2014-11-23 TRAFFIC ANALYSIS EXERCISE - ANSWERS

BASIC ANSWERS:

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

172.16.165.132

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

00:0c:29:c5:b7:a1

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

192.30.138.146

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

hijinksensue.com

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

37.143.15.180 (over port 51439)

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

g.trinketking.com:51439 and h.trinketking.com:51439

ANSWERS TO THE MORE ADVANCED QUESTIONS:

1) What is the exploit kit (EK) that delivers the malware?

Sweet Orange

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

static.charlotteretirementcommunities.com/k?tstmp=3701802802

3) What is the IP address of the redirect URL that points to the exploit kit (EK) landing page?

50.87.149.90

4) Submit the pcap to VirusTotal and find out what snort alerts triggered. Do any of the alerts indicate what this exploit kit this is?

No. (at least, not when I submitted it)

https://www.virustotal.com/en/file/ecaf7cfa63aaa1897039e5fc1ad1fdecb947970ca5be619861c88c44889ee14c/analysis/

5) Extract the malware payload from the pcap. What is the MD5 or SHA256 hash?

MD5: 1408275c2e2c8fe5e83227ba371ac6b3
SHA256: cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d

https://www.virustotal.com/en/file/cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d/analysis/

https://malwr.com/analysis/OTVkZmRkNTcyYzgxNGIxYTlhYTc3ZTgyZGE0YjYxMTg/

ANSWERS TO THE EXTRA QUESTIONS:

1) If you use Suricata, what EmergingThreats signatures fire on the exploit kit traffic?

CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Event Message
1	2014-11-23 00:58:46	172.16.165.132	49388	50.87.149.90	80	ET CURRENT_EVENTS Sweet Orange CDN Gate Sept 09 2014 Method 2
3	2014-11-23 00:58:47	37.143.15.180	51439	172.16.165.132	49393	ET CURRENT_EVENTS Possible Sweet Orange Landing Nov 3 2014
3	2014-11-23 00:58:47	37.143.15.180	51439	172.16.165.132	49393	ET CURRENT_EVENTS SweetOrange EK Landing Nov 19 2014
1	2014-11-23 00:58:49	172.16.165.132	49398	37.143.15.180	51439	ET CURRENT_EVENTS Possible Sweet Orange CVE-2014-6332 Payload Request
1	2014-11-23 00:59:51	50.87.149.90	80	172.16.165.132	49388	ET CURRENT_EVENTS Possible Sweet Orange redirection Nov 4 2014

ET CURRENT_EVENTS Sweet Orange CDN Gate Sept 09 2014 Method 2 (sid:2019146)
ET CURRENT_EVENTS Possible Sweet Orange Landing Nov 3 2014 (sid:2019643)
ET CURRENT_EVENTS SweetOrange EK Landing Nov 19 2014 (sid:2019751)
ET CURRENT_EVENTS Possible Sweet Orange CVE-2014-6332 Payload Request (sid:2019752)
ET CURRENT_EVENTS Possible Sweet Orange redirection Nov 4 2014 (sid:2019642)

2) What exploit (which CVE) is used by this EK?

CVE-2014-6332

This is part of the EK landing page. For details on how this works in Sweet Orange EK, see:

http://malware.dontneedcoffee.com/2014/11/cve-2014-6332.html

To see what Kafeine is talking about in the above blog post, you should export the EK landing page from the pcap, deobfuscate the text, and decode the base64-encoded strings.