplamaya karar vermişler. Bu listeyi ara ara kontrol ederken, tesadüfen Teknosa'da gezerken gördüğüm Sandisk Ultra 16 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.

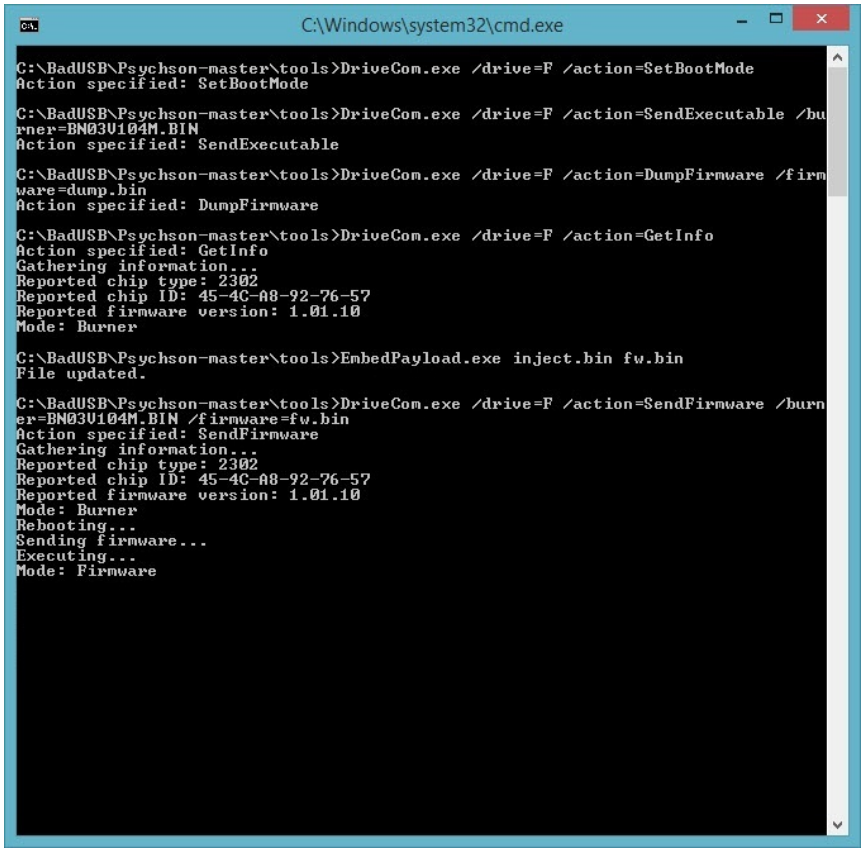


Adımlardan birinde yaptığım dikkatsizlikten dolayı aldığım bu diski çöpe atmak zorunda kaldım :) Ardından bu defa biraz daha temkinli davranarak iki tane daha Sandisk Ultra aldım ve yine bir dikkatsizlik sonucunda disklerinden birini daha çöpe atmak zorunda kaldım. Allah'ın hakkı üçtür diyerek BadUSB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





Sonunda 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.



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

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

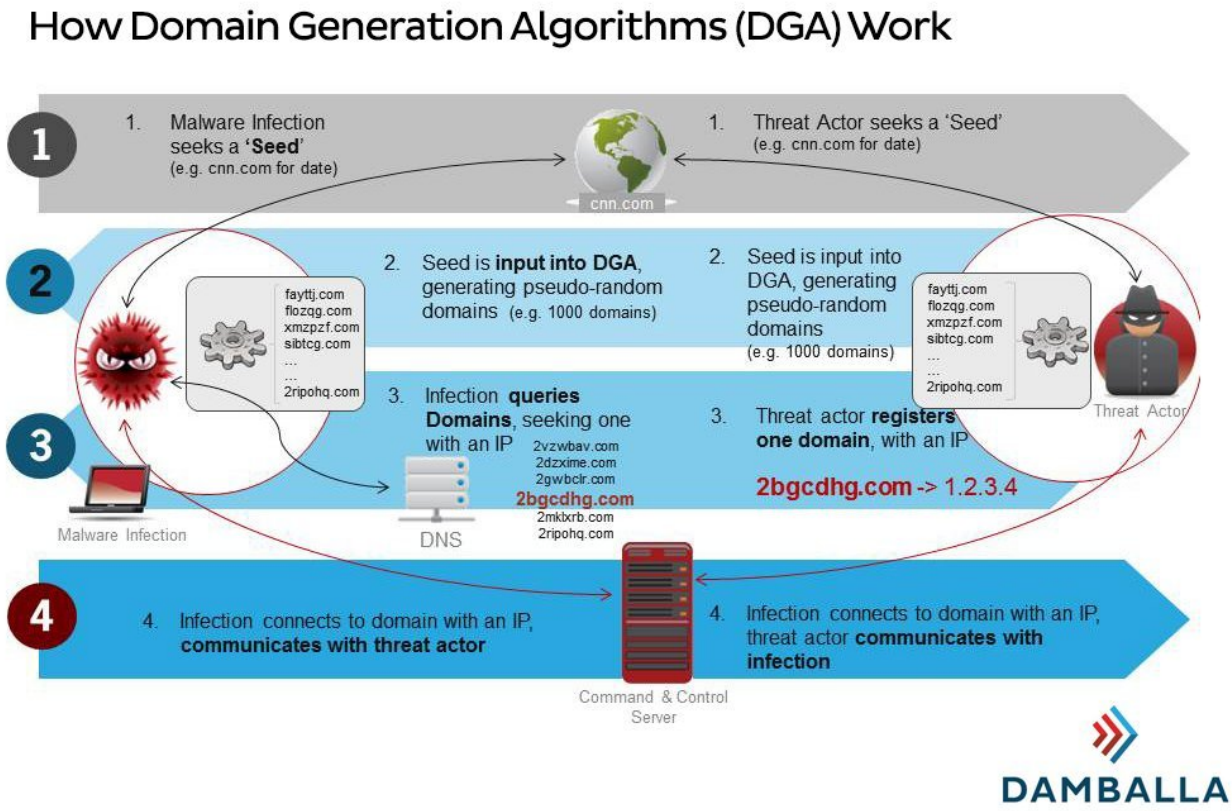
Not: BadUSB'ye dönüştürülmüş USB ile ilgili hazırlamış olduğum videoyu aşağıdan izleyebilirsiniz.

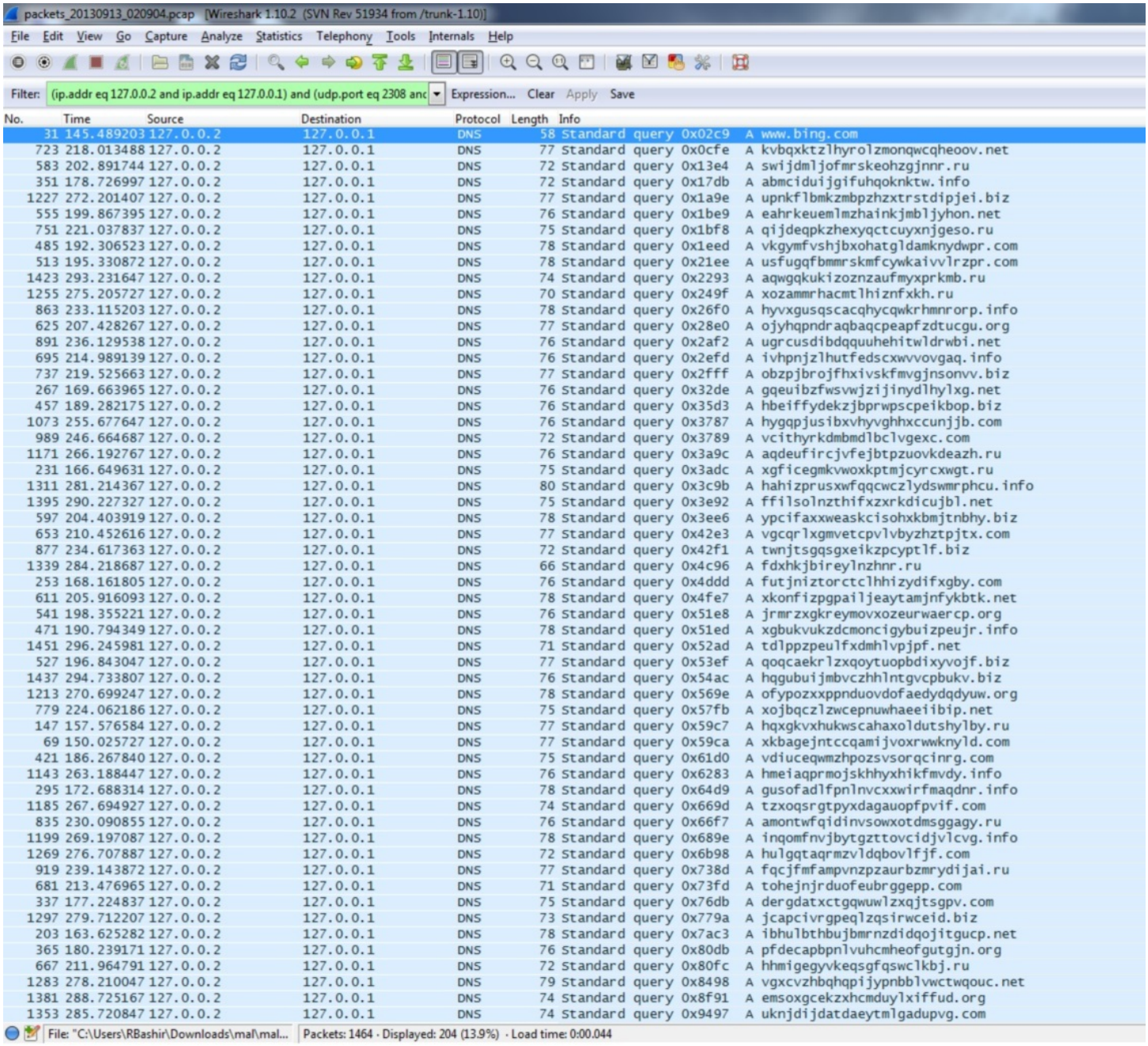
Hesperbot DGA Analizi

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

By M.S on October 1st, 2014

Alan adı üretme algoritması (DGA), zararlı yazılımlar tarafından yeni bir alan adı üretmek amacıyla kullanılan algoritmalardır. 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.





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

Günümüz zararlı yazılımlarında ise DGA, çoğunlukla ana haberleşme yönteminden ziyade yedek yöntem olarak kullanılmaktadır. Örneğin GameOver Zeus zararlı yazılımı DGA'yı, kullandığı ilk iki yöntem çalışmadığı taktirde üçüncü yöntem olarak 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 yani alan adlarının, yazılım geliştiricinden önce kayıt edilebilmesine imkan tanımasıdır. Bu sayede uzmanlar, Conficker örneğinde olduğu gibi zararlı yazılımlar ile ilgili çeşitli bilgileri toplayabilmekte, kimi zaman ise zararlı yazılımları kontrol altına alabilmektedirler.

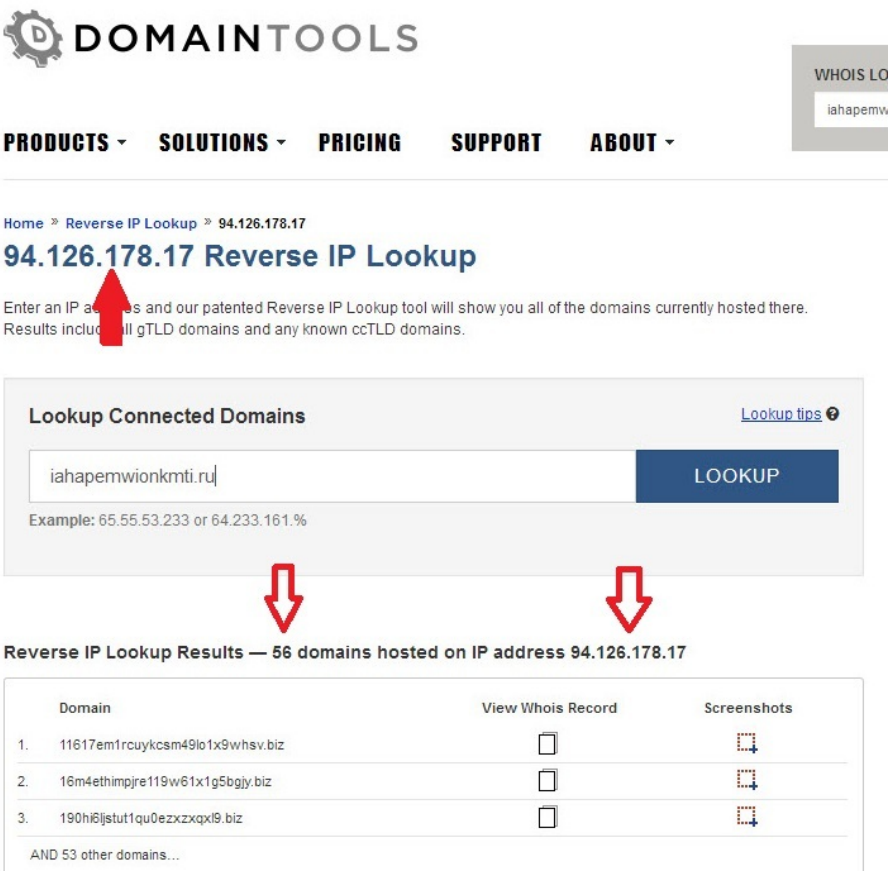
Gündemi, analiz yazılarını takip edenler, ileri seviye Hesperbot bankacılık zararlı yazılımının, 1.5 yıldır ülkemizin ve vatandaşlarımızın üzerinde kara bulut gibi dolaştığını biliyordur. Geçtiğimiz ayın başında Tübitak, Hesperbot ile ilgili yeni bir yazı yayınlayarak bu zararlı yazılımın ülkemizde hala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

> *Bu vesileyle Tübitak Bilgem Siber Güvenlik Enstitüsü'ne, Hesperbot ile mücadele adına verdiği emeklerinden dolayı teşekkür etmek isterim.*

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

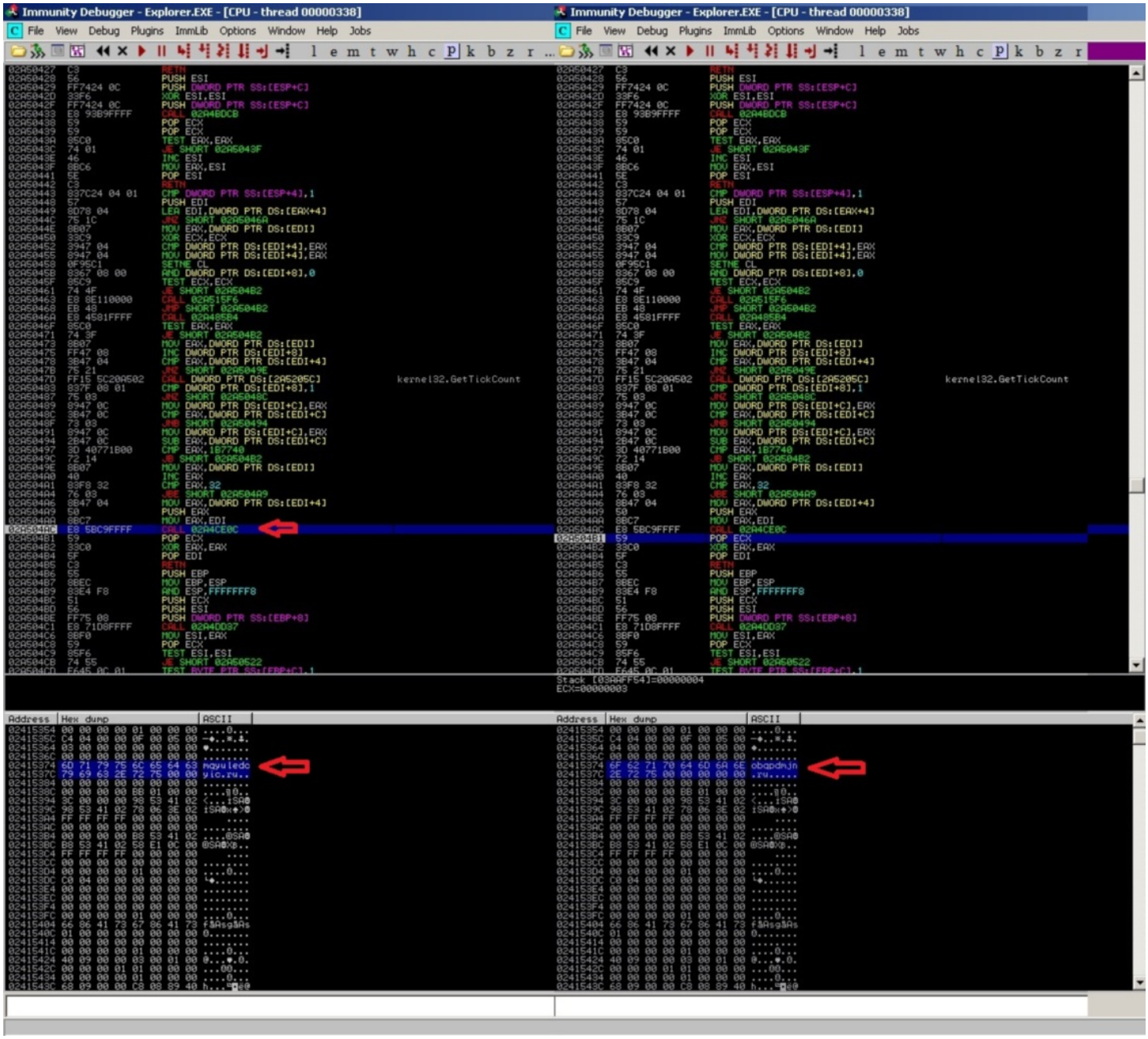
#	Result	Protocol	Host	URL
356	200	HTTP	Tunnel to	www.yahoo.com:443
357	200	HTTPS	www.yahoo.com	/
358	200	HTTP	tools.google.com	/service/update2?w=6:EFH2B5jVGzF8R2tlTLHZGsVhFz0shG_-IACVF03N
359	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
360	502	HTTP	Tunnel to	followtweetertag.com:443
361	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
362	301	HTTP	yahoo.com	/
363	200	HTTP	Tunnel to	www.yahoo.com:443
364	200	HTTP	Tunnel to	www.yahoo.com:443
365	200	HTTPS	www.yahoo.com	/
366	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
367	502	HTTP	Tunnel to	followtweetertag.com:443
368	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
369	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
370	301	HTTP	microsoft.com	/
371	200	HTTP	www.microsoft.com	/
372	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
373	502	HTTP	Tunnel to	followtweetertag.com:443
374	302	HTTP	google.com	/
375	200	HTTP	www.google.com.tr	/?gfe_rd=cr&ei=sq4JVJmFHsao8wfLvICGADA
376	502	HTTP	Tunnel to	followtweetertag.com:443
377	301	HTTP	yahoo.com	/
378	200	HTTP	Tunnel to	www.yahoo.com:443
379	200	HTTP	Tunnel to	www.yahoo.com:443
380	200	HTTPS	www.yahoo.com	/
381	502	HTTP	Tunnel to	followtweetertag.com:443
382	301	HTTP	yahoo.com	/
383	200	HTTP	Tunnel to	www.yahoo.com:443
384	200	HTTP	Tunnel to	www.yahoo.com:443
385	200	HTTPS	www.yahoo.com	/
386	502	HTTP	Tunnel to	followtweetertag.com:443
387	301	HTTP	wikipedia.org	/
388	200	HTTP	www.wikipedia.org	/
389	502	HTTP	Tunnel to	followtweetertag.com:443
390	301	HTTP	microsoft.com	/
391	200	HTTP	www.microsoft.com	/
392	502	HTTP	Tunnel to	followtweetertag.com:443
393	301	HTTP	yahoo.com	/
394	200	HTTP	Tunnel to	www.yahoo.com:443
395	200	HTTP	Tunnel to	www.yahoo.com:443
396	200	HTTPS	www.yahoo.com	/
397	302	HTTP	cache.pack.google.com	/edgedl/update2/1.3.24.15/GoogleUpdateSetup.exe
398	200	HTTP	Tunnel to	iahapemwionkmti.ru:443
399	200	HTTPS	iahapemwionkmti.ru	/g



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

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

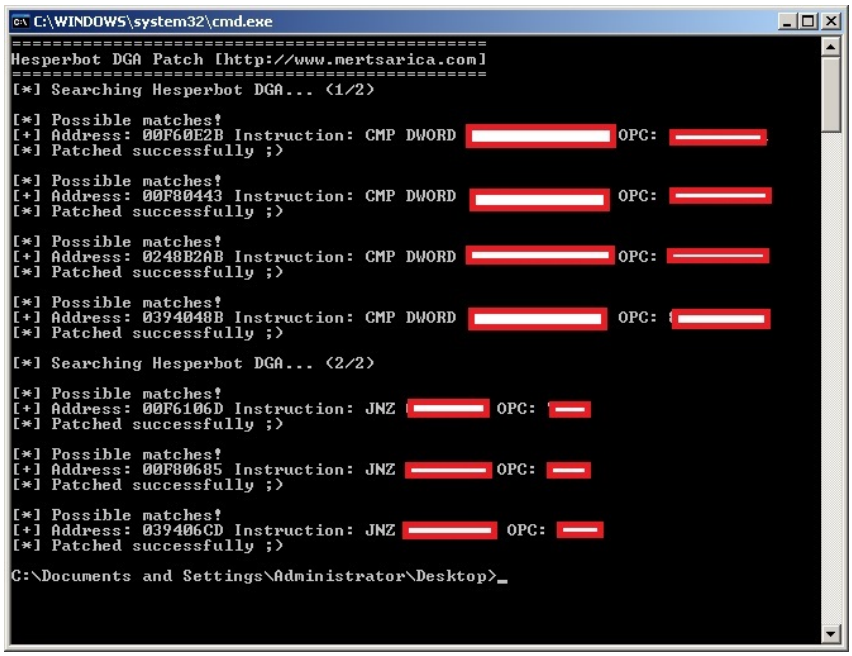
DGA'nın fonksiyonunu bulup incelediğimde ve dallanıp budaklanan alt fonksiyonlarını gördüğümde önümde izlemem gereken iki yol vardı. Birincisi ya tüm fonksiyonların ve komutların üzerinden teker teker geçecektim ve DGA'ya göre alan adı üreten bir kod yazacaktım veya DGA fonksiyonunu yamayarak (patching),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



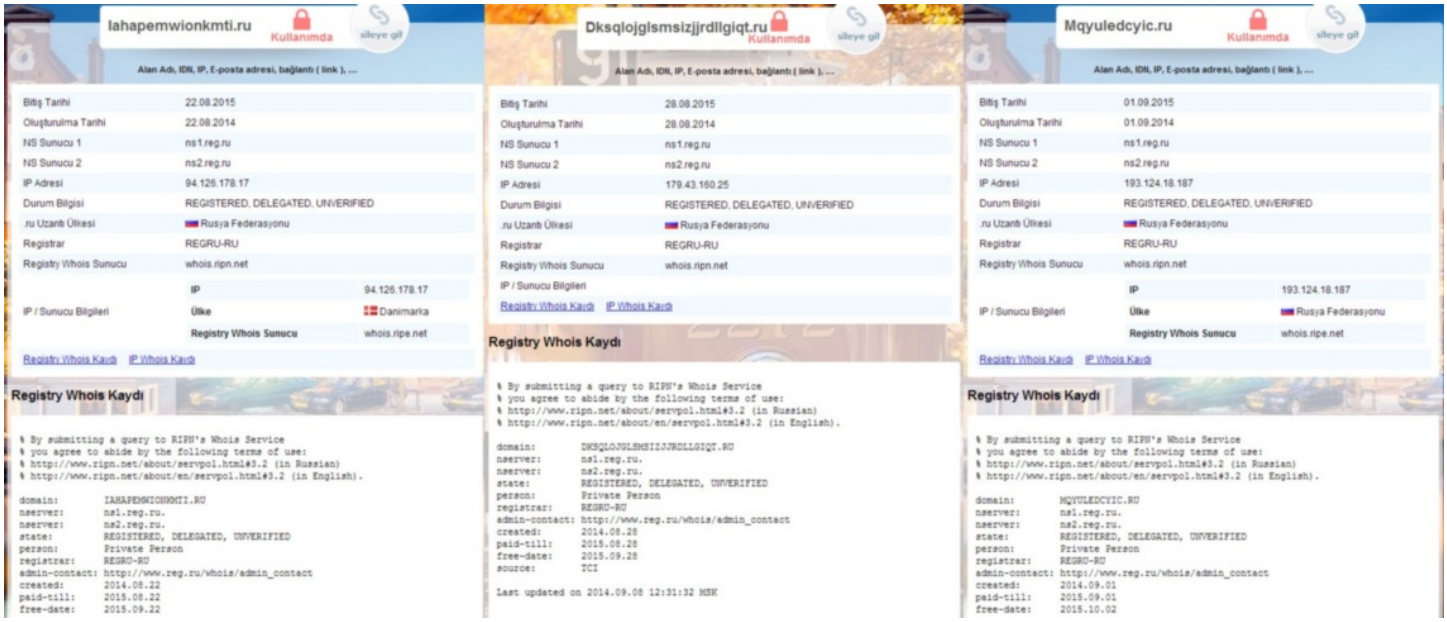
Hesperbot paketlenmiş (packed) bir zararlı yazılım olduğu için DGA fonksiyonunu yamamak için ya paketini açıp, çalışabilir hale getirecek ve gerekli değişiklikleri (patching) disk üzerindeyken yapacaktım ya da bellekte çalışır haldeyken yapacaktım. Yine fazla zahmete girmek yerine (sanırım tembelim) ikinci yolu, bellek üzerinde değişik yapmayı seçtim. Bellek manipülasyonu için eskiden pydbg aracını kullanıyordum fakat zaman içinde geliştirimesine 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 çalıştırdım ve Hesperbot'un kısa bir süre içinde yeni alan adlarını üretmesini sağlayarak mutlu sona ulaştım. (Hesperbot geliştiricilerinin ekmeğine yağ sürmemek için bazı kısımlar sansürlenmiştir.)



