

**Harsimran Kaur V00879358**

**Maninder Singh V00879900**

(Weight: 20%; Due: July 28, 2017)

### Case Description

The security officer responsible for the network of a corporation is suspecting that the machine used by one of the employees has been infected with malware, after visiting some compromised website. The suspicion was based on observing significant departure of the infected host activity from the network baselines.

Network traffic sample involving the compromised host activity is provided in TCPDUMP format (as a separate file: elec570-project-2017.pcap). As a forensic analyst, you have been tasked to analyze the network capture and decode the suspicious activities involved.

The trace file can be downloaded at:

<https://drive.google.com/file/d/0B1xnRxT-Y8DMZEE5UzgzbHBEQIE/view?usp=sharing>

### Task

More specifically, you must provide answers to the following questions:

1. Identify the following characteristics for the infected host (2.5%):

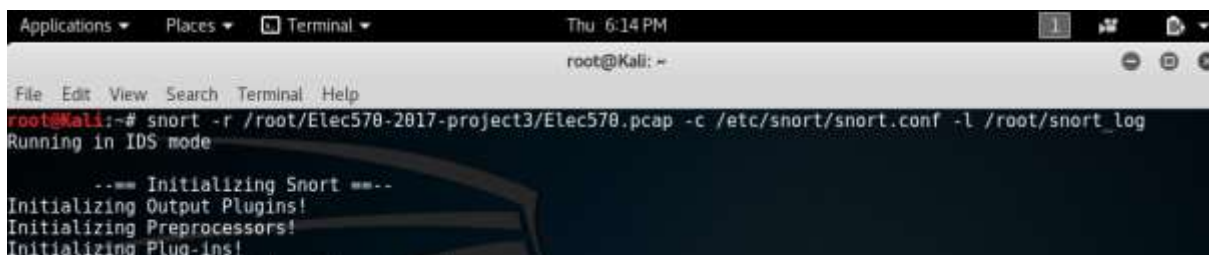
- a) IP address of computer
- b) Host name of computer
- c) MAC address of computer
- d) Operating System (OS)

Answer:

Step 1: To analyse the PCAP file first we need to identify the source address and destination address within which the communication took place.

We can do this by generating alerts using snort by following command.

**Snort -r /root/Elec570-2017-project3/Elec570.pcap -c /etc/snort/snort.conf -l /root/snort\_log**



```
root@Kali: ~# snort -r /root/Elec570-2017-project3/Elec570.pcap -c /etc/snort/snort.conf -l /root/snort_log
Running in IDS mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
```

In this case, the alerts will be stored in the directory named snort\_log and at the end we saw the run statistics as shown below.

```

Applications ▾ Places ▾ Terminal ▾ Thu 6:15 PM
root@kali: ~

File Edit View Search Terminal Help
Self-referencing paths ("./"): 0
HTTP Response Gzip packets extracted: 28
Gzip Compressed Data Processed: 302070.00
Gzip Decompressed Data Processed: 945090.00
Total packets processed: 1847

=====
SMTP Preprocessor Statistics
Total sessions: 0
Max concurrent sessions: 0

=====
dcerpc2 Preprocessor Statistics
Total sessions: 0

=====
SSL Preprocessor:
SSL packets decoded: 710
Client Hello: 72
Server Hello: 72
Certificate: 64
Server Done: 182
Client Key Exchange: 64
Server Key Exchange: 50
Change Cipher: 136
Finished: 0
Client Application: 53
Server Application: 27
Alert: 11
Unrecognized records: 383
Completed handshakes: 0
Bad handshakes: 0
Sessions ignored: 26
Detection disabled: 6

=====
SIP Preprocessor Statistics
Total sessions: 0

=====
Snort exiting
root@kali:~#

```

At the end of the run in the specified snort output directory, we found two directories which are newly created:

1. Snort alerts log file (snort\_alert.csv).
2. Snort analysis log file which stores the actions taken by Snort during the analysis.

Step 2:

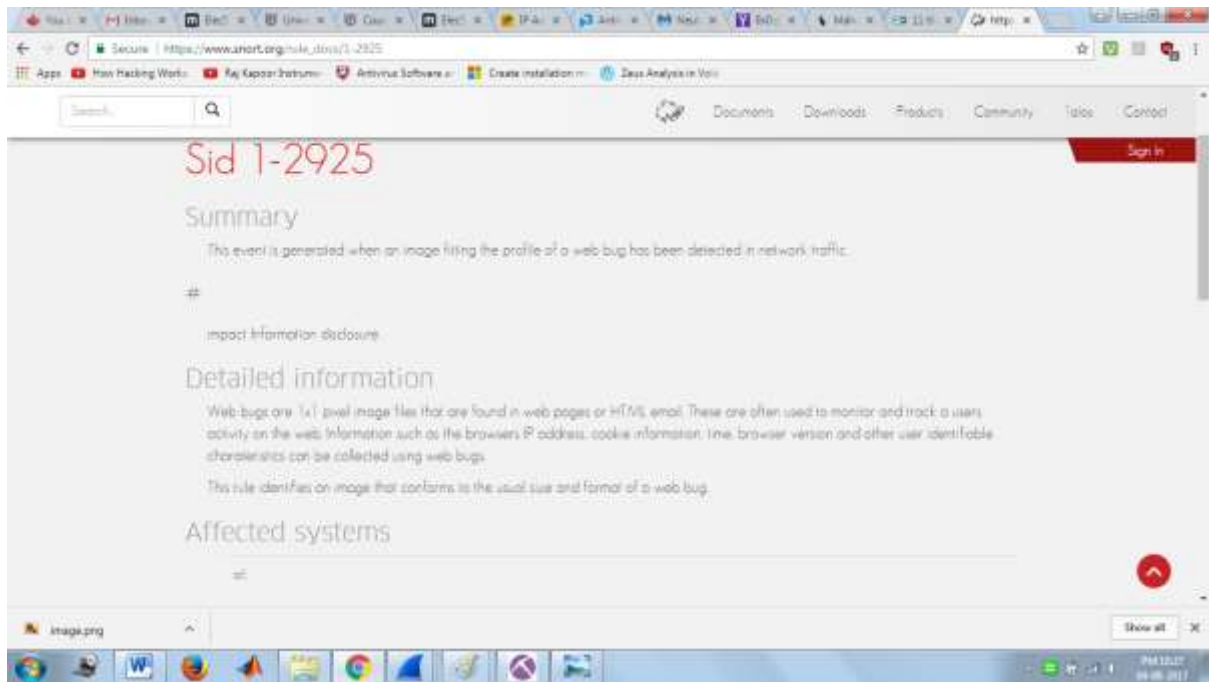
We need to open the snort\_alert.csv file. For this we installed libreoffice which is software used to open .csv files in Linux.

When we opened the file we found the following details about the communication:

event_details															
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	08/19-17:21:18.903909	1	2525	3	INFO web bug 0x0 gif attempt	TCP	216.58.192.174	80	172.16.174.93	49187	00:04:6D:5C:26:DA:10x1B8	***AD***	0xA0B1A4 0x7826		
2	08/19-17:21:19.439403	1	2525	3	INFO web bug 0x0 gif attempt	TCP	54.225.202.140	80	172.16.174.93	49198	00:04:6D:5C:26:DA:10x1AE	***AD***	0x89AD0 0x1AA1		
3	08/19-17:21:22.278274	1	2525	3	INFO web bug 0x0 gif attempt	TCP	52.0.159.120	80	172.16.174.93	49220	00:04:6D:5C:26:DA:10x140	***AD***	0xC80F7F 0x2FD4		
4	08/19-17:21:22.384296	1	2525	3	INFO web bug 0x0 gif attempt	TCP	173.241.242.143	80	172.16.174.93	49231	00:04:6D:5C:26:DA:10x174	***AD***	0x134D81 0x8E10		
5	08/19-17:21:22.683754	1	2525	3	INFO web bug 0x0 gif attempt	TCP	52.205.230.186	80	172.16.174.93	49233	00:04:6D:5C:26:DA:10x252	***AD***	0x1AE77C 0xF8FB		
6	08/19-17:21:58.446478	1	2525	3	INFO web bug 0x0 gif attempt	TCP	216.58.192.174	80	172.16.174.93	49187	00:04:6D:5C:26:DA:10x1AB	***AD***	0xA0B1A5 0x7826		

Column headers are as follow (left to right):

**Alert Time Rule\_Signature\_ID Message Protocol SrcIP SrcPort DestIP DestPort**



From the screen shot above we come to know that 1x1 pixel may get installed on victims PC which is invisible and tracks the user's activity.

It seems that at this stage the attack was initiated by several hosts 216.58.192.174, 54.225.202.140, 52.0.159.120, 173.241.242.143, 52.205.210.146, 216.58.192.174 targeting a host IP 172.16.174.93

The target hosts are private IP addresses, however the attackers seems to be at remote host. So we used ipvoid.com to check the location and find out whether it is blacklisted or not.

First we check 216.58.192.174 this IP is safe.

IP Address Information	
Analysis Date	2017-07-31 01:15:31
Blacklist Status	<b>POSSIBLY SAFE 0/97</b>
IP Address	<b>216.58.192.174</b> Find Sites   IP Whois
Reverse DNS	ord36s02-in-f174.1e100.net
ASN	AS15169
ASN Owner	Google Inc.
ISP	Google
Continent	North America
Country Code	(US) United States
Latitude / Longitude	37.4192 / -122.0574 Google Map
City	Mountain View
Region	California

Then we scanned IP address 54.225.202.140 which is blacklisted.

www.ipvoid.com/ip-blacklist-check/

IP Reputation Feeds»

### IP Address Information

Analysis Date	2017-07-31 01:19:58
Blacklist Status	<b>BLACKLISTED 1/97</b>
IP Address	<b>54.225.202.140</b> Find Sites   IP Whois
Reverse DNS	ec2-54-225-202-140.compute-1.amazonaws.com
ASN	AS14618
ASN Owner	Amazon.com, Inc.
ISP	Amazon.com
Continent	North America
Country Code	(US) United States
Latitude / Longitude	39.0481 / -77.4728 Google Map
City	Ashburn

Then the third IP is 52.0.159.120 which is also blacklisted

www.ipvoid.com/ip-blacklist-check/

IP Reputation Feeds»

### IP Address Information

Analysis Date	2017-07-31 01:24:24
Blacklist Status	<b>BLACKLISTED 1/97</b>
IP Address	<b>52.0.159.120</b> Find Sites   IP Whois
Reverse DNS	ec2-52-0-159-120.compute-1.amazonaws.com
ASN	AS14618
ASN Owner	Amazon.com, Inc.
ISP	Amazon.com
Continent	North America
Country Code	(US) United States
Latitude / Longitude	39.0481 / -77.4728 Google Map

Then we checked IP 173.241.242.143. This is also blacklisted

not signed in (l) x M Inbox (5,772) - harsimra x Course: 201705 ELEC 570 x Elec570\_Tutorial\_7.pdf x Ele

www.ipvoid.com/ip-blacklist-check/ How Hacking Works x Raj Kapoor Instrume Antivirus Software an Create installation m Zeus Analysis in Vol

IP Reputation Feeds»

IP Address Information

Analysis Date	2017-08-03 22:03:03
Elapsed Time	3 seconds
Blacklist Status	BLACKLISTED 1/95
IP Address	173.241.242.143 Find Sites   IP Whois
Reverse DNS	ox-173-241-242-143.xv.dc.openx.org
ASN	AS36089
ASN Owner	OPENX TECHNOLOGIES, INC.
ISP	Openx Technologies
Continent	North America
Country Code	🇺🇸 (US) United States
Latitude / Longitude	40.7143 / -74.006 Google Map

Then we checked IP 52.205.210.146. This is safe.

