2014-12-08 TRAFFIC ANALYSIS EXERCISE - ANSWERS

BASIC QUESTIONS:

1) What is the date and time of this activity?
2) What is the IP address of the Windows host that gets infected?
3) What is the MAC address of the infected Windows host?
4) What is the host name of the infected Windows host?
5) What is the domain name of the compromised web site?
6) What is the IP address of the compromised web site?
7) What is the domain name that delivered the exploit kit (EK) and malware payload?
8) What is the IP address that delivered the EK and malware payload?

MORE ADVANCED QUESTIONS:

1) What snort events (either VRT or EmergingThreats) are generated by this pcap?
2) What EK is this (Angler, Nuclear, Neutrino, etc)?
3) What is the redirect URL that points to the EK landing page?
4) What is the IP address of the redirect URL that points to the EK landing page?
5) How many times is the malware payload delivered? (It's encrypted each time.)
6) Which HTTP request (GET or POST) is the post-infection traffic caused by the malware?

EXTRA QUESTIONS:

1) What browser was used by the infected Windows host?
2) What different exploits were sent by the EK during this infection?
3) What is the date of these exploits? (When were they created or modified?)
4) What is the size of the malware payload?

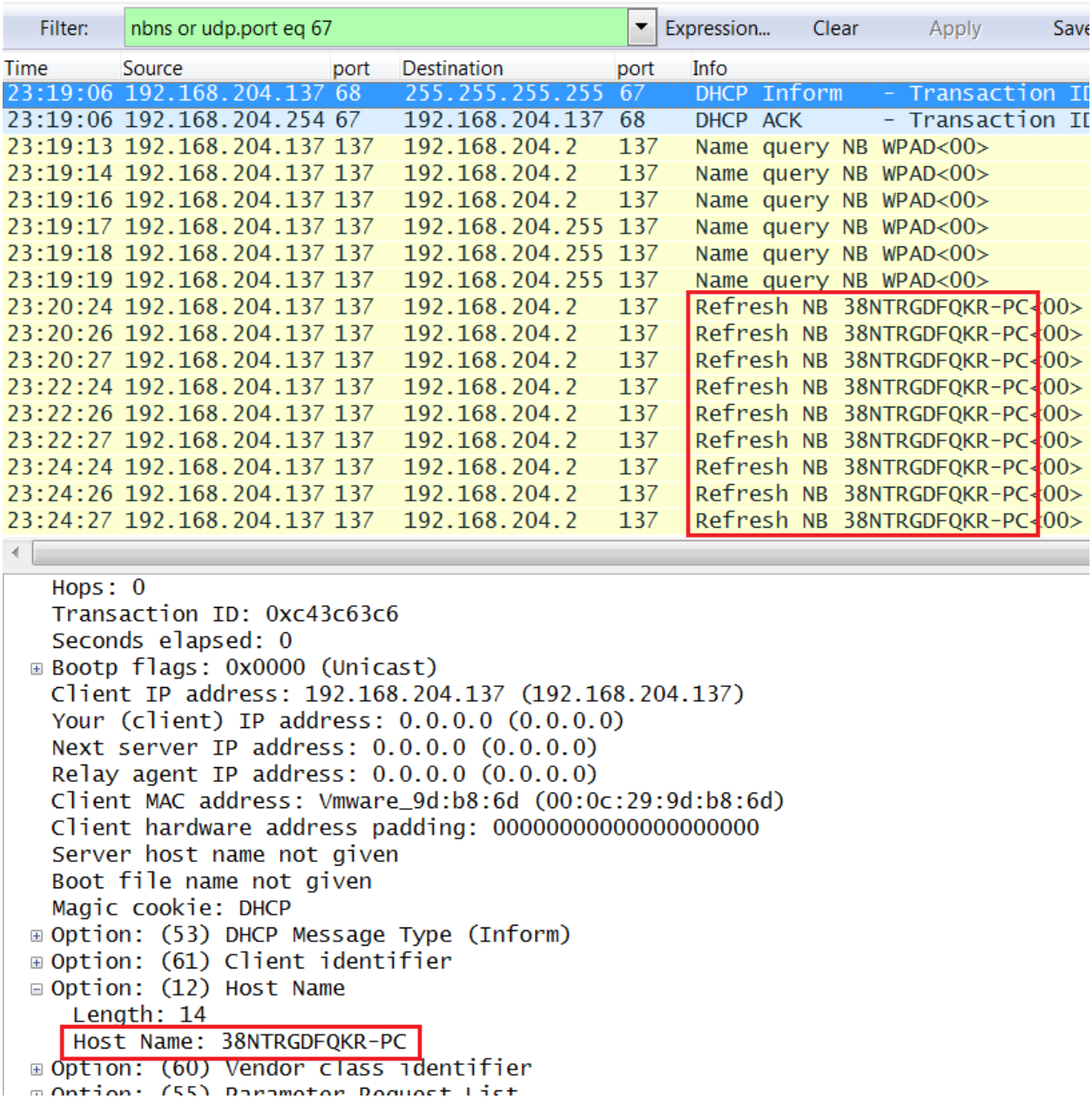
BASIC ANSWERS:

