

Bu yazımda <https://malware-traffic-analysis.net/2014/12/04/index.html> sitesindeki pcap dosyasını inceleyerek sitede sorulan soruları yanıtlıyacağım. Soruları yanıtlamadan önce zararlı yazılımın özet ilerleyişini açıklayayım.

Bu uyarıları inceledikten sonra pcap dosyasına dönerek incelemeye başladım. İlk olarak pcap dosyasının bulunduğu sitede de bahsedilen “basic” filtreyi kullandım ve ilk pakette yönlendirme yapıldığını gördüm (status 302).

The image shows a Wireshark packet capture window titled "2014-12-04-traffic-analysis-exercise.pcap". The packet list on the left shows a series of packets from 18 to 917. The packet details pane on the right shows the selected packet (No. 18) which is an HTTP GET request. The status line indicates "302 Found". The response body contains a redirect to "http://www.google.at/?gfe_rd=cr&ei=caeAVNyDM86o8wf654FA".

No.	Time	Source	src port	Destination
18	0.498959	192.168.137.62	50393	74.125.232.64
32	2.886210	192.168.137.62	50396	173.194.116.111
112	4.811335	192.168.137.62	50397	173.194.116.111
113	4.811337	192.168.137.62	50399	173.194.116.111
114	4.811683	192.168.137.62	50398	173.194.116.111
182	5.217755	192.168.137.62	50401	173.194.67.94
193	5.217757	192.168.137.62	50400	173.194.67.94
243	5.415690	192.168.137.62	50403	173.194.78.94
244	5.415691	192.168.137.62	50402	173.194.78.94
419	6.126229	192.168.137.62	50404	173.194.78.103
480	6.238078	192.168.137.62	50405	173.194.78.103
504	6.358914	192.168.137.62	50406	173.194.116.111
505	6.358916	192.168.137.62	50407	173.194.116.111
603	7.032364	192.168.137.62	50408	74.125.232.69
694	7.032366	192.168.137.62	50409	74.125.232.69
831	11.326928	192.168.137.62	50410	173.194.116.111
866	14.192779	192.168.137.62	50411	173.194.116.111
870	14.887272	192.168.137.62	50411	173.194.116.111
882	15.409224	192.168.137.62	50412	216.9.81.189
891	20.811960	192.168.137.62	50413	216.9.81.189
916	21.211265	192.168.137.62	50415	216.9.81.189
917	21.211267	192.168.137.62	50416	216.9.81.189

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: google.com
Connection: Keep-Alive

HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Location: http://www.google.at/?gfe_rd=cr&ei=caeAVNyDM86o8wf654FA
Content-Length: 256
Date: Thu, 04 Dec 2014 18:26:57 GMT
Server: GFE/2.0
Alternate-Protocol: 80:quic,p=0.02

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.at/?gfe_rd=cr&ei=caeAVNyDM86o8wf654FA">here</A>
</BODY></HTML>
```

Yönlendirme yaptığı siteyi ilk gönderdiği istek paketine dönen cevap paketinden hemen sonra görebiliriz. Buradaki pakette ilk dikkat çeken URL kısmında “earsurgery.org” alan adında farklı bir site adresine gidiliyordu. Bunun dışında anormal bir durum göremedim.

The image shows a Wireshark packet capture window titled "Wireshark - Follow TCP Stream (tcp.stream eq 18) - 2014-12-04-traffic-analysis-exercise.pcap". The packet list on the left shows a series of packets from 18 to 917. The packet details pane on the right shows the selected packet (No. 18) which is an HTTP GET request. The status line indicates "200 OK". The response body contains a redirect to "http://www.google.at/?gfe_rd=cr&ei=caeAVNyDM86o8wf654FA".

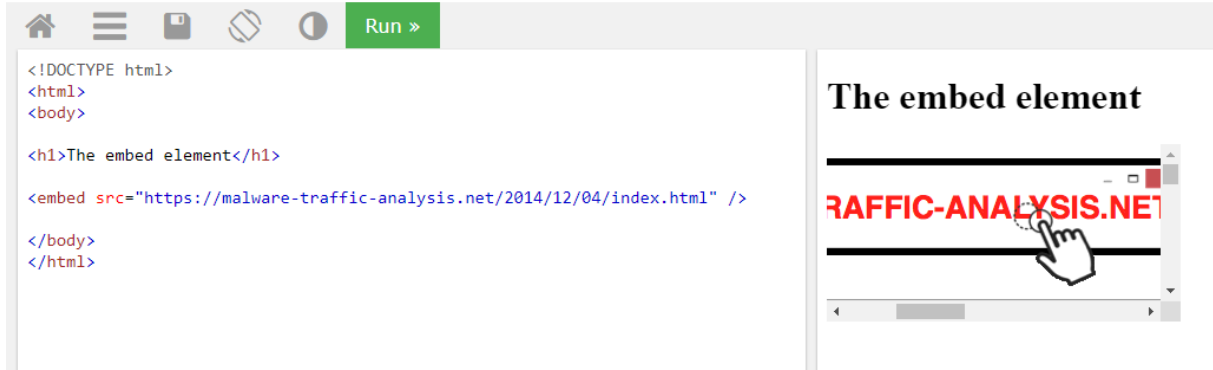
```
GET /url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCQqFjAA&url=http%3A%2F%2Fwww.earsurgery.org%2F&ei=e6eAVJG0Bjbjaqm9gWg&usq=AFQjCNEsqoW9ENBFsvEzZQIy1-s5KA1Rag&bvm=bv.80642063,d.bGQ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: www.google.at
Connection: Keep-Alive
Cookie: PREF=ID=b648836f9bae87ab:U=2ac186418173f160:FF=0:TM=1417717619:LM=1417717621:S=Dq05AsDd2VnDTIFT;NID=67=f9Imwce6neDp3tgAm0upu_ncwP9-GETSbgcpmEontnA3iHTG6vvrnZbVImpGKXAtJTLF22emKD7jvhvMigI16b6Gn4-McNKQBG_gjPRsqWd54FT8Lr-4EDriTM-PrWARi; OGPC=5-1:

