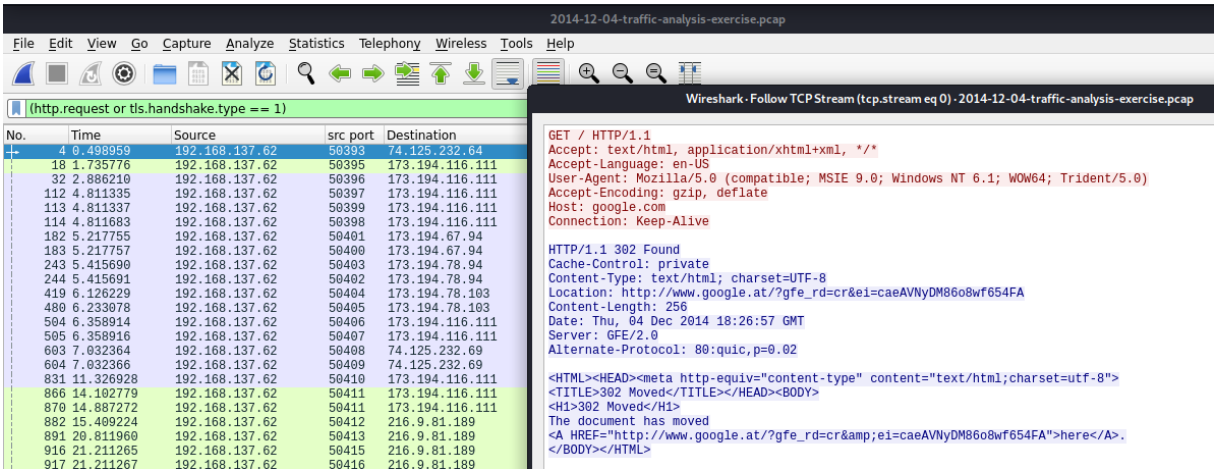
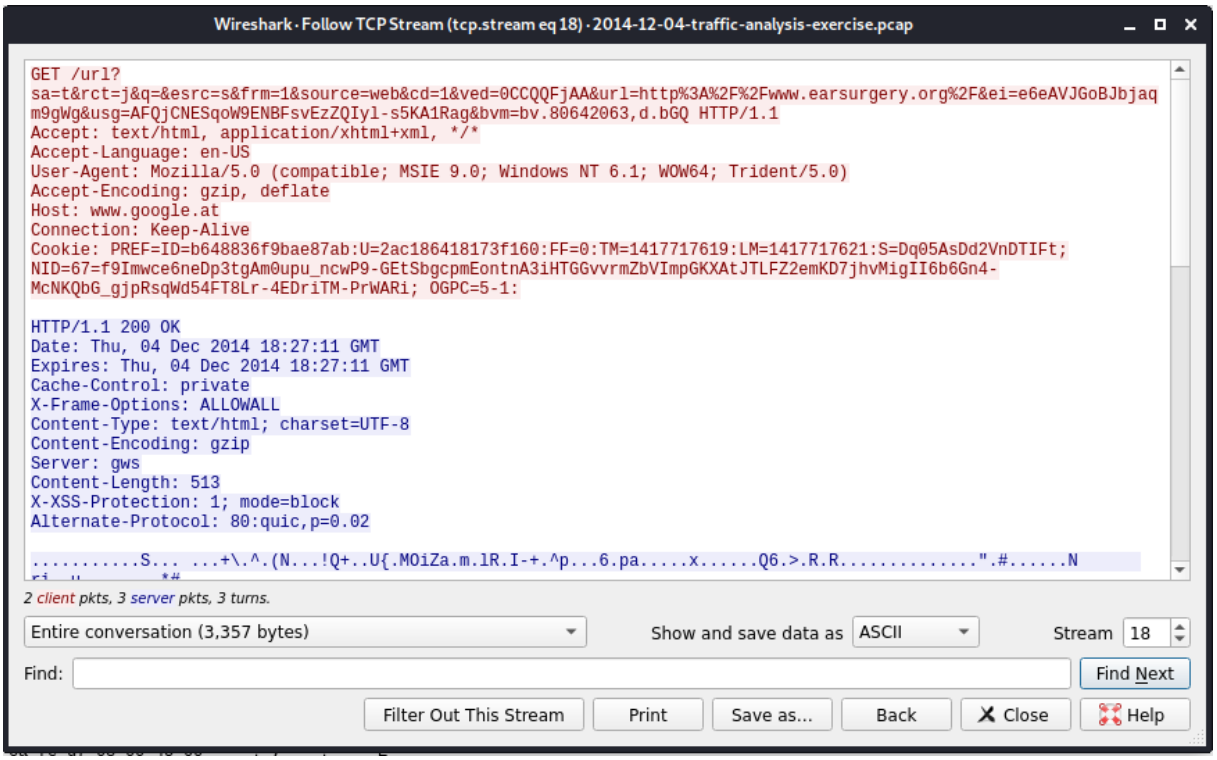
Bu yazımda https://malware-traffic-analysis.net/2014/12/04/index.html sitesindeki pcap dosyasını inceleyerek sitede sorulan soruları yanıtlayacağım. Soruları yanıtlamadan önce zararlı yazılımın özet ilerleyişini açıklayayım.