1) What is the date and time of this activity?
A: Infection traffic starts at: 2014-12-08 23:18 UTC

2) What is the IP address of the Windows host that gets infected?
A: 192.168.204.137

3) What is the MAC address of the infected Windows host?
A: 00:0c:29:9d:b8:6d

4) What is the host name of the infected Windows host?
A: 38NTRGDFQKR-PC



5) What is the domain name of the compromised web site?
A: www.excelforum.com

6) What is the IP address of the compromised web site?
A: 69.167.155.134

7) What is the domain name that delivered the exploit kit (EK) and malware payload?
A: digiwebname.in

8) What is the IP address that delivered the EK and malware payload?
A: 205.234.186.111

MORE ADVANCED ANSWERS:

1) What snort events (either VRT or EmergingThreats) are generated by this pcap?
A: VRT ruleset:

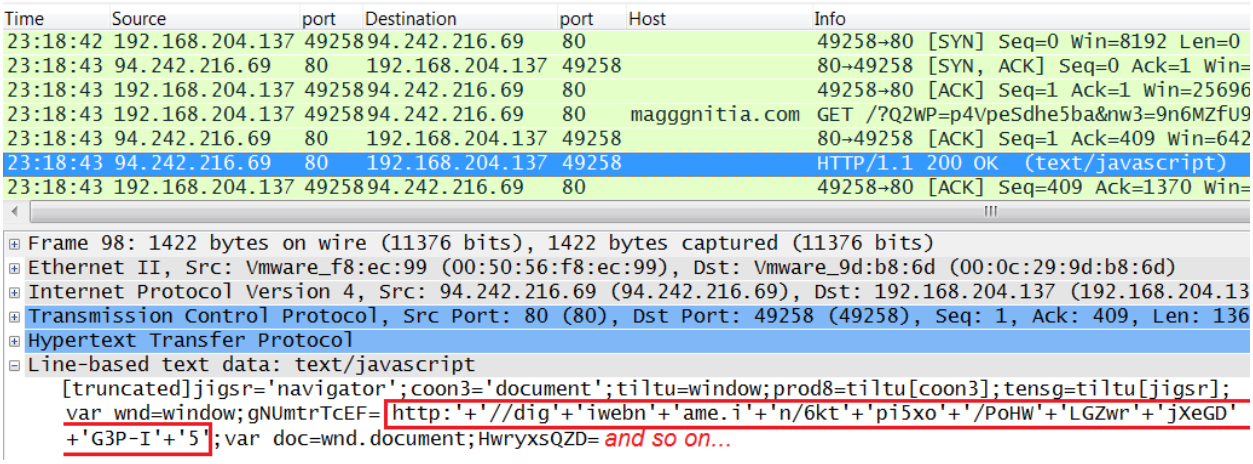
[1:1841:17] BROWSER-FIREFOX Mozilla 1.0 Javascript arbitrary cookie access attempt
[1:32481:1] POLICY-OTHER Remote non-JavaScript file found in script tag src attribute
[1:29443:8] EXPLOIT-KIT Fiesta exploit kit outbound connection attempt
[1:31902:1] EXPLOIT-KIT Multiple exploit kit flash file download
[1:28238:1] EXPLOIT-KIT Multiple exploit kits malicious pdf download
[1:28612:2] EXPLOIT-KIT Multiple exploit kit Silverlight exploit download
[1:27816:5] EXPLOIT-KIT Multiple exploit kit jar file download attempt