HTTP/1.1 200 OK
Date: Thu, 04 Dec 2014 18:27:11 GMT
Expires: Thu, 04 Dec 2014 18:27:11 GMT
Cache-Control: private
X-Frame-Options: ALLOWALL
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 513
X-XSS-Protection: 1; mode=block
Alternate-Protocol: 80:quic,p=0.02

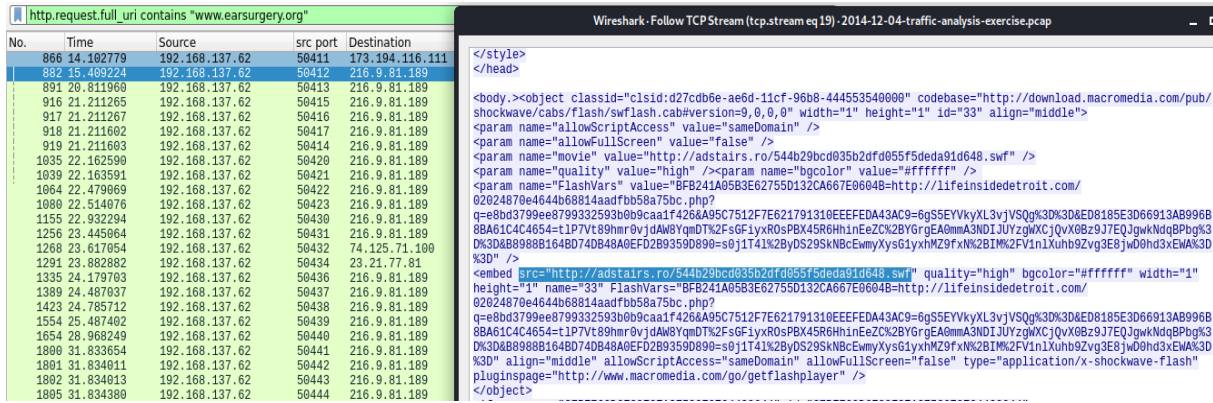
.....S...+..^.(N...!Q+..U{.MOiZa.m.lR.I-+.^p...6.pa....x....Q6.>.R.R.....".#.....N
```

Bu durumu incelemek için “earsurgery.org” adresi filtreleyerek trafiği incelemeye başladım. Filtreleme sonrası yönlendirdiği web sitesinin html kodundaki yönlendirme etiketlerini incelerken “embed” etiketi içerisinde bir “.swf” uzantılı dosyayı sayfada görüntülediğini gördüm (dosyanın indirilmesini sağlıyor) . (“embed” etiketinin işlevi hakkında bir fikriniz yoksa görseldeki gibi bir veriyi sitemizde

göstermemize olanak sağlıyor diyebiliriz. Aşağıda da incelediğimiz sitenin adresini örnek olarak gösterdim.)

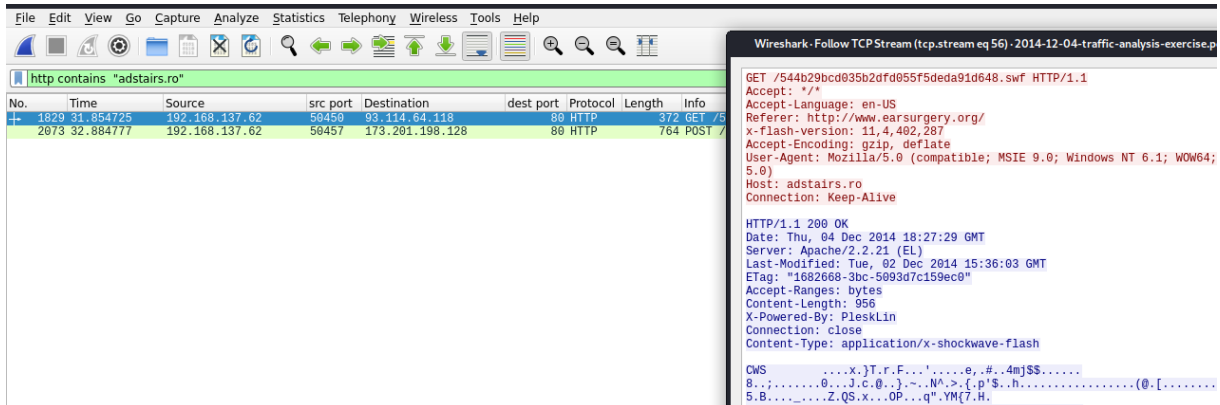


(“embed” etiketi çalışma şekli)



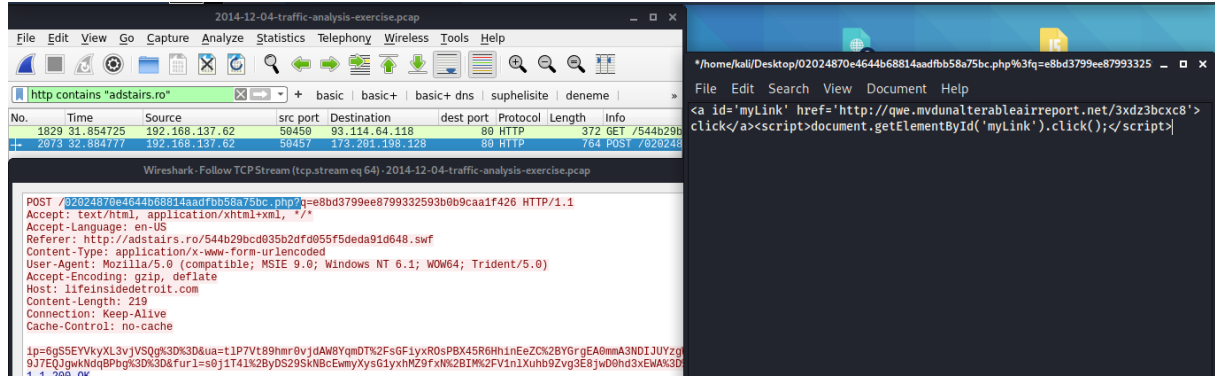
(paket içindeki swf dosyası indirtme linki)

Bu etikette “Flashvars” özneteliğini kullanarak adresi Flash dosyasına dosya açılmadan aktarılmasını sağlıyormuş. Flashvars özneteliğinin işlevi için <https://helpx.adobe.com/tr/flash/kb/pass-variables-swfs-flashvars.html> veya <https://www.mediacollege.com/adobe/flash/actionsript/flashvars.html> adresine göz atabilirsiniz. Daha sonra “adstairs.ro” sitesini filtreleyerek trafiğini incelemeye başladım. Filtrelediğimde iki trafik içerdiğini gördüm. İlki Flash dosyası indiriyordu. Virüs Total linkine özet sonundan erişebilirsiniz.

