# 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*

1. What is the host name of the Windows VM that gets infected?

*K34EN6W3N-PC*

1. What is the MAC address of the infected VM?

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

1. What is the IP address of the compromised web site?

*82.150.140.30*

1. What is the domain name of the compromised web site?

*www.ciniholland.nl*

1. What is the IP address and domain name that delivered the exploit kit and malware?

*37.200.69.143*

1. 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/*

1. 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*

1. How many times was the payload delivered?

*3*

1. 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*

1. 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/*

1. Extract the exploit file(s). What is(are) the md5 file hash(es)?

*Flash exploit: 7b3baa7d6bb3720f369219789e38d6ab*

*Java exploit: 1e34fdebbf655cebea78b45e43520ddf*

1. 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*