EmergingThreats ruleset:

ET CURRENT_EVENTS Fiesta EK Landing Nov 05 2014 (sid:2019655)
ET CURRENT_EVENTS Fiesta Flash Exploit URI Struct (sid:2019612)
ET CURRENT_EVENTS Fiesta Flash Exploit Download (sid:2018411)
ET CURRENT_EVENTS Fiesta PDF Exploit Download (sid:2018408)
ET CURRENT_EVENTS Fiesta SilverLight Exploit Download (sid:2018409)
ET CURRENT_EVENTS Fiesta SilverLight 4.x Exploit URI Struct (sid:2019623)
ET CURRENT_EVENTS Unknown - Java Request - gt 60char hex-ascii (sid:2014912)
ET CURRENT_EVENTS Fiesta Java Exploit/Payload URI Struct (sid:2019611)
ET CURRENT_EVENTS Fiesta URI Struct (sid:2018407)

2) What EK is this (Angler, Nuclear, Neutrino, etc)?
A: Fiesta EK

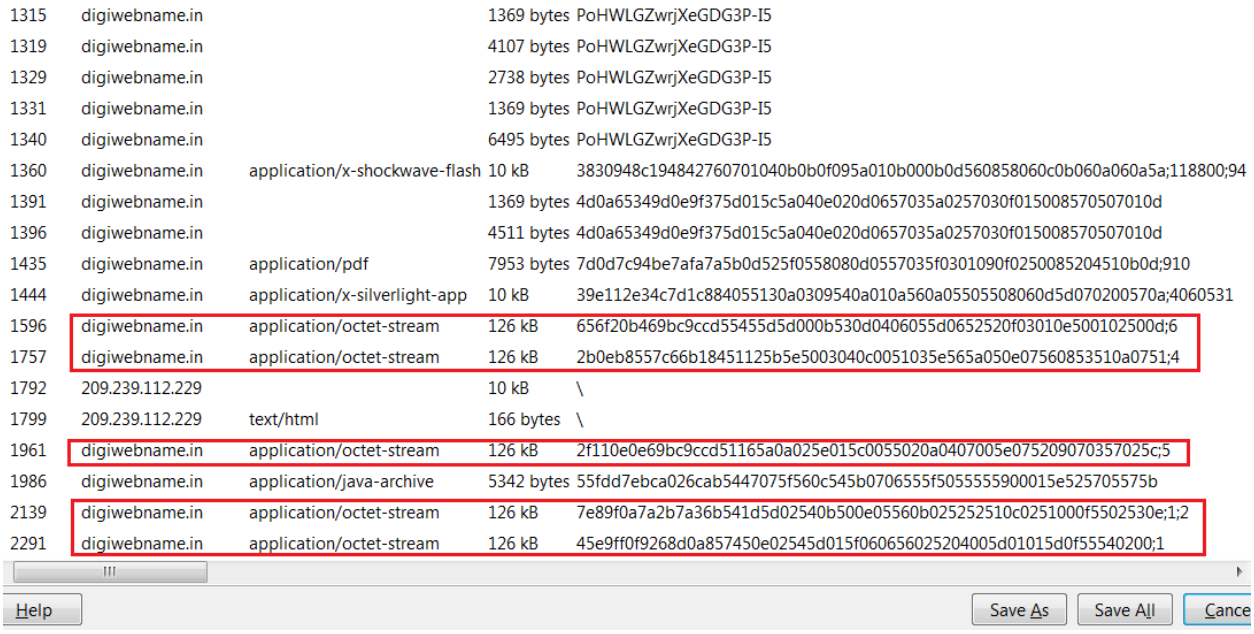
3) What is the redirect URL that points to the EK landing page?
A: magggnitia.com/?Q2WP=p4VpeSdhe5ba&nw3=9n6MZfU9I_1Ydl8y&9M5to=_8w6t8o4W_abrev&GgiMa=8Hfr8Tlcgkd0sfV&t6Mry=I6n2



4) What is the IP address of the redirect URL that points to the EK landing page?
A: 94.242.216.69

5) How many times is the malware payload delivered? (It's encrypted each time.)
A: Five

Explanation: A quick way to check is to export HTTP objects and see what is sent as an executable or application/octet-stream.