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	dksqlojglsmsizjjrdllgiqt.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	ueizvrprmwmdyejmhkycig.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	mvpwppgsujt.ru:443
4276	502	HTTP	Tunnel to	qhreuqyk.ru:443
4277	502	HTTP	Tunnel to	wjikevjm.ru:443
4278	502	HTTP	Tunnel to	agxqstwcoc.ru:443
4279	502	HTTP	Tunnel to	trzxvhstxnthwccego.ru:443
4280	502	HTTP	Tunnel to	oibldgaj.ru:443
4281	502	HTTP	Tunnel to	hkxjpbah.ru:443
4282	502	HTTP	Tunnel to	hkpjfcip.ru:443
4283	502	HTTP	Tunnel to	gstbidaxyepl.ru:443
4284	502	HTTP	Tunnel to	rbmccpnyjjsmhg.ru:443
4285	502	HTTP	Tunnel to	qfqyqwzqqxmevjjtwrmsgsg.ru:443
4286	502	HTTP	Tunnel to	ytigdmjmkhmaavjpyfimro.ru:443
4287	502	HTTP	Tunnel to	uxzusbcu.ru:443
4288	502	HTTP	Tunnel to	ejmlcqdjijixzfn.ru:443
4289	502	HTTP	Tunnel to	difnjbmlrezxkiwyjhqknja.ru:443
4290	502	HTTP	Tunnel to	qcnqcqiy.ru:443
4291	502	HTTP	Tunnel to	phplstknpzvzxaakybc.ru:443
4292	502	HTTP	Tunnel to	xcofeihllcuzdvbsduugpjl.ru: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	rysiakzkrkwyxhzxlqidnekd.ru:443
4299	502	HTTP	Tunnel to	kivhkjgvsephj.ru:443
4300	502	HTTP	Tunnel to	yvncjjmqkrt.ru:443
4301	502	HTTP	Tunnel to	sykrqgfhekgtplpi.ru:443
4302	502	HTTP	Tunnel to	mdfftmsx.ru:443



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

Linux'te Zararlı Yazılım Analizi için Faydalı Araçlar

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

By M.S on September 1st, 2014

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

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

Fakat zararlı yazılım analizi ile ilgili kitaplara, eğitimlere, yazılara 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 etmek istediğiniz zaman, Linux'e kıyasla çok daha fazla araç bulmanız da bu sebepten ötürü şaşırtıcı değildir.

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

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

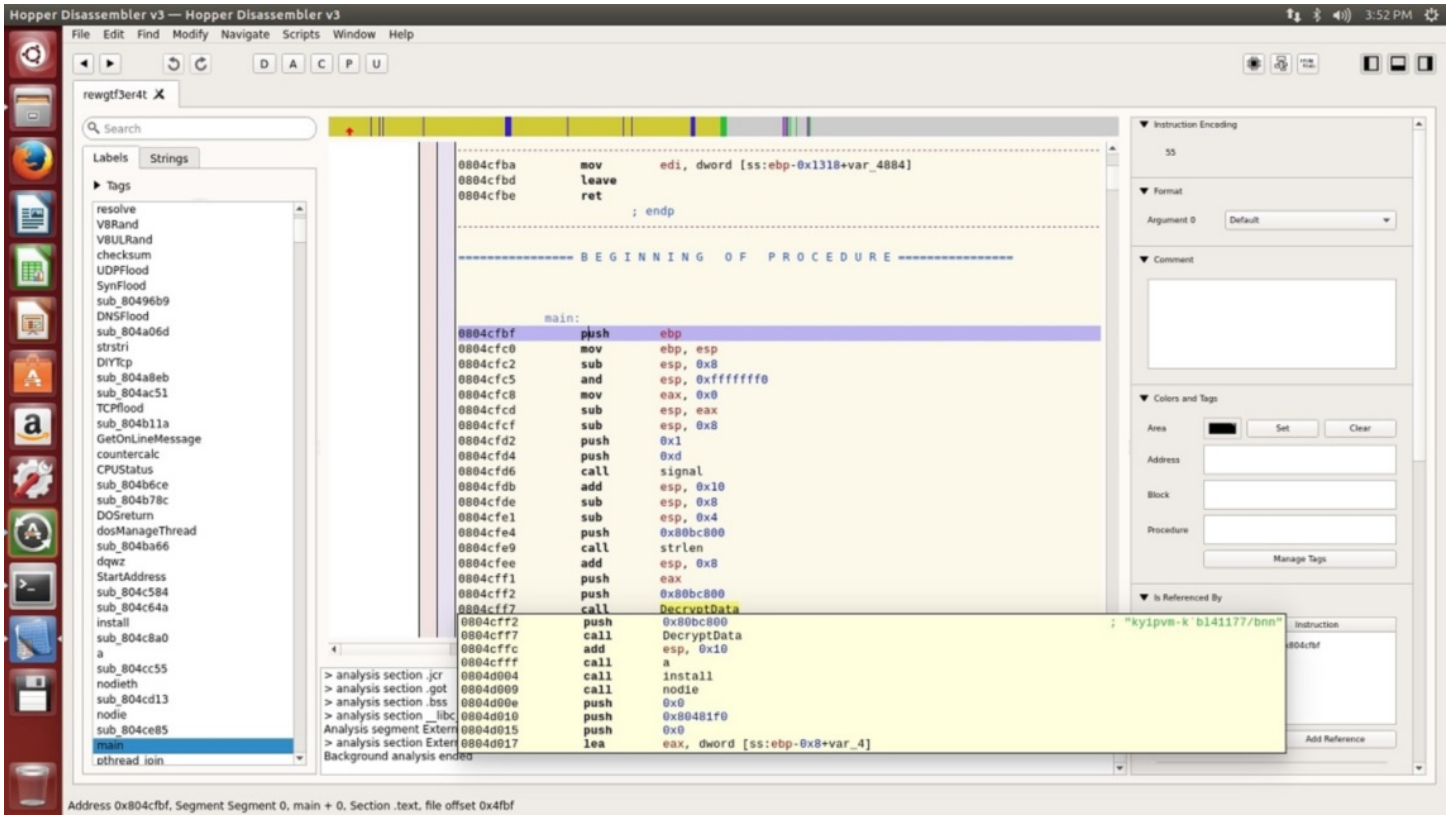
İçinizi çok daraltmadan, OllyDbg / Immunity Debugger ve IDA Pro'ya alternatif olarak zararlı yazılım analizi ve tersine mühendislik için Linux üzerinde kullanabileceğiniz, benim de çok işime yarayan iki araçtan kısaca bahsetmek istiyorum; EDB ve Hopper

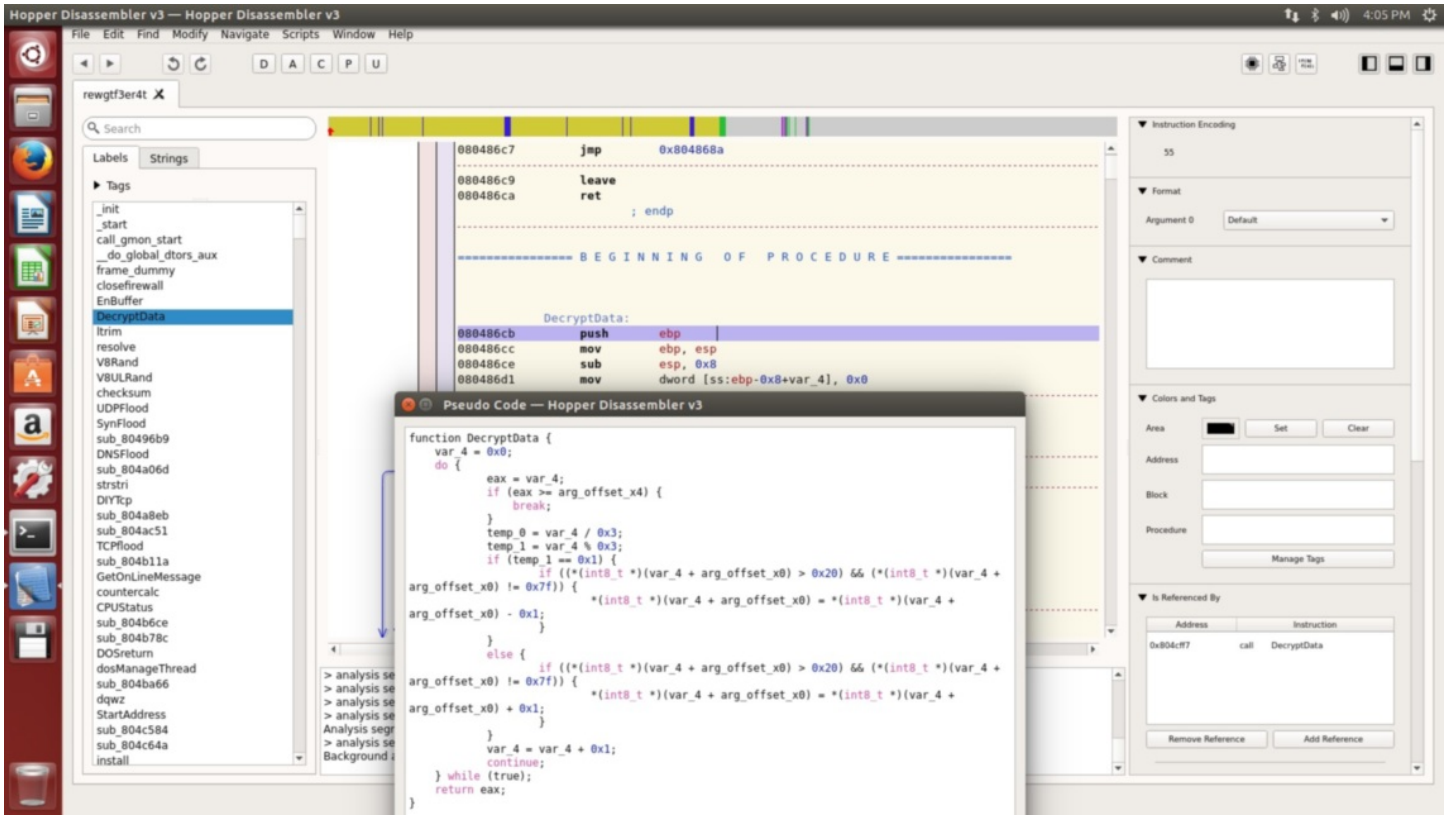
EDB: Windows'ta OllyDbg ile sıkça kod analizi yapan kahramanımız Evan, günün birinde Linux'te OllyDbg gibi kullanışlı bir hata ayıklayıcıya ihtiyaç duyar, bulamaz ve EDB'yi geliştirmeye başlar. Windows'ta OllyDbg kullananlar için biçilmiş kaftan olan EDB ile ELF dosyalarını hem disassemble edebilir hem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

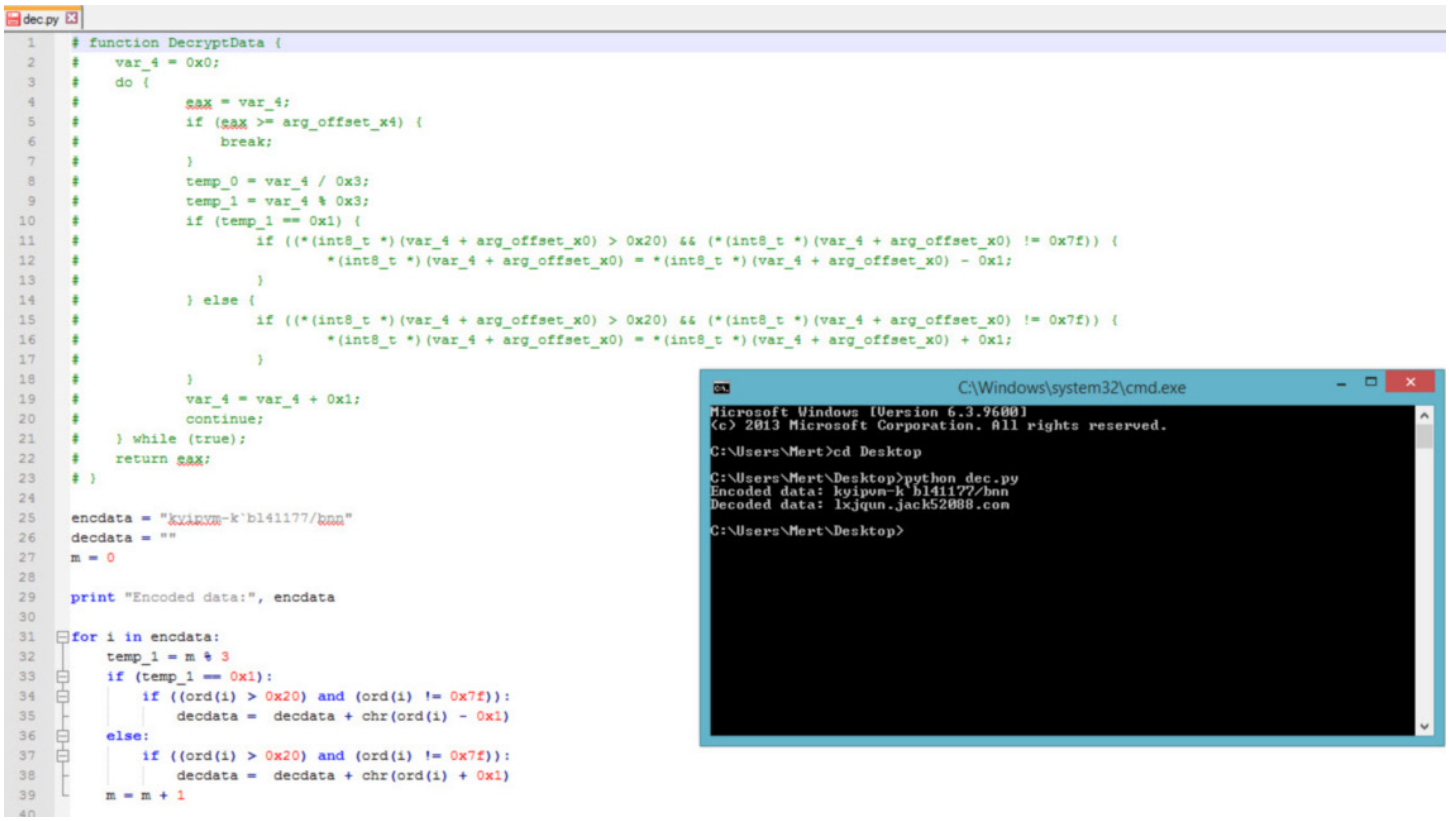
Hopper: Hopper, IDA Pro'ya alternatif olarak kullanabileceğiz, bütçenizi çok zorlamayacak (89$), Mac OS X'te de çalışabilen, hem hata ayıklayıcı, hem disassembler hem de sözde (pseudocode kod çeviricisi (decompiler) olarak kullanabileceğiniz bir araçtır. Python desteğine ve Objective-C desteğine de sahip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

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

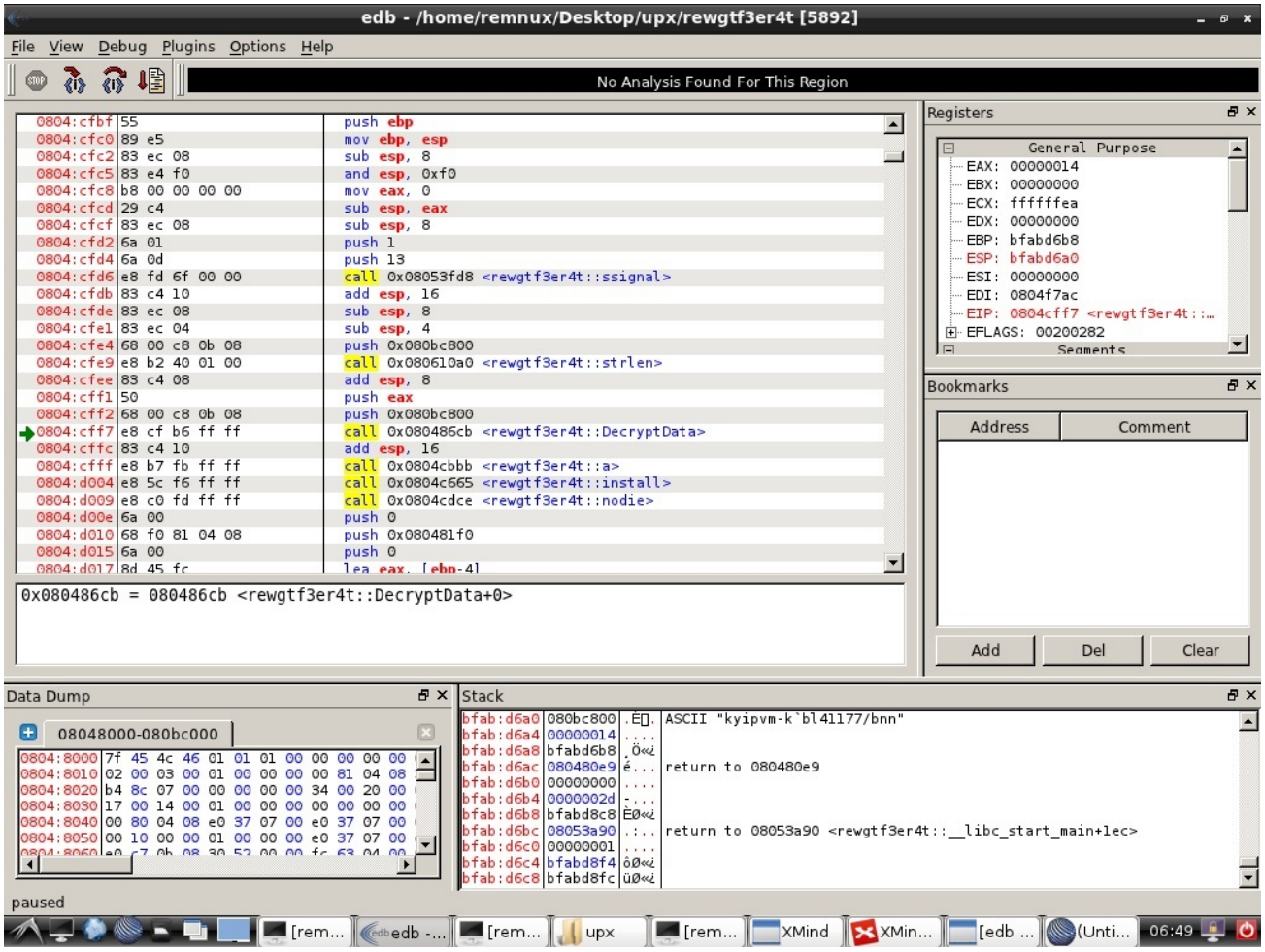
Hopper ile ELF dosyasına göz attığımızda yapacağımız ilk iş programın başlangıç fonksiyonu olan main fonksiyonuna göz atmak olacaktır. Bu fonksiyona göz attığımızda şüpheli DecryptData fonksiyonunun çağrılmadan önce yığına (stack) gizlenmiş veriyi (kyipvm-k`bl41177/bnn) kopyalandığını görebiliyoruz.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

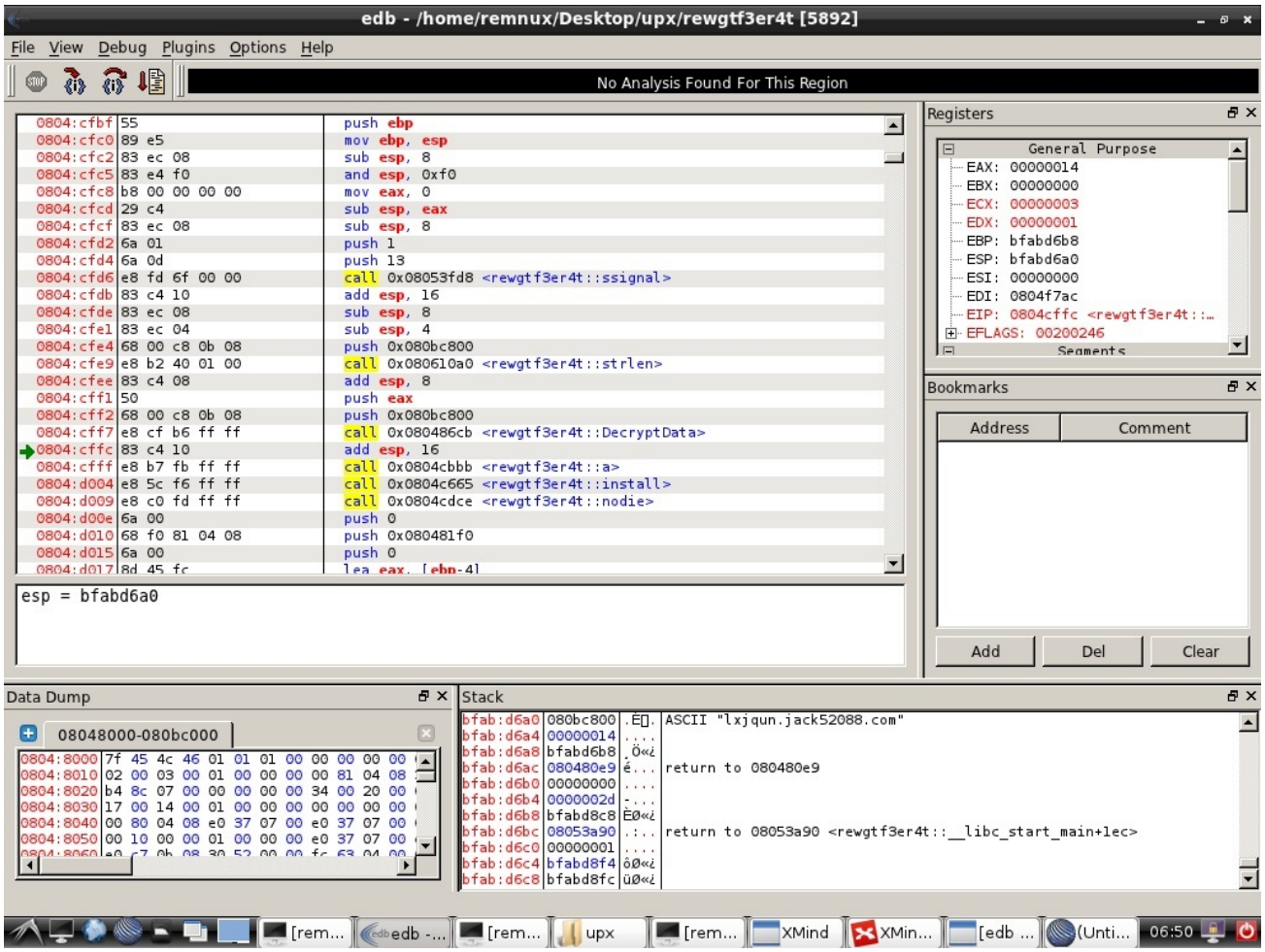






Disassembler ve programlama ile uğraşmak istemiyorum, kısa yoldan OllyDbg'da olduğu gibi fonksiyonun (DecryptData) üzerinden hızlıca geçerek fonksiyonun gizlenmiş veriyi çözmesini sağlayayım diyenler için ise EDB hemen imdadımıza yetişiyor. EDB'ye zararlı yazılımı yükledikten sonra main fonksiyonuna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





