2015-02-08 - TRAFFIC ANALYSIS EXERCISE

SCENARIO

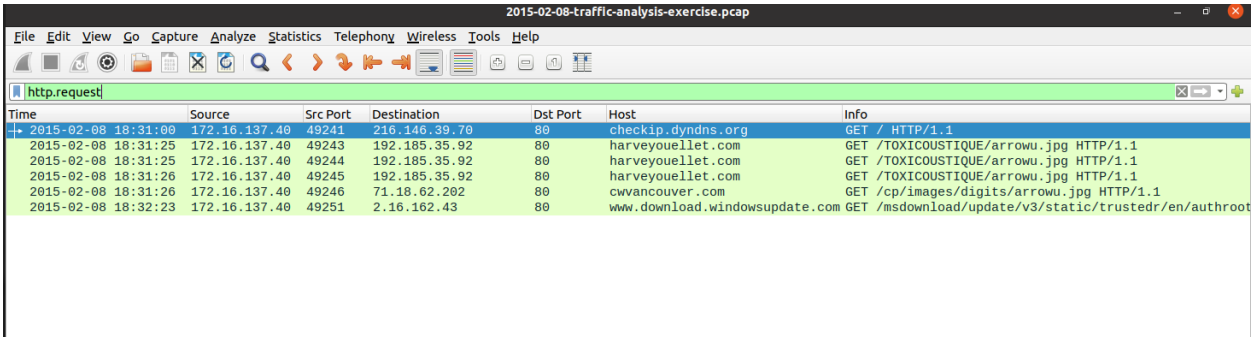
Mike calls the Help Desk and says his desktop computer is "acting weird" but he refuses to provide any details. The Help Desk reports it to your organization's Security Operations Center (SOC). A phone call to Mike doesn't reveal any details. He insists his computer is "acting weird" but will not say what, exactly, is wrong.

One of the SOC analysts searched through network traffic and retrieved a pcap related to this activity. This traffic occurred shortly before Mike called the Help Desk. The analyst cannot figure out what happened, so you've been asked to take a look.

You review the pcap and take notes. First, you document the following:

- Date and time of the activity

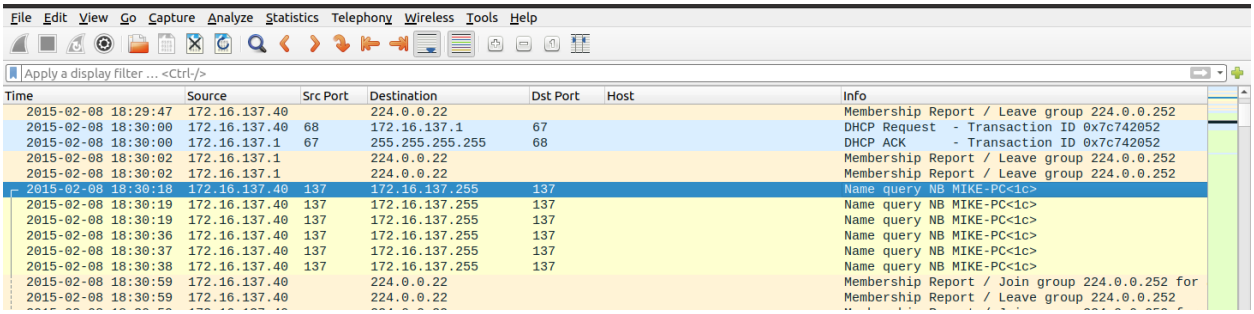
  2015-2-08 at 18:31 UTC



Time	Source	Src Port	Destination	Dst Port	Host	Info
2015-02-08 18:31:00	172.16.137.40	49241	216.146.39.70	80	checkip.dyndns.org	GET / HTTP/1.1
2015-02-08 18:31:25	172.16.137.40	49243	192.185.35.92	80	harveyouellet.com	GET /TOXICOUSTIQUE/arrowu.jpg HTTP/1.1
2015-02-08 18:31:25	172.16.137.40	49244	192.185.35.92	80	harveyouellet.com	GET /TOXICOUSTIQUE/arrowu.jpg HTTP/1.1
2015-02-08 18:31:26	172.16.137.40	49245	192.185.35.92	80	harveyouellet.com	GET /TOXICOUSTIQUE/arrowu.jpg HTTP/1.1
2015-02-08 18:31:26	172.16.137.40	49246	71.18.62.202	80	cwvancouver.com	GET /cp/images/digits/arrowu.jpg HTTP/1.1
2015-02-08 18:32:23	172.16.137.40	49251	2.16.162.43	80	www.download.windowsupdate.com	GET /msdownload/update/v3/static/trustedr/en/authroot