1315	digiwebname.in		1369 bytes	PoHWLGZwrjXeGDG3P-I5
1319	digiwebname.in		4107 bytes	PoHWLGZwrjXeGDG3P-I5
1329	digiwebname.in		2738 bytes	PoHWLGZwrjXeGDG3P-I5
1331	digiwebname.in		1369 bytes	PoHWLGZwrjXeGDG3P-I5
1340	digiwebname.in		6495 bytes	PoHWLGZwrjXeGDG3P-I5
1360	digiwebname.in	application/x-shockwave-flash	10 kB	3830948c194842760701040b0b0f095a010b000b0d560858060c0b060a060a5a;118800;94
1391	digiwebname.in		1369 bytes	4d0a65349d0e9f375d015c5a040e020d0657035a0257030f0150085705070l0d
1396	digiwebname.in		4511 bytes	4d0a65349d0e9f375d015c5a040e020d0657035a0257030f0150085705070l0d
1435	digiwebname.in	application/pdf	7953 bytes	7d0d7c94be7afa7a5b0d525f0558080d0557035f0301090f0250085204510b0d;910
1444	digiwebname.in	application/x-silverlight-app	10 kB	39e112e34c7d1c884055130a0309540a010a560a05505508060d5d070200570a;4060531
1596	digiwebname.in	application/octet-stream	126 kB	656f20b469bc9ccd55455d5d000b530d0406055d0652520f03010e500102500d;6
1757	digiwebname.in	application/octet-stream	126 kB	2b0eb8557c66b18451125b5e5003040c0051035e565a050e07560853510a0751;4
1792	209.239.112.229		10 kB	\
1799	209.239.112.229	text/html	166 bytes	\
1961	digiwebname.in	application/octet-stream	126 kB	2f110e0e69bc9ccd51165a0a025e015c0055020a0407005e075209070357025c;5
1986	digiwebname.in	application/java-archive	5342 bytes	55fdd7ebca026cab5447075f560c545b0706555f5055555900015e525705575b
2139	digiwebname.in	application/octet-stream	126 kB	7e89f0a7a2b7a36b541d5d02540b500e05560b025252510c0251000f5502530e;1;2
2291	digiwebname.in	application/octet-stream	126 kB	45e9ff0f9268d0a857450e02545d015f0606560252040050d01015d0f55540200;1

Help Save As Save All Cance

6) Which HTTP request (GET or POST) is the post-infection traffic caused by the malware?
A: 209.239.112.229 - POST /

Explanation: This one seems out of place with the other traffic. For proof, I had a copy of the decrypted payload from the infected VM. I submitted it to VirusTotal and Malwr.com. The Malwr.com analysis shows the same POST to 209.239.112.229 caused by this malware.

https://malwr.com/analysis/MmNiMTdhZTFhMGRmNDAwZjg2ZDhhMDZjODFjMGY3NjI/

EXTRA ANSWERS:

1) What browser was used by the infected Windows host?
A: Internet Explorer 8 (see any of the TCP streams from traffic to the compromised website).

