Writeup: TRAFFIC ANALYSIS EXERCISE

4 minute read Published: 10 Aug, 2019

> Found the great website of @malware_traffic about network traffic related to
> malware infections. This is a subject that interests me a lot so I thought I
> would give the exercises a try and see if I can find something!

Malware Traffic Analysis

@malware_traffic's blog has a lot of knowledge so I highly recommend to bookmark it somewhere. The real treasure is of course the amazing exercises page. Depending on the exercise, you get a pcap and other files. The pcap file is a traffic capture which we can analyse in Wireshark and find out where things went wrong!

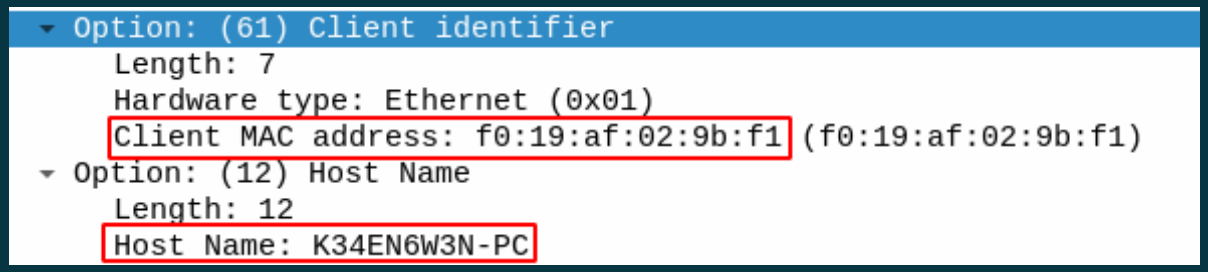
Being able to effectively analyse traffic is a very important skill for the security for any organisation. It helps the security team to find out where the problem happened and how to mitigate it. It is also super fun!

The first exercise

Today, I'll start with the exercise "2014-11-16 - TRAFFIC ANALYSIS EXERCISE". The writeup will be about the level 1 and level 2 questions this time:

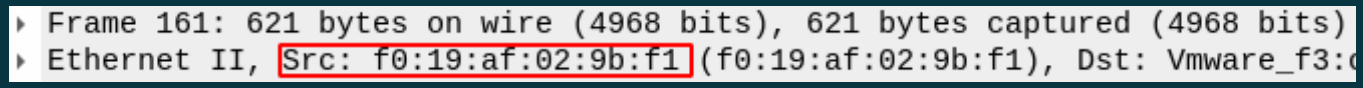
```
LEVEL 1 QUESTIONS:

1) What is the IP address of the Windows VM that gets infected?
2) What is the host name of the Windows VM that gets infected?
3) What is the MAC address of the infected VM?
4) What is the IP address of the compromised web site?
5) What is the domain name of the compromised web site?
6) What is the IP address and domain name that delivered the exploit kit and
malware?

LEVEL 2 QUESTIONS:

1) What is the redirect URL that points to the exploit kit (EK) landing page?
2) Besides the landing page (which contains the CVE-2013-2551 IE exploit), what
other exploit(s) sent by the EK?
3) How many times was the payload delivered?
4) Submit the pcap to VirusTotal and find out what snort alerts triggered. What
are the EK names are shown in the Suricata alerts?



## Level 1 questions

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

The source of all traffic is 172.16.165.165, so I can assume that this is the
infected VM.

2) What is the host name of the Windows VM that gets infected?
```

There are many ways to check that as demonstrated in this article. I chose to filter the traffic on bootp to reveal the DHCP traffic. I selected one of the frames, and in the frame details, I went to Bootstrap Protocol and then in the options we find the hostname and MAC address:



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

We got the MAC address in the 2nd question, but alternatively, we can see it in all the frames' details:



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

If we filter the GET requests (http.request.method == GET), we can follow the referers. The user visited "ciniholland" and through the referers of each GET requests, we see that it leads to a very suspicious website which initiates downloads on the machine.

So I assume ciniholland.nl/ is the compromised website and its IP is 82.150.140.30

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

Answered above: ciniholland.nl/

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

If we follow the GET requests, we can clearly see that the final website initiates downloads on the now compromised machine:

172.16.165.165	www.ciniholland.nl	HTTP	457 GET /wp-con
172.16.165.165	www.ciniholland.nl	HTTP	448 GET /wp-con
172.16.165.165	ytimg.l.google.com	HTTP	602 GET /embed/
172.16.165.165	www.ciniholland.nl	HTTP	350 GET /favico
172.16.165.165	24corp-shop.com	HTTP	585 GET / HTTP/
172.16.165.165	24corp-shop.com	HTTP	585 GET / HTTP/
172.16.165.165	24corp-shop.com	HTTP	413 GET /source
172.16.165.165	stand.trustandprobaterealty.com	HTTP	695 GET /?PHPSS
172.16.165.165	stand.trustandprobaterealty.com	HTTP	695 GET /?PHPSS
172.16.165.165	stand.trustandprobaterealty.com	HTTP	475 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	475 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	676 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	677 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	441 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	441 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	443 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	443 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	351 GET /index.
172.16.165.165	stand.trustandprobaterealty.com	HTTP	351 GET /index.