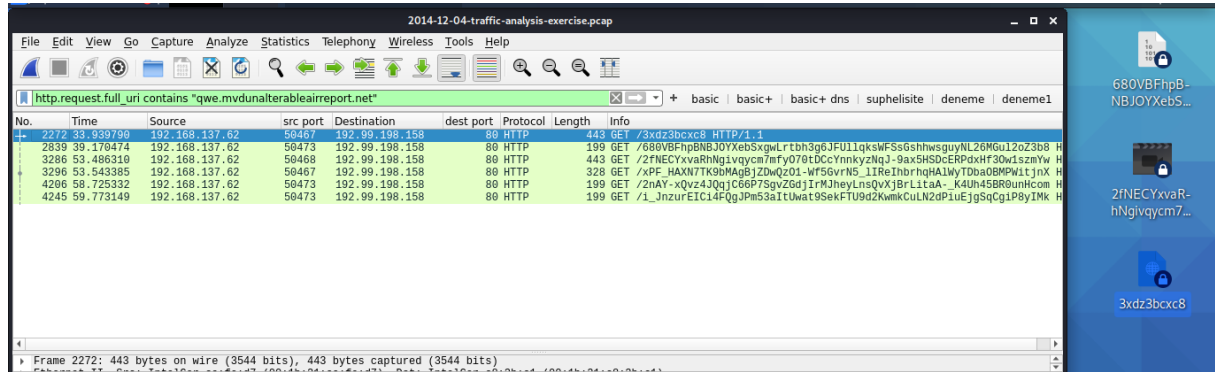


İkinci paketi açtığımda şifreli olduğunu gördüm. Paketi masaüstüme çıkardım ve içeriği aşağıdaki gibi “lifeinsidedetroit.com” adresine göndererek aşağıdaki sayfayı yüklüyordu. Flash sürümü için

https://www.cvedetails.com/vulnerability-list/vendor_id-53/product_id-6761/version_id-137508/Adobe-Flash-Player-11.4.402.287.html inceleyebilirsiniz.



Görüldüğü gibi sayfa açıldığında “a” etiketi arasında tanımlanan adrese “click” fonksiyonu ile yönlendiriyor. Yönlendirdiği sitenin trafiğini incelemek için de kullandığım filtre aşağıdaki gibidir. Buradaki trafikte biri web sitesi ve biri Flah olmak üzere üç farklı dosya indirildiğini gördüm. Dosyalar aşağıdaki görseldeki gibidir.



Dosyalardan birinin Flash dosyası, birinin türü belirlenmeyen veri dosyası olduğunu gördükten sonra md5 hash değerlerini alarak Virus Total sitesinde tarattım. Linklerine trafik özetinin sonundan erişebilirsiniz. Daha sonra son olarak yüklenen web sitesinin içeriğine yöneldim. Web sayfasındaki javascript kodunun anlaşılır olmadığını görünce sayfayı web sitemde açarak debug etmeye karar verdim. Debug öncesi ve debug sonrası elde ettiğim yapılar aşağıdaki gibidir (debug sonrası halini bir javascript dosyası oluşturarak düzenlemeye çalıştım).



(debug öncesi)