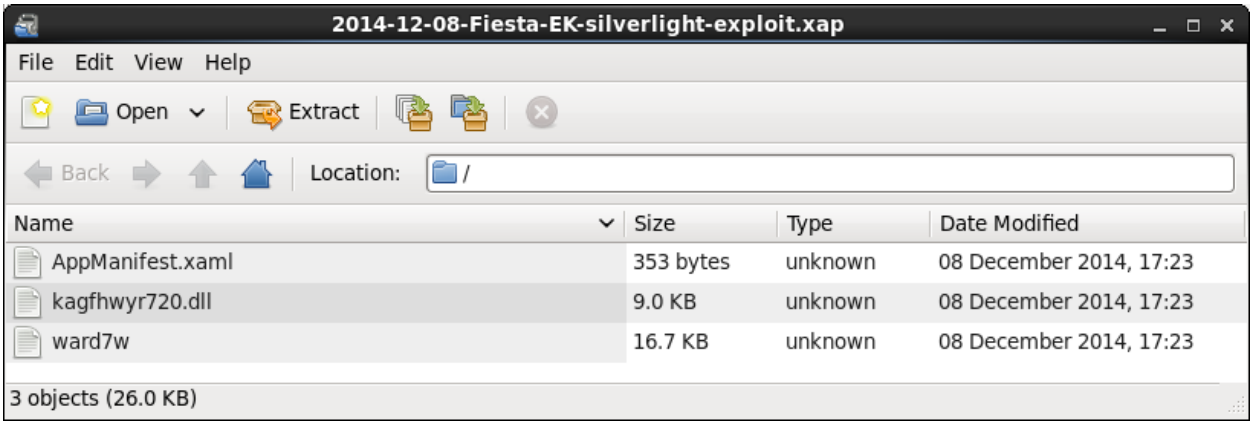
```
GET / HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml
+xml, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/
vnd.ms-powerpoint, application/msword, */*
Referer: http://www.google.de/url?url=http://www.excelforum.com/
&rct=j&frm=1&q=&esrc=s&sa=U&ei=yDGGVJmOOMv6UpregYgB&ved=0CCsQFjAD&usg=AFQjCNEaastQ
4Jl1-R8Ba_-j6m7GMzl4dg
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
Accept-Encoding: gzip, deflate
Host: www.excelforum.com
Connection: Keep-Alive
```

2) What different exploits were sent by the EK during this infection?
A: Flash, PDF, Silverlight, and Java. Since the payload was sent 5 times, there was another exploit, probably IE exploit CVE-2013-2551, which was likely part of the landing page.

1315	digiwebname.in		1369 bytes	PoHWLGZwrjXeGDG3P-I5
1319	digiwebname.in		4107 bytes	PoHWLGZwrjXeGDG3P-I5
1329	digiwebname.in		2738 bytes	PoHWLGZwrjXeGDG3P-I5
1331	digiwebname.in		1369 bytes	PoHWLGZwrjXeGDG3P-I5
1340	digiwebname.in		6495 bytes	PoHWLGZwrjXeGDG3P-I5
1360	digiwebname.in	application/x-shockwave-flash	10 kB	3830948c194842760701040b0b0f095a010b000b0d560858060c0b060a060a5a;118800;94
1391	digiwebname.in		1369 bytes	4d0a65349d0e9f375d015c5a040e020d0657035a0257030f015008570507010d
1396	digiwebname.in		4511 bytes	4d0a65349d0e9f375d015c5a040e020d0657035a0257030f015008570507010d
1435	digiwebname.in	application/pdf	7953 bytes	7d0d7c94be7afa7a5b0d525f0558080d0557035f0301090f0250085204510b0d;910
1444	digiwebname.in	application/x-silverlight-app	10 kB	39e112e34c7d1c884055130a0309540a010a560a05505508060d5d070200570a;4060531
1596	digiwebname.in	application/octet-stream	126 kB	656f20b469bc9ccd55455d5d000b530d0406055d0652520f03010e500102500d;6
1757	digiwebname.in	application/octet-stream	126 kB	2b0eb8557c66b18451125b5e5003040c0051035e565a050e07560853510a0751;4
1792	209.239.112.229		10 kB	\
1799	209.239.112.229	text/html	166 bytes	\
1961	digiwebname.in	application/octet-stream	126 kB	2f110e0e69bc9ccd51165a0a025e015c0055020a0407005e075209070357025c;5
1986	digiwebname.in	application/java-archive	5342 bytes	55fdd7ebca026cab5447075f560c545b0706555f5055555900015e525705575b
2139	digiwebname.in	application/octet-stream	126 kB	7e89f0a7a2b7a36b541d5d02540b500e05560b025252510c0251000f5502530e;1;2
2291	digiwebname.in	application/octet-stream	126 kB	45e9ff0f9268d0a857450e02545d015f060656025204005d01015d0f55540200;1

3) What is the date of these exploits? (When were they created or modified?)
A: 2014-12-08

Explanation: If you export the Java or Silverlight exploits, you can find this. These files are archives. The dates of the files within these archives will show when they were created or modified.



4) What is the size of the malware payload?
A: About 126 KB. The decrypted payload that I retrieved from the infected VM was 125952 bytes.

https://www.virustotal.com/en/file/3774e7546ec414266ab302b585415000c85a5fc3d00097486d228e45bbf40d6a/analysis/