- IP address of Mike desktop computer

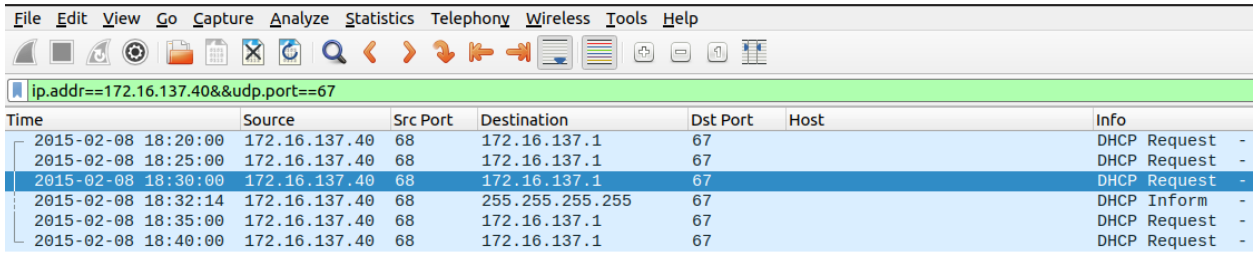
  172.16.137.40



Time	Source	Src Port	Destination	Dst Port	Host	Info
2015-02-08 18:29:47	172.16.137.40		224.0.0.22			Membership Report / Leave group 224.0.0.252
2015-02-08 18:30:00	172.16.137.40	68	172.16.137.1	67		DHCP Request - Transaction ID 0x7c742052
2015-02-08 18:30:00	172.16.137.1	67	255.255.255.255	68		DHCP ACK - Transaction ID 0x7c742052
2015-02-08 18:30:02	172.16.137.1		224.0.0.22			Membership Report / Leave group 224.0.0.252
2015-02-08 18:30:02	172.16.137.1		224.0.0.22			Membership Report / Leave group 224.0.0.252
2015-02-08 18:30:18	172.16.137.40	137	172.16.137.255	137		Name query NB MIKE-PC<1c>
2015-02-08 18:30:19	172.16.137.40	137	172.16.137.255	137		Name query NB MIKE-PC<1c>
2015-02-08 18:30:19	172.16.137.40	137	172.16.137.255	137		Name query NB MIKE-PC<1c>
2015-02-08 18:30:36	172.16.137.40	137	172.16.137.255	137		Name query NB MIKE-PC<1c>
2015-02-08 18:30:37	172.16.137.40	137	172.16.137.255	137		Name query NB MIKE-PC<1c>
2015-02-08 18:30:38	172.16.137.40	137	172.16.137.255	137		Name query NB MIKE-PC<1c>
2015-02-08 18:30:59	172.16.137.40		224.0.0.22			Membership Report / Join group 224.0.0.252 for
2015-02-08 18:30:59	172.16.137.40		224.0.0.22			Membership Report / Leave group 224.0.0.252

- Host name of Mike's desktop computer

  Mike-PC



Time	Source	Src Port	Destination	Dst Port	Host	Info
2015-02-08 18:20:00	172.16.137.40	68	172.16.137.1	67		DHCP Request -
2015-02-08 18:25:00	172.16.137.40	68	172.16.137.1	67		DHCP Request -
2015-02-08 18:30:00	172.16.137.40	68	172.16.137.1	67		DHCP Request -
2015-02-08 18:32:14	172.16.137.40	68	255.255.255.255	67		DHCP Inform -
2015-02-08 18:35:00	172.16.137.40	68	172.16.137.1	67		DHCP Request -
2015-02-08 18:40:00	172.16.137.40	68	172.16.137.1	67		DHCP Request -

```
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Dec_ef:ab:7c (08:00:2b:ef:ab:7c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Request)
  ▸ Option: (61) Client identifier
  ▾ Option: (12) Host Name
      Length: 7
      Host Name: Mike-PC
  ▸ Option: (81) Client Fully Qualified Domain Name
  ▸ Option: (60) Vendor class identifier
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
    Padding: 0000
```