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

Kullanıcı Dostluğu vs Kullanıcı Güvenliği

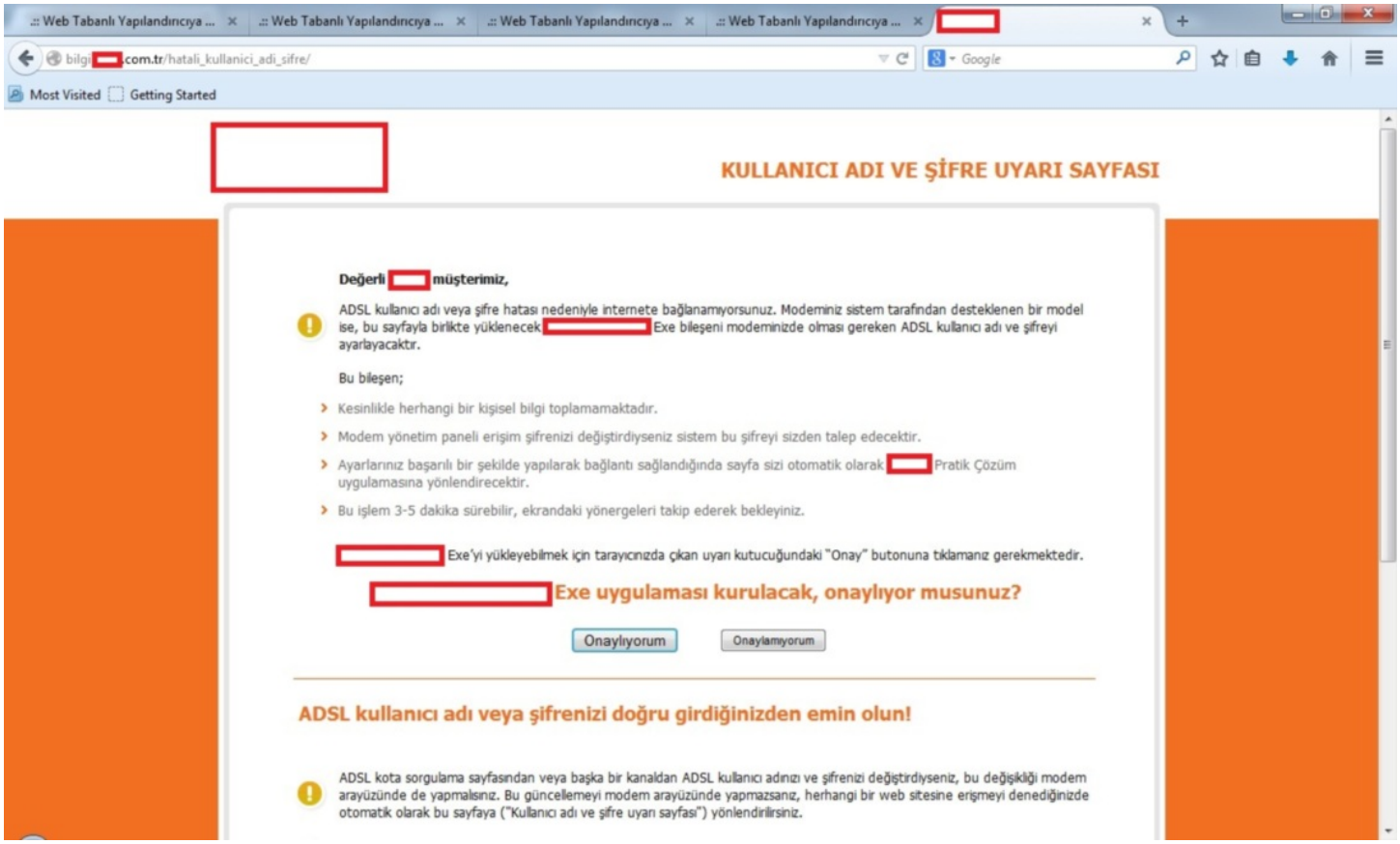
Source: https://www.mertsarica.com/kullanici-dostlugu/

By M.S on August 1st, 2014

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

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

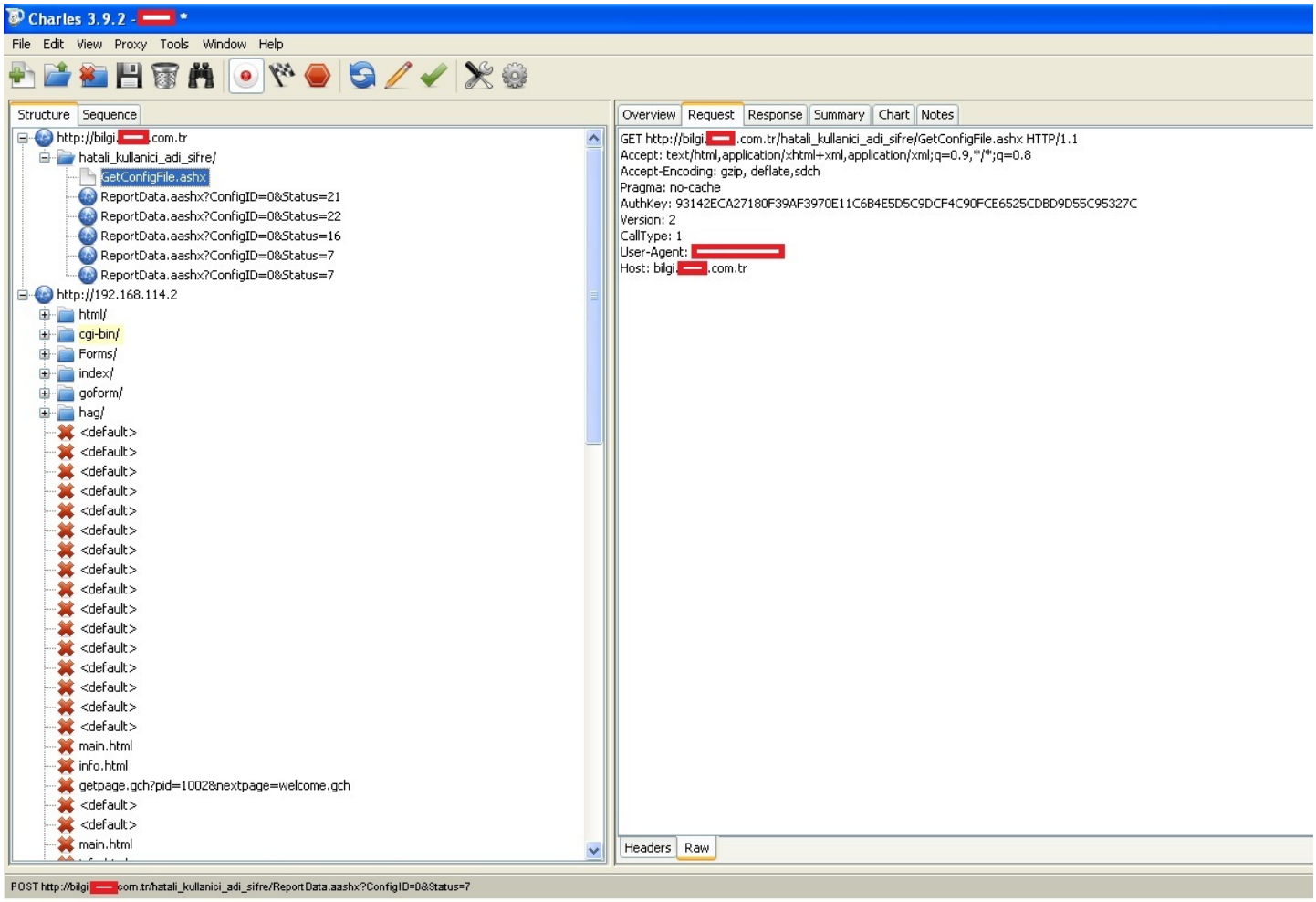
Çalışmalar esnasında modemi fabrika ayarlarına döndürdüğümde ISS'in beni şifre unuttum sayfasına yönlendirdiğini gördüm. Bu sayfada, ISS'in hazırlamış olduğu uygulamayı indirip, çalıştırmam durumunda, modemimin ADSL kullanıcı adı ve şifre bilgilerimin bu uygulama tarafından otomatik olarak modeme girileceği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

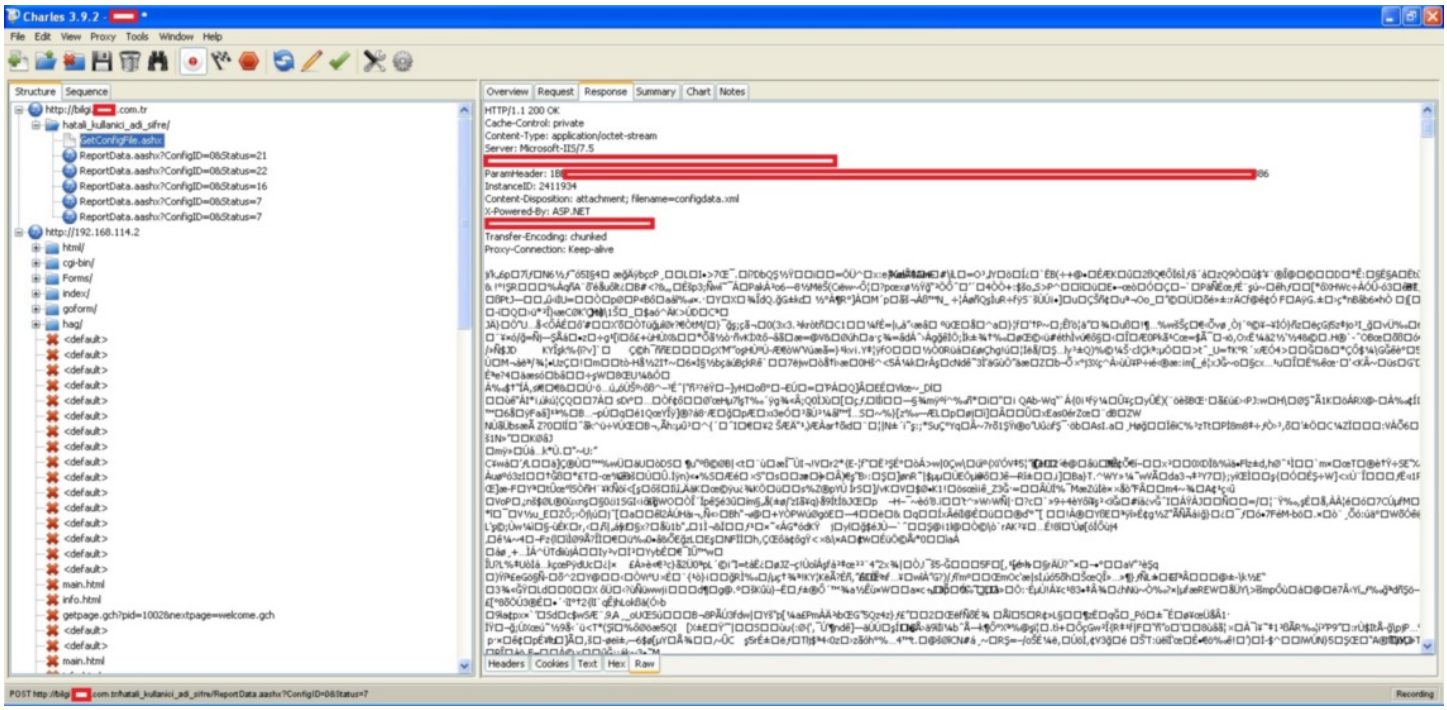


Yazımın başında da belirttiğim gibi bu tür otomatik şifre hatırlama, şifre girme gibi kullanıcı dostu araçlar, güvenli tasarlanmadığı taktirde güvenlik zafiyetlerine yol açabildiği için uygulamayı sistemime indirip, Immunity Debugger ve Charles Proxy araçları ile kısaca incelemeye karar verdim. Uygulamayı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

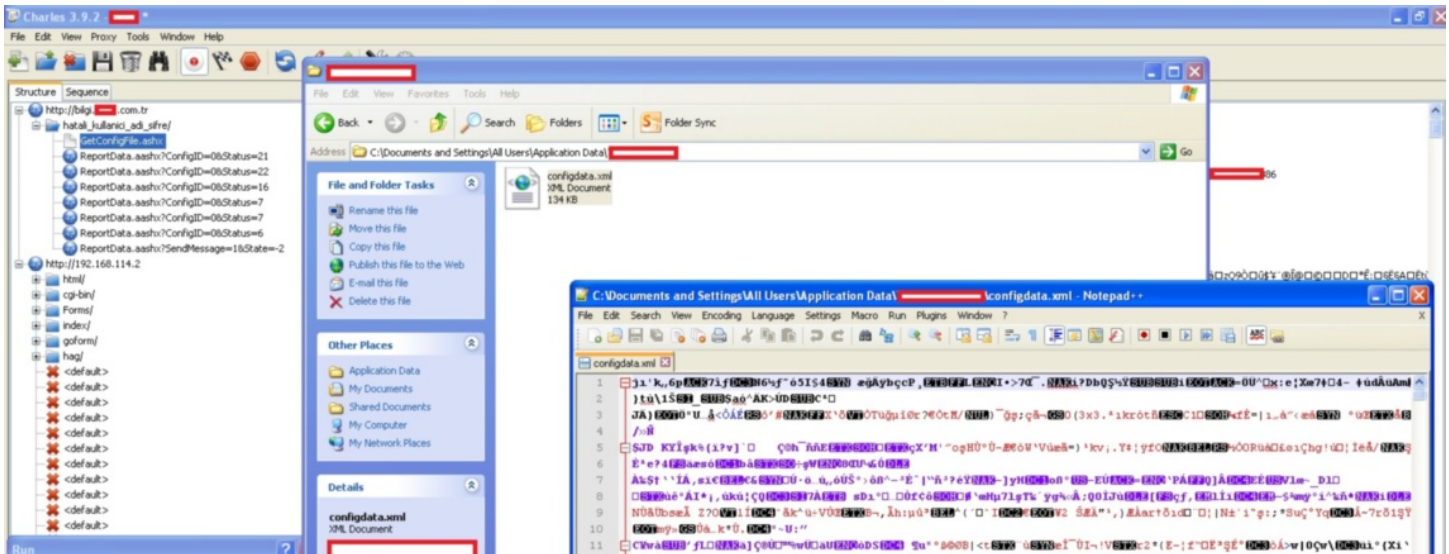

Bu uygulamanın amacı modeminize [redacted] ADSL Kullanıcı Adı ve Şifrenizi otomatik olarak ayarlamaktır.
Çalıştırmak için Başlat'a tıklayınız.
BAŞLAT
KAPAT


Modeminize erişim sağlanıyor, lütfen bekleyiniz.
BAŞLAT
İPTAL


Charles 3.9.2 - [redacted] *
File Edit View Proxy Tools Window Help
Structure Sequence
http://bilgi[redacted].com.tr
hatali_kullanici_adi_sifre/
GetConfigFile.ashx
ReportData.aashx?ConfigID=0&Status=21
ReportData.aashx?ConfigID=0&Status=22
ReportData.aashx?ConfigID=0&Status=16
ReportData.aashx?ConfigID=0&Status=7
ReportData.aashx?ConfigID=0&Status=7
http://192.168.114.2
html/
cgi-bin/
Forms/
index/
goform/
hag/
<default>
main.html
info.html
getpage.gch?pid=1002&nextpage=welcome.gch
main.html
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
Headers Raw
POST http://bilgi[redacted].com.tr/hatali_kullanici_adi_sifre/ReportData.aashx?ConfigID=0&Status=7



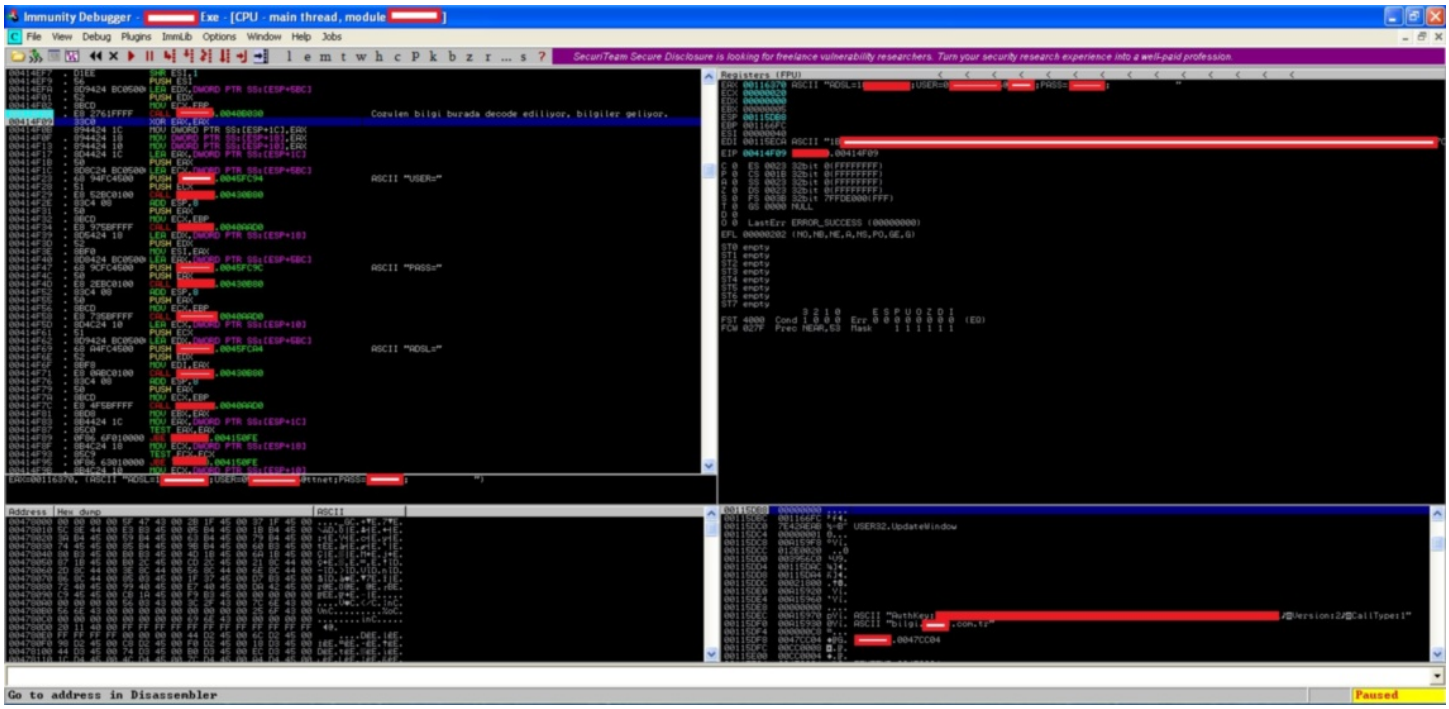
Uygulamayı incelemeye devam ettiğimde, uygulamanın sunucudan indirdiği şifreli içeriği, dosya sistemi üzerinde configdata.xml adı altında bir dosyaya şifreli olarak kaydettiğini gördüm.

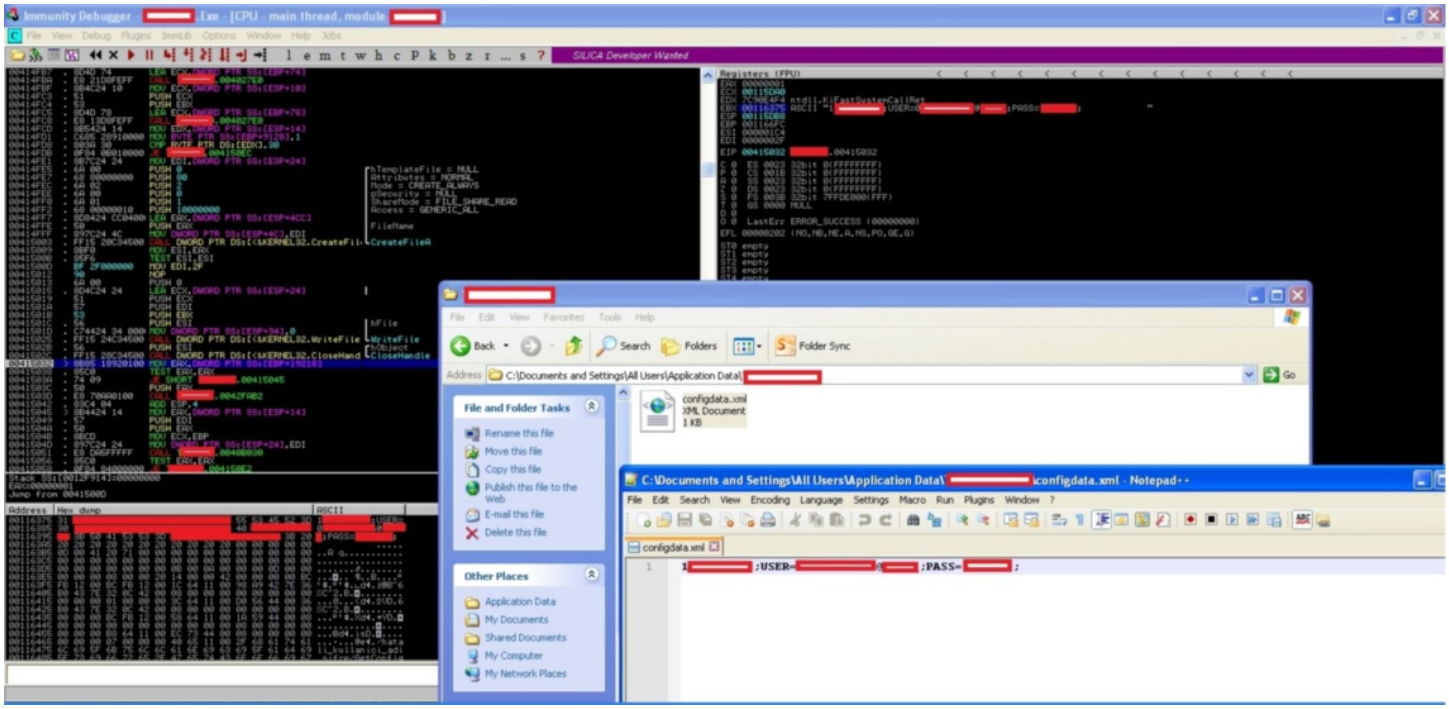


Bu uygulamanın doğru ADSL kullanıcı adı ve şifremi nasıl indirdiğini ve bu bilginin bu şifreli dosya içinde yer alıp almadığını öğrenmek için uygulamayı Immunity Debugger ile incelemeye başladım. Web trafiği ile ilgili fonksiyonları biraz inceledikten sonra indirilen bu şifreli içeriğin aslında hangi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

Sistemime bulaşmış bir zararlı yazılımın, şifreli ADSL kullanıcı adı ve şifremin açık/şifresiz haline ulaşmasının ne kadar kolay olup 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 izleyebileceği yollar üzerine biraz düşünmeye başladım. Aklıma gelen ilk üç yol; 1-) Şifre çözme fonksiyonunun algoritmasını anlayıp, başka bir programlama diline çevirecek 2-) Code cave yöntemi ile akışı kodun farklı bir yerinde oluşturduğu koda gönderecek 3-) Uygulama üzerinde diske veri yazmak için kullanılan API'ler (WriteFile, CreateFile) var ise uygulama yamalanarak (patch), şifrenin çözülmüş halinin bu API'lere yönlendirilecek ve şifreli bilgiler açık olan diske yazılacak

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





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

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

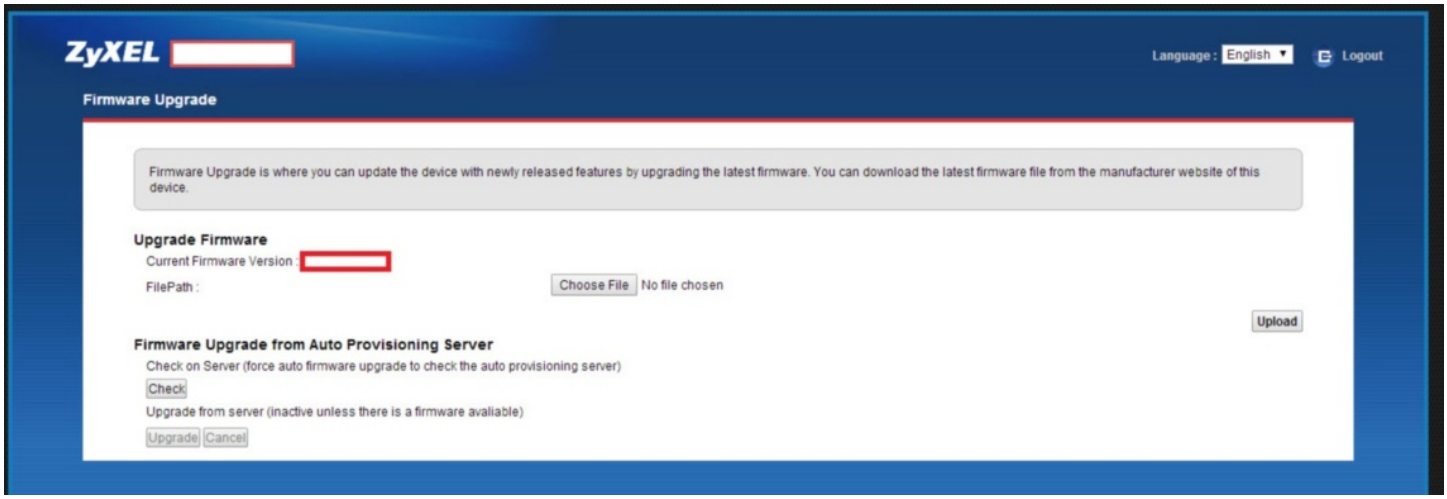
Hediye Modemler Ne Kadar Güvenli?