M Inbox x Course: x Elec570 x ceng420 x Course: x Elec570 x f

www.ipvoid.com/ip-blacklist-check/ x Hacking Works x Raj Kapoor Instrume Antivirus Software an Create installation m Zeus Analysis in

IP Reputation Feeds»

IP Address Information

Analysis Date	2017-07-31 01:31:36
Blacklist Status	POSSIBLY SAFE 0/97
IP Address	52.205.210.146 Find Sites   IP Whois
Reverse DNS	ec2-52-205-210-146.compute-1.amazonaws.com
ASN	AS14618
ASN Owner	Amazon.com, Inc.
ISP	Amazon.com
Continent	North America
Country Code	🇺🇸 (US) United States
Latitude / Longitude	39.0481 / -77.4728 Google Map
City	Ashburn

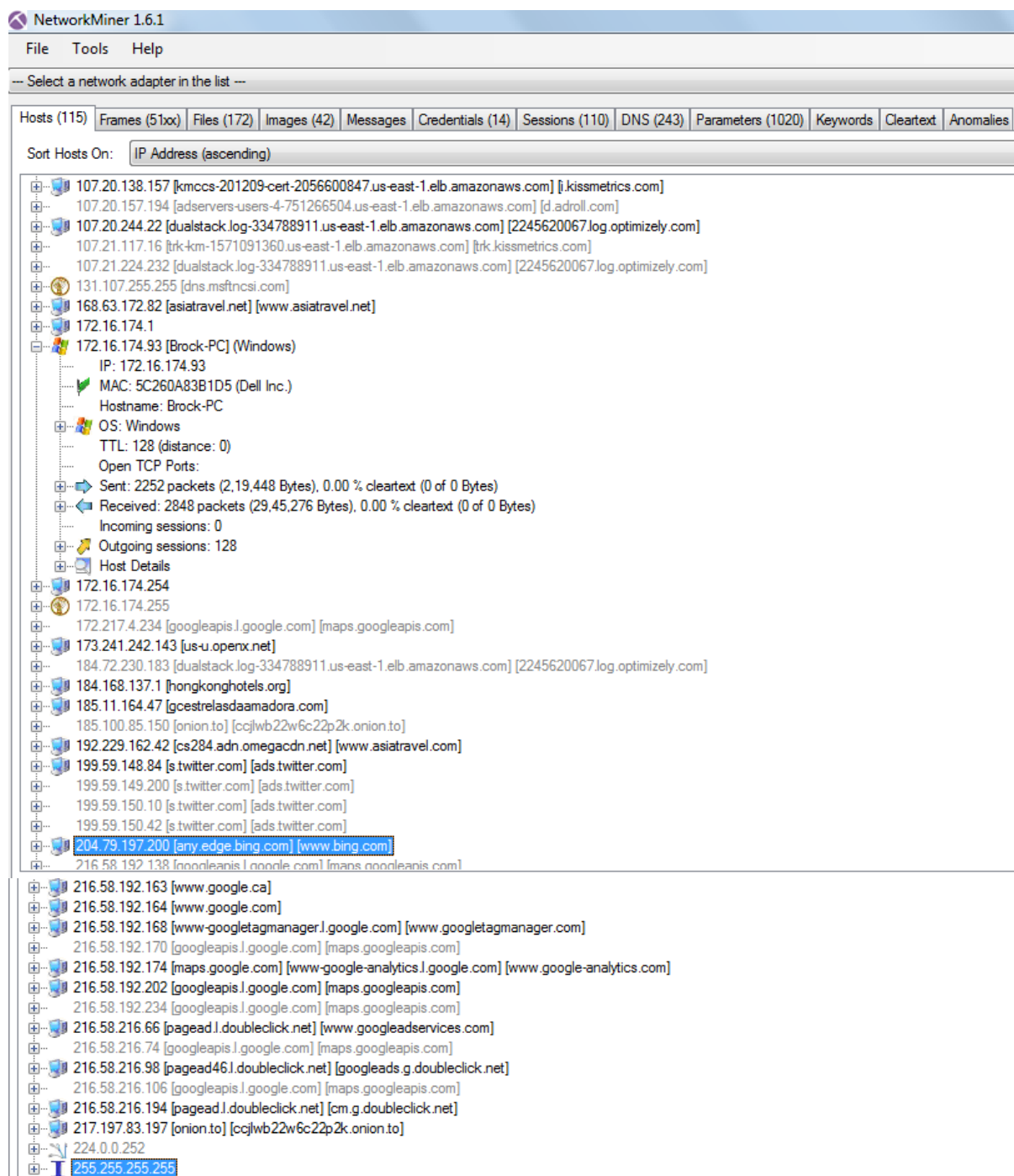
While we have some idea of hosts involved in the attack, we will use NetworkMiner to identify all hosts and corresponding OS.

To run NetworkMiner

Click on menu File->Open; select the trace file.





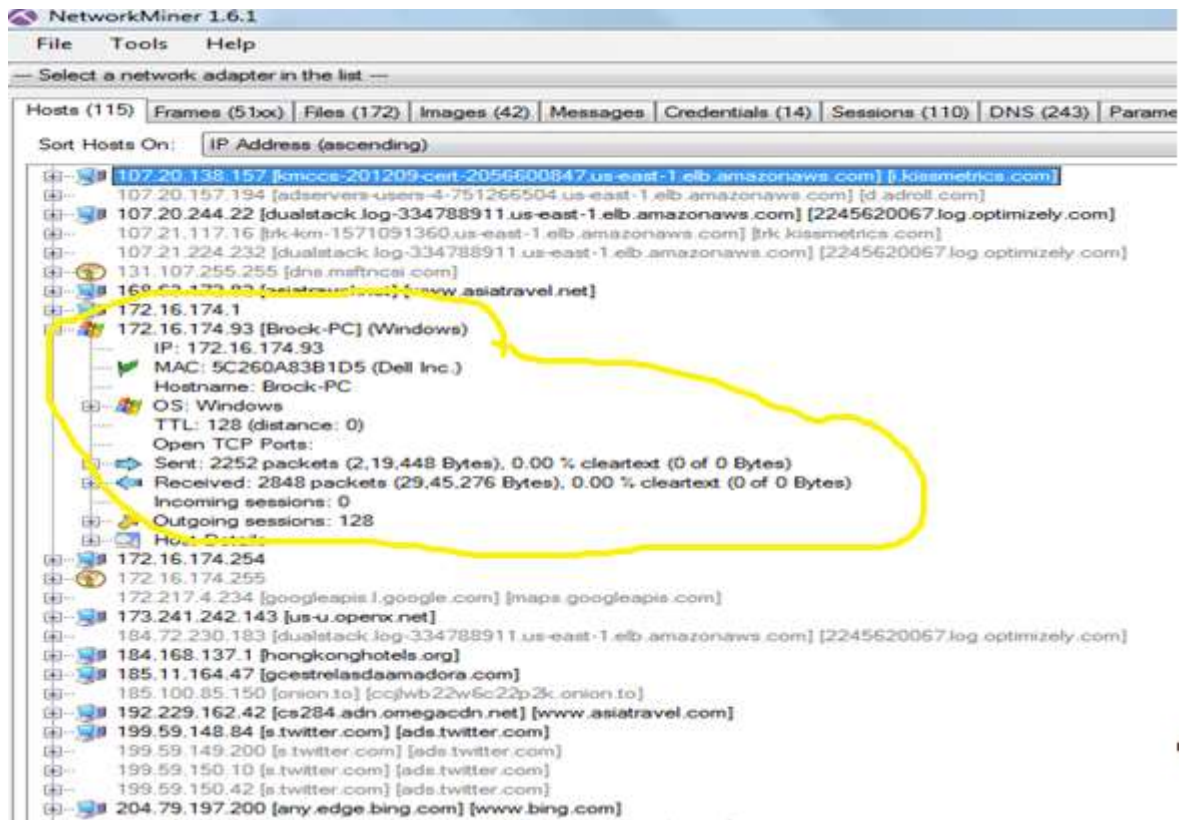


Here we found that there are a number of other hosts involved in the attack.

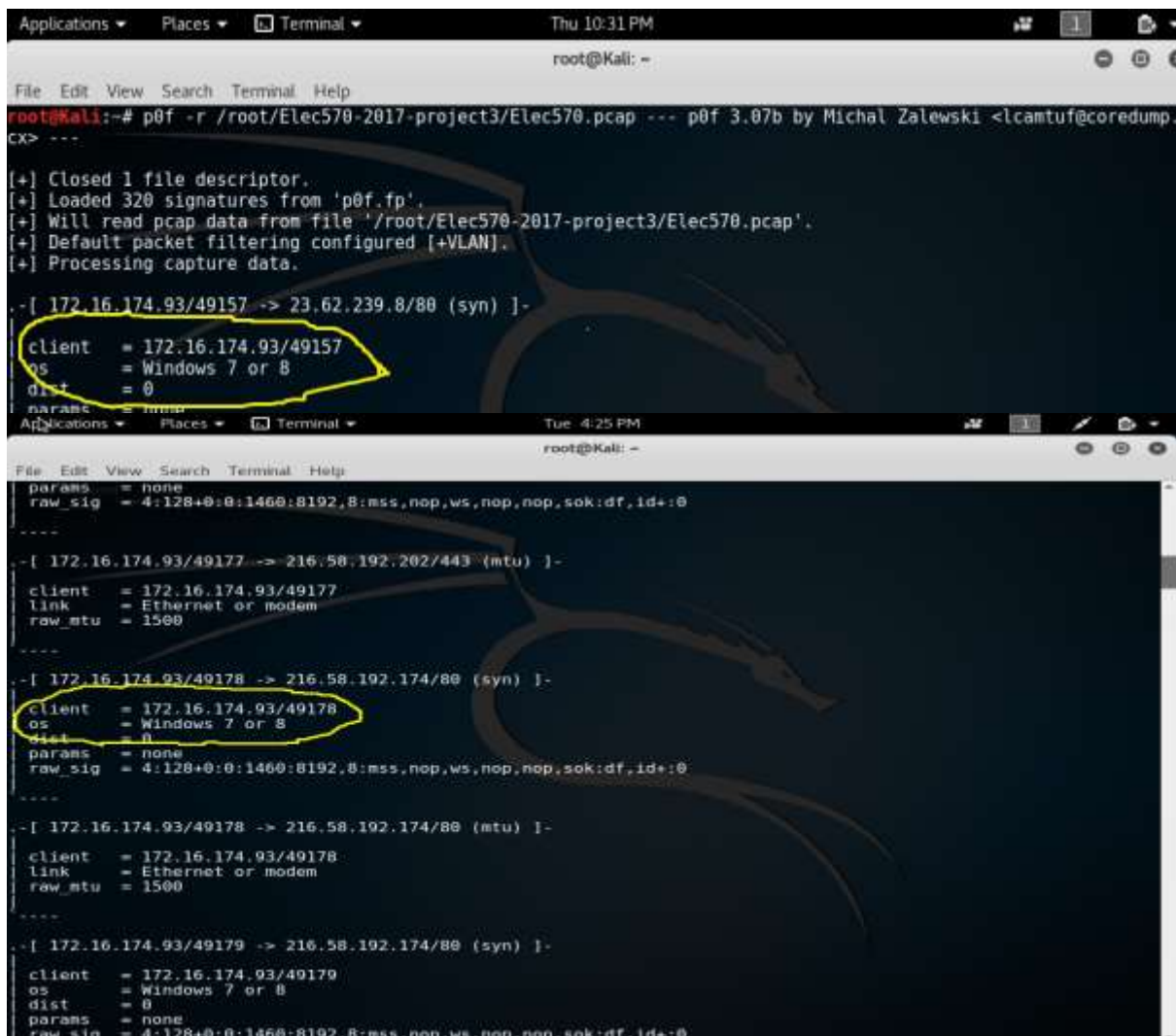
Now as per the snort\_alert.csv file we found that the destination address of all source IPs is 172.16.174.93. So we found the system name and other information using Network Miner. Also on carefully analysing the PCAP file we found that this is the system involved rest are the URLs of websites.