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).

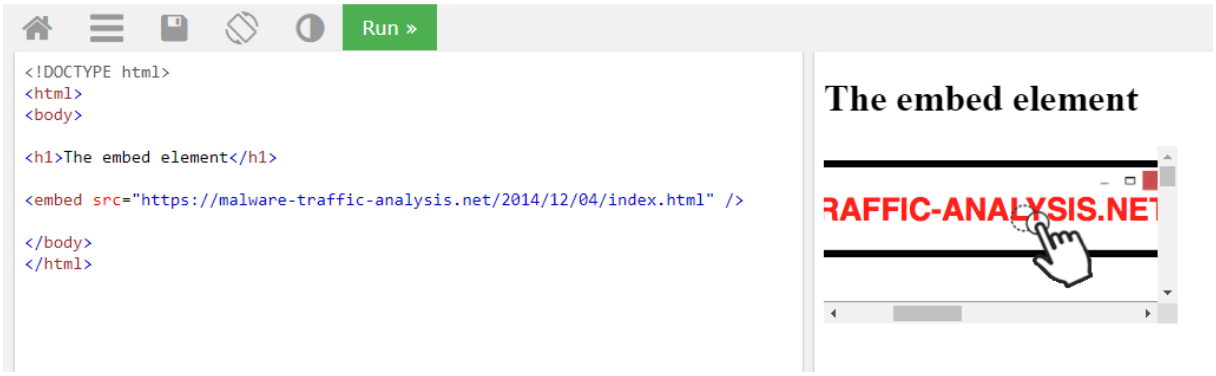


Yönlendirme yaptığı siteyi ilk gönderdiği istek paketine dönen cevap paketinden hemen sonra görebiliriz. Buradaki pakette ilk dikkat çeken URL kısmında “earsurgey.org” alan adında farklı bir site adresine gidiliyordu. Bunun dışında anormal bir durum göremedim.

