2014-12-15 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Below is a link to the pcap for this week's traffic analysis exercise.

http://malware-traffic-analysis.net/2014/12/15/2014-12-15-traffic-analysis-exercise.pcap

Secnario: 3 windows computers are active in this pcap. At least one of them hits an exploit kit. You must determine if any of these hosts were infected.

BASIC QUESTIONS:

1) What are the host names of the 3 Windows hosts from the pcap?
2) What is(are) the IP address(es) of the Windows host(s) that hit an exploit kit?
3) What is(are) the MAC address(es) of the Windows host(s) that hit an exploit kit?
4) What is(are) the domain name(s) of the compromised web site(s)?
5) What is(are) the IP address(es) of the compromised web site(s)?
6) What is(are) the domain name(s) for the exploit kit(s)?
7) What is(are) the IP address(es) for the exploit kit(s)?
8) Did any of these hosts get infected? If so, which host(s)?

BASIC ANSWERS:

1) What are the host names of the 3 Windows hosts from the pcap?
2) What is(are) the IP address(es) of the Windows host(s) that hit an exploit kit?
3) What is(are) the MAC address(es) of the Windows host(s) that hit an exploit kit?

Here are the 3 hosts from the pcap:

MYHUMPS-PC - 192.168.204.137 - 00:0c:29:9d:b8:6d
ROCKETMAN-PC - 192.168.204.139 - 00:0c:29:61:c1:89
WORKSTATION6 - 192.168.204.146 - 00:0c:29:fc:bc:2e

MYHUMPS-PC on 192.168.204.137 is the only one that hit an exploit kit.

4) What is(are) the domain name(s) of the compromised web site(s)?
5) What is(are) the IP address(es) of the compromised web site(s)?

www.theopen.be - 213.186.33.19

6) What is(are) the domain name(s) for the exploit kit(s)?
7) What is(are) the IP address(es) for the exploit kit(s)?

epzqy.iphaeba.eu:22780 - 168.235.69.48

(22780 is the non-standard port used for this HTTP traffic)

8) Did any of these hosts get infected? If so, which host(s)?

Yes. MYHUMPS-PC on 192.168.204.137 hit the exploit kit (EK), and the EK returned a malware payload.

EXTRA QUESTIONS:

1) What is(are) the exploit kit(s) noted in the pcap?
2) What type of exploit was used by this(these) exploit kit(s)? (Flash, Java, IE, etc)
3) What URL(s) acted as a redirect between the compromised website(s) and the exploit kit?
4) What is(are) the IP address(es) of the redirect URL(s)?

EXTRA ANSWERS:

1) What is(are) the exploit kit(s) noted in the pcap?

The new Neutrino EK. I saw the following events while infecting the VM:

Src IP	SPort	Dst IP	DPort	Pr	Event Message
168.235.69.248	22780	192.168.204.137	49177	6	ET CURRENT_EVENTS Job314/Neutrino Reboot EK Landing Nov 20 2014
192.168.204.137	49177	168.235.69.248	22780	6	ET CURRENT_EVENTS Job314/Neutrino Reboot EK Flash Exploit Nov 20 2014
192.168.204.137	49181	168.235.69.248	22780	6	ET MALWARE User-Agent (Mozilla) - Possible Spyware Related
192.168.204.137	49181	168.235.69.248	22780	6	ET CURRENT_EVENTS Job314/Neutrino Reboot EK Payload Nov 20 2014
192.168.204.139	49210	50.57.227.160	80	6	ET CURRENT_EVENTS Malvertising Redirection to Exploit Kit Aug 07 2014

The last alert is a malvertising redirect ROCKETMAN-PC on 192.168.204.139 hit after the Neutrino EK traffic. That redirect didn't lead to any exploit kit activity.

2) What type of exploit was used by this(these) exploit kit(s)? (Flash, Java, IE, etc)

A Flash exploit was sent right before the malware payload was sent. See the image below:

```
GET /restless/neck/deliver/59491/satisfy/eater/warm/81110/journal/48950/ HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://epzqy.iphaeba.eu:22780/flow/17610/avenue/67785/source/43028/
total/7782/misery/swirl/some/29364/patience/interval/ford/settle/knot/554
x-flash-version: 11,8,800,94
Accept-Encoding: gzip, deflate
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)
Host: epzqy.iphaeba.eu:22780
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Mon, 15 Dec 2014 19:10:50 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Last-Modified: Mon, 15 Dec 2014 18:10:58 GMT
Content-Encoding: gzip

400a
............@..CWS b...x....XSK.(.wzB
....{.*H.D.."-.U.4).....`EA.j....PH..%...bEQA.....{.y....y..!{f...
[R!.s.... ...#KB..a
```

The malware payload was sent once. It was encrypted, and I don't know how to decode it. I also don't know if the malware payload was sent because of the Flash exploit, or because of an IE exploit in the landing page.

```
GET /claim.pl?pardon=anything&peeve=42623&september=7795&former=66329&lick=18925&favour=dress
HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla
Host: epzqy.iphaeba.eu:22780

HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Mon, 15 Dec 2014 19:10:54 GMT
Content-Type: application/octet-stream
Content-Length: 103936
Connection: keep-alive
Last-Modified: Mon, 15 Dec 2014 13:45:32 GMT
ETag: "548ee5fc-19600"
Accept-Ranges: bytes

0.._...J...\2...F)...$........u.<~2.f<.L.'...6...$.;P...E-.....e...!.3|.p%
*.......p=E...A..F`......3.ID..._K..Xrmw.......3.7..G...<..4.XO.c...#..K0.]Pmi.I.....D..^...
Q..H
...F...'.Y..Ofjff0.I......,...Z.)=.O.nA6...L.U.P..xo(...].........3n.."'.....r.mG
=.7...9.....h.-3.u..)..<r
........[..%.'..}.....z...8.(.r....X.?.T;..........9...V.Tu. .7?..{5.)
+Z........O..........S3.<n........%...p...9.........e.r.m4..|VR2.Ze2i...\..Q..... .......
+....`........C.?<3a.......3....^...i.......Sw.h....4..`
```

3) What URL(s) acted as a redirect between the compromised website(s) and the exploit kit?
4) What is(are) the IP address(es) of the redirect URL(s)?

http://col.reganhosting.com/link on 185.14.30.113