- IP address of computer- 172.16.174.93
- Host name of computer- Brock-PC
- MAC address of computer- 5C260A83B1D5
- Operating System (OS)- Windows

To make sure that the operating system is correct we run the same PCAP file using p0f



The operating system figure printing may include false positives so we have used p0f to run the PCAP file as follows:





2. What is the IP address and URL of the compromised website the user looked at that triggered the malware traffic (i.e. before the malware traffic happened)? (2.5%)

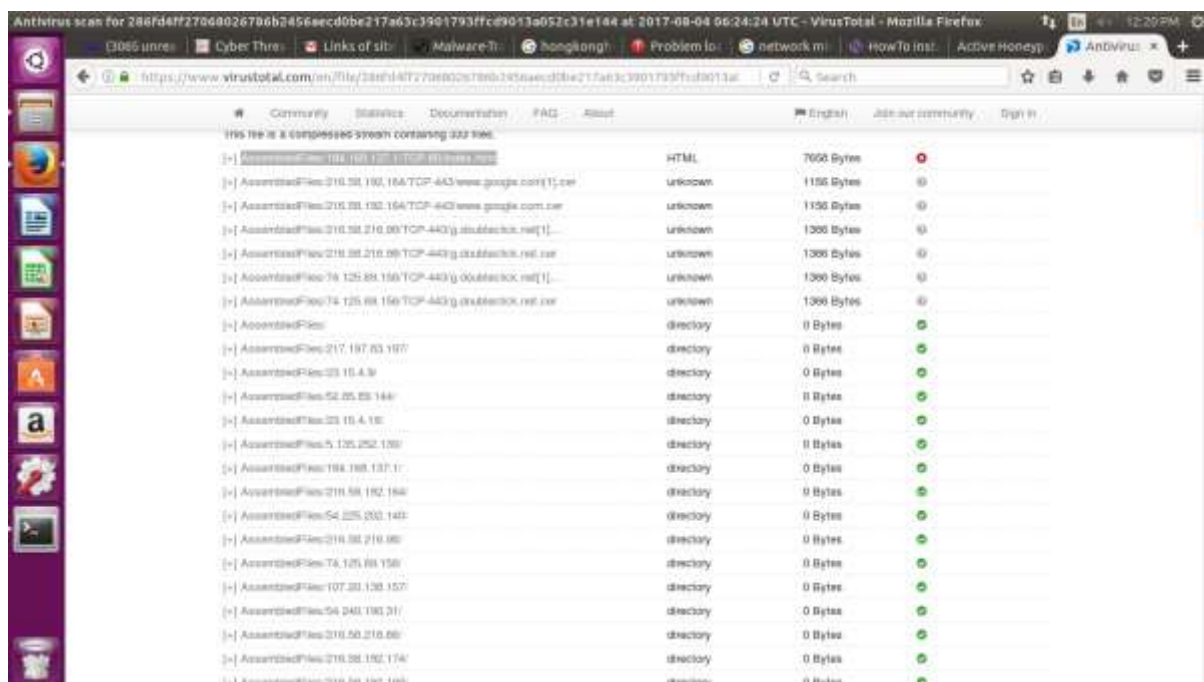
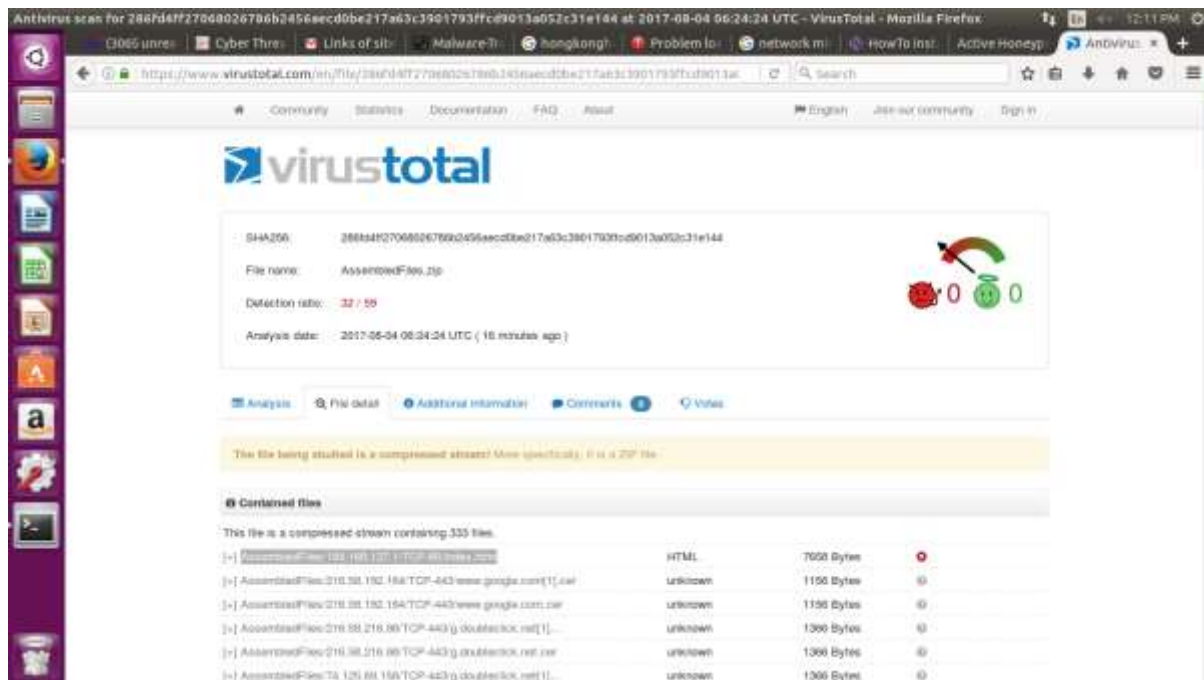
Answer:

First we go to networkminer folder as follows:

C:\Users\Kirat\Downloads\NetworkMiner\_1-6-1\assembledfiles

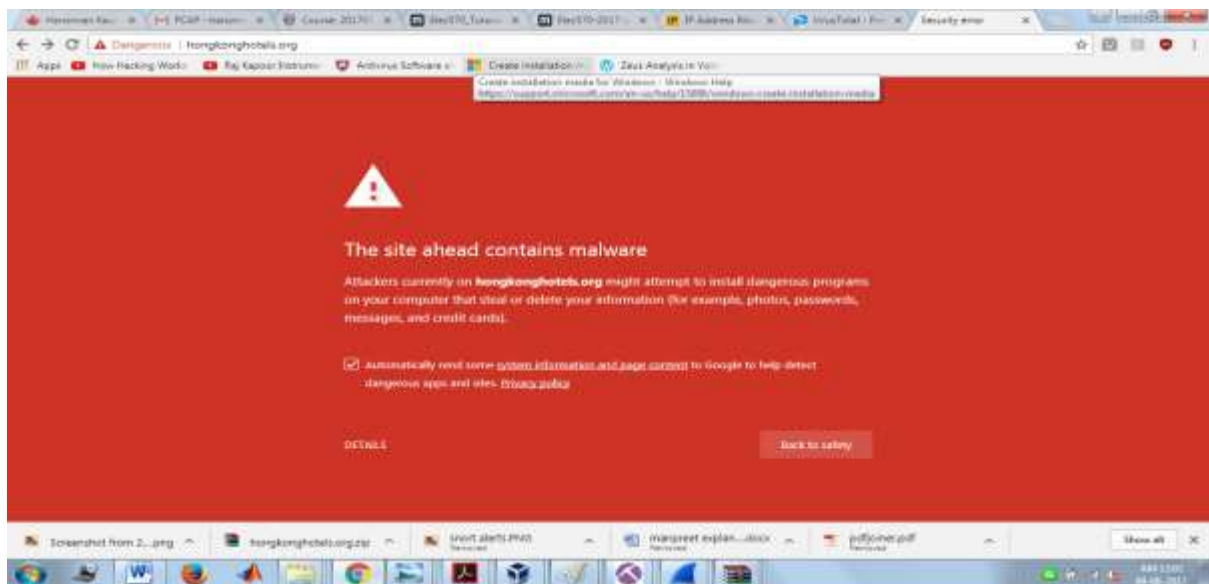
Then to analyse the files using VirusTotal we zipped the AssembledFiles into AssembledFiles.rar then we uploaded this file onto

<https://virustotal.com> then we found that only 184.168.137.1 is malicious.

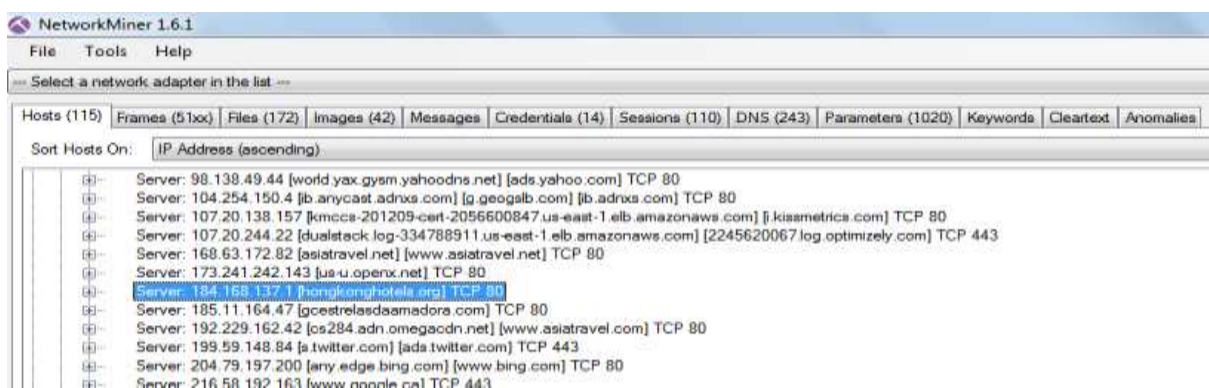


So we tried investigating it further. Analysis shows that this is a malicious website

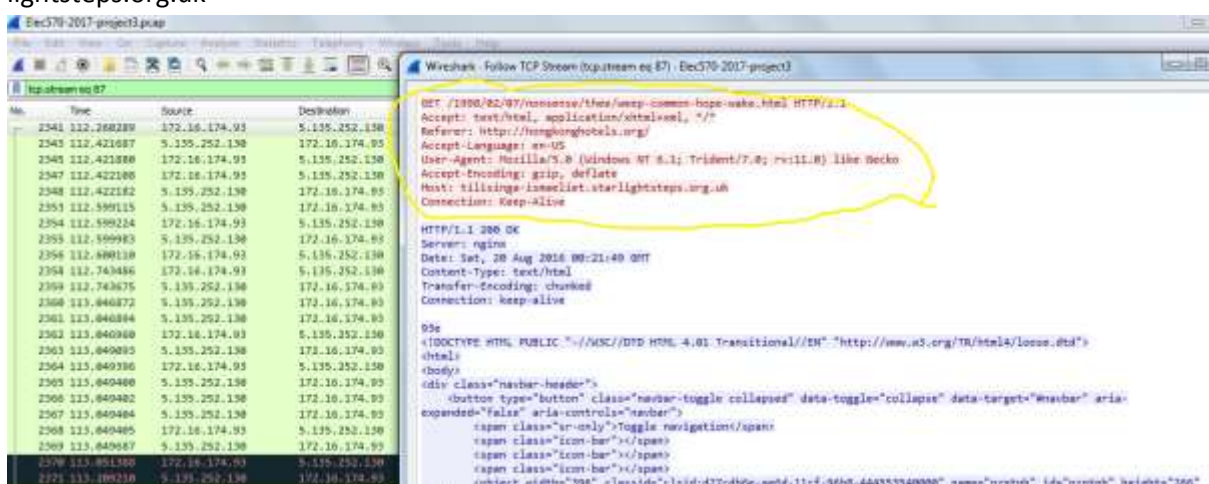




So the IP address is 184.168.137.1 and the URL of the compromised website is hongkonghotels.org which we found in NetworkMiner.