```

function Target() {
window['aHorUa'] = true; paps0 = '';
window.sf325gtgs7sfdj = window.sf325gtgs7sfdj = window.sf325gtgs7sfdj = window.sf325gtgs7sfdj = false; }

function gs7sfd(txt) {
var v1='XM'+LD'+OM', v2 = 'pa'+rseE'+rr'+or', v3 = 'loa'+dX'+ML', v4 = 'DT'+D X'+HTML 1.0 Transitional', v5 = 'err'+orC'+ode';
var resInf = new ActiveXObject("Microsoft.+v1), subpath= "c:\\Windows\\System32\\drivers\\"+txt+".sys";
resInf.async = true;
resInf[v3](<!DOCTYPE html PUBLIC "-//W3C//+v4+//EN" "res://+ subpath + ">');
if (resInf[v2][v5] != 0) { var pe=resInf[v2], err = "Error Code: " + pe[v5] + "\n"; err += "Error Reason: " + pe.reason; err += "Error Line: " + pe.line;
if (err.indexOf("-2147023083") > 0) { return 1; } else { return 0; } } return 0; }

var tmp;
try{ tmp = new ActiveXObject("Kaspersky.IeVirtualKeyboardPlugin.JavascriptApi.1"); }catch(e){ tmp = false; }

if (tmp || gs7sfd("kl1") || gs7sfd("tmactmon") || gs7sfd("tmcomm") || gs7sfd("tmevtmgr") || gs7sfd("TMEBC32") || gs7sfd("tmeext") || gs7sfd("tmnciesc") || gs7sfd("tmtdi")
{ Target(); }
else { function Check(s){ x = document.createElement('script'); x.onload = Target; x.src = s; document.body.appendChild(x); return 0; }

var kv1 = "res://C:\\Program Files", kv2 = "\\Kaspersky Lab\\Kaspersky ", kv3 = "Anti-Virus ", kv4="Internet Security ", kv5="\\shellx.dll/#2/#102", kv6="\\mfc42.dll/#2/#
for (var i = 0; i < pathdata.length; ++i) Check(pathdata[i]);