And its IP address is 37.200.69.143

Level 2 questions

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

As I checked the different GET requests in the first level, I found out that the referer to the first EK landing page (stand.trustandprobaterealty.com) was: 24corp-shop.com

I can also export the HTML object (File –> Export Object –> HTTP), then download the 24corp-shop.com html file. Open it in a text editor and I find:

```
</HEAD>

<body bgcolor=#ffffff><div align='center'><iframe src='http://stand.trustandprobaterealty.com/?
PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM' border=0 width=125
height=10 scrolling=no></iframe></div>

<BR><BR><BR>
```

2) Besides the landing page (which contains the CVE-2013-2551 IE exploit), what other exploit(s) sent by the EK?

By checking the the HTML object (File –> Export Object –> HTTP), I can see two other exploits: a Flash and a Java.

1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8 227 bytes
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8 227 bytes
2469	stand.trustandprobaterealty.com	text/xml	572 bytes
2475	stand.trustandprobaterealty.com	text/xml	572 bytes
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB

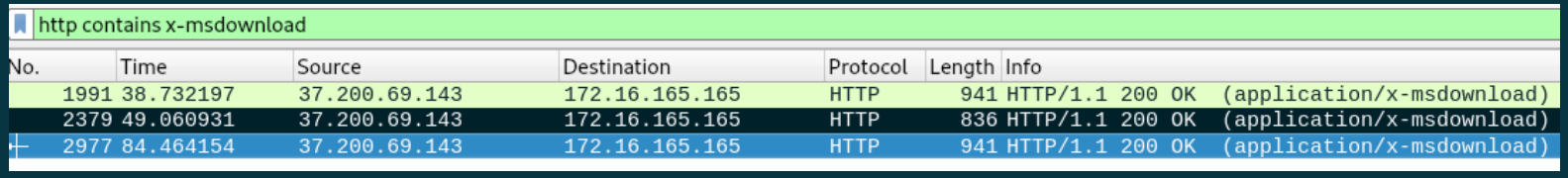
Alternatively, I had found them during my first recon in the list of HTTP GET requests by following the HTTP stream:

```
HTTP/1.1 200 OK
Server: nginx/0.7.67
Date: Sun, 16 Nov 2014 02:12:19 GMT
Content-Type: application/x-shockwave-flash
Connection: keep-alive
Content-Length: 8227
X-Powered-By: PHP/5.4.4-14+deb7u14
```

```
HTTP/1.1 200 OK
Server: nginx/0.7.67
Date: Sun, 16 Nov 2014 02:12:39 GMT
Content-Type: application/java-archive
Connection: keep-alive
Content-Length: 10606
X-Powered-By: PHP/5.4.4-14+deb7u14
```

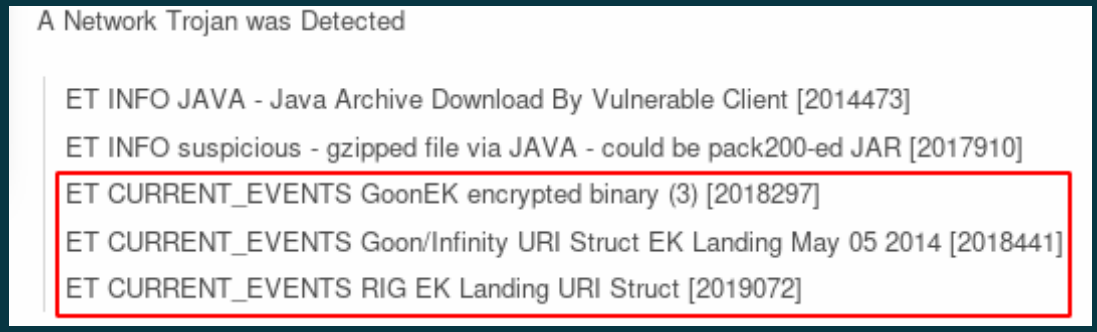
3) How many times was the payload delivered?

I'm not 100% sure, but I can't see any other name for the payload than x-msdownload, and a quick filtering give us 3 deliveries:



4) Submit the pcap to VirusTotal and find out what snort alerts triggered. What are the EK names are shown in the Suricata alerts?

I didn’t know about VirusTotal, so it was a nice question to introduce it. Here is what I found there:

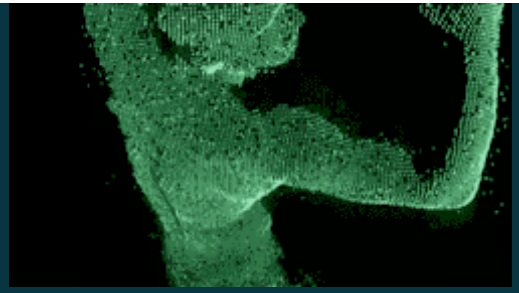


ET CURRENT_EVENTS GoonEK ET CURRENT_EVENTS Goon/Infinity URI Struct EK ET CURRENT_EVENTS RIG EK

This is all for today!

I learned a lot through each question. It’s a quick writeup, but I spend a lot of time digging for the answers. I won’t do a writeup for all the exercises, but I will make one for the most interesting exercises.

Thank you for reading this and get in contact if you have any question, recommendation, spotted mistakes, etc.



Published by theyknow 10 Aug, 2019 in post and tagged forensic, malware, traffic analysis and wireshark using 810 words.

Related Content

- i18 Challenge - Part 1 – 5 minutes
- i18 Challenge - Part 2 – 4 minutes
- Pentesting tools – 8 minutes