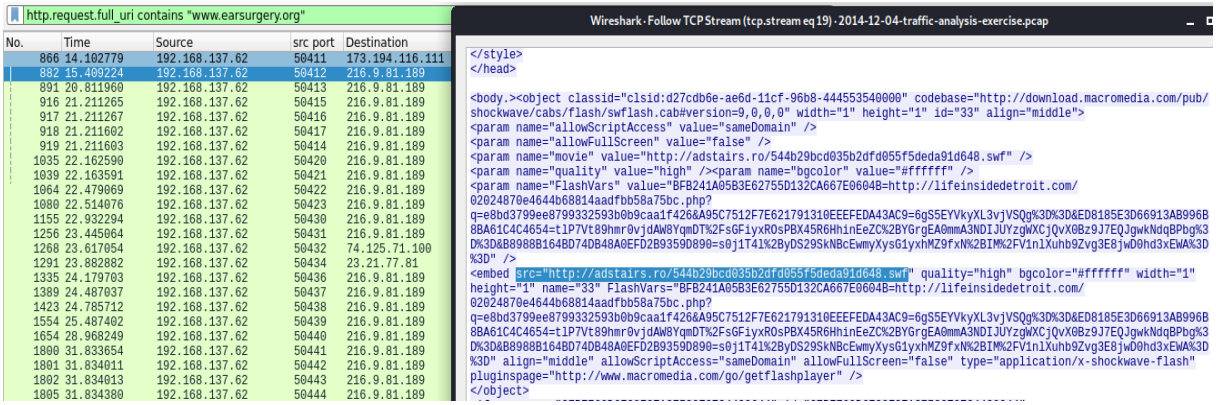


Bu durumu incelemek için “earsurgey.org” adresi filtreleyerek trafiği incelemeye başladım. Filtreleme sonrası yönlendirdiği web sitesinin html kodundaki yönlendirme etiketlerini incelerken “embed” etiketi içerisinde bir “.swf“ uzantılı dosyayı sayfada görüntülediğini gördüm (dosyanın indirilmesini sağlıyor)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

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

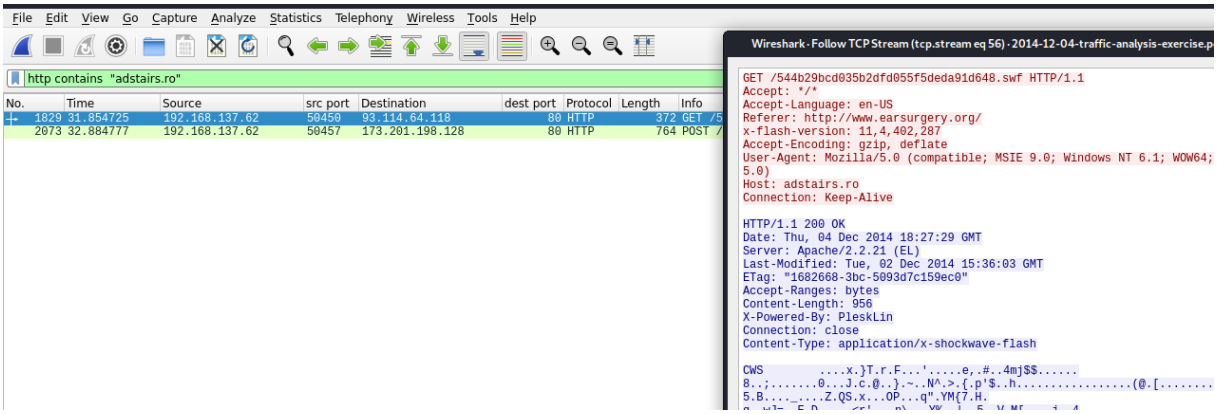


(“embed” etiketi çalışma şekli)



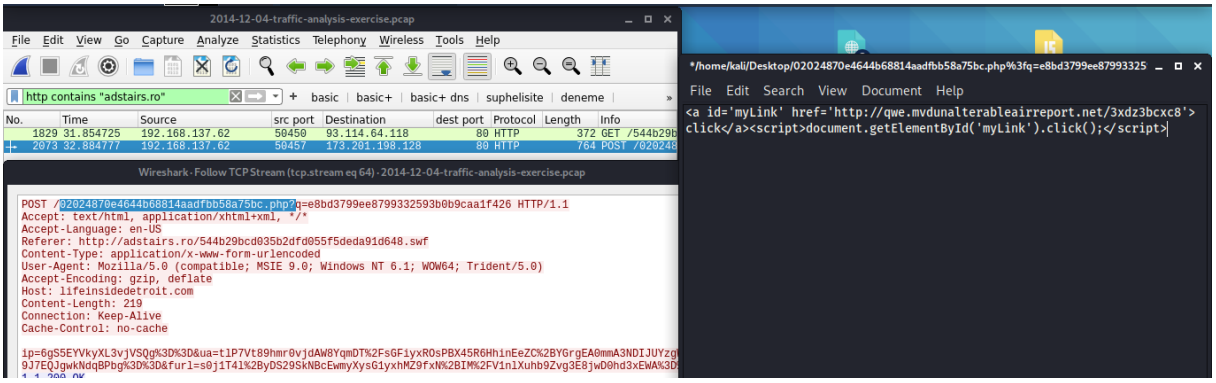
(paket içindeki swf dosyası indirtme linki)