Then we found another evidence that confirms that 184.168.137.1 is malicious URL which triggered the malware traffic because in the TCP stream of 5.135.252.130 which is the URL that is responsible for malware delivering as we will explain in the next section it is referring to tilisinga-ismaeliet.starlightsteps.org.uk

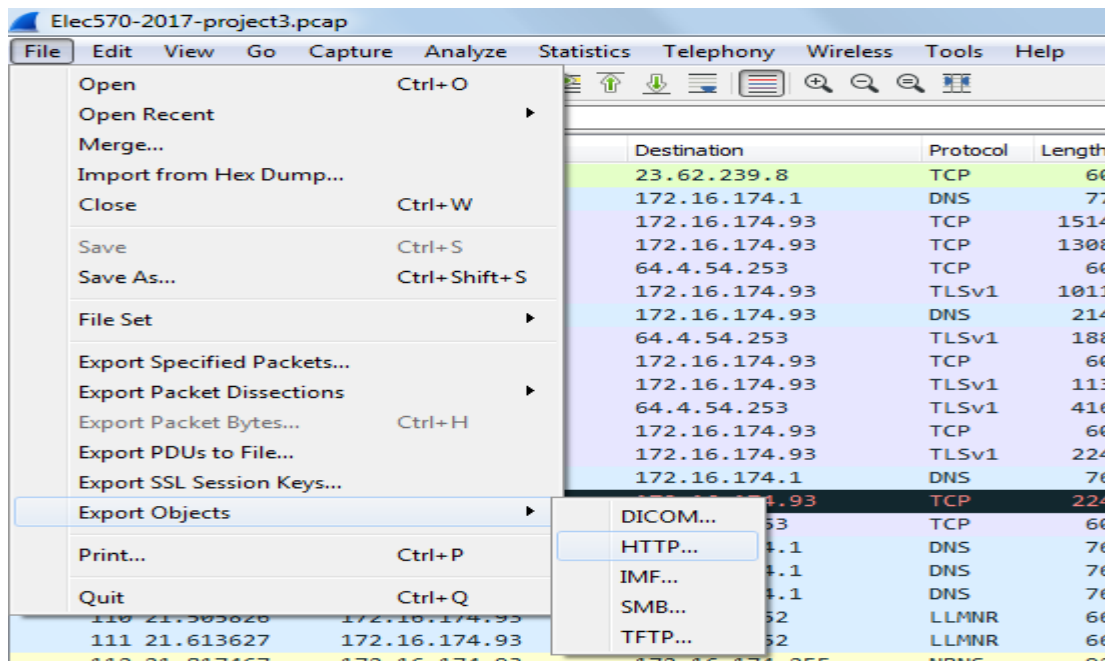


Host	Hongkonghotels.org
IP address	184.168.137.1
MAC address	0046DF6E7B3

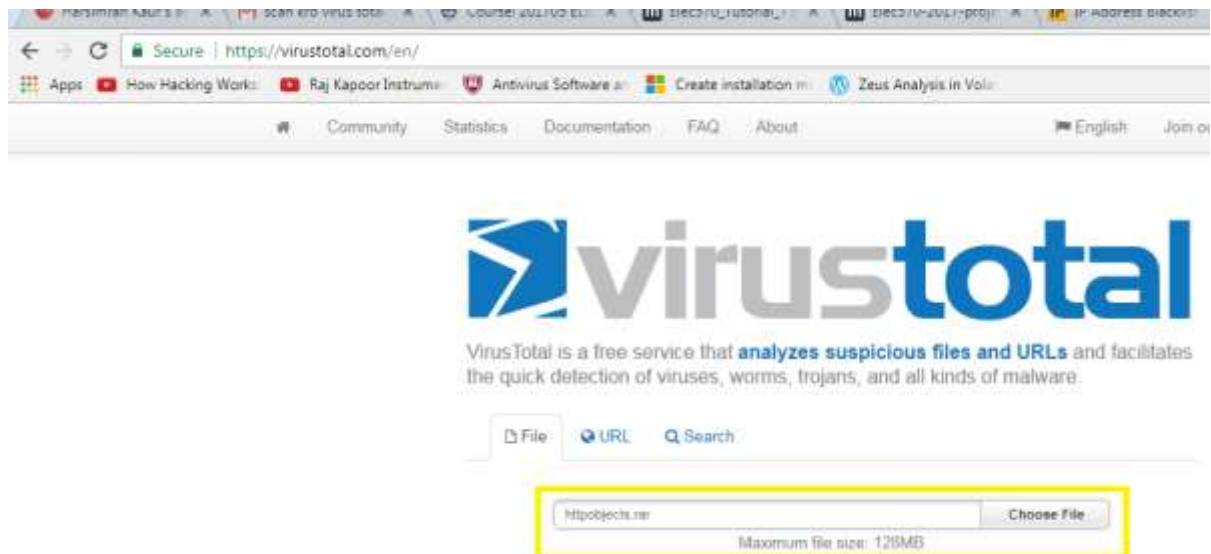
### 3. What is the IP address and domain name that delivered the malware? (2.5%)

Answer: To find this we uploaded the file in wireshark then,

File->export Objects-> http



Then we downloaded all the http objects in a folder called httpobjects





https://www.virustotal.com/en/file/c03740a43e55f818f1422cb67ade11ac7e66db2a7d8950a23c7ede34f55aa35d/

Community Statistics Documentation FAQ About English Join our community Sign in

# virustotal

SHA256: c03740a43e55f818f1422cb67ade11ac7e66db2a7d8950a23c7ede34f55aa35d

File name: weep-common-hope-wake.html

Detection ratio: 18 / 58

Analysis date: 2017-08-04 00:31:46 UTC ( 6 minutes ago )

Analysis Relationships Additional information Comments Votes

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.4825430	20170804
AegisLab	Html.Exploit.Kit.c	20170803
ALYac	Trojan.GenericKD.4825430	20170803

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.4825430	20170804
AegisLab	Html.Exploit.Kit.c	20170803
ALYac	Trojan.GenericKD.4825430	20170803
Arcabit	Trojan.Generic.D49A156	20170803
Avira (no cloud)	HTML.Agent.bio	20170804
BitDefender	Trojan.GenericKD.4825430	20170803
CAT-QuickHeal	JS.Neutrino.Susp.B	20170803
Cyren	Trojan.YWAW-8	20170804
Emsisoft	Trojan.GenericKD.4825430 (B)	20170803
F-Secure	Trojan.GenericKD.4825430	20170803
GData	HTML.Exploit.Kit.Q	20170803
Ikarus	HTML.Agent	20170803

We analysed all the http objects but only weep-common-hope-wake.html came out to be malicious so, we explored further to find out is it the real one and what is the IP address that delivered it?

Etc570-2017-project3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
2330	112.152372	184.168.137.1	172.16.174.93	HTTP	952	HTTP/1.1 200 OK [3F68 3F2F image]
2339	112.152508	172.16.174.93	184.168.137.1	TCP	60	49238 → 80 [ACK] Seq=658 Ack=12952 Win=63345 Len=0
2340	112.209971	172.16.174.1	172.16.174.93	DNS	117	Standard query response 0x4000 A tllisings-linsellist.starlightsteps.org.uk A 9.135.252.138
2341	112.209289	172.16.174.93	9.135.252.138	TCP	60	49244 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
2342	112.209295	172.16.174.93	9.135.252.138	TCP	60	49245 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
2343	112.421687	9.135.252.138	172.16.174.93	TCP	60	80 → 49244 [SYN, ACK] Seq=0 Ack=1 Win=64248 Len=0 MSS=1460
2344	112.421701	9.135.252.138	172.16.174.93	TCP	60	80 → 49245 [SYN, ACK] Seq=0 Ack=1 Win=64248 Len=0 MSS=1460
2345	112.421888	172.16.174.93	9.135.252.138	TCP	60	49244 → 80 [ACK] Seq=1 Ack=1 Win=0 Len=0
2346	112.421887	172.16.174.93	9.135.252.138	TCP	60	49245 → 80 [ACK] Seq=1 Ack=1 Win=0 Len=0
2347	112.422188	172.16.174.93	9.135.252.138	HTTP	411	GET /1596/82/97/notes/Time/weep-common-hope-wake.html HTTP/1.1
2348	112.422182	9.135.252.138	172.16.174.93	TCP	60	80 → 49244 [ACK] Seq=1 Ack=356 Win=64248 Len=0
2349	112.441874	52.209.210.146	172.16.174.93	TCP	60	80 → 49232 [FIN, PSH, ACK] Seq=1 Ack=1 Win=0 Len=0
2350	112.442828	172.16.174.93	52.209.210.146	TCP	60	49232 → 80 [ACK] Seq=1 Ack=2 Win=64248 Len=0
2351	112.537588	52.209.210.146	172.16.174.93	TCP	60	80 → 49233 [FIN, PSH, ACK] Seq=1073 Ack=799 Win=0 Len=0
2352	112.537707	172.16.174.93	52.209.210.146	TCP	60	49233 → 80 [ACK] Seq=799 Ack=1074 Win=63168 Len=0
2353	112.598115	9.135.252.138	172.16.174.93	TCP	1411	80 → 49244 [PSH, ACK] Seq=1 Ack=318 Win=0 Len=1357 [TCP segment of a reassembled PDU]
2354	112.599224	172.16.174.93	9.135.252.138	TCP	60	49244 → 80 [ACK] Seq=358 Ack=1358 Win=62081 Len=0
2355	112.599803	9.135.252.138	172.16.174.93	HTTP	1223	HTTP/1.1 200 OK [text/html]
2356	112.600110	172.16.174.93	9.135.252.138	TCP	60	49244 → 80 [ACK] Seq=358 Ack=1527 Win=64248 Len=0
2357	112.633119	172.16.174.93	172.16.174.1	DNS	76	Standard query 0x2501 A wpod.localdomain
2358	112.763486	172.16.174.93	9.135.252.138	HTTP	467	GET /article/1002540/slip-shrug-flap-able.swf HTTP/1.1
2359	112.743675	9.135.252.138	172.16.174.93	TCP	60	80 → 49244 [ACK] Seq=2527 Ack=771 Win=64248 Len=0
2360	113.040872	9.135.252.138	172.16.174.93	TCP	1514	80 → 49244 [ACK] Seq=2527 Ack=771 Win=64248 Len=1400 [TCP segment of a reassembled PDU]
2361	113.040894	9.135.252.138	172.16.174.93	TCP	1308	80 → 49244 [PSH, ACK] Seq=3987 Ack=771 Win=64248 Len=1254 [TCP segment of a reassembled PDU]
2362	113.040950	172.16.174.93	9.135.252.138	TCP	60	49244 → 80 [ACK] Seq=771 Ack=5261 Win=64248 Len=0
2363	113.040963	9.135.252.138	172.16.174.93	TCP	1411	80 → 49244 [PSH, ACK] Seq=5261 Ack=771 Win=64248 Len=1357 [TCP segment of a reassembled PDU]
2364	113.043306	172.16.174.93	9.135.252.138	TCP	60	49244 → 80 [ACK] Seq=771 Ack=6508 Win=62081 Len=0
2365	113.043400	9.135.252.138	172.16.174.93	TCP	1514	80 → 49244 [ACK] Seq=5338 Ack=771 Win=64248 Len=1400 [TCP segment of a reassembled PDU]

Frame 2364: 68 bytes on wire (480 bits), 68 bytes captured (480 bits)

Ethernet II, Src: Dell\_E3:bl:ds (5c:28:da:83:bl:ds), Dst: Cisco\_F6:a7:b3 (00:04:0d:f6:a7:b3)