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

By M.S on July 1st, 2014

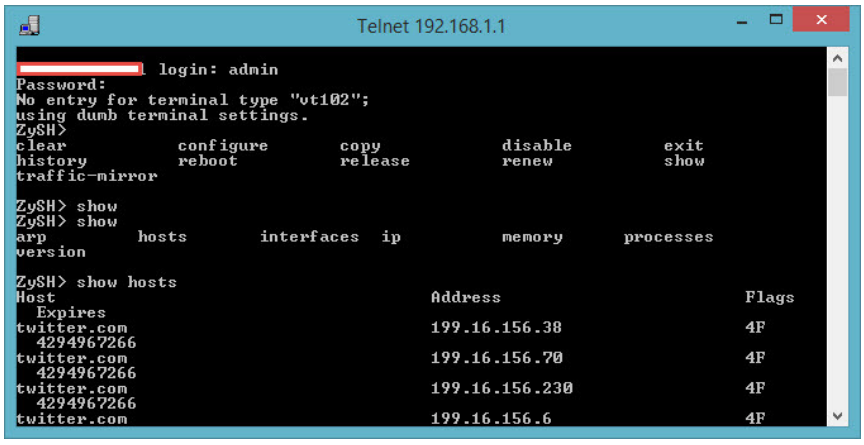
Bir öğle vakti iş arkadaşlarımla yürürken, internet servis sağlayıcılarının (ISS) müşterilerine dağıttığı modemlere ISS çalışanlarının uzaktan bağlanabileceği ile ilgili bir konu açılıverdi. Ben de cihaz yazılımının (firmware) güncellenmesi durumunda ISS'in modemlere nasıl erişim sağlayabileceklerini sorgularken, bir arkadaşım cihaz yazılımı güncellemesinin de ISSler'in sunucuları üzerinden gerçekleştiğini belirtti. NSA'in cihaz yazılımlarına (firmware) arka kapı yerleştirdiği, devletimizin ISSler üzerinden SSL 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 modemi kullanan ve bu konuyu irdelememiş bir güvenlik uzmanı olarak eve gider gitmez Zyxel marka modemime kısaca göz atmaya karar verdim.

İlk yaptığım iş modemin 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 modemin tüm trafiğini izleyecektim (sniff) ve ipucu elde etmeye çalışacaktım ya da modemin arabirimi (console) üzerinden komutlar ile bunu öğrenecektim. Kolay yoldan ilermeye karar vererek modeme telnet ile eriştim ve desteklediği komutları teker teker incelemeye başladım.

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

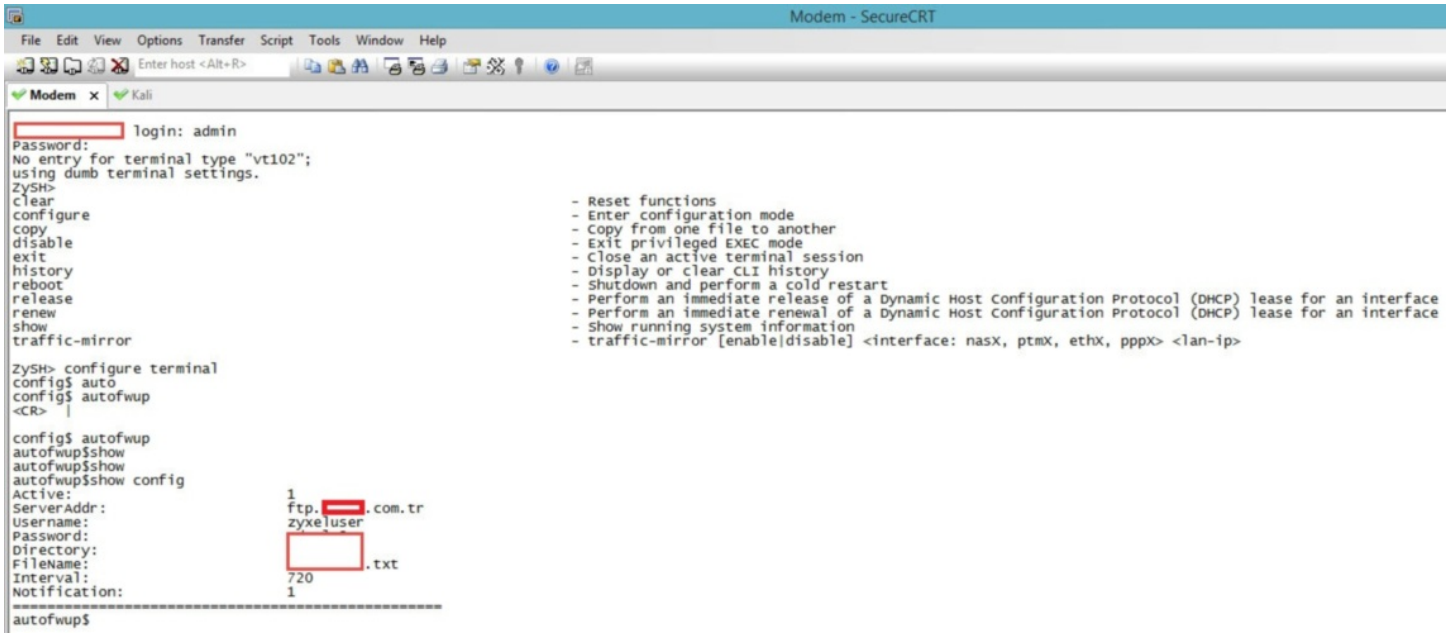


Amacım güncel cihaz yazılımının nereden kontrol edildiği bilgisini öğrenmek olduğu için, modemin web arayüzünden cihaz yazılımını kontrol et butonuna bastım ve ardından telnet arabirimi üzerinden show hosts komutunu çalıştırarak, cihaz yazılımının kontrol edildiği sunucuyu aramaya başladım. Çok geçmeden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

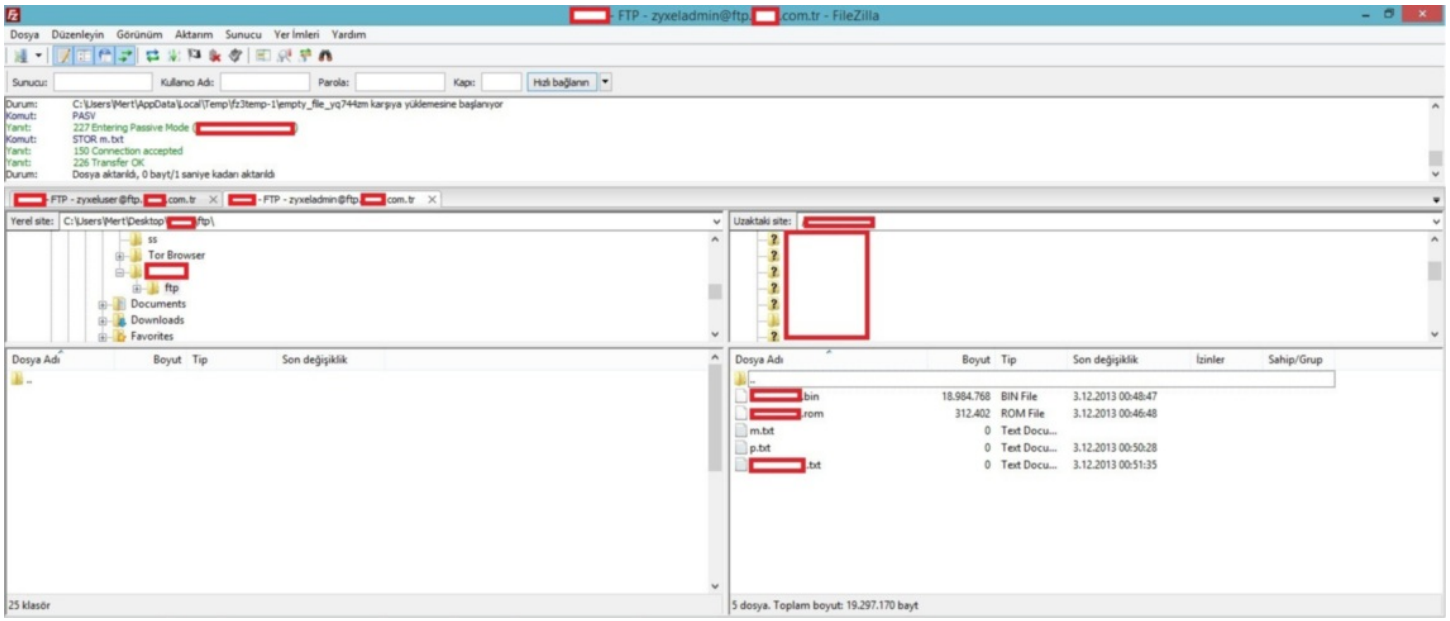
1- Trafiğinizi izleyen NSA, cihaz yazılımı kontrol butonuna basıldıktan sonra sunucudan size gelen cihaz yazılımını arka kapı yüklü olan bir yazılım ile değiştirebilir mi ?

2- FTP kullanıcı adı ve şifresi 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 autofwup komutunun FTP sunucusuna bağlanmak için gerekli bilgileri (kullanıcı adı: zyxeluser) gösterdiğini buldum.



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



ISS'in müşterilerinin güvenliği adına hemen bu durumu ISS yetkilileri ile paylaşmaya (responsible disclosure) karar verdim. Paylaşımda 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 bilgisi paylaşılmıştı. (Kendilerine hem hızlı geri dönüş yaptıkları hem de aksiyon aldıkları için teşekkür etmeyi ihmal etmeyelim.)

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

1- FTP üzerinden cihaz yazılımı güncellemesi yedek yöntem ise yazılımı kontrol et butonuna basıldığında neden birincil yöntem kullanılmıyordu ?
2- Sosyal mühendislik saldırısı ile hedef kullanıcıya bir e-posta gönderilse ve yeni güncelleme için bu botuna basın denilse ve öncesinde de bu FTP sunucusunda ilgili yazılım başka bir zararlı yazılım ile değiştirilse (imzalı olduğu düşünülse) modem yükleme yapmayacak mıydı ?

3- Zyxel marka modemler dışında diğer marka modemler de aynı şekilde FTP sunucusu üzerinden bu kontrolü yapıyor muydu ?

4- Cihaz yazılımı kontrolü, Zyxel marka modemler dışında diğer marka modemler tarafından da yapılıyor mu ?

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

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Rehber Hırsızı Hesperbot

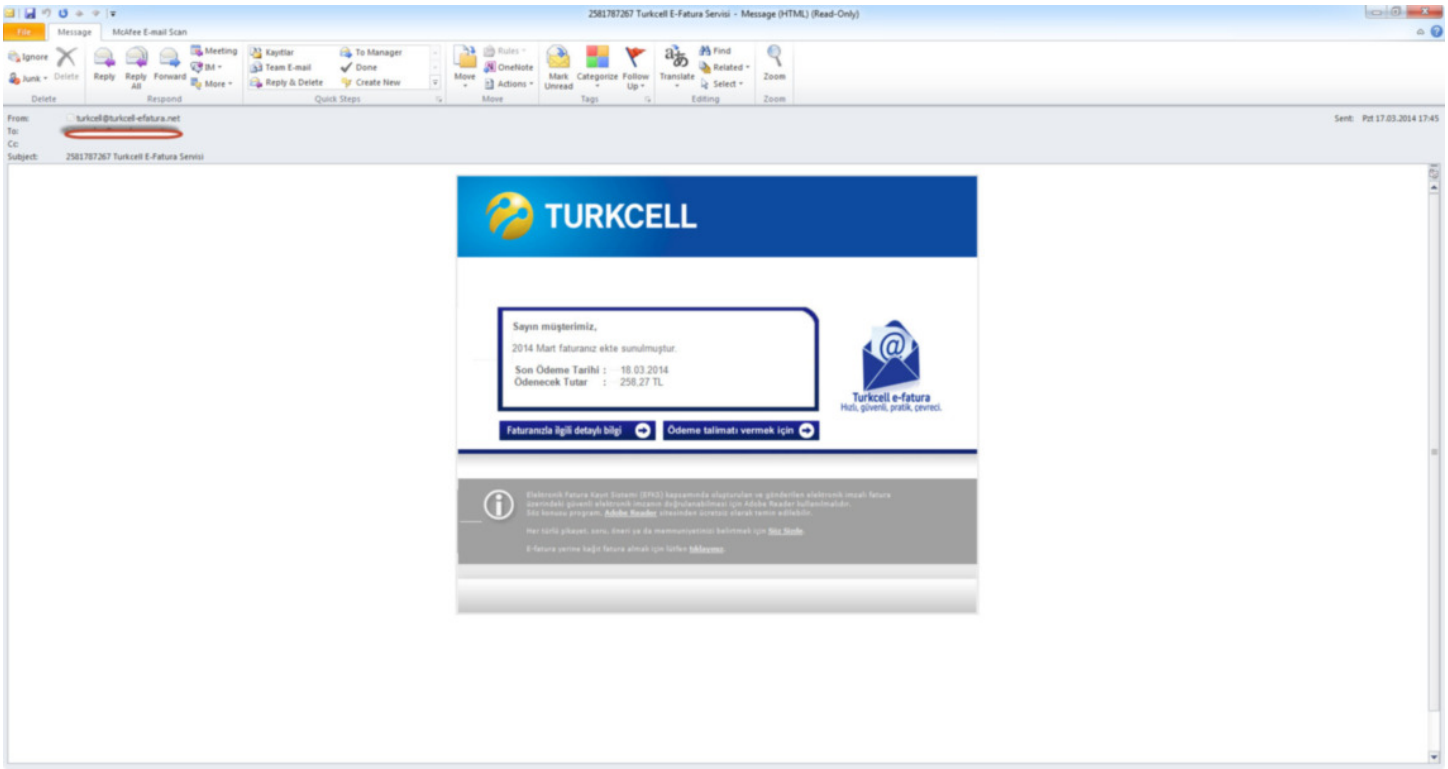
Source: https://www.mertsarica.com/rehber-hirsizi-hesperbot/

By M.S on June 2nd, 2014

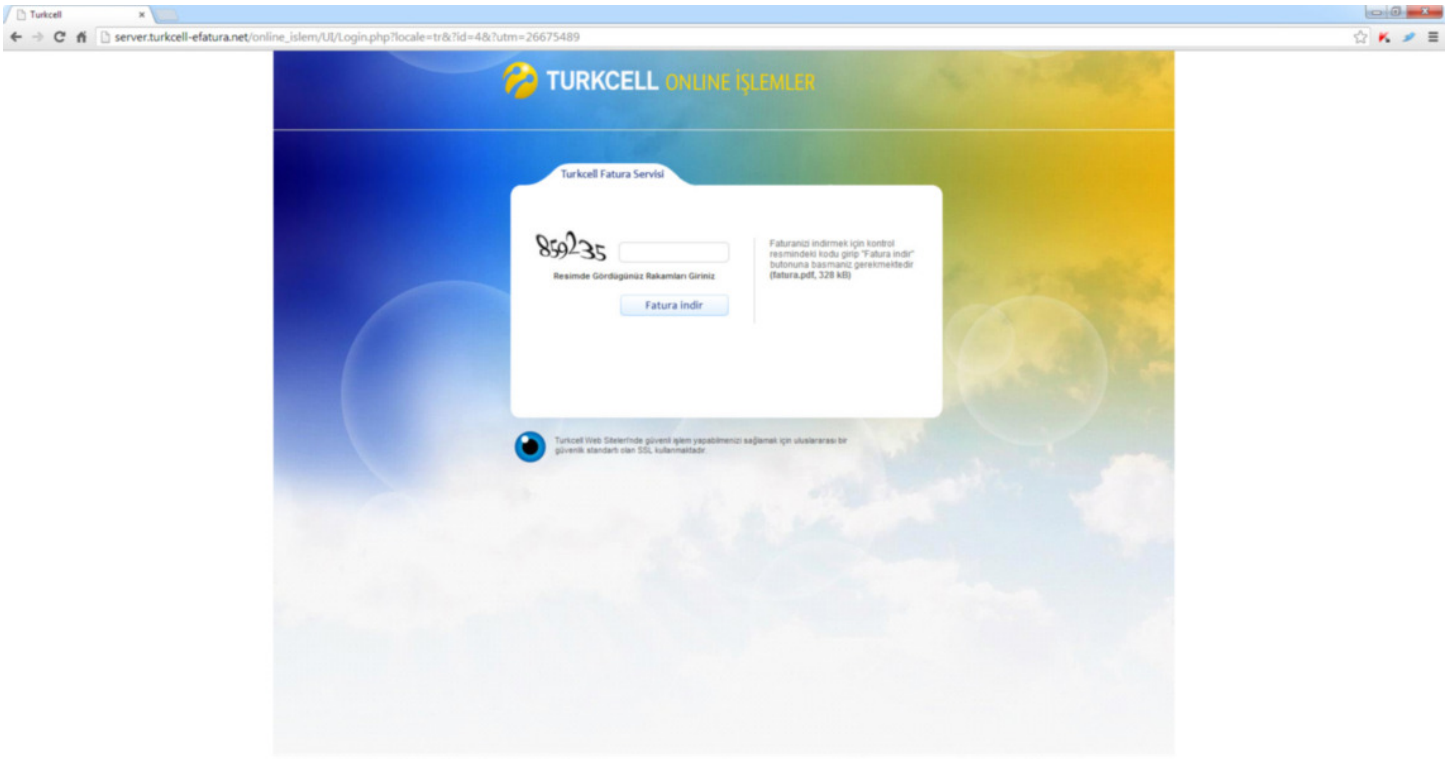
Son 1.5 yıldır hız kesmeden sahte fatura e-postaları ile ağına internet bankacılığı kullanıcılarını düşürmeye çalışan Hesperbot için son aylarda daha fazla mesai saati harcadığımı farkettim.

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

> *Hesperbot'un en son salgında kullandığı sahte e-posta mesajını ve zararlı yazılımı yaymak için kullandığı web sitesini aşağıda görebilirsiniz.*
>
> *Sahte Fatura E-postası:*

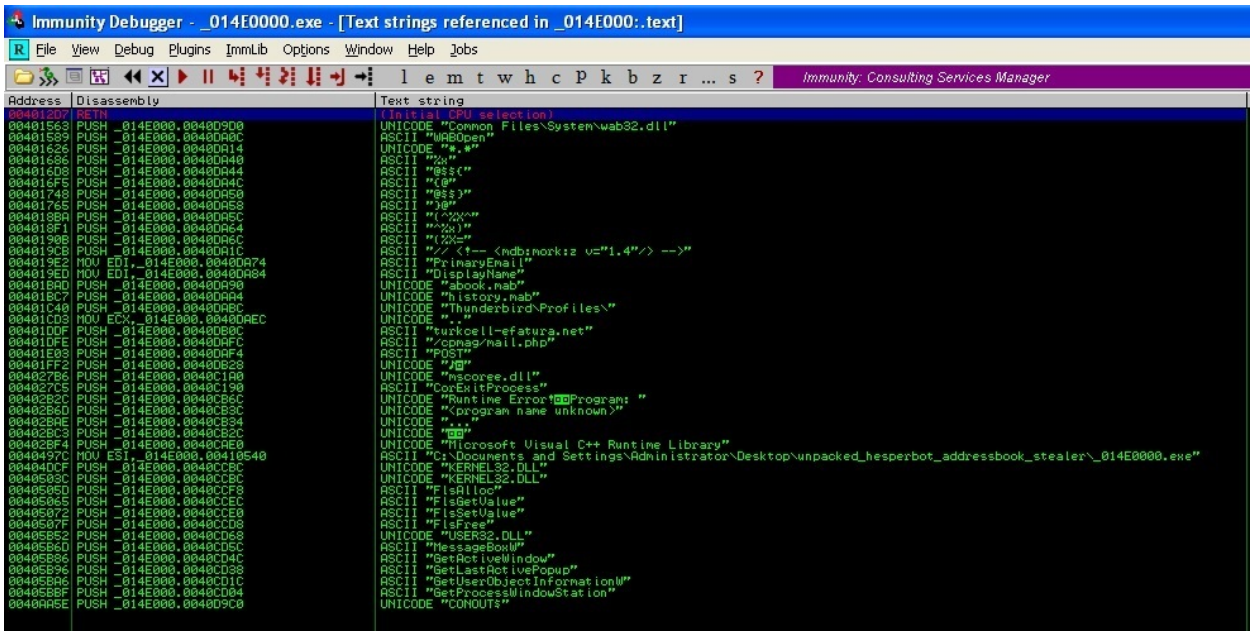


> *Sahte Fatura Web Sitesi:*

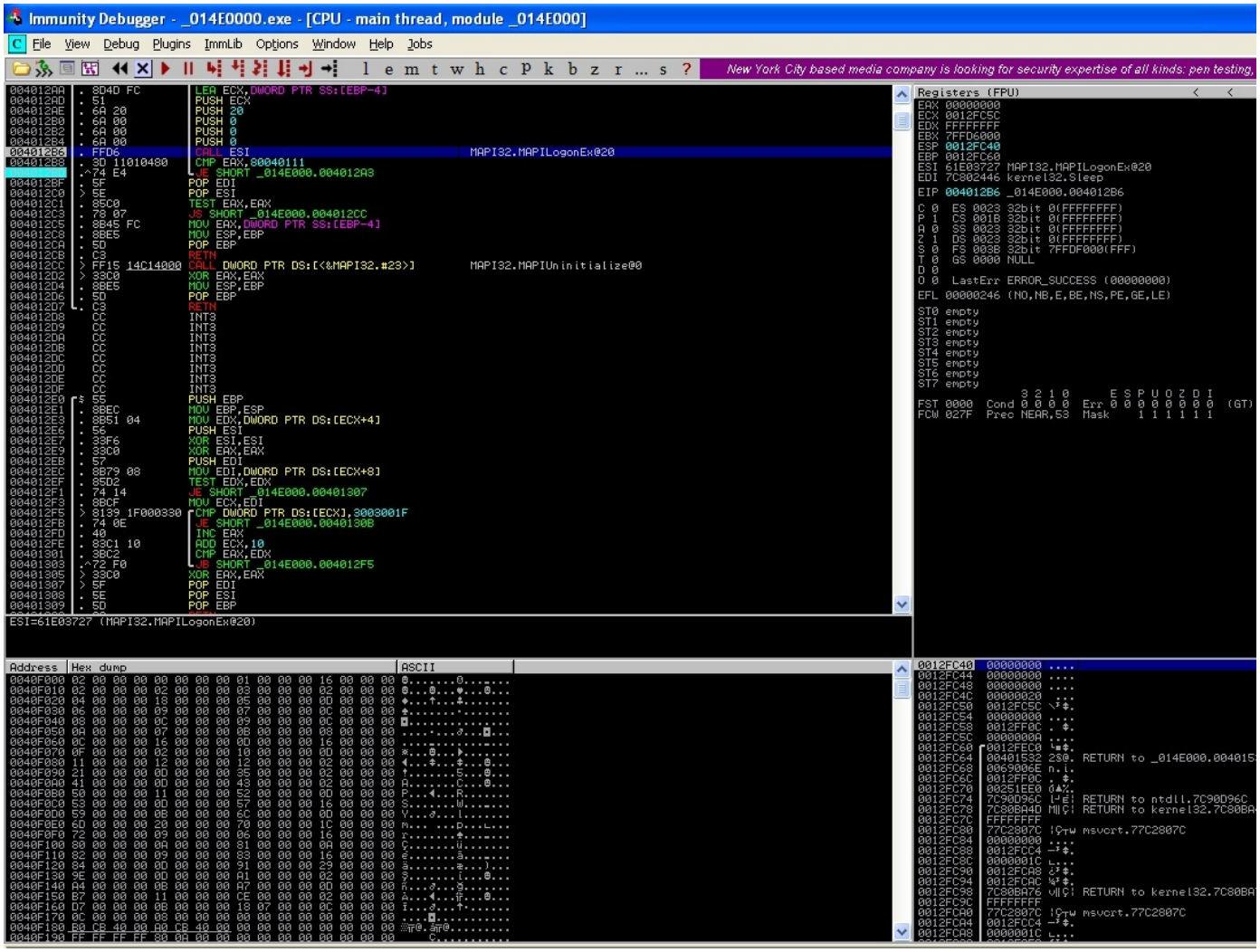


ESET'in Hesperbot raporu incelendiğinde, zararlı yazılımın hedef sistemden e-posta adreslerini çaldığı ve uzaktaki sunucuya bu bilgileri ilettiği belirtiliyordu fakat bununla ilgili teknik detaylara yer verilmemişti. Hesperbot'u detaylı bir şekilde incelerken, bulaştığı sistemdeki e-posta bilgilerini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