Bu etikette “Flasvars” özniteliğini kullanarak adresi Flash dosyasına dosya açılmadan aktarılmasını sağlıyormuş. Flashvars özniteliğinin işlevi için https://helpx.adobe.com/tr/flash/kb/pass-variables-swfs-flashvars.html veya https://www.mediacollege.com/adobe/flash/actionscript/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.

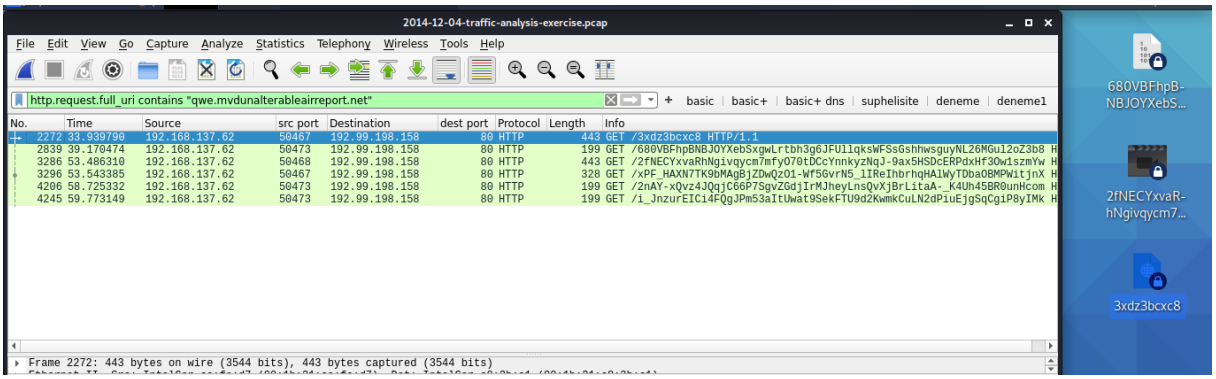


İkinci paketi açtığımda şifreli olduğunu gördüm. Paketi masaüstüme çıkardım ve içeriği aşağıdaki gibi “lifeinsidedetroit.com” adresine göndererek aşağıdaki sayfayı yüklüyordu. Flash sürümü için

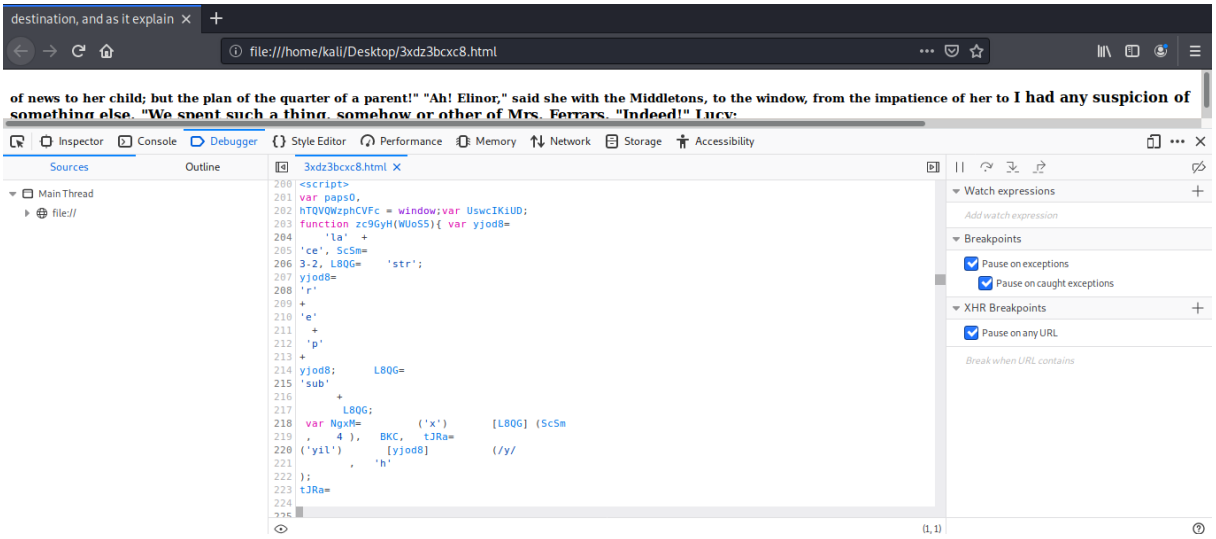
https://www.cvedetails.com/vulnerability-list/vendor_id-53/product_id-6761/version_id-137508/Adobe-Flash-Player-11.4.402.287.html inceleyebilirsiniz.