function pausecomp(millis) { var date = new Date(); var curDate = null; do { curDate = new Date(); } while(curDate-date < millis); } pausecomp(1000); }

```

(debug sonrası)

Kodu gördükten sonra içeriğini daha net anlayabilmek için internete bakındığımda şu sayfadaki yazıyı buldum.

<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/endless-evasion-racing-game/>

Gördüm ki her ne kadar temsil edildikleri yöntemler farklı olsa da kod içerisinde de bu sitede verilen uzantılarla aynı uzantıdaki sistem ve uygulama dosyaları taranıyordu. Yazıda da açıklandığı gibi tespit edilmekten kaçınmak için kullanılan bir yöntem olduğundan bahsediyor. Trafiği tanımlayabildiğim kısmı buraya kadardı. Bundan sonra soruları cevaplamaya başlayabiliriz.

Flash dosyası: (adstairs.ro)

<https://www.virustotal.com/gui/file/f4e0c392b0249bd307b818cffa8a5b8ee5259a44fa0405f445e279da7e1206e6/detection>

Tanımsız veri dosyası için: (qwe.mvdunalterableirreport.net)

<https://www.virustotal.com/gui/file/56ff9d6a452cbd91733ca40a62b3957763c8b59ca6b34a9a6c9a96c7c850b6c9/details>

Yüklenen html sayfası için: (qwe.mvdunalterableirreport.net)

<https://www.virustotal.com/gui/file/5fea68286308c28a085d623f905689ad626636f68ff42ae924d373211b16868f/detection>

Flash dosyası için: (qwe.mvdunalterableirreport.net)

<https://www.virustotal.com/gui/file/9ab41d23faf07b25e378489e585ff83d39a10a6ff5eca5b7bb96f321992ce744/detection>

PCAP:

<https://www.virustotal.com/gui/file/6ba80e45e35260a70899b1d79ea7965deae621a2851aa6eec56a122c23dd133/details>

TEMEL SORULAR:

1) Virüs bulaşan Windows ana bilgisayarının IP adresi nedir?

- "dhcp" fitresini kullanarak 192.168.137.62 olduğunu görebiliriz.

2) Virüs bulaşmış Windows ana bilgisayarının MAC adresi nedir?

- Aynı filtrenin ("dhcp") sonucunda 192.168.137.62 kaynak IP adresli paketin Ethernet çerçevesine bakarak 00:1b:21ca:fe:d7 olarak buluruz.

3) Güvenliği ihlal edilen web sitesinin alan adı nedir?

- İçerisine "embed" etiketiyle link bulunduran "earsurgery.com" sitesidir.

4) Güvenliği ihlal edilen web sitesinin IP adresi nedir?

- ' http.request.full_uri contains "earsurgery.org" ' filtresini kullanarak IP adresini 216.9.82.189 olarak bulunur.

5) Açıklardan yararlanma kitini ve kötü amaçlı yazılım yükünü sağlayan alan adı nedir?

-Trafik akışında da görüldüğü öncelikle "adstairs.ro" sitesinden indirilen Flash dosyasından dolayı "earsurgery.com" sitesi ve devamında "lifeinsidedetroit.com" sitesinde bir yönlendirme linki ile "qwe.mvdunalterableirreport.net" sitesinden indirmeler yapılmıştı. Bu yüzden kötü amaçlı yazılım yükünü sağlayan alan adına "qwe.mvdunalterableirreport.net" ve ""earsurgery.com" alan adlarını verebiliriz. (Cevap dosyasında sadece "qwe.mvdunalterableirreport.net" sitesini vermiş ama "adstais.ro" sitesinde de zararlı yazılım içeren Flash dosyası vardı. (Henüz içeriğini analiz edemediğim için tam olarak bir cevap veremiyorum ama İçerisine zararlı yazılıma yönlendirme linki yerleştirildiği için görülmüyor olabilir. Yani işlevi sadece zararlı yazılıma yönlendirmek için kullanılıyor olabilir.))

6) Açıklardan yararlanma kitini ve kötü amaçlı yazılım yükünü sağlayan IP adresi nedir?

-IP adresini de dördüncü soruda kullandığımız filtreyi kullanarak benzer şekilde 192.99.198.158 ("qwe.mvdunalterableirreport.net") ve 92.11464.118 ("adstais.ro") olduğunu bulabiliriz.

DAHA GELİŞMİŞ SORULAR:

1) Bu pcap tarafından hangi snort olayları (VRT veya EmergingThreats) üretilir?

-

2) Kullanım kiti (EK) nedir?

- Angler exploit kit (<https://www.2-remove-virus.com/tr/angler-exploit-kit-nedir/>)

3) Açıklardan yararlanma kiti (EK) açılış sayfasına işaret eden yönlendirme URL'si nedir?

- "lifeinsidedetroit.com" sitesinden yapılmıştır. URL kısmına trafik özeti kısmından ulaşabilirsiniz.

4) Yararlanma kiti (EK) açılış sayfasına işaret eden yönlendirme URL'sinin IP adresi nedir?

- "lifeinsidedetroit.com" sitesinin trafik özeti kısmında hedef IP kısmına bakarsanız 173.201.198.128 olduğunu görebilirsiniz.

5) Hangi TCP akışı, teslim edilen kötü amaçlı yazılım yükünü gösterir?

- Kötü amaçlı yazılımı gösteren sitenin kurban bilgisayara gönderdiği paketleri incelerken "application/octet-stream" tipide dosya yüklendiğini gördüm.

Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
5064	qwe.mvdunalterableairreport.net	application/x-shockwave-flash	44 kB	2fNECYxvaRhNgivqycm7
5066	qwe.mvdunalterableairreport.net	text/html	94 kB	xPF_HAXN7TK9bMAgBjZI
5066	qwe.mvdunalterableairreport.net	text/html	46 kB	xPF_HAXN7TK9bMAgBjZI
5105	qwe.mvdunalterableairreport.net	application/octet-stream	84 kB	i_JnzurEICi4FQgJpM53alt
5105	qwe.mvdunalterableairreport.net	text/html	0 bytes	i_JnzurEICi4FQgJpM53alt
5105	qwe.mvdunalterableairreport.net	text/html	0 bytes	i_JnzurEICi4FQgJpM53alt

Wireshark - Follow TCP Stream (tcp.stream eq 80) - 2014-12-04-traffic-analysis-exercise.pcap