- MAC address of Mike's desktop computer

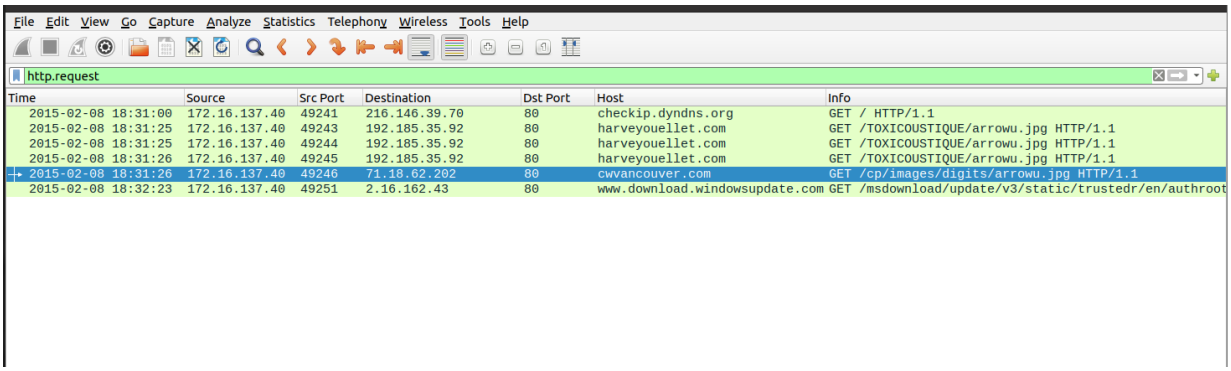
  08:00:26:ef:ab:7c

FIRST DECISION POINT

Based on your analysis of the traffic, you call Mike and tell him what you think has happened. Mike confirms your assessment, and he's somewhat embarrassed by his actions. The SOC follows established procedures to handle the incident, and you draft a report. Case closed! You're back on the hunt, reviewing more IDS events for the rest of your 12-hour shift. (Only 11 hours left!)

Looking at the HTTP requests I have got 4 URL's, however, two of them are suspicious