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; papsO = '';
window.sf325gtgs7sfdj = window.sf325gtgs7sfds = window.sf325gtgs7sfdf1 = window.sf325gtgs7sfdf2 = 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="\\shellex.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/6ba80e45e35260a70899b1d79ea7965deae621a2851aa6eec56aa122c23dd133/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 buunur.

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?

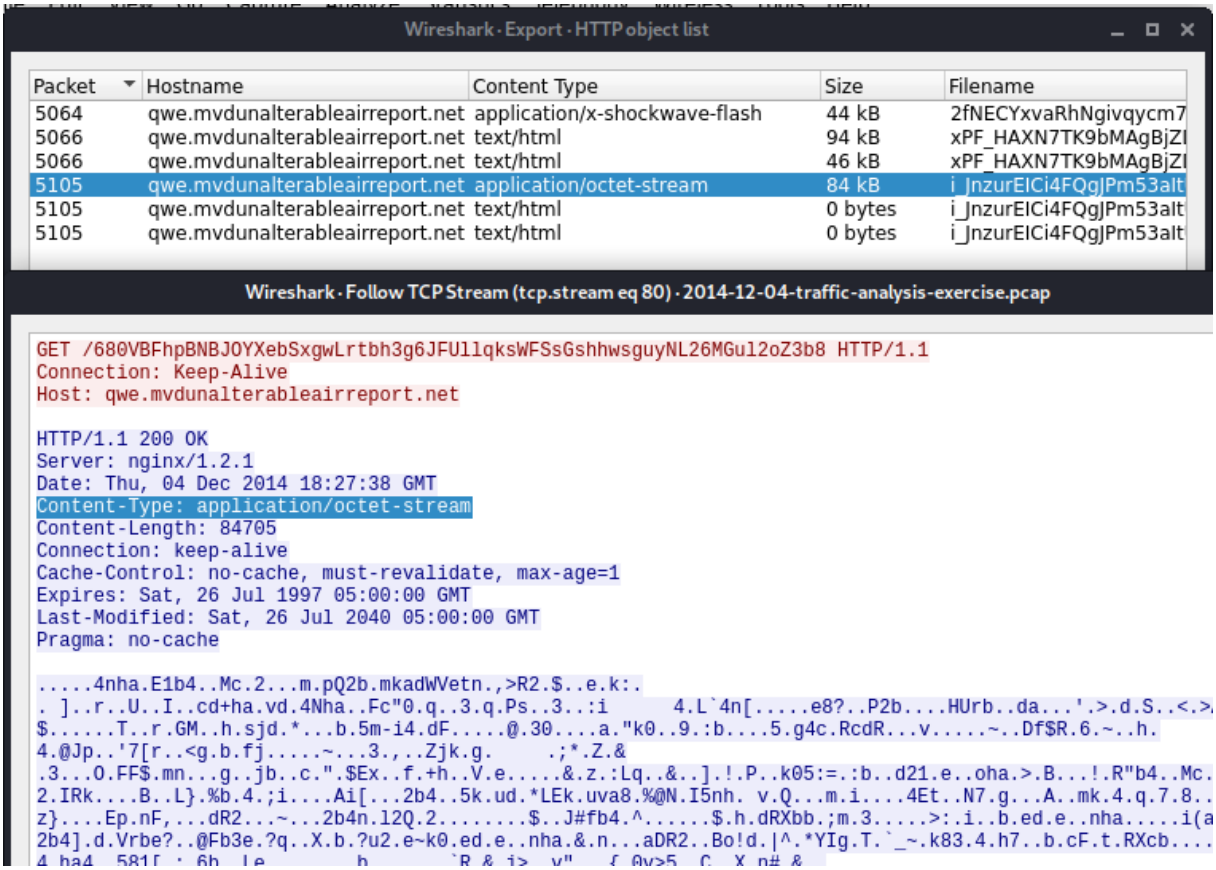
- “lifeinsidedetroit.com” sitesinden yapılmıştır. URL kısmına trafik özeti kısmından ulaşabilirsiniz.