```
GET /680VBFhpBNBJOYXebSxgwLrtbh3g6JFU1lqksWFSsGshhwsGuyNL26MGU12oZ3b8 HTTP/1.1
Connection: Keep-Alive
Host: qwe.mvdunalterableairreport.net

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Thu, 04 Dec 2014 18:27:38 GMT
Content-Type: application/octet-stream
Content-Length: 84705
Connection: keep-alive
Cache-Control: no-cache, must-revalidate, max-age=1
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Last-Modified: Sat, 26 Jul 2040 05:00:00 GMT
Pragma: no-cache

....4nha.E1b4..Mc.2...m.pQ2b.mkadWVetn.,>R2.$..e.k:..
.].r..U..I..cd+ha.vd.4Nha..Fc"0.q..3.q.Ps..3...i 4.L`4n[....e8?...P2b...HURb..da...'.>.d.S.<.>
$. ....T..r.GM..h.sjd.*...b.5m-i4.dF....@.30....a."k0..9.:b....5.g4c.RcdR...v.....~.DfSR.6.~..h.
4.@Jp..'7[r..<g.b.fj....~...3.,..Zjk.g. ;*.Z.&
.3...0.FFS.mn...g..jb..c". $Ex..f.+h..V.e....&.z.:Lq..&..].!..P..k05:=.:b..d21.e..oha.>.B...!..R"b4..Mc.
2.IRk...B..L].%b.4.;i...Ai[...2b4..5k.ud.*LEk.uva8.%@N.I5nh. v.Q...m.i....4Et..N7.g...A..mk.4.q.7.8..
z}....Ep.nF,...dR2...~...2b4n.l2Q.2.....$.J#fb4.^.....$.h.dRXbb.;m.3.....>:i..b.ed.e..nha....i(a
2b4].d.Vrbe?..@Fb3e.?q..X.b.?u2.e~k0.ed.e..nha.&.n...aDR2..Bo!d.|^.*YIg.T._~.k83.4.h7..b.cF.t.RXcb...
4 ha4 581f : 6h le h "R & i> v" f 0v>5 c X n# &
```

<https://file.org/extension/octet-stream> sitesinde bulduklarına göre web tarayıcılarının dosya ekinin bilinmeyen bir dosya türüne ait olduğunu anlaması için geliştirildiğini anlatıyor. Dosyanın uzantısını düzenleyerek (hangi formatta ise) dosyanın uygun uygulamalar ile açılacağından bahsediyor. Bu trafikte ise “octet-stream” formatından herhangi bir dosya indirilebilir olduğu için “tcp.stream == 80” diyebiliriz.

6) Bu kötü amaçlı yazılım bulaşmasının neden olduğu HTTPS geri arama trafiğinin alan adı ve IP adresi nedir?

- Burada “HTTPS” olduğu için SSL/TLS trafiğine baktığımızda aşağıdaki görselde de görüldüğü gibi öncelikle “Google.at” sitesinde gönderilen “Client Hello” paketi yerini “aemmiphbwueuef59.com” ile değiştiriyor. IP adresi 209.126.97.209 olarak bulunur. (Yani anladığım kadarıyla “callback” kötü amaçlı yazılım bulaşması sonrası farklı bir siteye kurban bilgisayardan bağlantı isteği göndermesiyle oluşuyor.)

<https://tools.ietf.org/id/draft-ietf-tls-esni-08.html#name-overview>

<https://serializethoughts.com/2014/07/27/dissecting-tls-client-hello-message>

tls.handshake.extensions_server_name									
No.	Time	Source	src port	Destination	dest port	Protocol	Length	Server Name	Info
112	4.811335	192.168.137.62	50397	173.194.116.111	443	TLSv1	203	www.google.at	Client Hello
113	4.811337	192.168.137.62	50399	173.194.116.111	443	TLSv1	203	www.google.at	Client Hello
114	4.811683	192.168.137.62	50398	173.194.116.111	443	TLSv1	203	www.google.at	Client Hello
594	6.358914	192.168.137.62	50406	173.194.116.111	443	TLSv1	203	www.google.at	Client Hello
595	6.358916	192.168.137.62	50407	173.194.116.111	443	TLSv1	203	www.google.at	Client Hello
831	11.326928	192.168.137.62	50410	173.194.116.111	443	TLSv1	203	www.google.at	Client Hello
2535	35.109309	192.168.137.62	50472	173.194.116.121	443	TLSv1	217	googleads.g.doubleclick.net	Client Hello
3114	48.292229	192.168.137.62	50476	209.126.97.209	443	TLSv1	178	aemmiphwueuf59.com	Client Hello
4249	59.835573	192.168.137.62	50494	209.126.97.209	443	TLSv1	178	aemmiphwueuf59.com	Client Hello