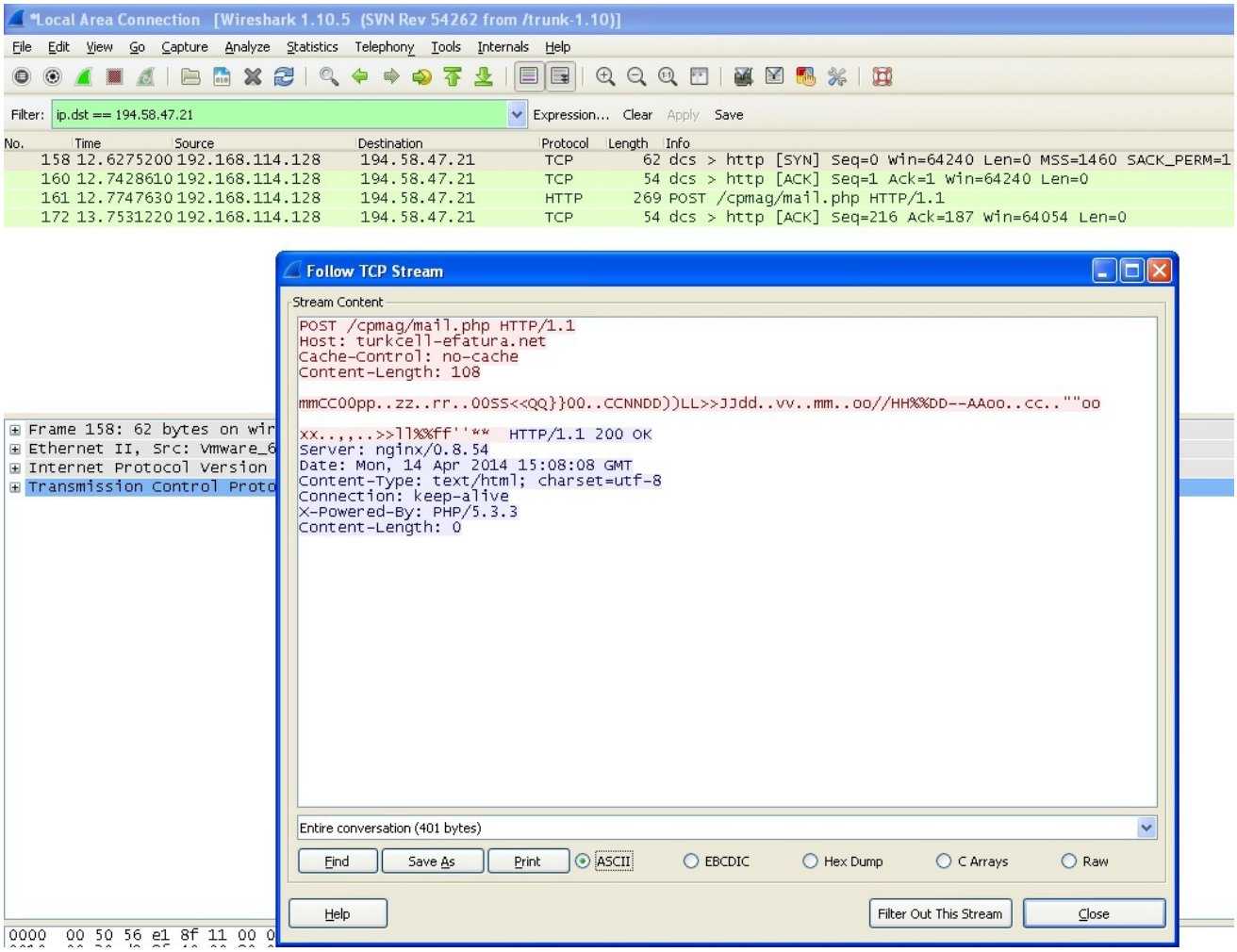
Hesperbot'un hedef sisteme bulaştıktan bir zaman sonra zararlı yazılımı yaymak amacıyla kullanmış olduğu sunucudan ege.xe adında bir yazılım indirdiğini tespit ettim. Paketlenmiş (packed) olan bu yazılımın uzantısını .exe olarak değiştirip her zamanki gibi Immunity Debugger aracı ile incelemeye başladım.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



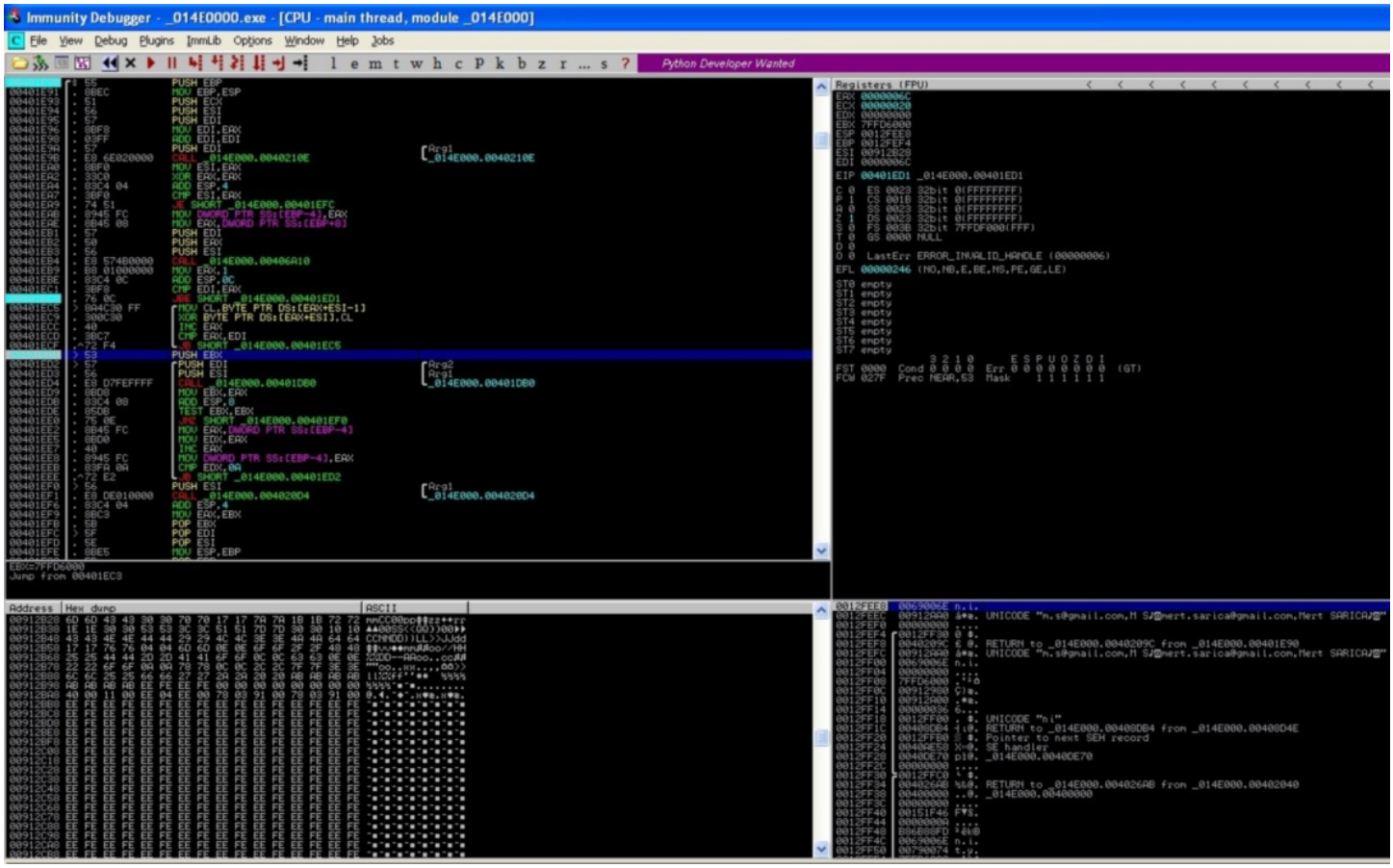
WABOpen fonksiyonundan bunun adres defterinde yer alan e-posta adres bilgilerini çaldığını tahmin etmem pek güç olmadı. Immunity Debugger ile yazılımı çalıştırdığımda herhangi bir HTTP trafiği oluşturmadığında birşeylerin ters gittiğini anladım. Yazılım çalışmasına rağmen herhangi bir web trafiği üretmemesi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



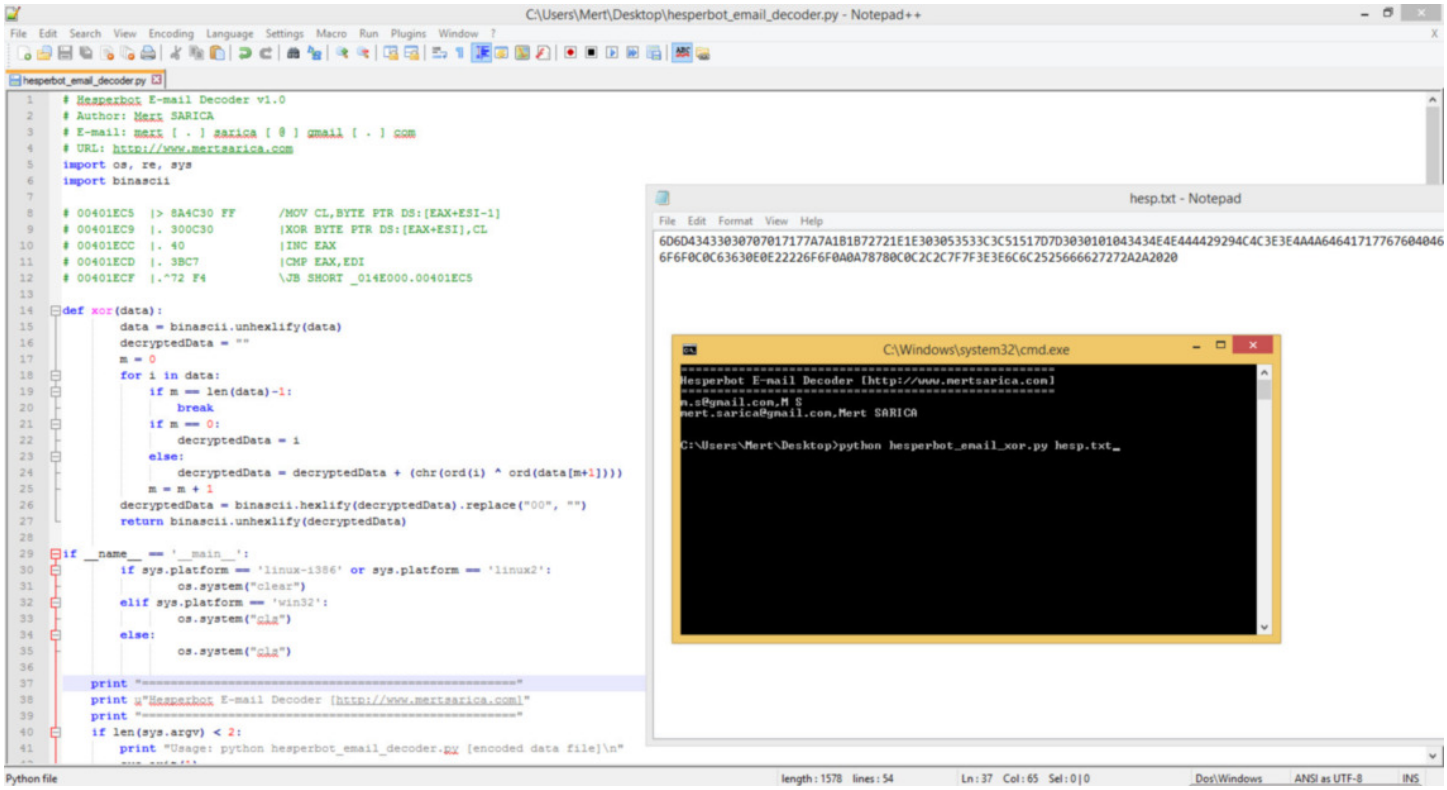
Yazılım son sürat çalıştıktan sonra oluşan trafiği Wireshark ile izlediğimde, uzaktaki sunucuya (http://turkcell-efatura.net/cpmag/mail.php) gönderilen e-posta bilgilerinin okunamaz halde (encoded) gönderildiğini gördüm ve bu fonksiyonu bulmaya karar verdim.



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.



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Virtual Pirate Network (VPN)

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

By M.S on May 1st, 2014

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

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

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

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

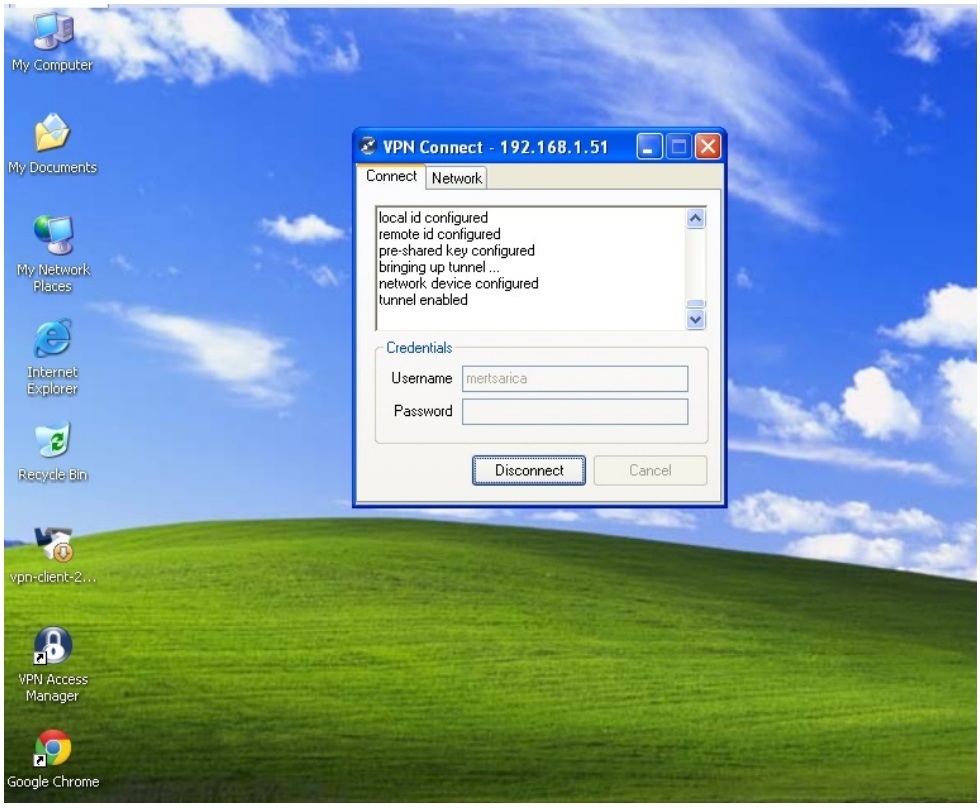
Herkesin elinin altında benim gibi VPN uygulaması kuracak hazır bir sistemi olmadığı için çoğu kimsenin ücretsiz VPN hizmetlerinden faydalandığını farkettim. Özellikle yakın çevremden gelen, hangi VPN uygulamasını yüklemeliyim ? Hangisi daha güvenli ? gibi sorular karşısında VPN kullanımının halk arasında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

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

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

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

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

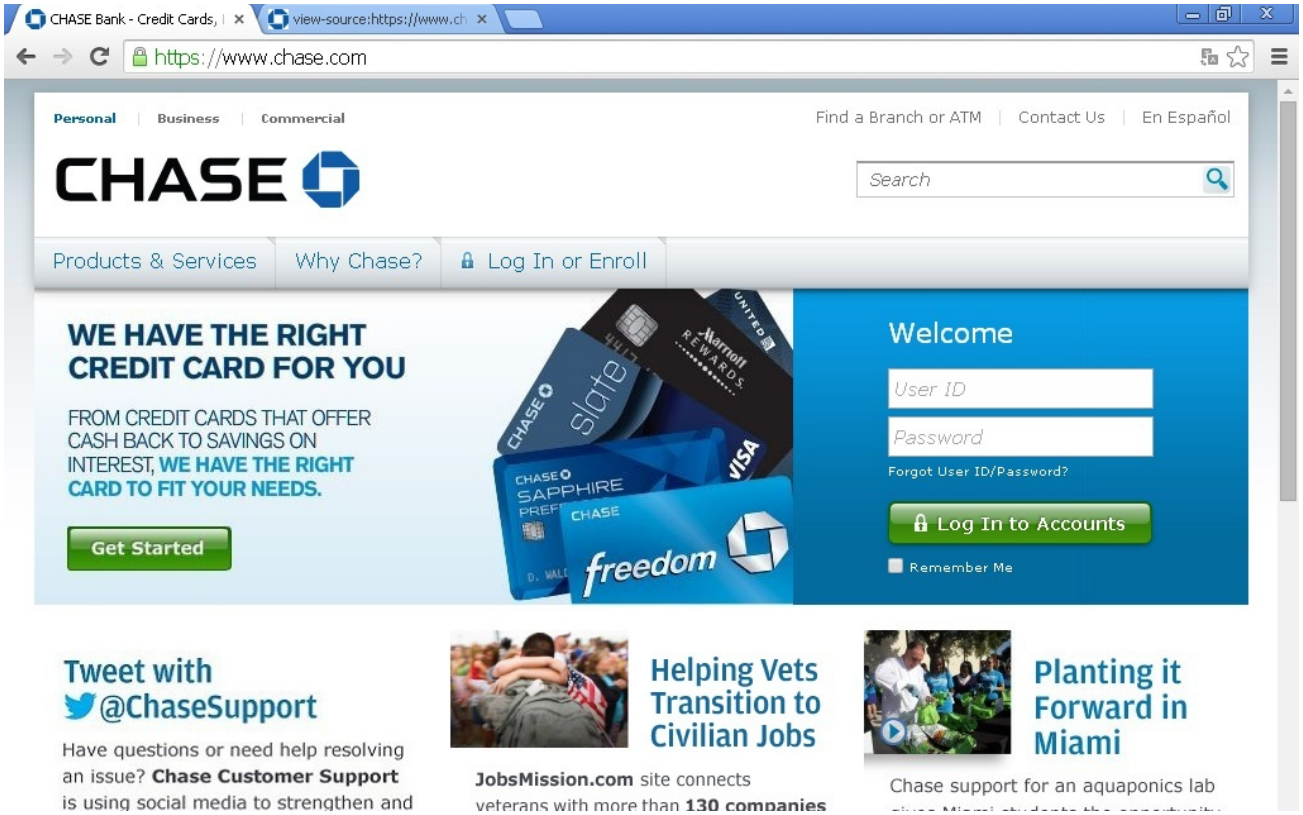


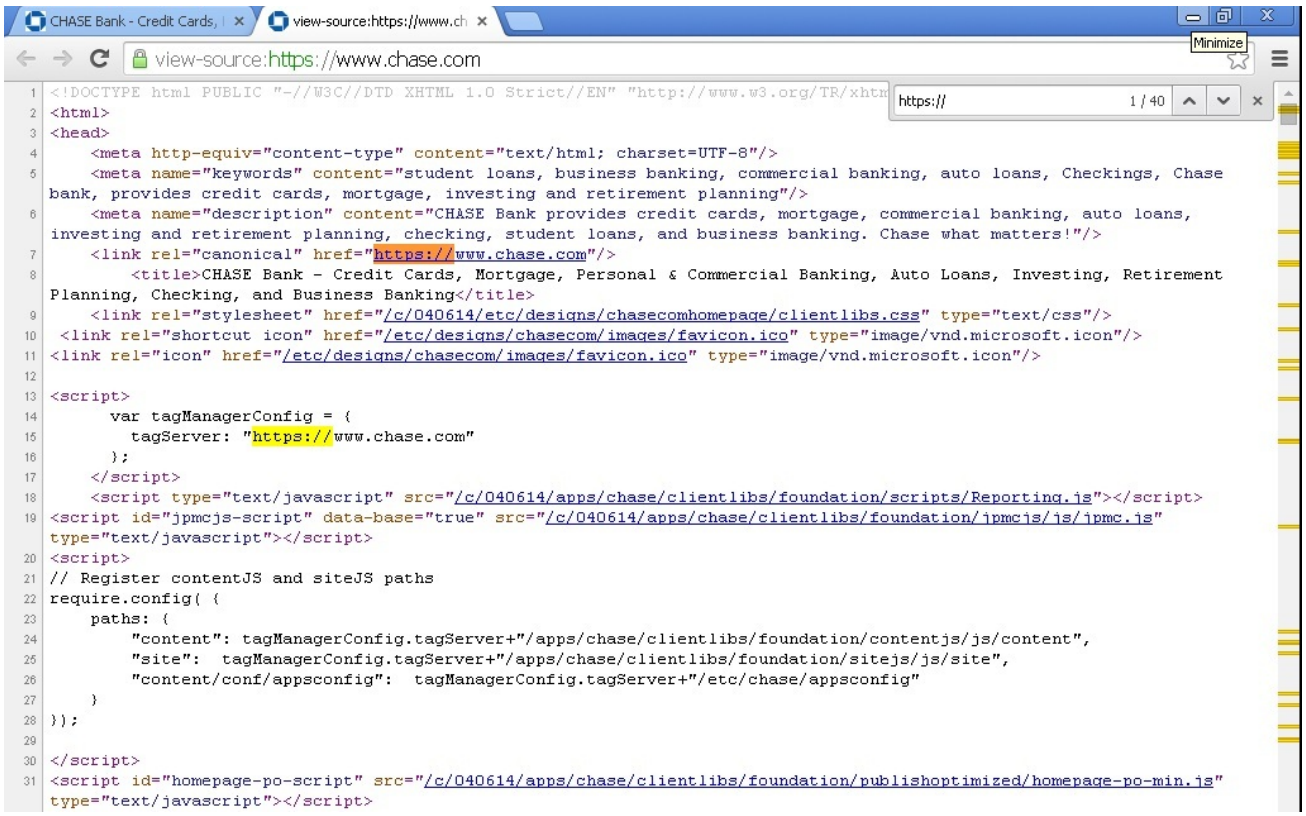
> *sslstrip aracı, http üzerinden gerçekleşen bir trafikte yer alan tüm https:// bağlantı adreslerini http:// ile değiştirerek kendisi üzerinden hedef sistem ile bağlantı kurarak ortadaki adam saldırısı (MITM) ile şifreleri çalabilmektedir.*