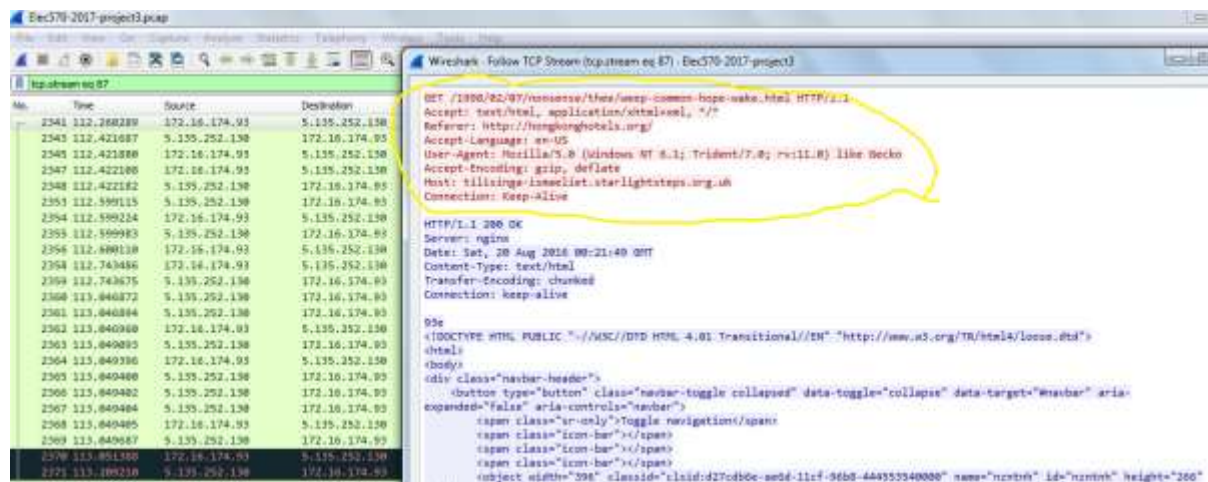
Internet Protocol Version 4, Src: 172.16.174.93, Dst: 9.135.252.138

Transmission Control Protocol, Src Port: 49244, Dst Port: 80, Seq: 771, Ack: 6508, Len: 0

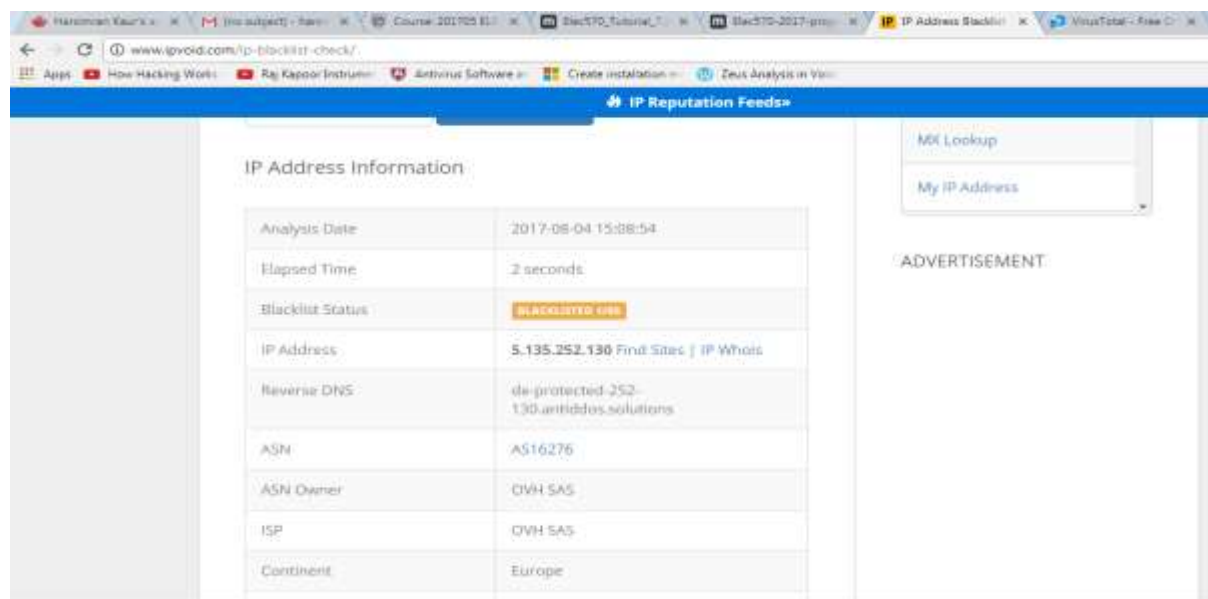
00 04 0d f6 a7 b3 5c 28 da 83 bl ds 00 08 45 00 ..R...V.....E.

Etc570-2017-project3 Packets: 530 / Displayed: 530 (100.0%) Load time: 0:0:43

Then we found the TCP stream of 5.135.252.130 using Wireshark.

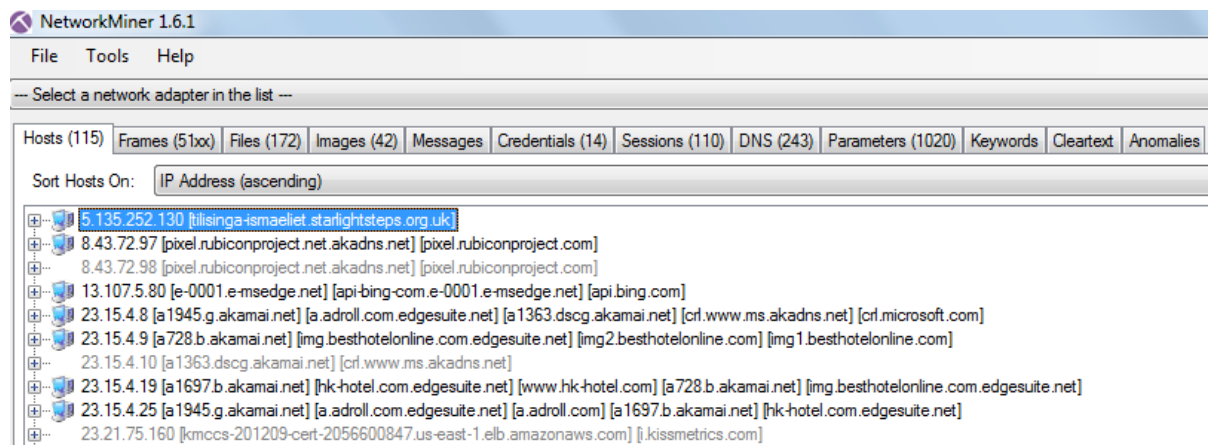


Now we can clearly see that referrer is hongkonghotels.org (which we found that it is malicious in the previous question) which is hosting tilisinga-ismaeliet.startlightsteps.org.uk. Then, we found if the URL is blacklisted in ipvoid.com and we found that it is blacklisted.



So the IP address and domain name that delivered the Malware is 5.135.252.130 and the ip address is tilisinga-ismaeliet.startlightsteps.org.uk

We confirmed the IP address and domain name using NetworkMiner also.

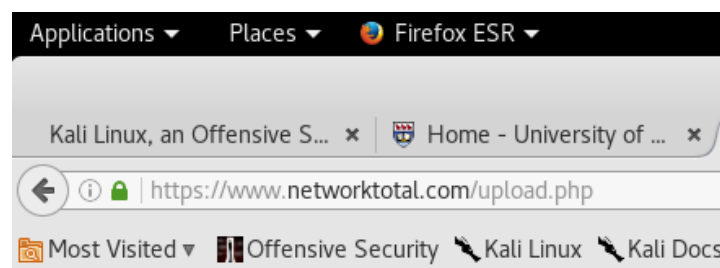
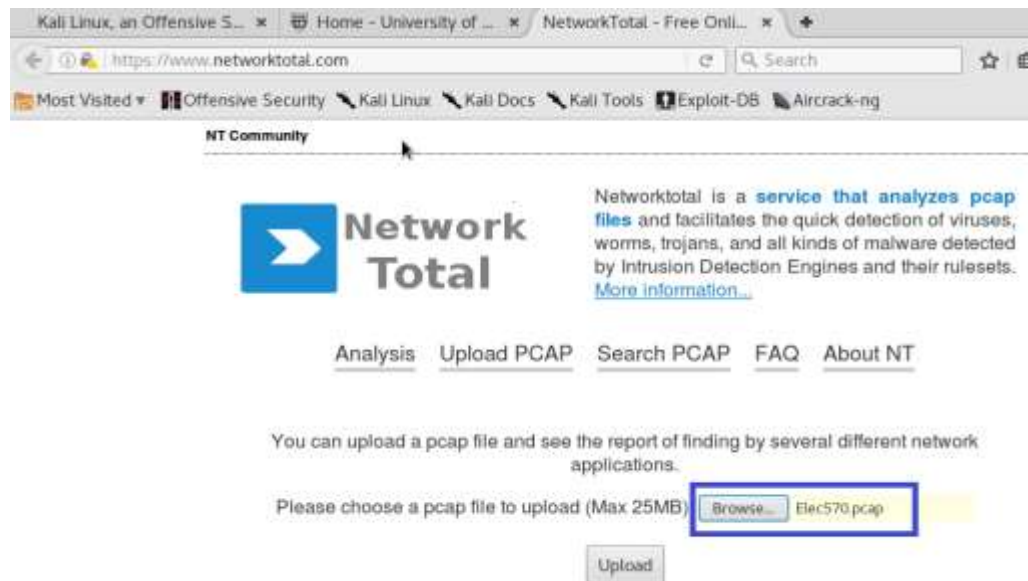


Ip Address	5.135.252.130
Host Name and URL	tilisinga-ismaeliet-startlightsteps.org.uk
MAC address	00046DF6E7B3

4. Identify the type of malware involved and check the payload by running the associated file (or files) against an online virus checker (i.e. VirusTotal). (3%)

Answer:

To identify the attacks missed by snort we uploaded the file PCAP file on networktotal.com



The file Elec570.pcap has been uploaded.  
The results should be present here when its done:

- [c0350c09198a99a3c6c72e48589d46f0](https://www.virustotal.com/gdetection/1/c0350c09198a99a3c6c72e48589d46f0/)



Date	MD5	sid	msg
Sat, 20 Aug 2016 02:21:17 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2210048-1]	SURICATA STREAM reassembly sequence GAP -- missing packet(s)
Sat, 20 Aug 2016 02:21:17 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2210048-1]	SURICATA STREAM reassembly sequence GAP -- missing packet(s)
Sat, 20 Aug 2016 02:21:37 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2210048-1]	SURICATA STREAM reassembly sequence GAP -- missing packet(s)
Sat, 20 Aug 2016 02:21:37 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2820852-3]	ETPRO CURRENT_EVENTS Job314/Neutrino Reboot EK Landing June 11 2016 M4 (with URI Primer)
Sat, 20 Aug 2016 02:21:36 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2022962-3]	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016
Sat, 20 Aug 2016 02:21:37 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2012897-4]	ET WEB_SERVER.PHP Possible http Remote File Inclusion Attempt
Sat, 20 Aug 2016 02:21:37 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2009131-8]	ET WEB_SERVER.PHP Generic Remote File Include Attempt (HTTP)
Sat, 20 Aug 2016 02:21:52 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2102925-5]	GPL WEB_CLIENT web bug 0x0 gif attempt
Sat, 20 Aug 2016 02:21:43 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2821016-1]	ETPRO TROJAN CryptXXX Jul 07 2016 request for ransom note 1
Sat, 20 Aug 2016 02:21:45 +0000	e309945eeb0e6f5dc66ca9aa83f7b83b [VT]	[1-2210048-1]	SURICATA STREAM reassembly sequence GAP -- missing packet(s)

Here we found that Neutrino Reboot Exploit Kit Landing is involved. Then we searched about it on internet. Also it can be seen that CryptXXX request for ransom note1 is also seen.