<ul style="list-style-type: none"> Ethernet II, Src: IntelCor-ca:fe:d7 (00:1b:21:ca:fe:d7), Dst: IntelCor_c8:3b:c1 (00:1b:21:c8:3b:c1) Internet Protocol Version 4, Src: 192.168.137.62, Dst: 209.126.97.209 Transmission Control Protocol, Src Port: 50494, Dst Port: 443, Seq: 1, Ack: 1, Len: 124 Transport Layer Security <ul style="list-style-type: none"> TLSv1 Record Layer: Handshake Protocol: Client Hello <ul style="list-style-type: none"> Content Type: Handshake (22) Version: TLS 1.0 (0x0301) Length: 119 Handshake Protocol: Client Hello <ul style="list-style-type: none"> Handshake Type: Client Hello (1) Length: 115 Version: TLS 1.0 (0x0301) Random: 5481f942f3fd4121d668825a644f031110df7ee5e0c6d8e1... Session ID Length: 0 Cipher Suites Length: 24 Cipher Suites (12 suites) Compression Methods Length: 1 Compression Methods (1 method) Extensions Length: 50 Extension: renegotiation_info (len=1) Extension: server_name (len=25) Extension: supported_groups (len=6)
--

EKSTRA SORULAR:

1) Kötü amaçlı yazılım yükünü çıkarın, gizlemesini kaldırın ve başlangıçta kabuk kodunu kaldırın. Bu size bulaşma için kullanılan gerçek yükü (bir DLL dosyası) vermelidir. Yükün MD5 karması nedir?

- (cevap anahtarından bakıldı) oktet/stream türündeki dosyanın trafiğine bakıldığında “adR2b4nh” karakterlerinin tekrarı dikkat çekiyor. Cevap anahtarında ise octet/stream dosyasıyla bu karakterleri xor yaparak

<https://www.virustotal.com/gui/file/d96b98cc0dbe7ea37250d4fca6d5d5656912f758de2b9bf6939c0d723119c56a/details> çıktısına ulaşıyor.

<https://malware.dontneedcoffee.com/2014/08/angler-ek-now-capable-of-fileless.html>

2) Yönlendirme URL'si ile bağlantılı olarak bir Flash dosyası kullanıldı. Bu flash dosyasını almak için hangi URL kullanıldı?

-Özet kısmında da açıkladığım gibi ilk olarak sayfada “embed” etiketleri arasında içerisinde bir link yerleştirilerek flash dosyası yükleniyordu. Bu uzantı

“adstairs.ro/544b29bcd035b2dfd055f5deda91d648.swf” uzantısıdır.

3) Trafikte, www.earthtools.org ve www.ecb.europa.eu için HTTP POST isteklerini görüyoruz. Bu HTTP POST isteklerini neden görüyoruz?

- POST isteklerini incelediğimizde ilk olarak “earthtools” sitesini kullanılarak saat bilgilerini gönderdiğini görüyoruz. Daha sonra “europa” ana bilgisayarında ise sanırım bulaşma öncesinden önceki üç ayın günlük ülkelerin para birimlerinin oranlarını gönderiyordu. Saat bilgileri ile sanırım araştırdığıma göre saat dilimini öğrenmek için kullanılıyor ama ülkelerin para durumunu neden gönderdiğini henüz anlamlandıramadım. (Gönderilen para oranlarının bilgisi gündelik gönderilmiş olsaydı kurban bilgisayarın gün içerisinde aktif olduğu saatleri öğrenmek için gönderildiğini düşünebilirdim.)

Wireshark - Follow TCP Stream (tcp.stream eq 81) · 2014-12-04-traffic-analysis-exercise.pcap

No.	Time	Source	src port	Destination	dest port	Protocol	Length	Size
2963	41.954765	192.168.137.62	50474	208.113.226.171	80	TCP	66	
2964	42.579691	208.113.226.171	80	192.168.137.62	50474	TCP	66	
2965	42.580835	192.168.137.62	50474	208.113.226.171	80	TCP	60	
2966	42.580927	192.168.137.62	50474	208.113.226.171	80	TCP	60	
2967	43.091727	208.113.226.171	80	192.168.137.62	50474	TCP	54	
2968	44.043416	208.113.226.171	80	192.168.137.62	50474	TCP	748	
2970	44.245319	192.168.137.62	50474	208.113.226.171	80	TCP	60	
3066	46.089115	208.113.226.171	80	192.168.137.62	50474	HTTP/XL	54	
3067	46.089452	192.168.137.62	50474	208.113.226.171	80	TCP	60	
3068	46.089453	192.168.137.62	50474	208.113.226.171	80	TCP	60	
3078	46.461986	208.113.226.171	80	192.168.137.62	50474	TCP	54	