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

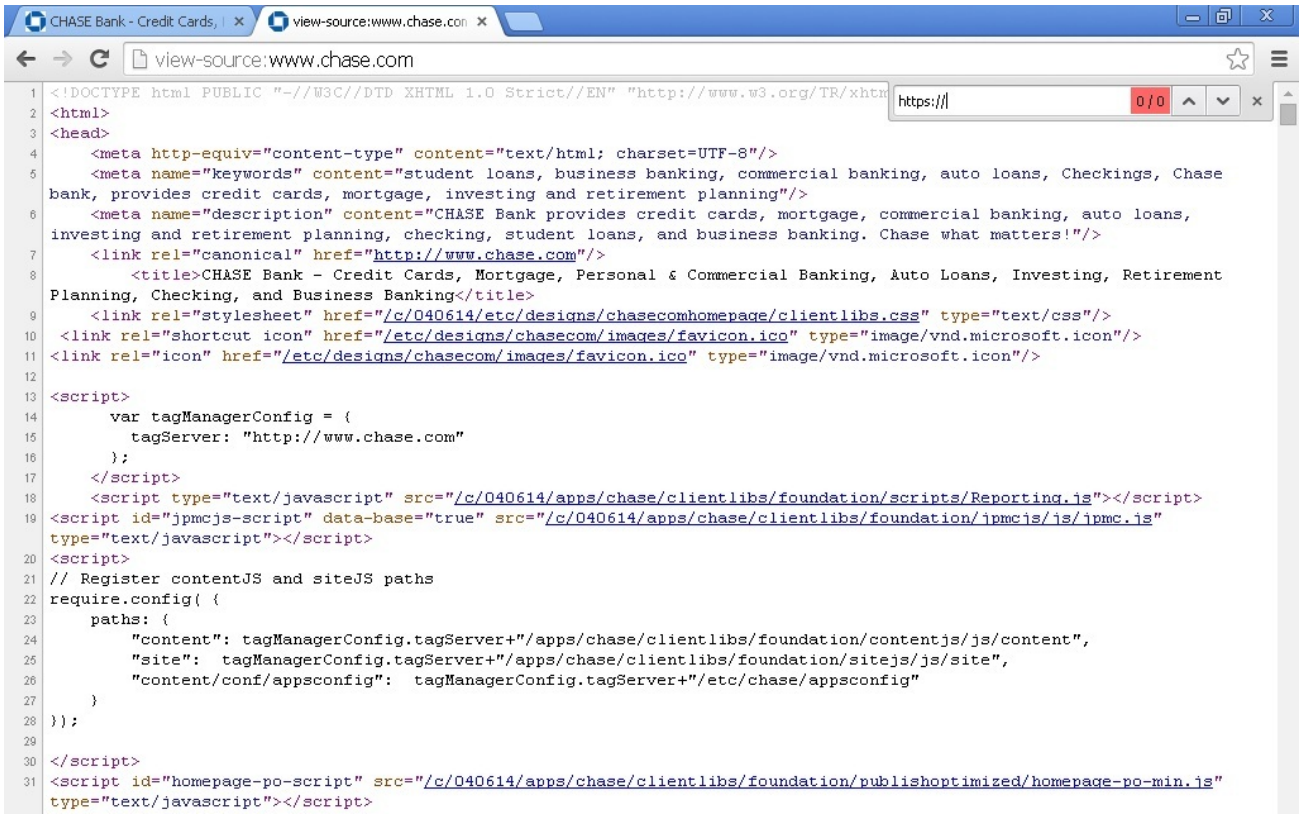
```
root@kali:/# cat /usr/local/bin/vpn.sh
#!/bin/bash
echo 1 > /proc/sys/net/ipv4/ip_forward
sleep 1
iptables -A FORWARD -o eth0 -i eth0 -s 10.71.80.0/24 -m conntrack --ctstate NEW -j ACCEPT
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
# iptables -t nat -F POSTROUTING
# iptables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

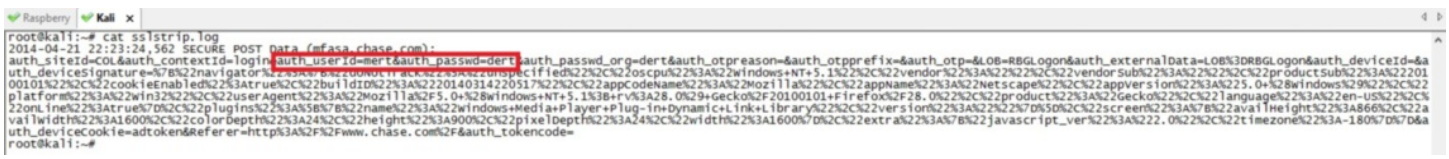
Simülasyon için öncelikle XP ile Kali arasında VPN bağlantısını kestim. Ardından Chase Bank'ın web sitesine http://www.chase.com adresinden bağlanmak istediğimde sunucunun beni otomatik olarak https://www.chase.com adresine yönlendirdiğini gördüm. Kaynak kodu üzerinde https:// önekini (prefix) arattığımda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





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





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

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

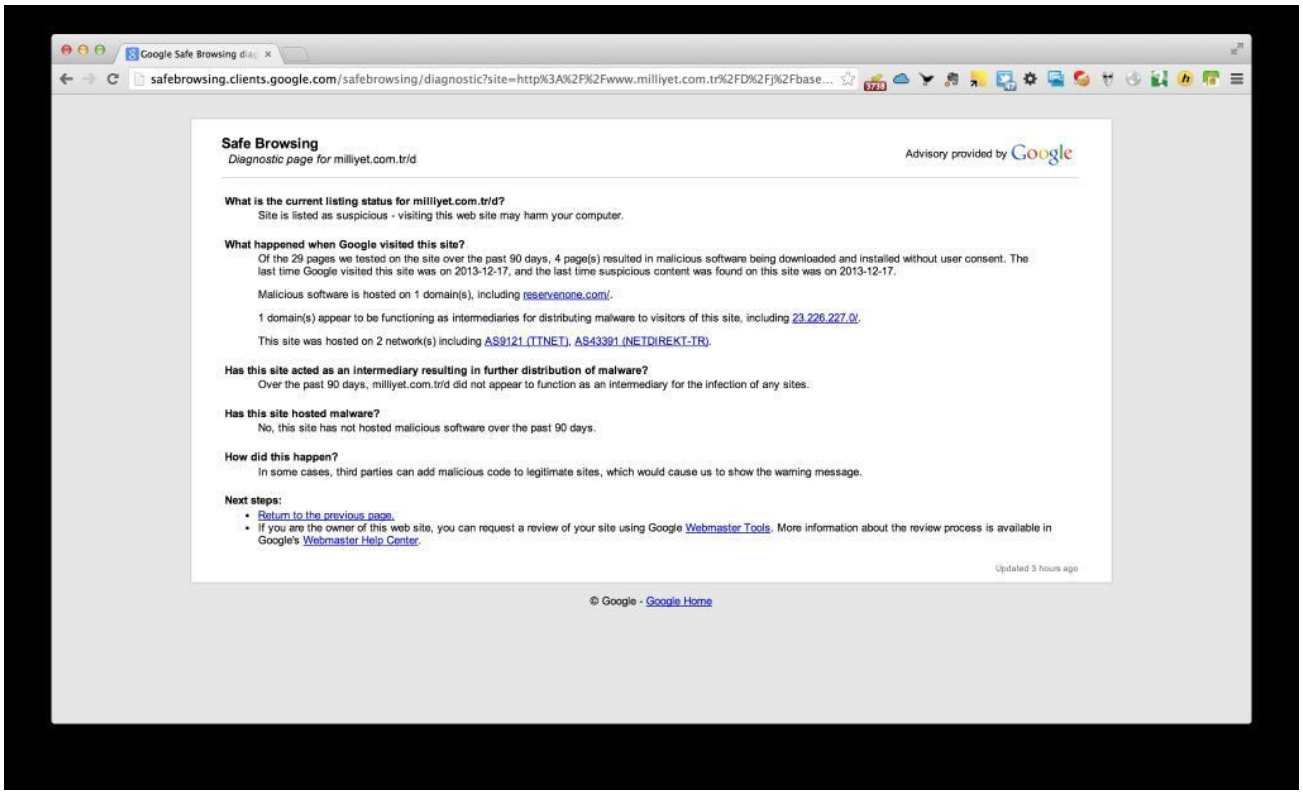
VirusTotal Proxy

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

By M.S on April 1st, 2014

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

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

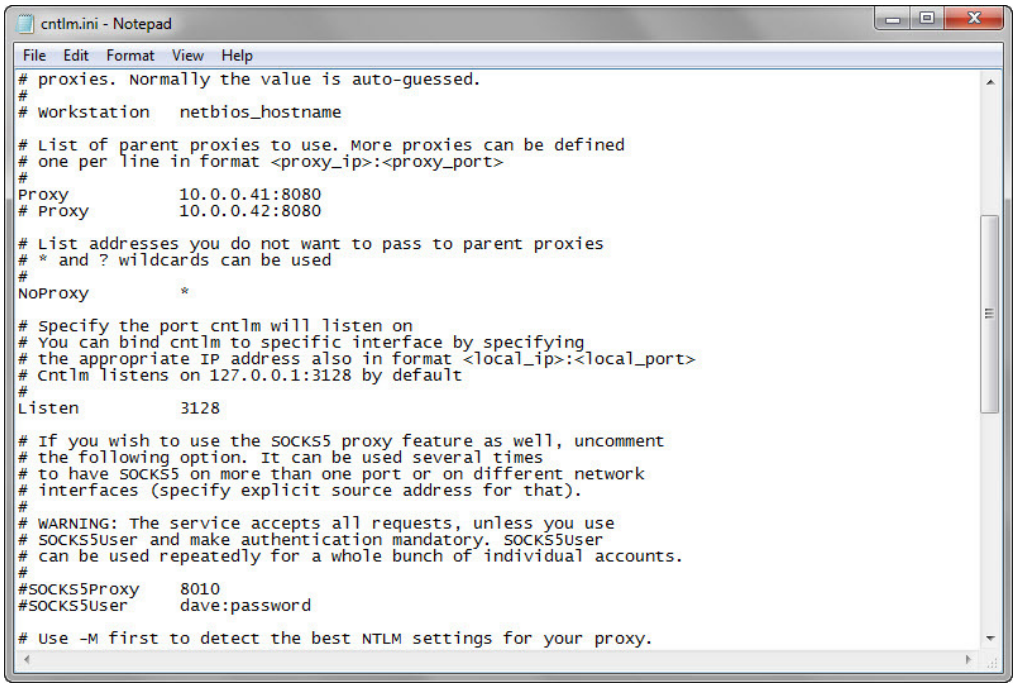


Elinizde en son teknoloji bir cihaz da olsa, Chrome gibi akıllı bir internet tarayıcısı da kullanıyor olsanız kimi zaman bu tehditler karşısında uyarı/alarm alana dek, sisteminiz veya kurumunuzun sistemleri çoktan art niyetli kişilerin kontrolü altına girmiş olabiliyor. Zararlı yazılım analizi ile ilgilenen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

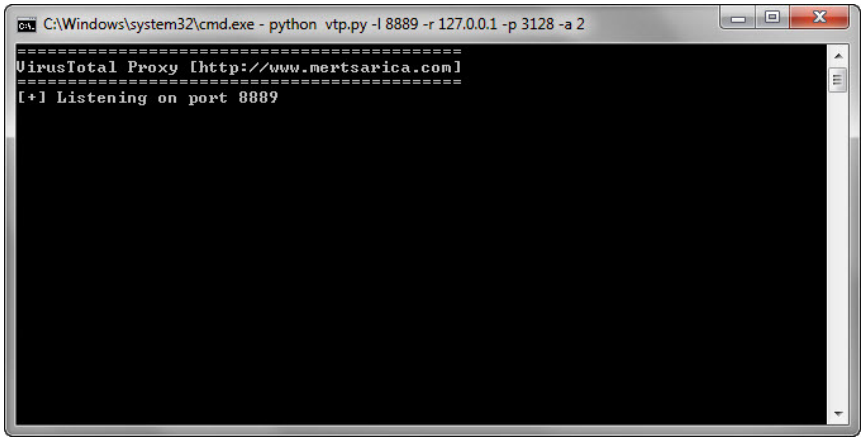
Bildiğiniz gibi VirusTotal, sadece zararlı yazılım analizi yapmakla kalmayıp ayrıca 52 farklı kaynak üzerinden zararlı URL, kod analizi gerçekleştirip, raporlayabiliyor. Çorbada tuzum olsun, kullanıcılar, güvenlik uzmanları, bu tehditlerden daha kısa sürede haberdar olabilsinler diye VirusTotal ile entegre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

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

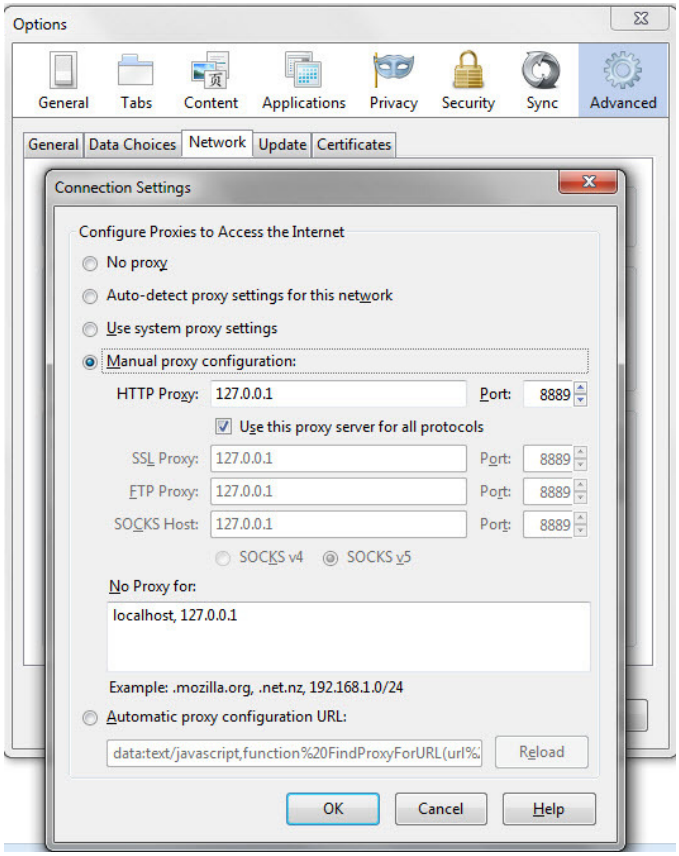
Aracın kullanımına geçmeden önce, sistem üzerinde mutlaka bir proxy aracının çalışması gerekiyor. Bunun için kendi sistemim üzerine açık kaynak kodlu CNTLM proxy aracını kurdum ve tüm trafik için proxy vazifesi görebilmesi adına ayar dosyasındaki (cntlm.ini) NoProxy ayarını * olarak değiştirdim ve 3128.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



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 kaçı zararlı kod tespit ederse sesli alarm üretmesi gerektiğini belirtiyorsunuz. (-a 2 ile 2 tane kaynak zararlı kod tespit ederse sesli alarm ver gibi)



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


Options
General
Tabs
Content
Applications
Privacy
Security
Sync
Advanced
General
Data Choices
Network
Update
Certificates
Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy: 127.0.0.1 Port: 8889
Use this proxy server for all protocols
SSL Proxy: 127.0.0.1 Port: 8889
FTP Proxy: 127.0.0.1 Port: 8889
SOCKS Host: 127.0.0.1 Port: 8889
SOCKS v4
SOCKS v5
No Proxy for:
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
data:text/javascript,function%20FindProxyForURL(url%
Reload
OK
Cancel
Help


Firefox
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
Bugünkü Gazete
Milliyet Emlak
Milliyet Heryerde
Milliyet Arşiv
Favorilerime ekle
Ana sayfam yap
Künye
Kampanyalar
28 Mart 2014, Cuma
Bizi izleyin:
Üyelik
CANLI BORSA
BIST 68.438 2,07
EURO 3,0080 -0,08
USD 2,1910 0,23
ALTIN 91,3900 0,64
Milliyet.com.tr
BASINDA GÜVEN
Türkiye'nin lider haber sitesi
kelime ya da haber
Ara
Hava
İSTANBUL
ADAYINIZI DESTEKLEMEK İÇİN
Son Dakika
Yazarlar
Siyaset
Ekonomi
Finans
Spor
SKORER
Dünya
Gündem
Magazin
Cadde
Milliyet.tv
SKORER tv
Tümü
FLAŞ
C:\Windows\system32\cmd.exe - python vtp.py -l 8889 -r 127.0.0.1 -p 3128 -a 2
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/submission/?force=1&url=http://pubads.g.doubleclick.net/&token=3102333978c58aaa6cbb1d11dc64ea0e07f074da619b27bd3539be1624253ffc
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/submission/?force=1&url=http://i.milliyet.com.tr/&token=c6ab91046a2386a777c54990caa8d4afdccbfcf448757561bf9c6a370ab5215d
Date: 28-3-2014 14:38:18 Domain: http://cdn.tccdn.com Detection Ratio: 0 / 52 Report URL: https://www.virustotal.com/en/url/submission/?force=1&url=http://cdn
İKA... SON DAKİKA... SON DAKİKA...
G.Saray'a nester! 5 isim yolcu...

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

Not #1: VirusTotal Proxy aracını buradan indirebilirsiniz.
Not #2: Programın ihtiyaç duyduğu Twisted Python kütüphanesini buradan indirebilirsiniz.
Not #3: VirusTotal, otomatize işlemler için API'lerinin kullanılmasını rica ediyor dolayısıyla VirusTotal Proxy aracını şüphelendiğiniz siteleri kontrol amaçlı kullanmanızı rica ederim. VirusTotal API'sine buradan ulaşabilirsiniz.

Sanal Obruk

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

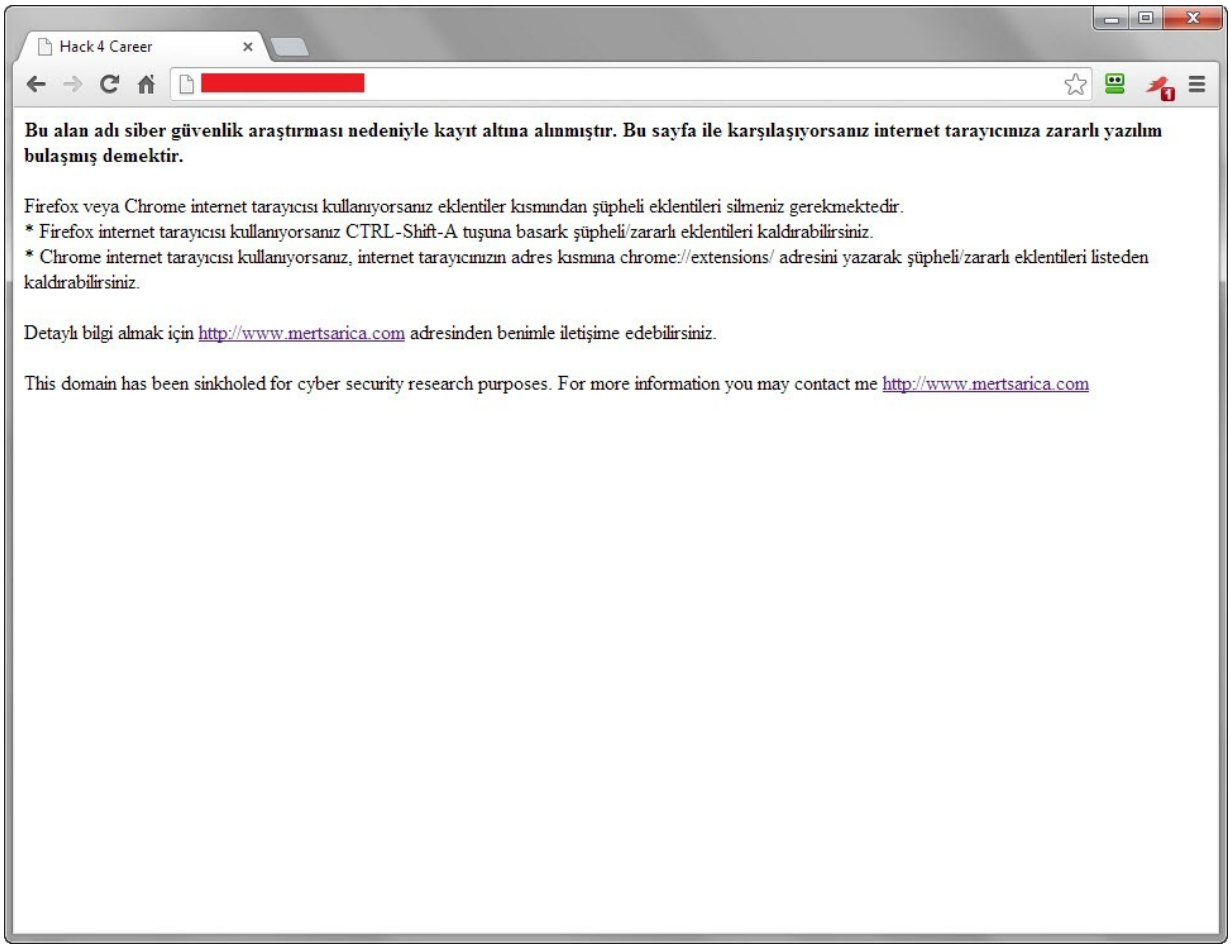
By M.S on March 1st, 2014

Obruk, yatay veya yataya yakın tabakalı kireçtaşlarında bulunan yeraltı nehirlerinin veya aktif mağara tavanlarının çökmesi sonucu oluşmuş baca veya kuyu görüntüsü veren derin çukurluklardır. Sanal obruk (sinkhole) ise zararlı yazılımlarla yapılan mücadelede, zararlı yazılım salgınını (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.

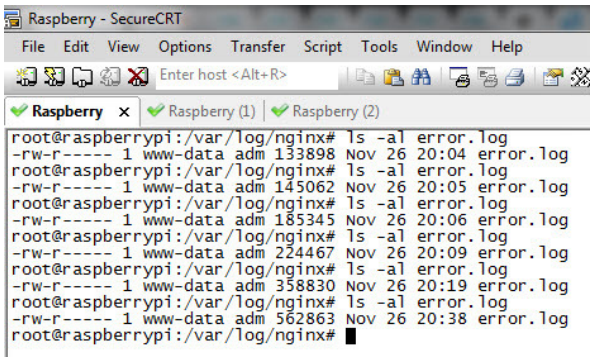
Bu yöntemde öncelikle zararlı yazılımın haberleştiği komuta kontrol merkezi tespit edilir. Ardından alan adını kayıt eden firma ile iletişime geçilerek alan adının güvenlik firmasına transfer edilmesi sağlanarak sunucu üzerine gelen trafik güvenlik firması tarafından analiz edilmektedir. Bunun dışında 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 kandırarak internet tarayıcılarına bulaşan ve sosyal medya hesaplarını ele geçirip reklam ve dolandırıcılık yapmaya çalışan çok sayıda zararlı yazılım ile karşılaştık ve hemen hemen her salgında zararlı yazılımların farklı alan adları ile haberleştiğini gördük. Bu salgınlarda dikkatimi çeken, yeni kayıt edilen her alan adının en fazla bir senelik alınması 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.

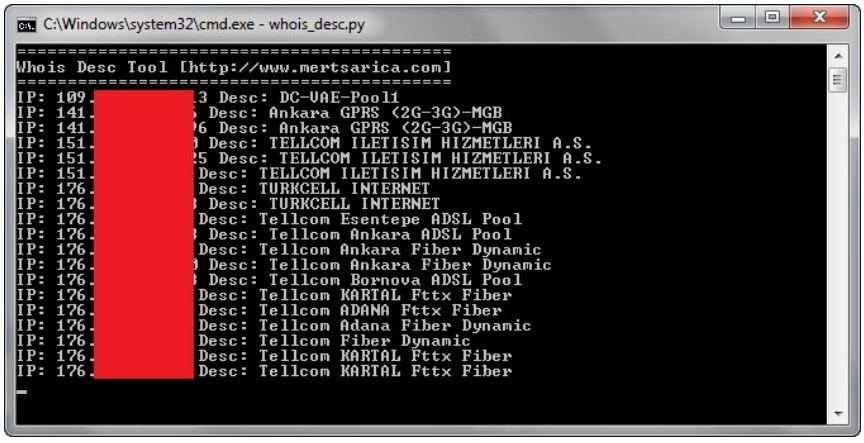


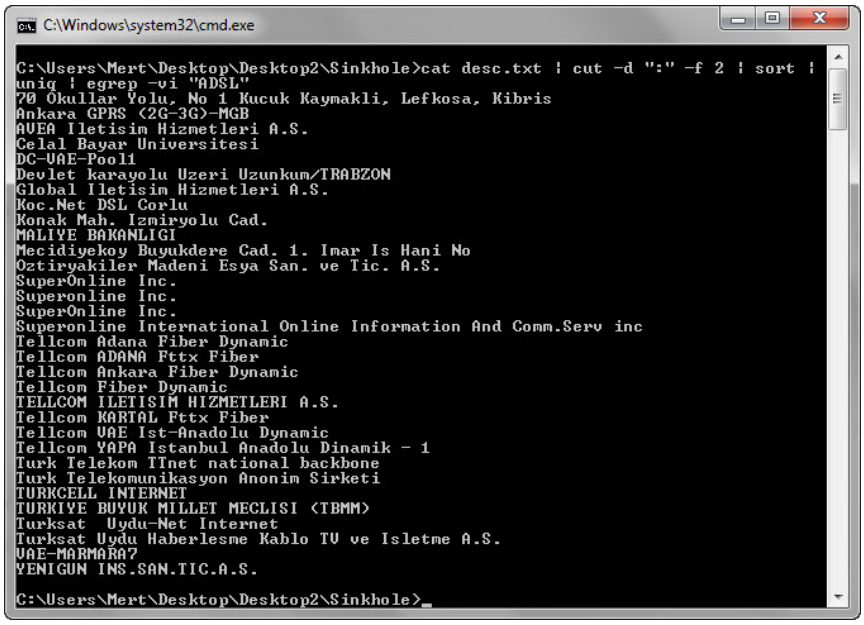
Trafiği izlemeye başladıktan 35 dakika sonra access.log dosyasının 400 KB olduğunu gördüm ve bu durum bana 1.5 sene sonra dahi zararlı yazılım bulaşmış sistemlerin halen aktif olduğunu göstermiş oldu.



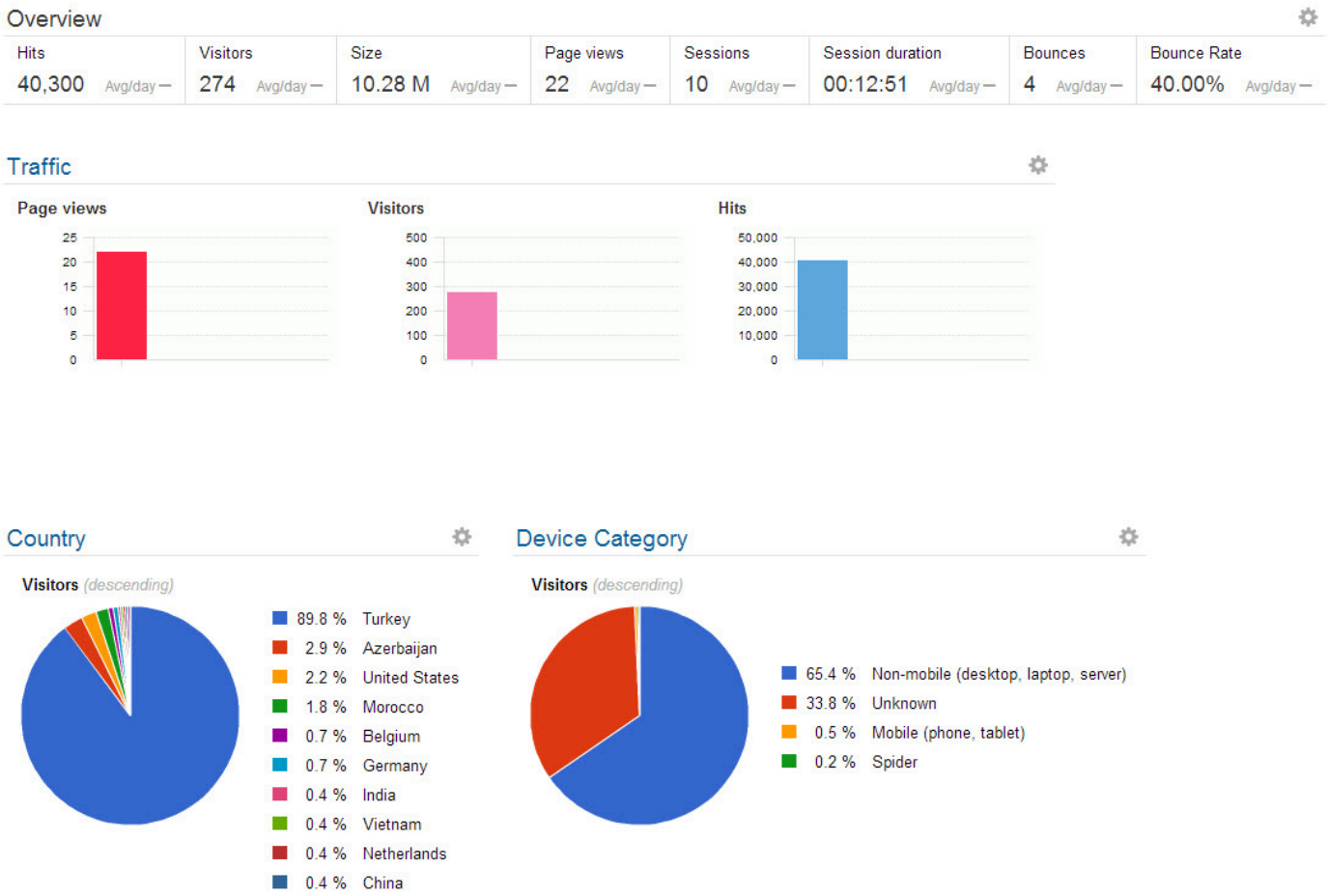
14 saatin sonunda access.log dosyasını, en son yıllar yıllar önce kullandığım Sawmill aracı ile incelemeye başladım ve alan adını bu zaman zarfında 274 kişinin ziyaret etmiş olduğunu ve 40.300 hit aldığını gördüm.

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





Zararlı yazılım, Javascript dosyası çağırdığı için normal olarak en çok çağırılan dosya uzantısı JS olmuştu. Ziyaretçilerin kullandığı internet tarayıcıları sıralamasında Firefox'un en üst sırada yer alması da bu zararlı yazılımdan en çok ve kalıcı olarak Firefox kullanıcılarının etkilendiğini gösteriyordu. Bu zararlı eklenti, ziyaret edilen her siteden gelen yanıt paketine, komuta kontrol merkezinden bir javascript dosyası 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.



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

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

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

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

Anti Scanner

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

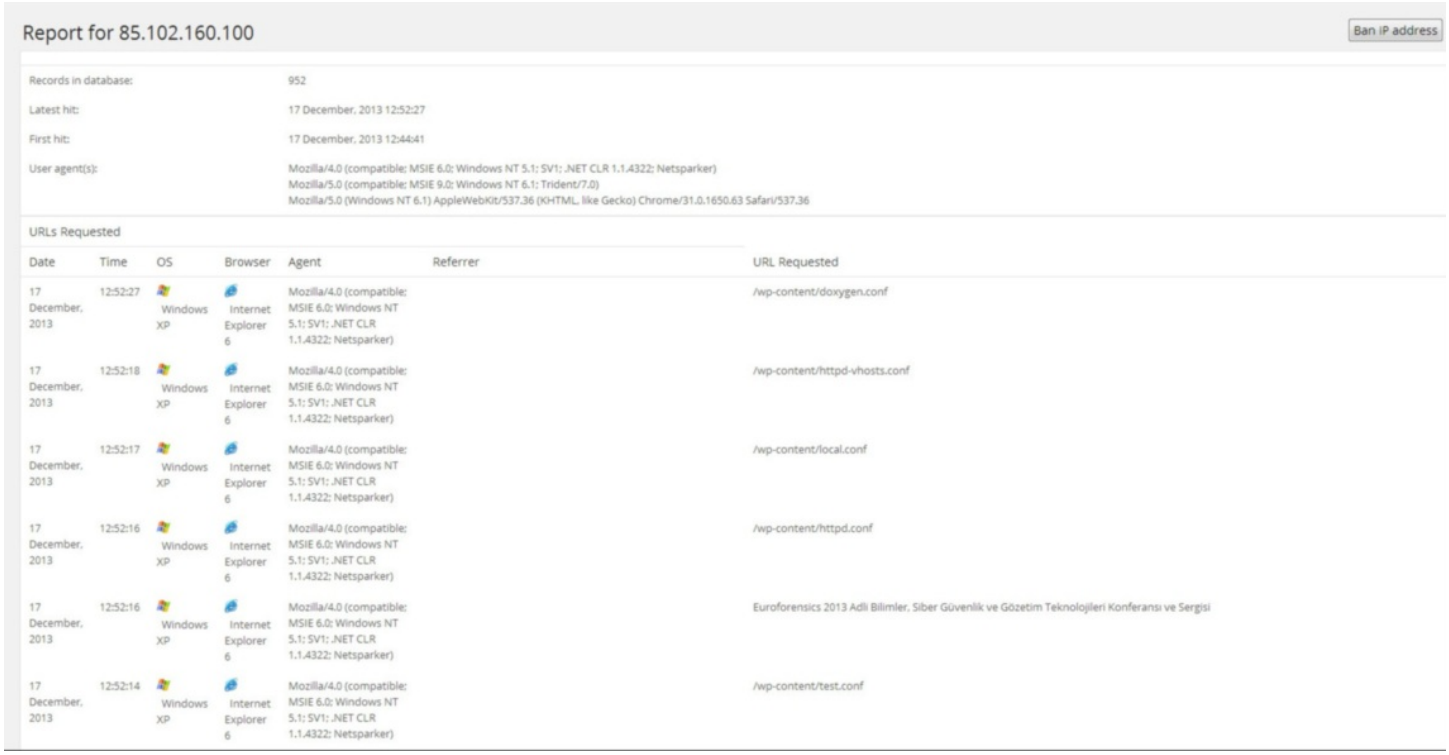
By M.S on February 3rd, 2014

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

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

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

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



Report for 85.102.160.100

Ban IP address

Records in database: 952

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

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

User agent(s): Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/7.0)
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36

URLs Requested

Date	Time	OS	Browser	Agent	Referrer	URL Requested
17 December, 2013	12:52:27	Windows XP	Internet Explorer 6	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)		/wp-content/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

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

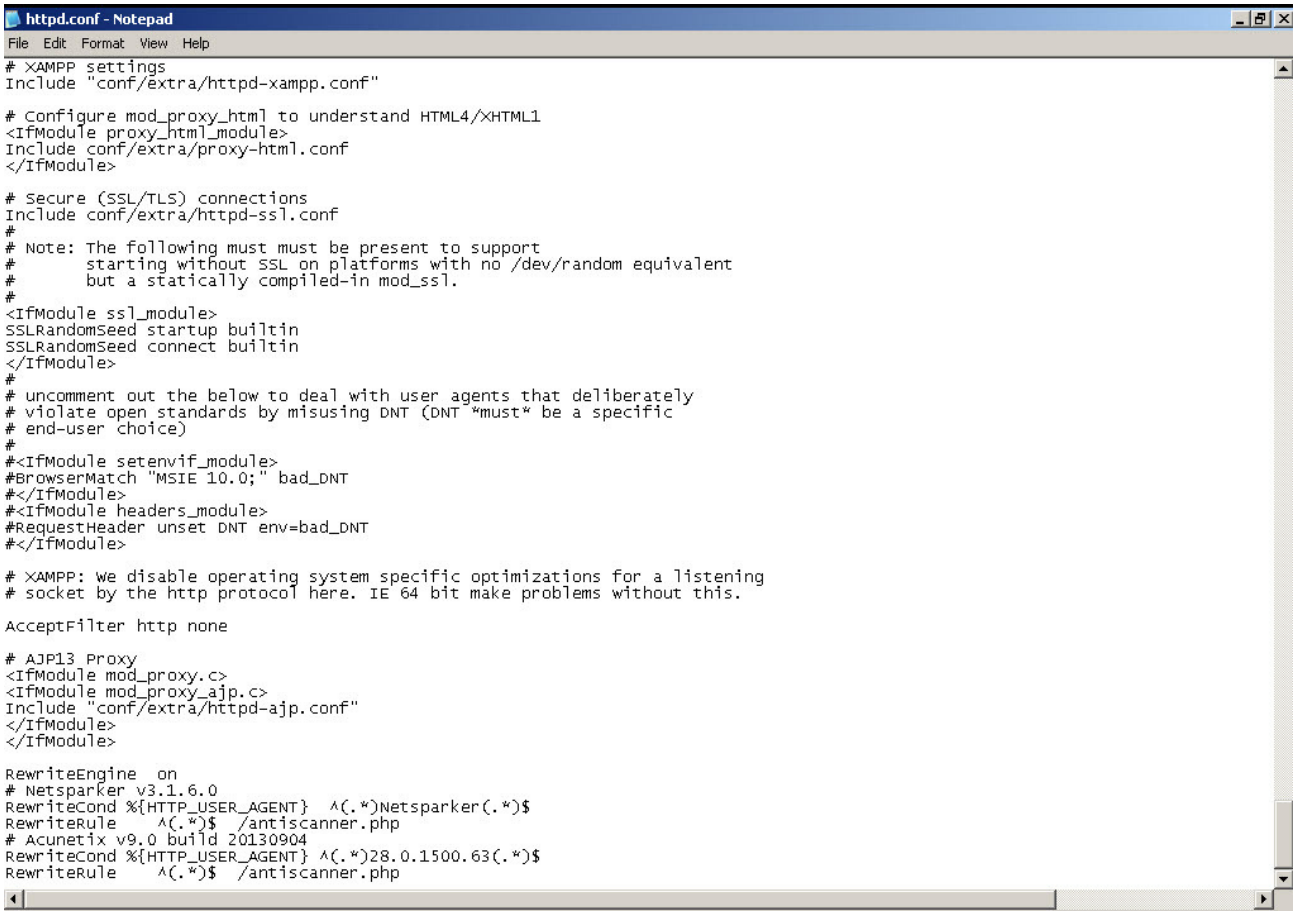
antiscanner.php