Harsimran Ka...
[no subject]
Course: 201701
Elec570\_Tutor...
Elec570-2017
IP Address

Secure
https://blog.malwarebytes.com/threats/neutrino/

Apps
How Hacking Works
Raj Kapoor Instrum...
Antivirus Software
Create installation
Zeus Analysis in Vol...

MalwarebytesLABS

# Neutrino

Posted: June 9, 2016

## Short bio

The Neutrino exploit kit is a malicious tool kit, which can be used by attackers who are not experts on computer security. Threat actors can have zero coding experience and still use exploit kits like Neutrino to conduct their illegal activity.

## History

Exploit kits, sometimes referred to as exploit packs, are toolkits that automate the exploitation of client-side vulnerabilities, often targeting browsers and applications that a website can invoke through the browser. Known exploit targets have been vulnerabilities in Adobe Reader, Java Runtime Environment, and Adobe Flash Player.

Neutrino began targeting CVE-2012-1723, CVE-2013-0431, and, CVE-2013-0422 all exploiting vulnerabilities in the Java Runtime Environment (JRE) component. It was marketed as a simple-to-use kit with a nicely user friendly control panel.

## Common infection method

Neutrino toolkit compromises systems by targeting various vendor vulnerabilities on the victim's machine.

Campaigns targeting WordPress have been observed using dynamic iframe injection. The goal of the campaign was to fully compromise the site, which included adding a webshell (Remote Access Tool (RAT) or backdoor), harvesting credentials, and finally injecting an iframe that loads a Neutrino landing page. The iframe is injected into the compromised site immediately after the BODY tag, which resembles recent Angler samples. Threat actors want to re-direct victims to their payload, which includes ransomware.

## Associated families

Exploit kits/packs and ransomware.

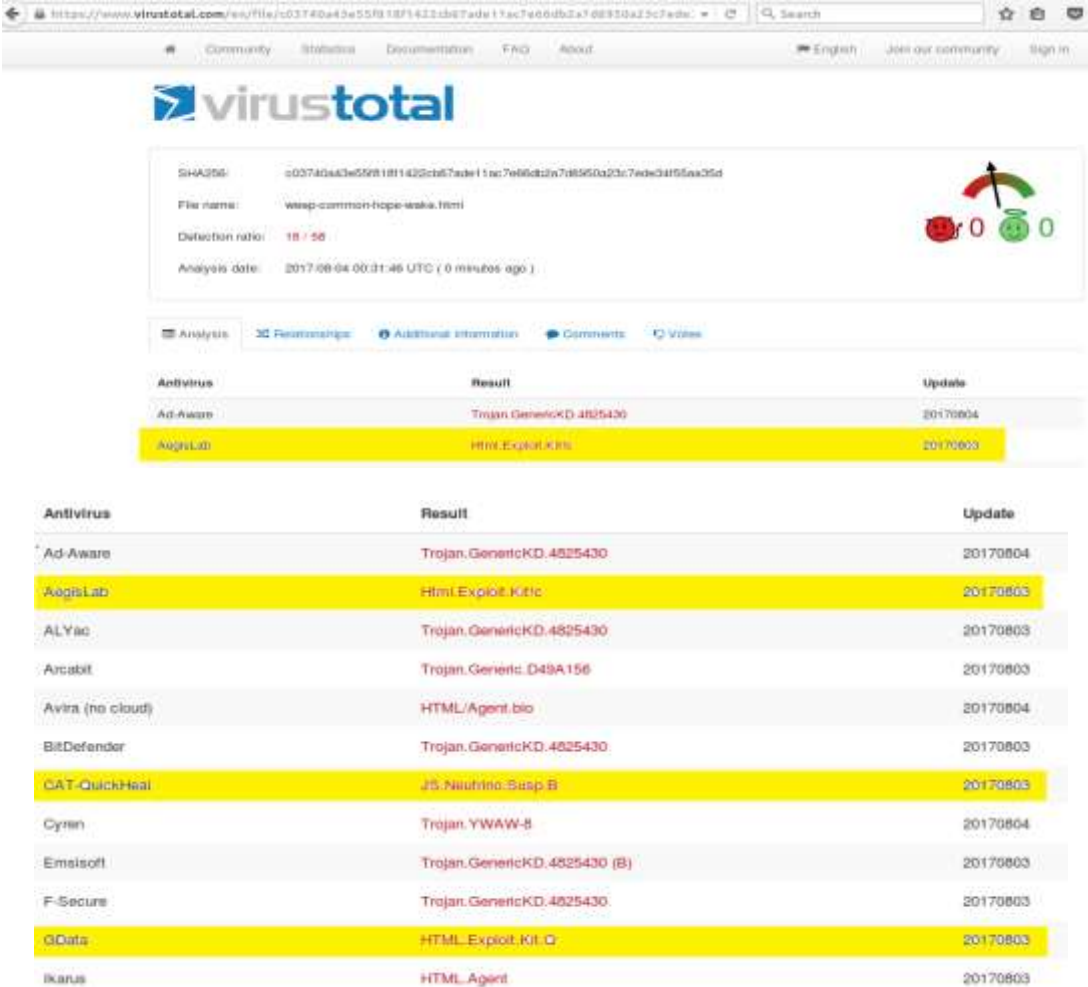
## Remediation

Malwarebytes Anti-Exploit stops Neutrino EK while Malwarebytes Anti-Malware already detects known dropped binaries, such as Andromeda/Gamarue malware. Keep your system patched and keep your applications updated.



Now it is confirmed that Ransomware is involved using neutrino exploit kit.

Now we found only one malicious file in the http objects. That is weep-common-hope-wake.html we analysed it using virustotal.com.



The screenshot shows the VirusTotal analysis page for the file `weep-common-hope-wake.html`. The file's SHA256 hash is `c037a0443e559818f1423cb57ade11ac7e66d23n7d8950a23c7ade3d4f55a25d`. The detection ratio is 18/56, and the analysis date is 2017-08-04 00:31:46 UTC. The analysis results table is as follows:

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.4825430	20170804
AegisLab	Html.Exploit.Kit.c	20170803
AlYac	Trojan.GenericKD.4825430	20170803
Arcabit	Trojan.Generic.D49A156	20170803
Avira (no cloud)	HTML.Agent.bio	20170804
BitDefender	Trojan.GenericKD.4825430	20170803
CAT-QuickHeal	JS.Neutrino.Susp.B	20170803
Cyren	Trojan.YVAW-B	20170804
Emsisoft	Trojan.GenericKD.4825430 (B)	20170803
F-Secure	Trojan.GenericKD.4825430	20170803
GData	HTML.Exploit.Kit.C	20170803
Ikarus	HTML.Agent	20170803

As highlighted in the above screen shot it is confirmed that **weep-common-hope-wake.html** is a Neutrino EK landing page.

So type of malware involved in **Ransomware**.

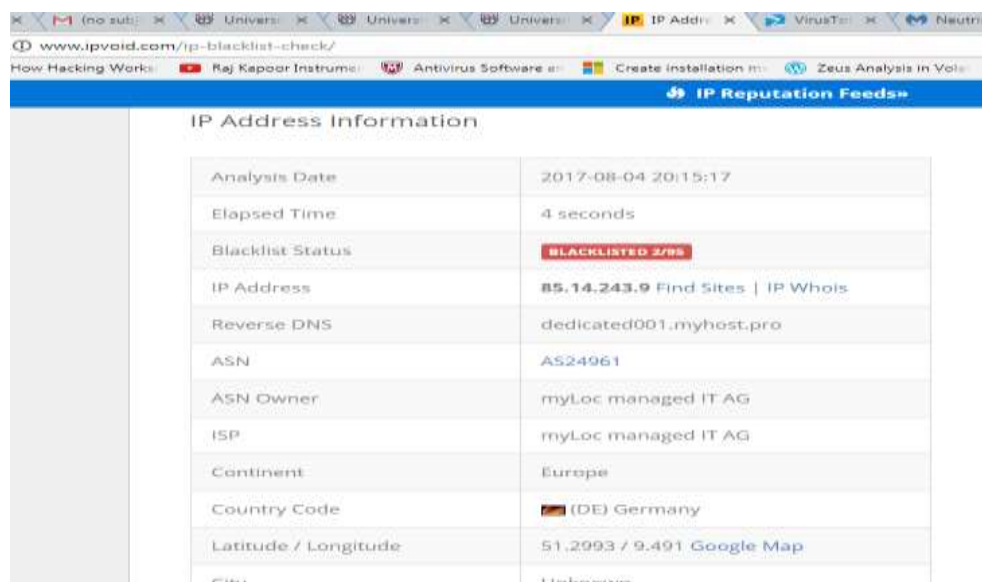
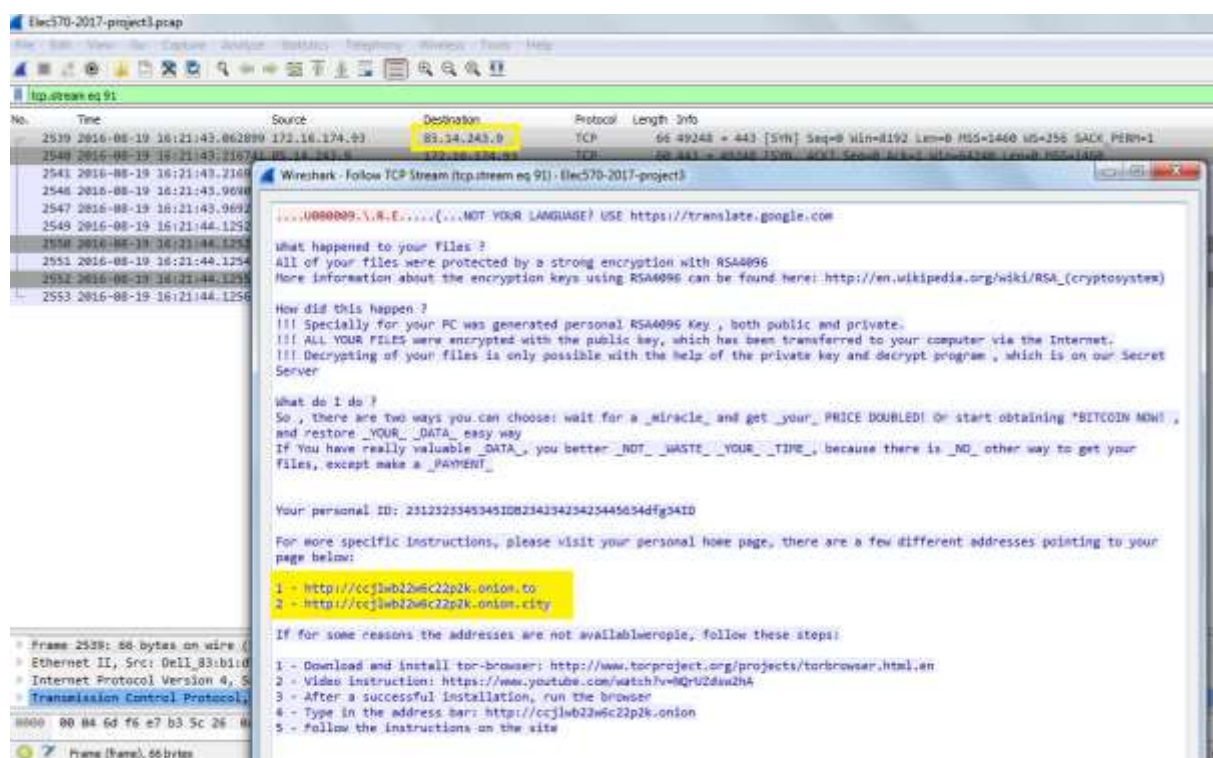
5. Identify other malicious hosts or sites with which the compromised host interacted. Only malicious hosts should be included in this list. Provide your response in a table listing the following (4%):