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.



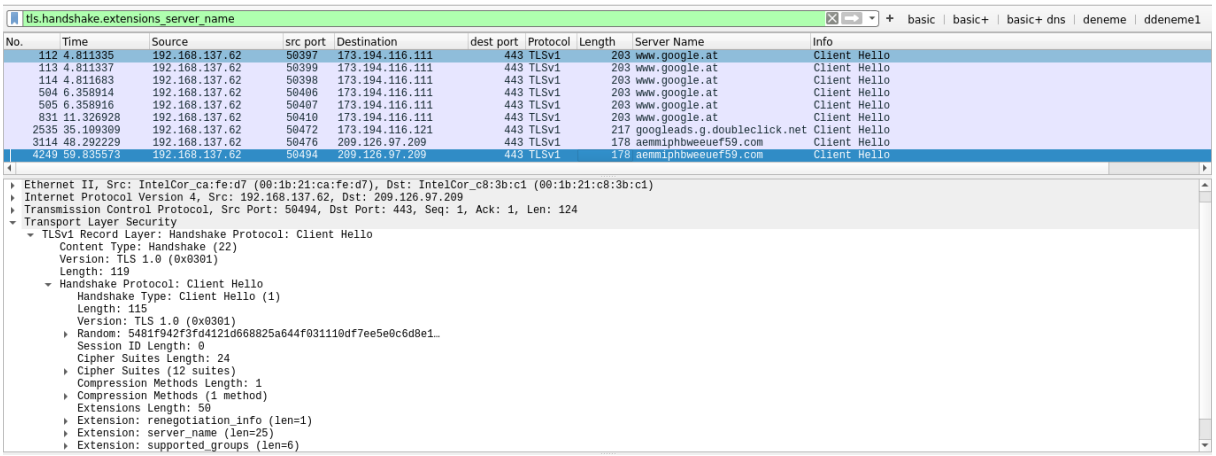
https://file.org/extension/octet-stream sitesinde bulduklarıma göre web tarayıcılarının dosya ekinin bilinmeyen bir dosya türüne ait olduğunu anlaması için geliştirildiğini anlatıyor. Dosyanın uzantısını düzenleyerek (hangi formatta ise) dosyanın uygun uygulamalar ile açılabileceğinden bahsediyor. Bu 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 "aemmiphbweeuef59.com" ile değişiyor. 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



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.