```php
<?php
function randString($length, $charset='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789')
{
    $str = '';
    $count = strlen($charset);
    while ($length--) {
        $str .= $charset[mt_rand(0, $count-1)];
    }
    return $str;
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Hack 4 Career - http://www.mertsarica.com</title>
<link rel="stylesheet" href="http://www.<?php echo randString(50);?>.com/<?php echo randString(50);?>.css" type="text/css" media="screen" />
<link rel="stylesheet" href="http://www.<?php echo randString(50);?>.com/<?php echo randString(50);?>.css" type="text/css" media="screen" />
<link rel="alternate" type="application/rss+xml" title="Hack 4 Career RSS Feed" href="http://www.<?php echo randString(50);?>.com/feed/" />
<link rel="alternate" type="application/atom+xml" title="Hack 4 Career Atom Feed" href="http://www.<?php echo randString(50);?>.com/feed/atom/" />
<link rel="pingback" href="http://www.<?php echo randString(50);?>.com/xmlrpc.php" />

<form action="<?php echo randString(50);?>.php" method="post">
 <p><?php echo randString(50);?>: <input type="text" name="<?php echo randString(50); ?>" /></p>
 <p><?php echo randString(50);?>: <input type="text" name="<?php echo randString(50); ?>" /></p>
 <p><input type="submit" /></p>
</form>

function antiscanner($antiscanner)<br \>
{<br \>
    return $antiscanner;<br \>
}<br \>

"/usr/local/<?php echo randString(50);?>"<br \>

"c:/<?php echo randString(50);?>"<br \>

define( 'DB_NAME',     'database' );<br \>
define( 'DB_USER',     'www.mertsarica.com' );<br \>
define( 'DB_PASSWORD', 'antiscanner' );<br \>
define( 'DB_HOST',     'localhost' );<br \>
define( 'DB_CHARSET',  'utf8' );<br \>