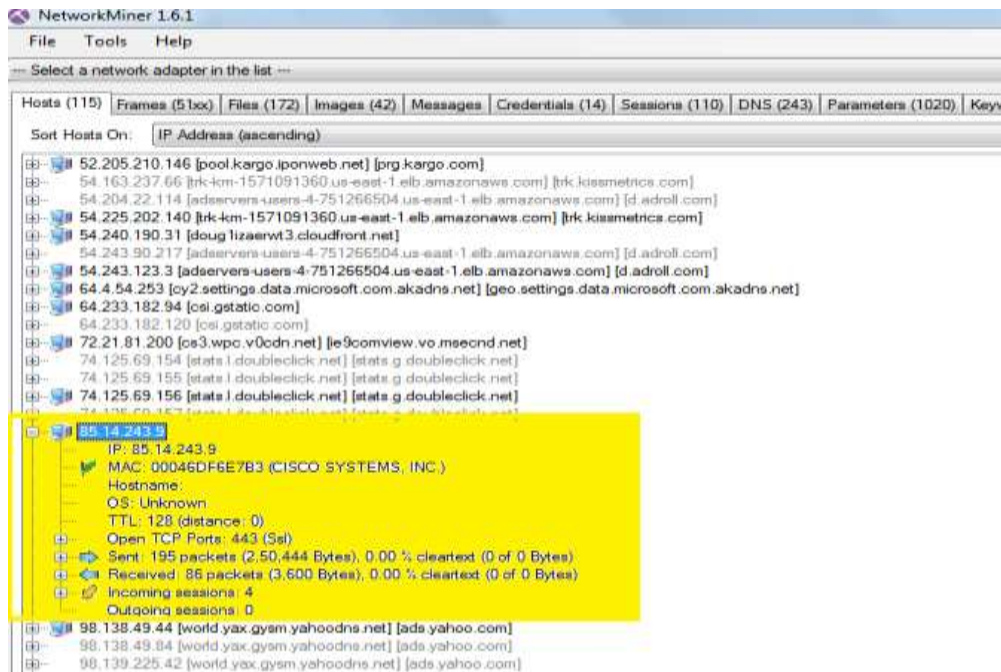
- Host name or URL
- Role
- Communication protocol or service
- Date and time range of the interaction (i.e. start date/time – end date/time)

Answer:

We found that the malicious 5.135.252.130 started interacting with the victim IP 172.16.174.93 at

1. The other host which we found interacting with 172.16.174.93 is 85.14.243.9. Here we found a Ransomware note which is giving the directions to use bit coin to transfer the money.





-Host name or URL - 85.14.243.9 URL is not specified yet.

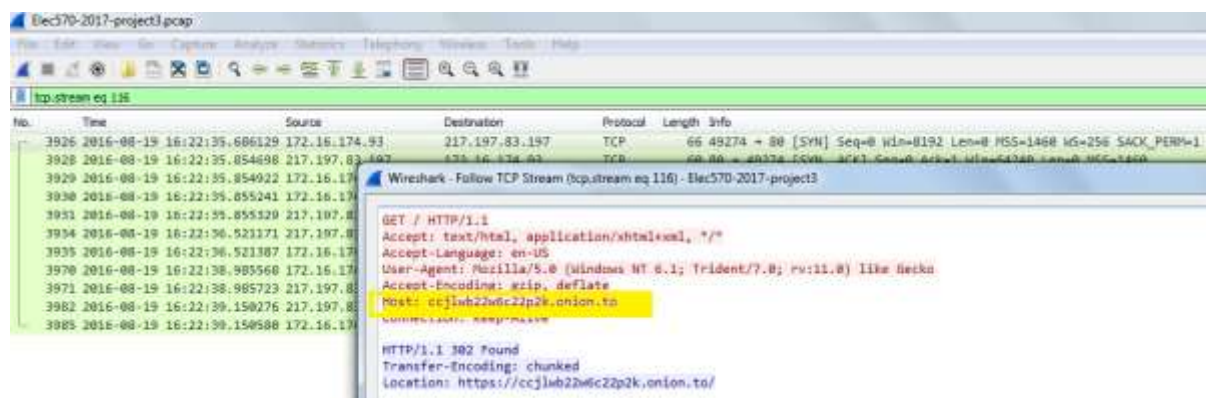
- Role – Ransomware note which is redirecting the user to payment method

-Communication Protocol- TCP 443 port

- Date and time range of the interaction (start date-19-08-2016/time-16:21:41 – end date-19-08-2016/time-16:21:50).

2. Another IP address which is interacting with 172.16.174.93 is 217.197.83.197 when we followed its stream we found the same HOST **ccjlwb22w6c22p2k.onion.to** which we found in Ransomware note and it is associated with dark net.

Then



Now in this screen shot also we found that it is interacting with the victim PC which is taken from NetworkMiner.



Hosts (115)	Frames (5100)	Files (172)	Images (42)	Messages	Credentials (14)	Sessions (110)	DNS (243)	Parameters (1020)	Keywords	Cleartext	Anomalies
Sort Hosts On: IP Address (ascending)											
<div> <div>Server: 107.20.138.157 [mccs-201209-cert-2056600847.us-east-1.elb.amazonaws.com] [i.kiasmetrics.com] TCP 80</div> <div>Server: 107.20.244.22 [dualstack.log-334788911.us-east-1.elb.amazonaws.com] [2245620067.log.optimizely.com] TCP 443</div> <div>Server: 168.63.172.82 [asiatravel.net] [www.asiatravel.net] TCP 80</div> <div>Server: 173.241.242.143 [us-u.openx.net] TCP 80</div> <div>Server: 184.168.137.1 [hongkonghotels.org] TCP 80</div> <div>Server: 185.11.164.47 [gcestralasdaamadora.com] TCP 80</div> <div>Server: 192.229.162.42 [ca284.adn.omegacdn.net] [www.asiatravel.com] TCP 80</div> <div>Server: 199.59.148.84 [s.twitter.com] [ads.twitter.com] TCP 443</div> <div>Server: 204.79.197.200 [any.edge.bing.com] [www.bing.com] TCP 80</div> <div>Server: 216.58.192.163 [www.google.ca] TCP 443</div> <div>Server: 216.58.192.164 [www.google.com] TCP 443</div> <div>Server: 216.58.192.168 [www.googletagmanager.l.google.com] [www.googletagmanager.com] TCP 80</div> <div>Server: 216.58.192.174 [maps.google.com] [www.google-analytics.l.google.com] [www.google-analytics.com] TCP 80</div> <div>Server: 216.58.192.202 [googleapis.l.google.com] [maps.googleapis.com] TCP 443</div> <div>Server: 216.58.192.202 [googleapis.l.google.com] [maps.googleapis.com] TCP 80</div> <div>Server: 216.58.216.66 [pagead.l.doubleclick.net] [www.googleadservices.com] TCP 80</div> <div>Server: 216.58.216.98 [pagead46.l.doubleclick.net] [googleads.g.doubleclick.net] TCP 443</div> <div>Server: 216.58.216.194 [pagead.l.doubleclick.net] [cm.g.doubleclick.net] TCP 443</div> <div>Server: 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] TCP 443</div> <div>Server: 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] TCP 80</div> </div>											
<div> <div>Host Details</div> <div>172.16.174.254</div> <div>172.16.174.255</div> <div>172.217.4.234 [googleapis.l.google.com] [maps.googleapis.com]</div> <div>173.241.242.143 [us-u.openx.net]</div> <div>184.72.230.183 [dualstack.log-334788911.us-east-1.elb.amazonaws.com] [2245620067.log.optimizely.com]</div> <div>184.168.137.1 [hongkonghotels.org]</div> <div>185.11.164.47 [gcestralasdaamadora.com]</div> <div>185.100.85.150 [onion.to] [ccjlwb22w6c22p2k.onion.to]</div> <div>185.100.85.150 [onion.to] [ccjlwb22w6c22p2k.onion.to]</div> </div>											

We also find using [ipvoid.com](http://ipvoid.com) to make sure it is malicious for sure.

<div> <div>www.ipvoid.com/ip-blacklist-check/</div> <div>How Hacking Works</div> <div>Raj Kapoor Instrume</div> <div>Antivirus Software</div> <div>Create installation m</div> <div>Zeus Analysis in</div> </div>	
IP Reputation Feeds	
IP Address Information	
Analysis Date	2017-08-04 20:50:06
Elapsed Time	4 seconds
Blacklist Status	BLACKLISTED 2/99
IP Address	217.197.83.197 Find Sites   IP Whois
Reverse DNS	onion.to
ASN	AS29670
ASN Owner	Individual Network Berlin e.V.
ISP	Individual Network Berlin e.V.
Continent	Europe
Country Code	🇩🇪 (DE) Germany
Latitude / Longitude	52.3689 / 13.1273 Google Map

-Host name or URL – 217.197.83.197 (ccjlwb22w6c22p2k.onion.to)

- Role – Ransomware url where payment is to be paid

-Communication Protocol- TCP 443 port

- Date and time range of the interaction (start date-19-08-2016/time-16:22:36 – end date-19-08-2016/time-16:22:48).

**6. Give an outline of the attack scenario by describing it in a few paragraphs and by providing a graphical sketch (4%).**

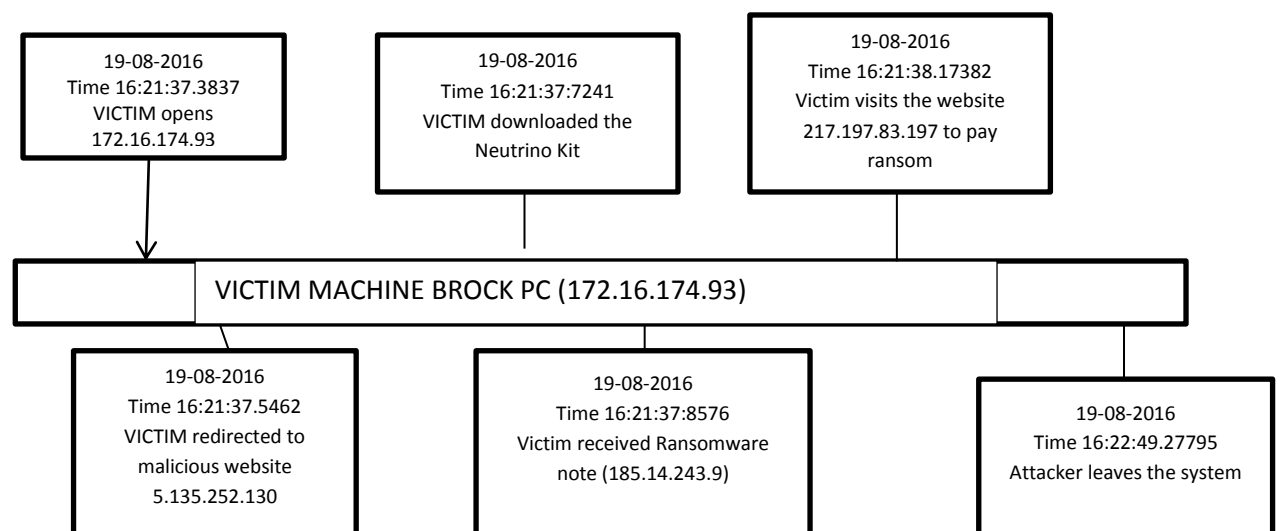
The attack started at Time: 16:21:21 on date 19-08-2016. And left the system at time 16:22:52. So we analysed all the IP addresses which are interacting with 172.16.174.93 in this timeline.