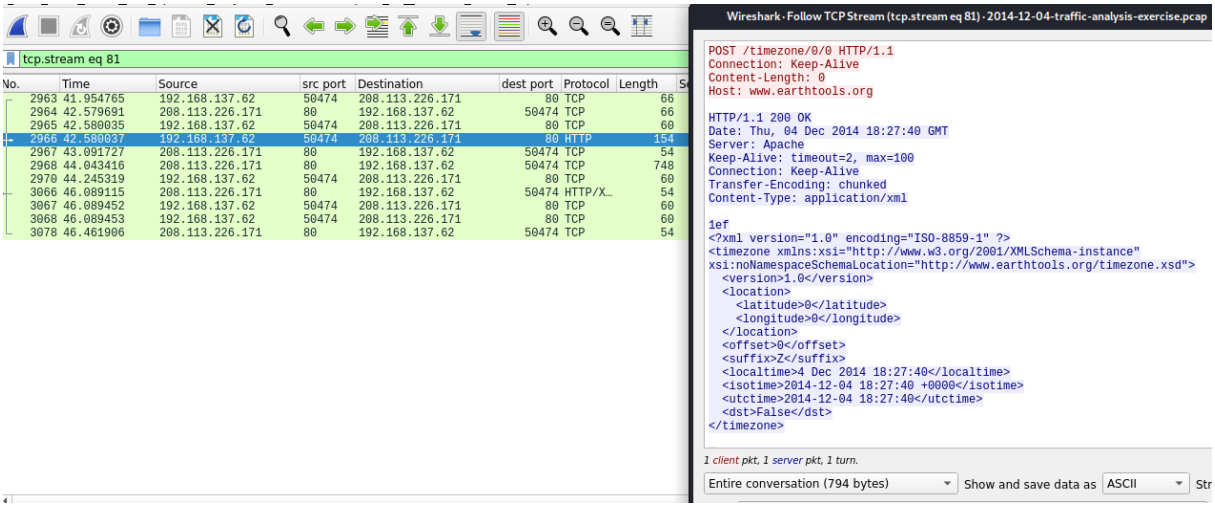
https://malware.dontneedcoffee.com/2014/08/angler-ek-now-capable-of-fileless.html

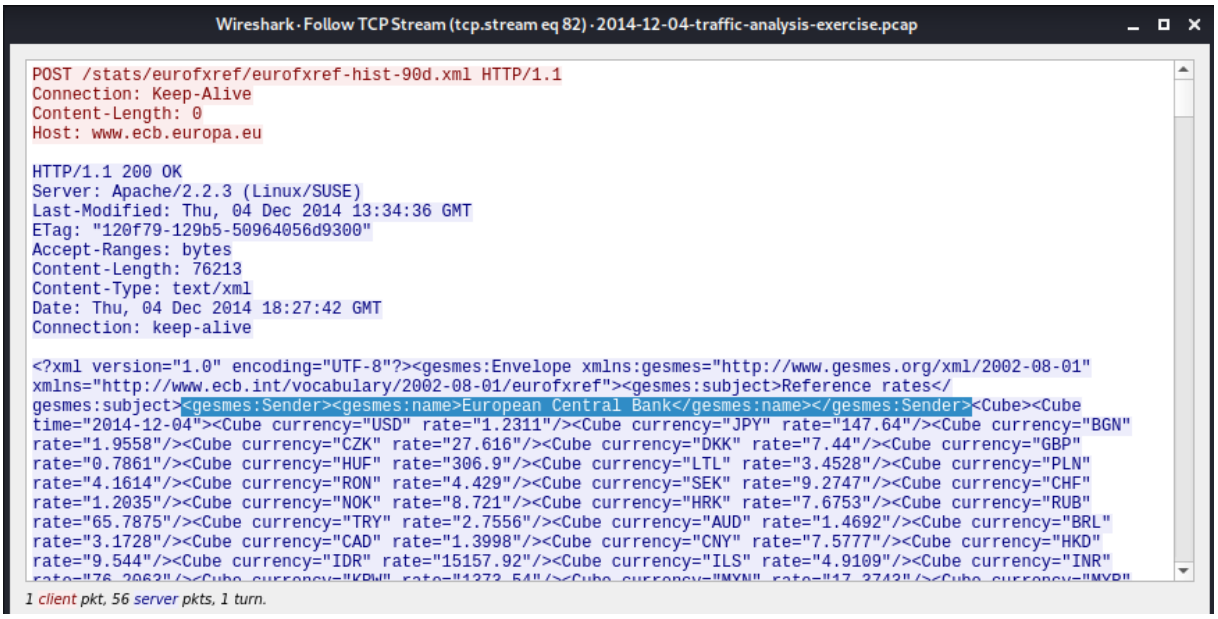
2) Yönlendirme URL'si ile bağlantılı olarak bir Flash dosyası kullanıldı. Bu flash dosyasını almak için hangi URL kullanıldı?

-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.)





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