<?php echo randString(50);?>@<?php echo randString(50);?>.com<br \>
</html>
```

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

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

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

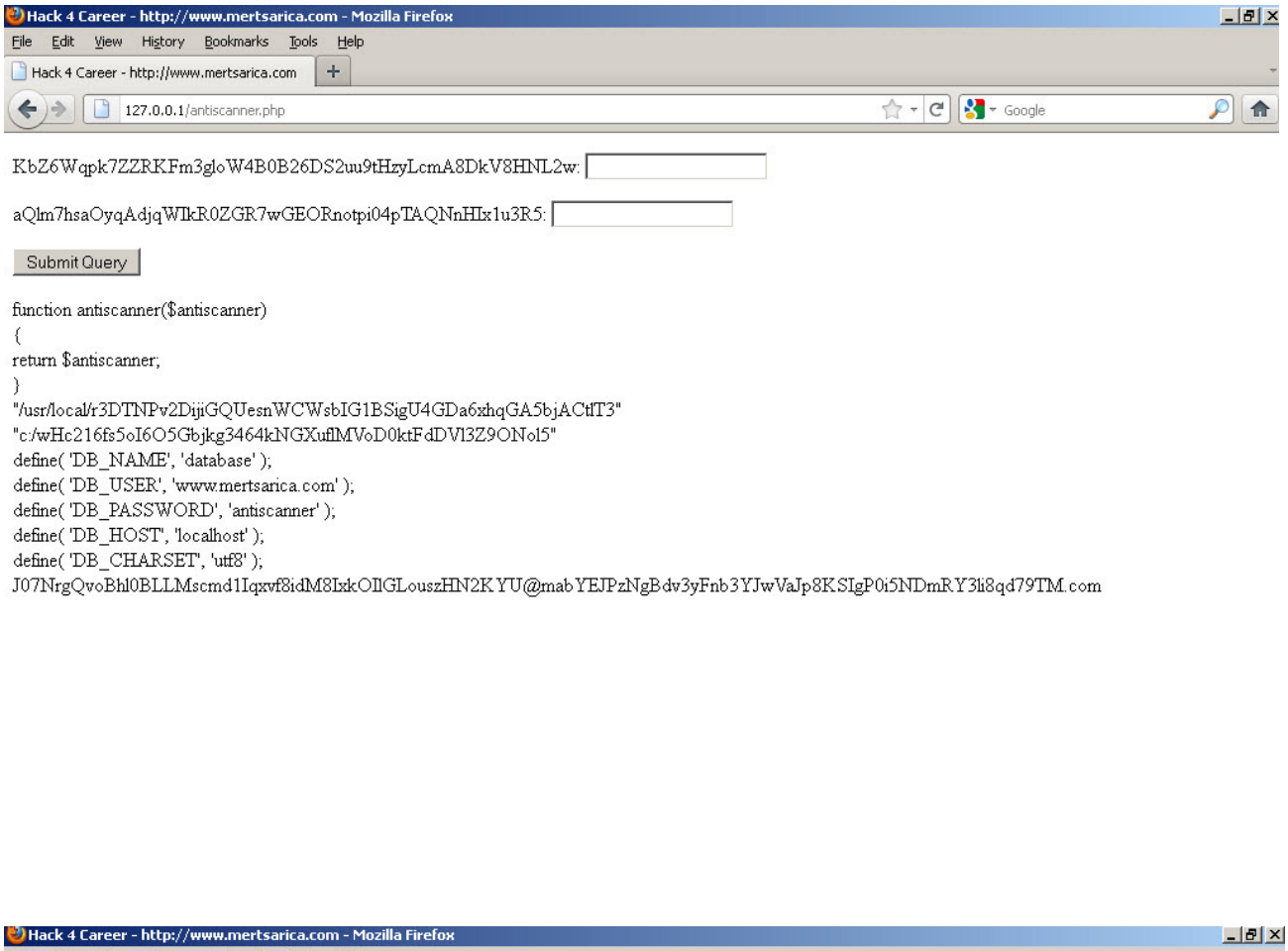


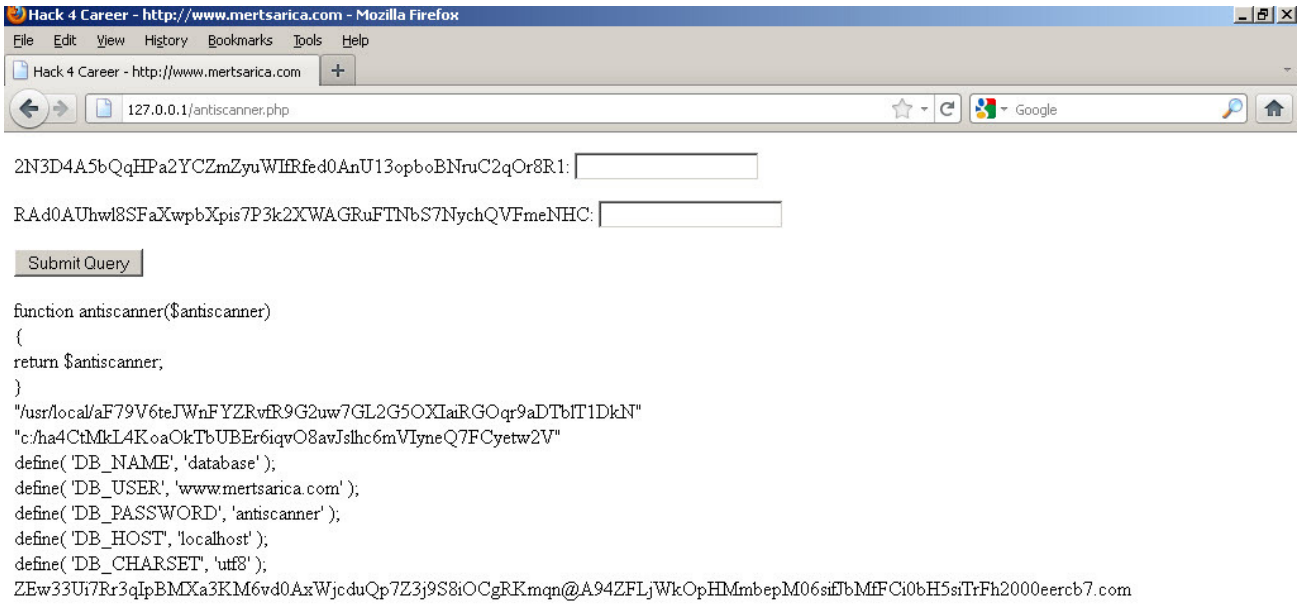
Yukardaki mod_rewrite kuralı ile USER-AGENT alanı, Netsparker veya Acunetix'in kullandığı değere eşit ise, istekleri otomatik olarak hazırladığım PHP uygulamasına (antiscanner.php) yönlendirdim.

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

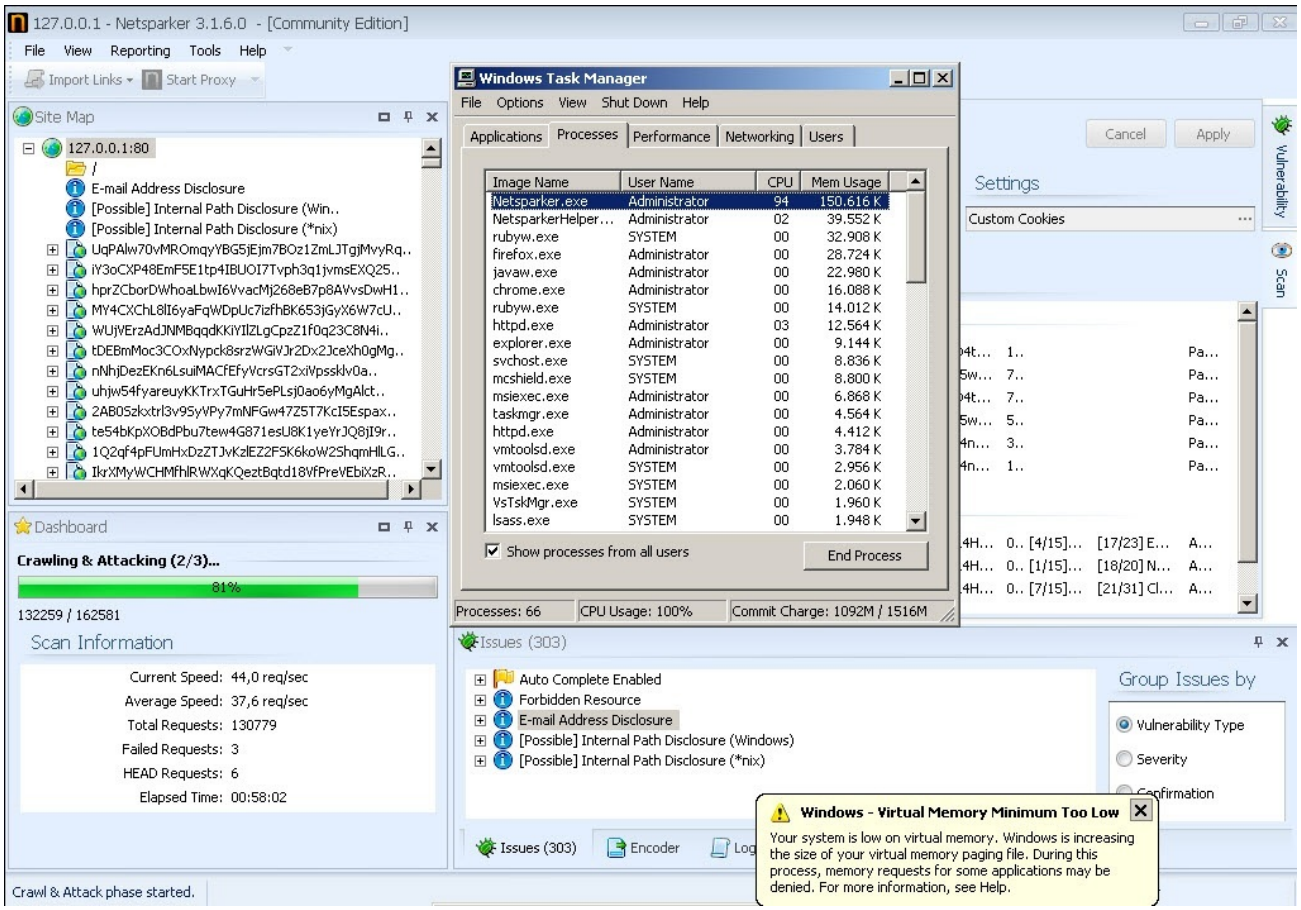
Hack4Career
http://www.mertsarica.com

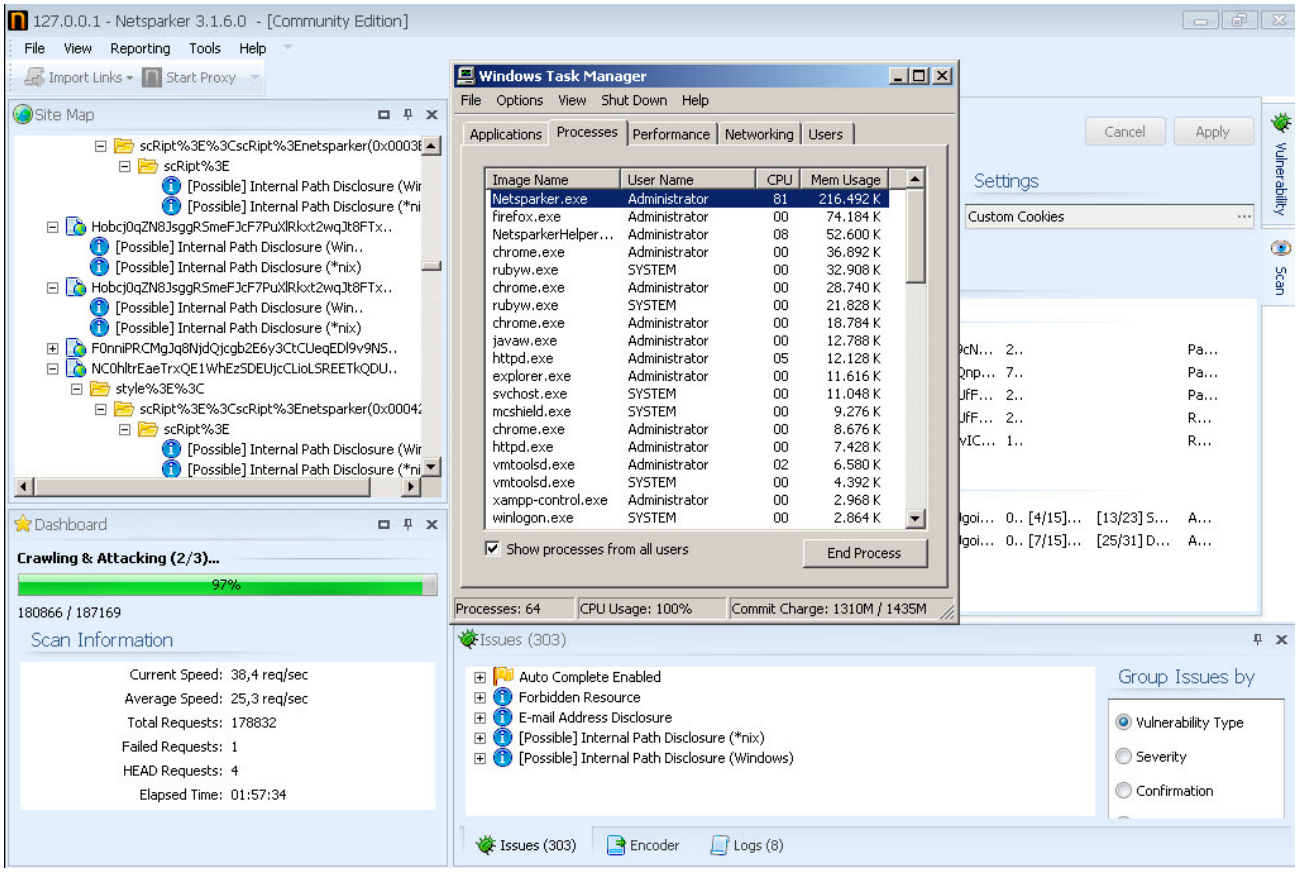
Ardından Firefox'un User Agent Switcher eklentisi ile USER-AGENT'ımı Netsparker olarak değiştirdikten sonra sayfanın her istekte farkı yanıt (form ve formun bulunduğu adres) döndüğünü doğruladım.



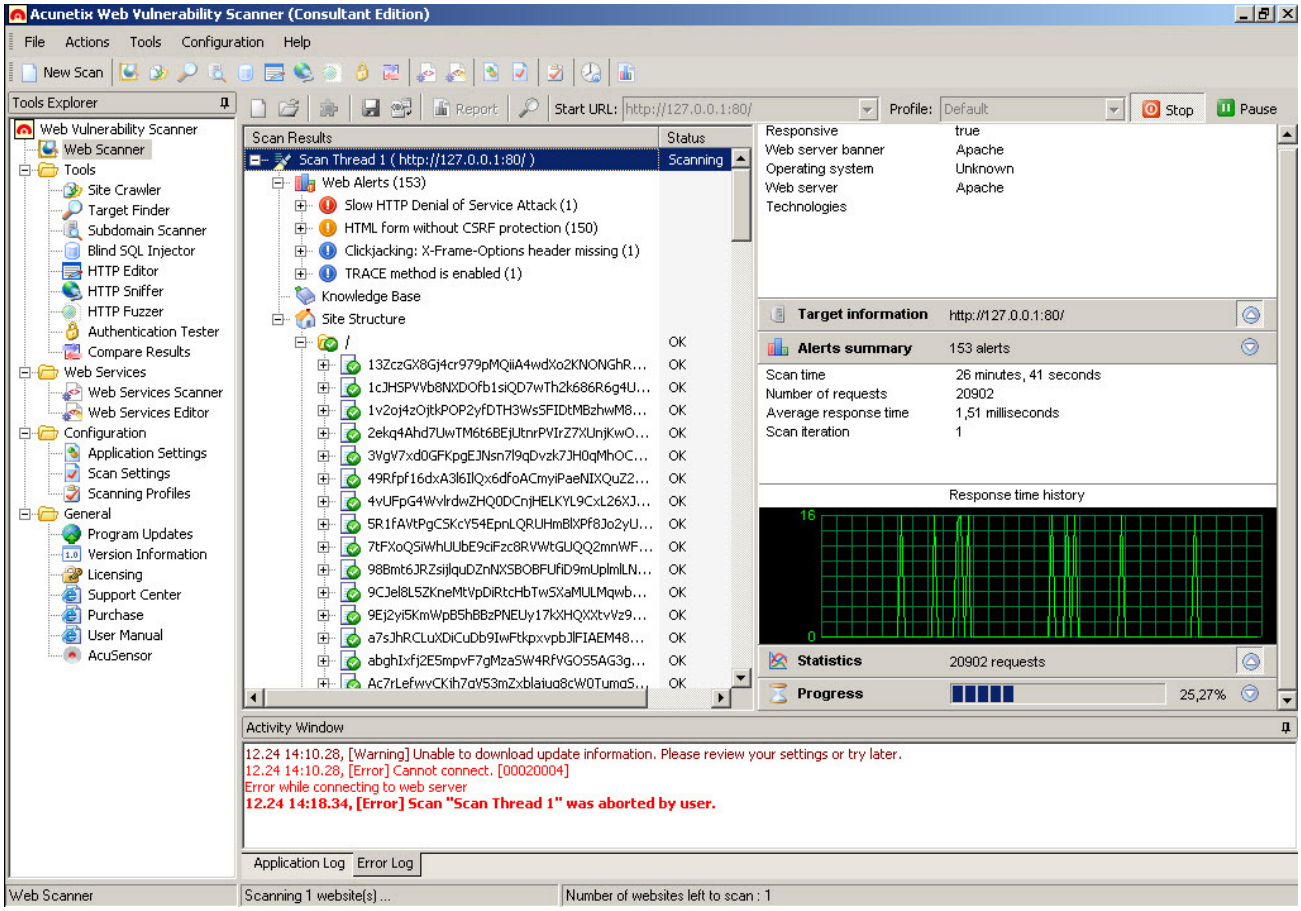


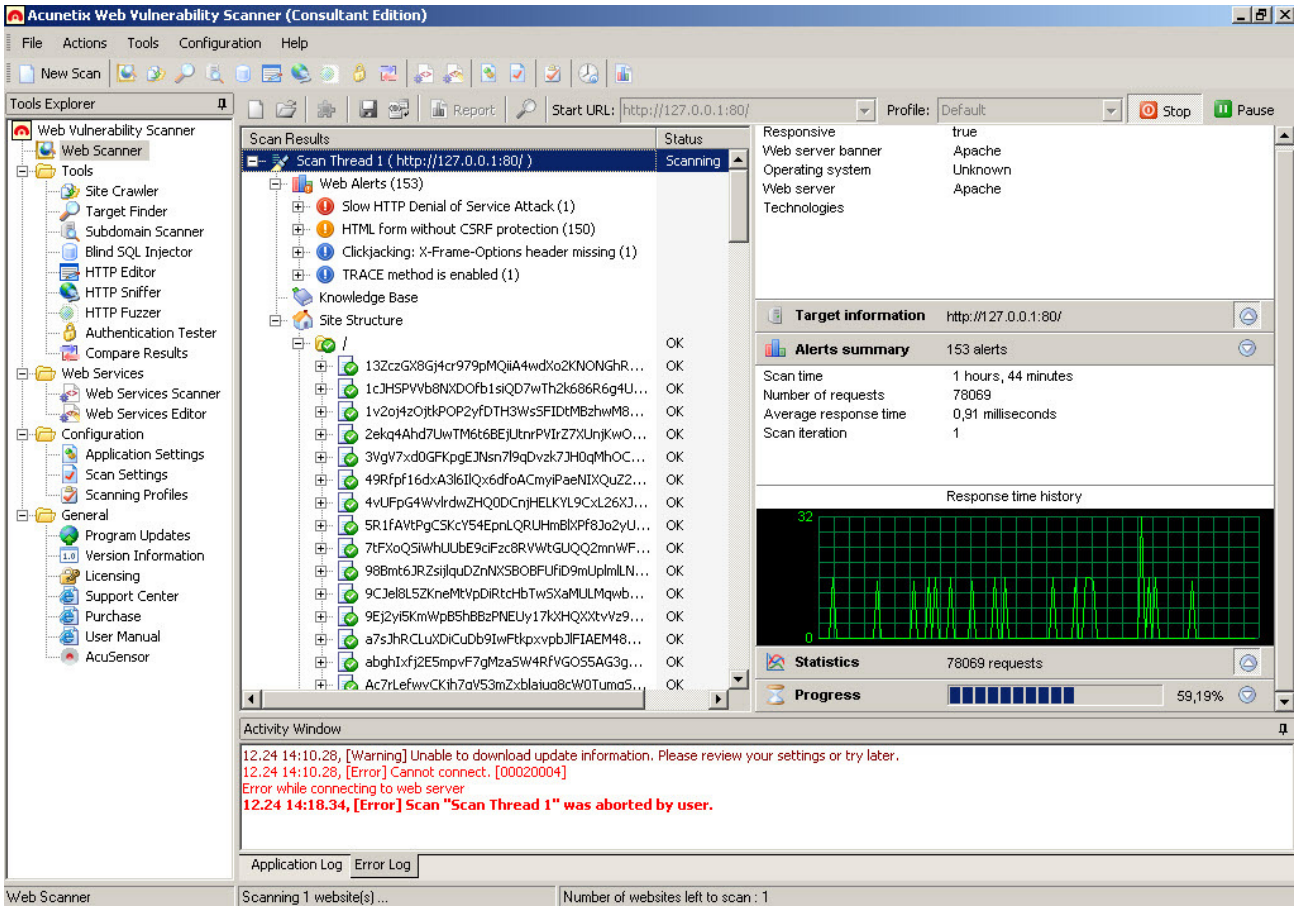
Sıra Netsparker ve Acunetix ile test yapmaya geldiğinde, Netsparker Community Edition sürümünün, başladığı taramayı 4 saat sonunda hala bitiremediğini ve artan bellek kullanımı nedeniyle işletim sistemi üzerinde bellek sorununa yol açtığını gördüm.





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





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

Örnek PHP uygulamasına ve mod_rewrite kuralı içeren httpd.conf dosyasını buradan indirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Mutlu Yıllar

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

By M.S on December 31st, 2013

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

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

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

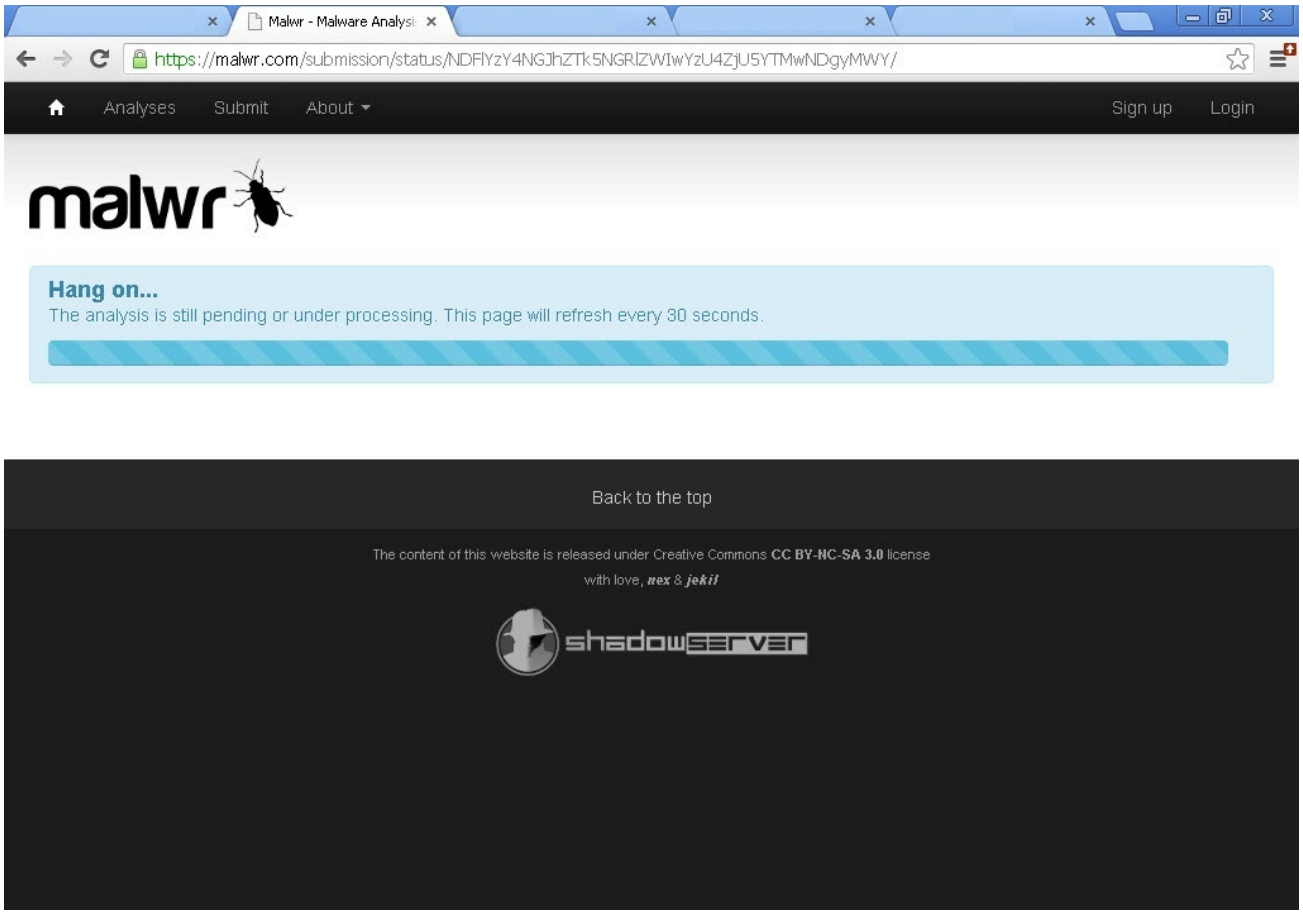
Yukarda da belirttiğim üzere geçtiğimiz yıllara oranla sızma testi uzmanlarına talep daha da arttı. Fakat buradan siber güvenlik uzmanlarını, sızma testi uzmanlarını kurnaz insan kaynakları danışmanlık firmalarına karşı uyarmakta fayda var. Kimi danışmanlık firmaları, Linkedin üzerinden grep CEH, grep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

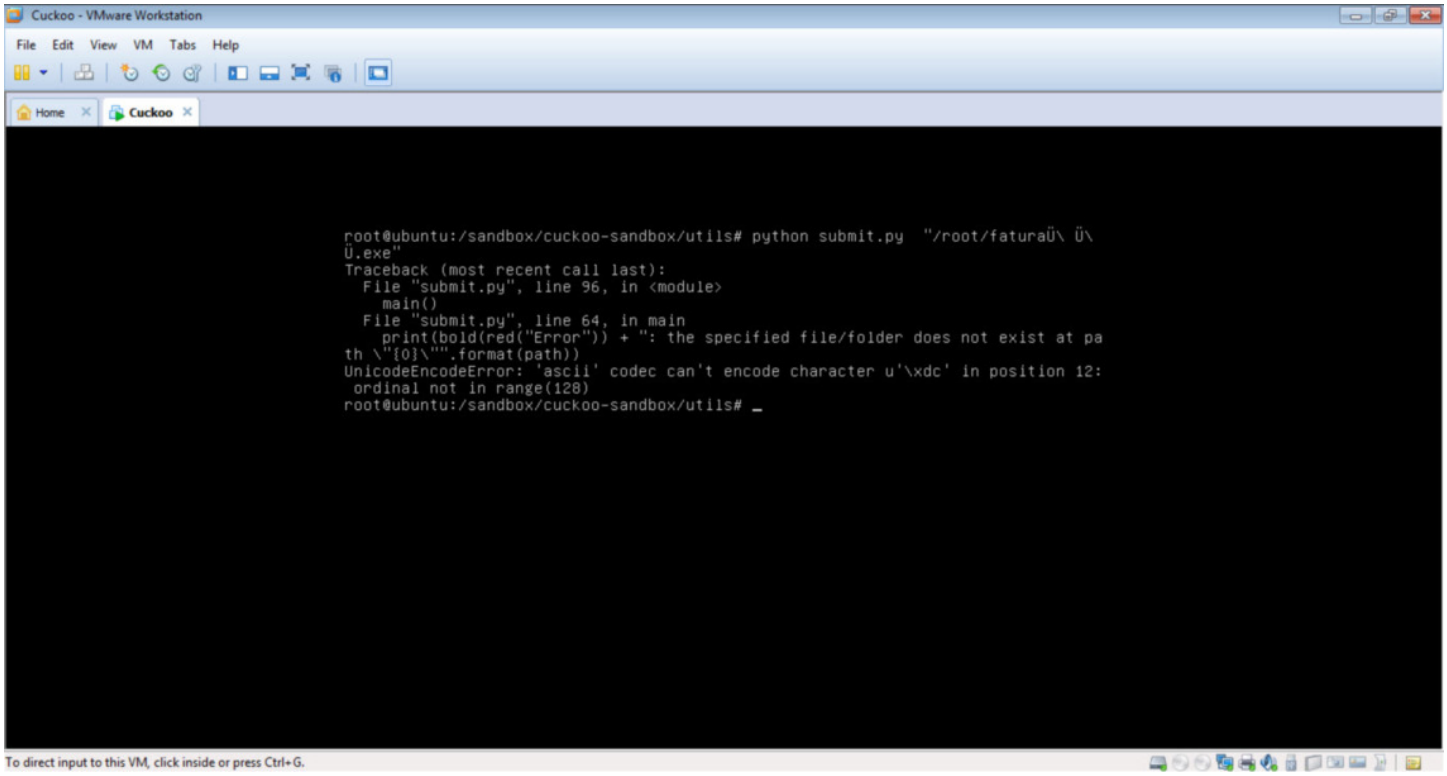
2013 yılı benim için bol bol sızma testi, zararlı yazılım analizi, blog yazısı, sunum, teknik çalışma ve Güvenlik TV ile geçti. Hacking haberleri sayesinde sızma testinin kurumlar için önemine dikkat çekmenin artık anlamsız olduğu şu günlerde, zararlı yazılım analizinin kurumlar için (özellikle bankacılık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

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

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

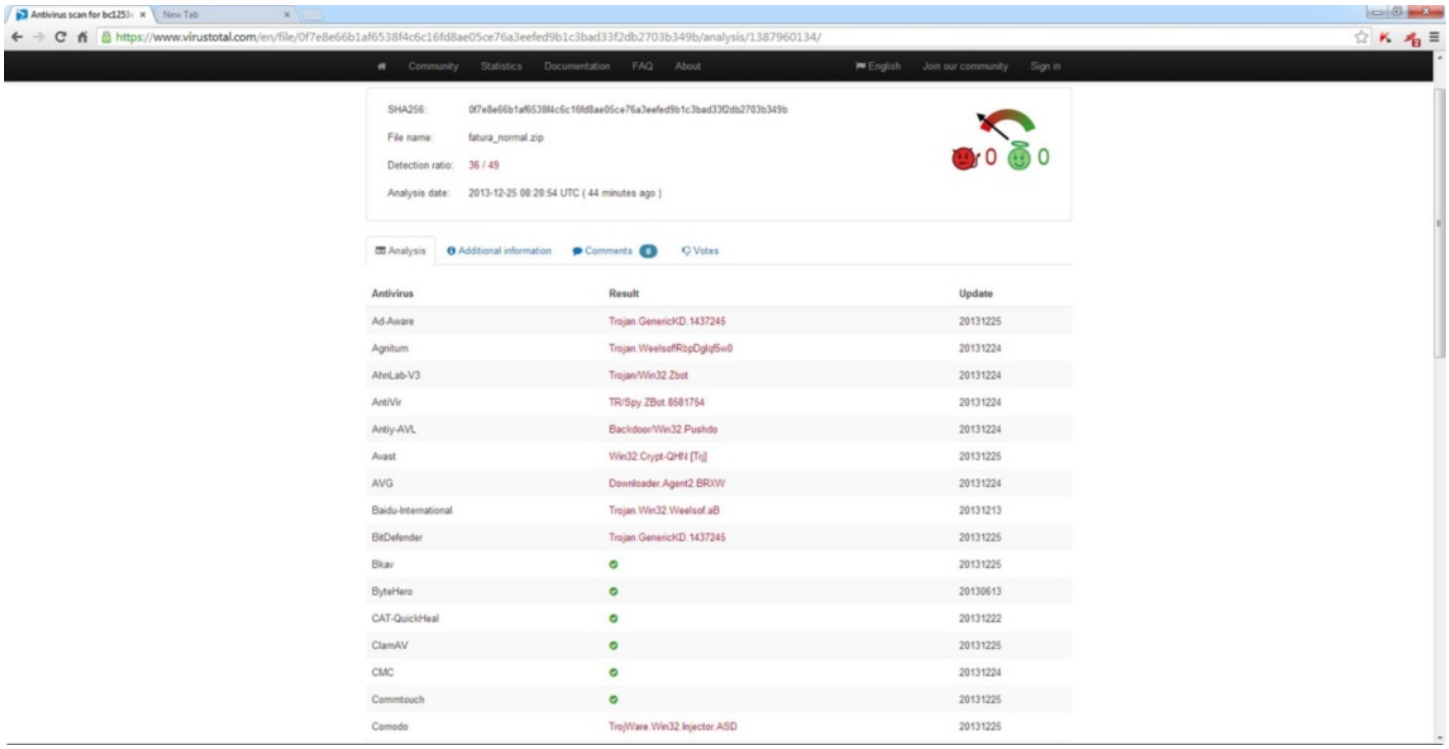
Günler önce faturaÜ Ü Ü.exe dosyasının, üzerinde Cuckoo Sandbox çalışan malwr.com adresine gönderilmiş ve hala kısır döngüde kalmış analizine buradan ulaşabilirsiniz.

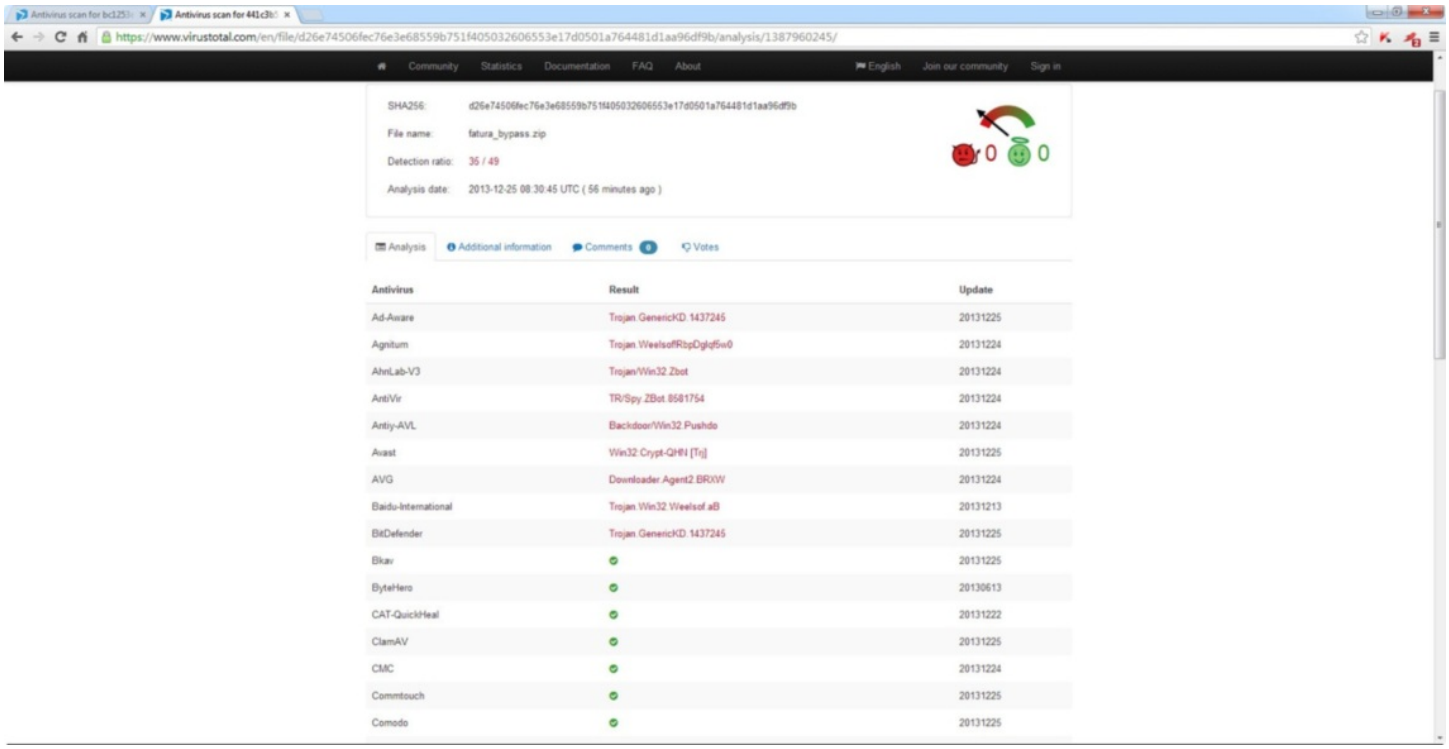




Tabii diyeceksiniz ki adını fatura.exe yapıp yollasam analiz başarıyla tamamlanmayacak mı ? Tamamlanacak fakat zararlı yazılım çalıştıktan sonra hangi isim altında çalışıp ona göre zararlı fonksiyonları çağıracaksa şekilde tasarlanmış olsaydı o da çözüm olamayacaktı kısaca kod analizi yapmadan her zaman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

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





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 :)