```

POST /timezone/0/0 HTTP/1.1
Connection: Keep-Alive
Content-Length: 0
Host: www.earthtools.org

HTTP/1.1 200 OK
Date: Thu, 04 Dec 2014 18:27:40 GMT
Server: Apache
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/xml

1ef
<?xml version="1.0" encoding="ISO-8859-1" ?>
<timezone xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.earthtools.org/timezone.xsd">
<version>1.0</version>
<location>
<latitude>0</latitude>
<longitude>0</longitude>
</location>
<offset>0</offset>
<suffix>Z</suffix>
<localtime>4 Dec 2014 18:27:40</localtime>
<isotime>2014-12-04 18:27:40 +0000</isotime>
<utctime>2014-12-04 18:27:40</utctime>
<dst>False</dst>
</timezone>
  
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (794 bytes) Show and save data as ASCII

Wireshark - Follow TCP Stream (tcp.stream eq 82) · 2014-12-04-traffic-analysis-exercise.pcap

```

POST /stats/eurofxref/eurofxref-hist-90d.xml HTTP/1.1
Connection: Keep-Alive
Content-Length: 0
Host: www.ecb.europa.eu

HTTP/1.1 200 OK
Server: Apache/2.2.3 (Linux/SUSE)
Last-Modified: Thu, 04 Dec 2014 13:34:36 GMT
ETag: "120f79-129b5-50964056d9300"
Accept-Ranges: bytes
Content-Length: 76213
Content-Type: text/xml
Date: Thu, 04 Dec 2014 18:27:42 GMT
Connection: keep-alive

<?xml version="1.0" encoding="UTF-8"?><gesmes:Envelope xmlns:gesmes="http://www.gesmes.org/xml/2002-08-01"
xmlns="http://www.ecb.int/vocabulary/2002-08-01/eurofxref"><gesmes:subject>Reference rates</
gesmes:subject><gesmes:Sender><gesmes:name>European Central Bank</gesmes:name></gesmes:Sender><Cube><Cube
time="2014-12-04"><Cube currency="USD" rate="1.2311"/><Cube currency="JPY" rate="147.64"/><Cube currency="BGN"
rate="1.9558"/><Cube currency="CZK" rate="27.616"/><Cube currency="DKK" rate="7.44"/><Cube currency="GBP"
rate="0.7861"/><Cube currency="HUF" rate="306.9"/><Cube currency="LTL" rate="3.4528"/><Cube currency="PLN"
rate="4.1614"/><Cube currency="RON" rate="4.429"/><Cube currency="SEK" rate="9.2747"/><Cube currency="CHF"
rate="1.2035"/><Cube currency="NOK" rate="8.721"/><Cube currency="HRK" rate="7.6753"/><Cube currency="RUB"
rate="65.7875"/><Cube currency="TRY" rate="2.7556"/><Cube currency="AUD" rate="1.4692"/><Cube currency="BRL"
rate="3.1728"/><Cube currency="CAD" rate="1.3998"/><Cube currency="CNY" rate="7.5777"/><Cube currency="HKD"
rate="9.544"/><Cube currency="IDR" rate="15157.92"/><Cube currency="ILS" rate="4.9109"/><Cube currency="INR"
rate="76.2062"/><Cube currency="KRW" rate="1172.54"/><Cube currency="MYR" rate="17.2742"/><Cube currency="MXV"
  
```

1 client pkt, 56 server pkts, 1 turn.

4) Virüs bulaşmış ana bilgisayar tarafından hangi web tarayıcısı kullanıldı?

- Trafikteki "User agent" kısmında "MSIE 9.0" gösteriyor. (İnternet Explorer 9)

```

GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: google.com
Connection: Keep-Alive
  
```

5) Bu enfeksiyon sırasında exploit kit tarafından hangi 3 exploit gönderildi ve hangisi başarılı oldu?

- Gönderilen üç dosya sırasıyla csw, html ve octet-stream türlerindedir. Ama henüz inceleyebilecek kadar bilgiye sahip değilim. İncelediğimde buraya ekleyeceğim

<https://suricata.lcpdn.net/rules/rule.php?sid=2017732>