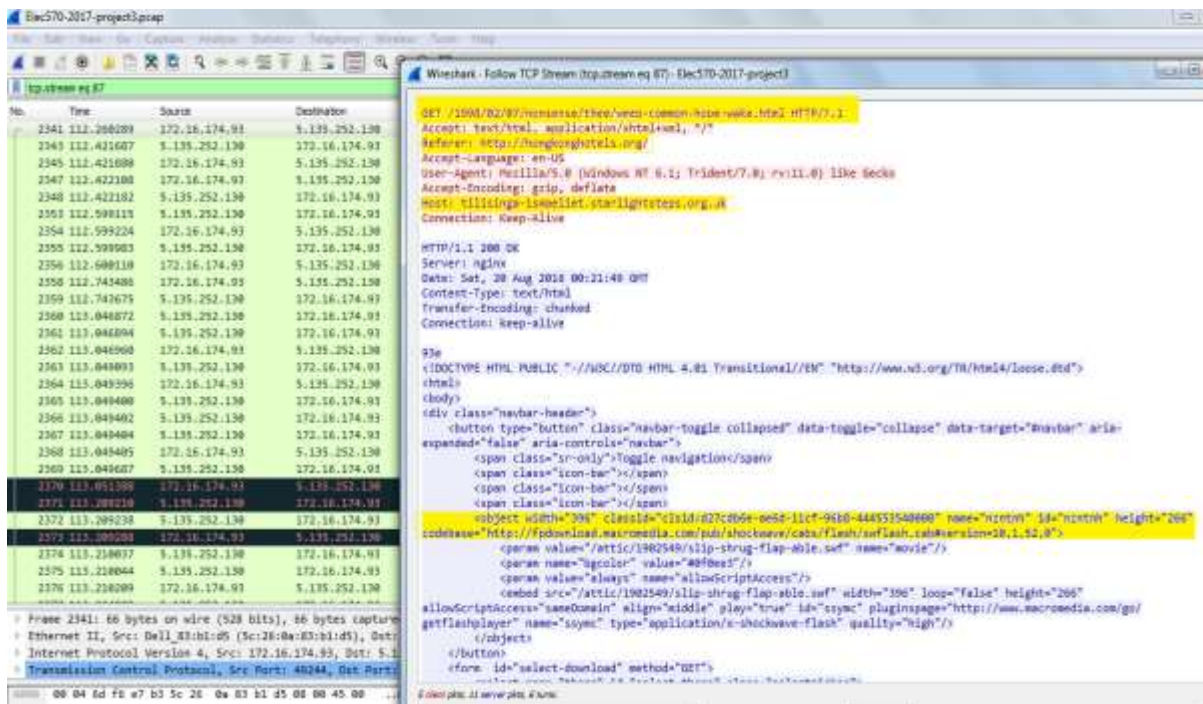
No.	Time	Source	Destination	Protocol	Length	Info
1846	2016-08-19 16:21:11.953913	8.43.72.87	172.16.174.93	TCP	60	48210 [SYN, ACK] Seq=84004248 Len=0 MSS=1460
1849	2016-08-19 16:21:11.954118	8.43.72.87	172.16.174.93	TCP	60	48217 [SYN, ACK] Seq=84004248 Len=0 MSS=1460

We basically describe how the attack occurred right from the point when Brock PC came into interaction with hongkonghotels.com

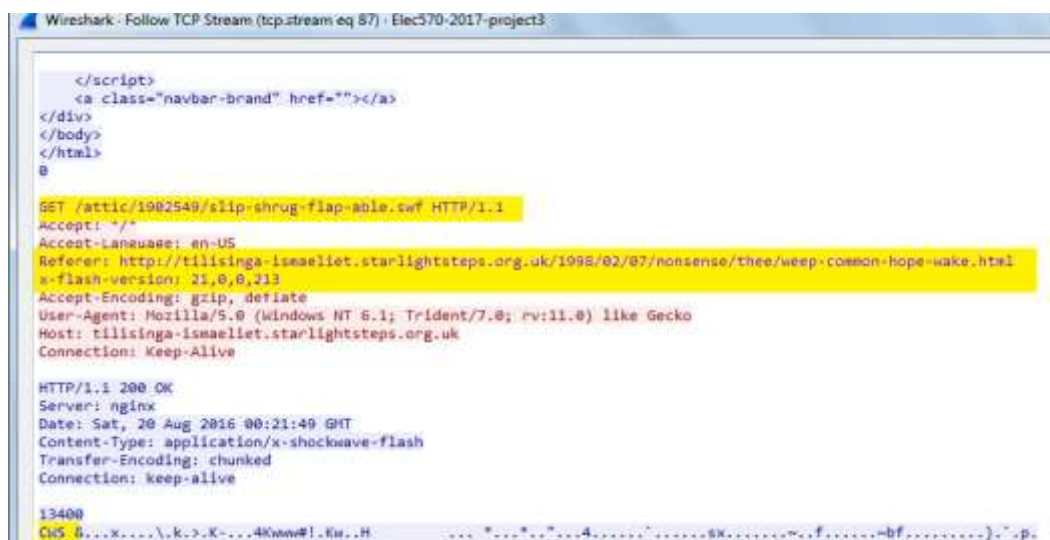
DATE	TIME	ACTIVITY
19-08-2016	16:21:37.3837	Victim Brock PC 172.16.174.93 opens hongkonghotels.org
	16:21:37.5462	It is redirected to 5.135.252.130 i.e. tilisinga-ismaeliet-startlightsteps.org.uk from there it getting Weep-common-hope-wake.html (which is basically Neutrino Ransomware kit URL)
	16:21:37.7241	Neutrino Kit Download OK
	16:21:37.8676	Victim received Ransomware note to deposit money using Bit Coin
	16:21:38.17382	Victim visited the website where he needs to pay ransom
19-08-2016	16:22:49.27795	Attacker leaves the system.



We have identified that IP **184.168.137.1** is malicious host which redirects it to landing page tilisinga-ismaeliet.starlightsteps.org.uk with IP 5.135.252.130 from where it is asking to get weep-common-hope-wake.html. but it needs macromedia shockwave player to get download.



Then it redirects the page to slip-shrug-flap-able.swf from where it downloaded the X-flash-version: 21, 0, 0, 213 as shown in the screen shot below.



Also CWS means compressed flash file and HTTP/1.1 200 ok means file is successfully downloaded. Then using referrer tilisinga-ismaeliet.startlightsteps.org.uk a 0X0 pixel byte file might be downloaded on the victim machine using spectre-survey-camera-market.html.



7. Briefly discuss remediation and mitigation solutions for such threat (2-3 paragraphs maximum) (1.5%).

Answer:

## 1. Back up your data

The **single biggest thing** that will defeat ransomware is **having a regularly updated backup**. If you are attacked with ransomware you may lose that document you started earlier this morning, but if you can restore your system to an earlier snapshot or clean up your machine and restore your other lost documents from backup, you can rest easy. Remember that Cryptolocker will also encrypt files on drives that are mapped. This includes any external drives such as a USB thumb drive, as well as any network or cloud file stores that you have assigned a drive letter. So, what you need is a regular backup regimen, to an external drive or backup service, one that is not assigned a drive letter or is disconnected when it is not doing backup.

The next three tips are meant to deal with how Cryptolocker has been behaving – this may not be the case forever, but these tips can help increase your overall security in small ways that help prevent against a number of different common malware techniques.

## 2. Show hidden file-extensions

One way that Cryptolocker frequently arrives is in a file that is named with the extension “.PDF.EXE”, counting on Window’s default behavior of hiding known file-extensions. If you re-enable the ability to see the full file-extension, it can be easier to spot suspicious files.

## 3.Filter EXEs in email

If your gateway mail scanner has the ability to filter files by extension, you may wish to deny mails sent with “.EXE” files, or to deny mails sent with files that have two file extensions, the last one being executable (“\*.\*.EXE” files, in filter-speak). If you do legitimately need to exchange executable files within your environment and are denying emails with “.EXE” files, you can do so with ZIP files (password-protected, of course) or via cloud services.

## 4.Disable files running from AppData/LocalAppData folders

You can create rules within Windows or with Intrusion Prevention Software, to disallow a particular, notable behavior used by Cryptolocker, which is to run its executable from the App Data or Local App Data folders. If (for some reason) you have legitimate software that you know is set to run not from the usual Program Files area but the App Data area, you will need to exclude it from this rule.

## 5. Use the [Cryptolocker Prevention Kit](#)

The Cryptolocker Prevention Kit is a tool created by Third Tier that automates the process of making a Group Policy to disable files running from the App Data and Local App Data folders, as well as disabling executable files from running from the Temp directory of various unzipping utilities. This tool is updated as new techniques are discovered for Cryptolocker, so you will want to check in periodically to make sure you have the latest version. If you need to create exemptions to these rules, [they provide this document](#) that explains that process.

## 6. Disable RDP

The Cryptolocker/Filecoder malware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely. If you do

not require the use of RDP, you can disable RDP to protect your machine from Filecoder and other RDP exploits. For instructions to do so, visit the appropriate Microsoft Knowledge Base article below:

- [Windows XP RDP disable](#)
- [Windows 7 RDP disable](#)
- [Windows 8 RDP disable](#)

## **7. Patch or Update your software**

These next two tips are more general malware-related advice, which applies equally to Cryptolocker as to any malware threat. Malware authors frequently rely on people running outdated software with known vulnerabilities, which they can exploit to silently get onto your system. It can significantly decrease the potential for ransomware-pain if you make a practice of updating your software often. Some vendors release security updates on a regular basis (Microsoft and Adobe both use the second Tuesday of the month), but there are often “out-of-band” or unscheduled updates in case of emergency. Enable automatic updates if you can, or go directly to the software vendor’s website, as malware authors like to disguise their creations as software update notifications too.

## **8. Use a reputable security suite**

It is always a good idea to have both anti-malware software and a software firewall to help you identify threats or suspicious behavior. Malware authors frequently send out new variants, to try to avoid detection, so this is why it is important to have both layers of protection. And at this point, most malware relies on remote instructions to carry out their misdeeds. If you run across a ransomware variant that is so new that it gets past anti-malware software, it may still be caught by a firewall when it attempts to connect with its Command and Control (C&C) server to receive instructions for encrypting your files.

If you find yourself in a position where you have already run a ransomware file without having performed any of the previous precautions, your options are quite a bit more limited. But all may not be lost. There are a few things you can do that *might* help mitigate the damage, particularly if the ransomware in question is Cryptolocker:

## **9. Disconnect from WiFi or unplug from the network immediately**

If you run a file that you suspect may be ransomware, but you have not yet seen the characteristic ransomware screen, if you act *very* quickly you might be able to stop communication with the C&C server before it finish encrypting your files. If you disconnect yourself from the network *immediately*(have I stressed enough that this must be done *right away*?), you might mitigate the damage. It takes some time to encrypt all your files, so you may be able to stop it before it succeeds in garbling them all. This technique is definitely not foolproof, and you might not be sufficiently lucky or be able to move more quickly than the malware, but disconnecting from the network may be better than doing nothing.

## **10. Use System Restore to get back to a known-clean state**

If you have System Restore enabled on your Windows machine, you might be able to take your system back to a known-clean state. But, again, you have to out-smart the malware. Newer versions of Cryptolocker can have the ability to delete “Shadow” files from System Restore, which means those files will not be there when you try to to replace your malware-damaged versions. Cryptolocker will start the deletion process whenever an executable file is run, so you will need to move very quickly as executables may be started as part of an automated process.



That is to say, executable files may be run without you knowing, as a normal part of your Windows system's operation.

## 11. Set the BIOS clock back

Cryptolocker has a payment timer that is generally set to 72 hours, after which time the price for your decryption key goes up significantly. (The price may vary as Bitcoin has a fairly volatile value. At the time of writing the initial price was .5 Bitcoin or \$300, which then goes up to 4 Bitcoin) You can "beat the clock" somewhat, by setting the BIOS clock back to a time before the 72 hour window is up. I give this advice reluctantly, as all it can do is keep you from having to pay the higher price, and **we strongly advise that you do not pay the ransom**. Paying the criminals may get your data back, but there have been plenty of cases where the decryption key never arrived or where it failed to properly decrypt the files. Plus, it encourages criminal behavior! Ransoming *anything* is not a legitimate business practice, and the malware authors are under no obligation to do as promised – they can take your money and provide nothing in return, because there is no backlash if the criminals fail to deliver.