1) harveyouellet.com
2) cwvancouver.com

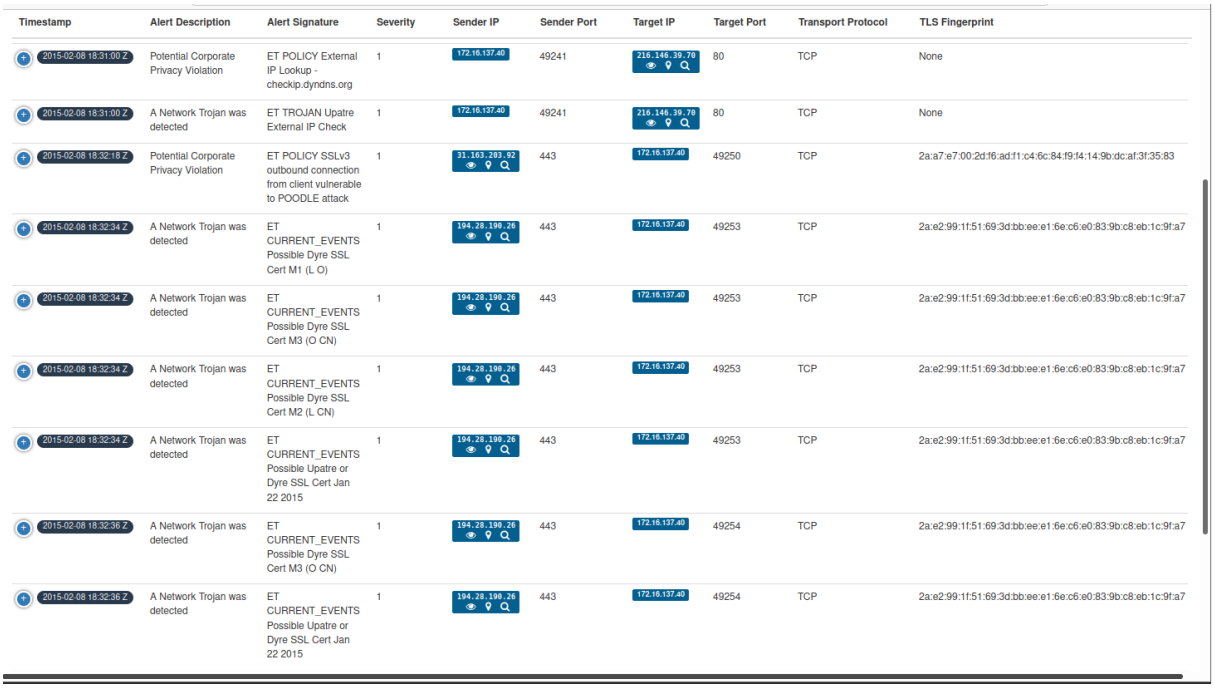


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

Time	Source	Src Port	Destination	Dst Port	Host	Info
2015-02-08 18:31:00	172.16.137.40	49241	216.146.39.70	80	checkip.dyndns.org	GET / HTTP/1.1
2015-02-08 18:31:25	172.16.137.40	49243	192.185.35.92	80	harveyouellet.com	GET /TOXICOUSTIQUE/arrowu.jpg HTTP/1.1
2015-02-08 18:31:25	172.16.137.40	49244	192.185.35.92	80	harveyouellet.com	GET /TOXICOUSTIQUE/arrowu.jpg HTTP/1.1
2015-02-08 18:31:26	172.16.137.40	49245	192.185.35.92	80	harveyouellet.com	GET /TOXICOUSTIQUE/arrowu.jpg HTTP/1.1
2015-02-08 18:31:26	172.16.137.40	49246	71.18.62.202	80	cwvancouver.com	GET /cp/images/digits/arrowu.jpg HTTP/1.1
2015-02-08 18:32:23	172.16.137.40	49251	2.16.162.43	80	www.download.windowsupdate.com	GET /msdownload/update/v3/static/trustedr/en/authroot

A quick google search gave me a trend micro blog with similar domain names. Uploaded the pcap file to packet total to check for any additional IOC's and found the following:



Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	TLS Fingerprint
2015-02-08 18:31:00 Z	Potential Corporate Privacy Violation	ET POLICY External IP Lookup - checkip.dyndns.org	1	172.16.137.40	49241	216.146.39.70	80	TCP	None
2015-02-08 18:31:00 Z	A Network Trojan was detected	ET TROJAN Upatre External IP Check	1	172.16.137.40	49241	216.146.39.70	80	TCP	None
2015-02-08 18:32:18 Z	Potential Corporate Privacy Violation	ET POLICY SSLv3 outbound connection from client vulnerable to POODLE attack	1	31.163.283.92	443	172.16.137.40	49250	TCP	2a:a7:e7:00:2d:f6:ad:f1:c4:6c:84:f9:f4:14:9b:dc:af:3f:35:83
2015-02-08 18:32:34 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Dyre SSL Cert M1 (L O)	1	194.28.190.26	443	172.16.137.40	49253	TCP	2a:e2:99:1f:51:69:3d:bb:ee:e1:6e:c6:e0:83:9b:c8:eb:1c:9f:a7
2015-02-08 18:32:34 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Dyre SSL Cert M3 (O CN)	1	194.28.190.26	443	172.16.137.40	49253	TCP	2a:e2:99:1f:51:69:3d:bb:ee:e1:6e:c6:e0:83:9b:c8:eb:1c:9f:a7
2015-02-08 18:32:34 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Dyre SSL Cert M2 (L CN)	1	194.28.190.26	443	172.16.137.40	49253	TCP	2a:e2:99:1f:51:69:3d:bb:ee:e1:6e:c6:e0:83:9b:c8:eb:1c:9f:a7
2015-02-08 18:32:34 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Upatre or Dyre SSL Cert Jan 22 2015	1	194.28.190.26	443	172.16.137.40	49253	TCP	2a:e2:99:1f:51:69:3d:bb:ee:e1:6e:c6:e0:83:9b:c8:eb:1c:9f:a7
2015-02-08 18:32:36 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Dyre SSL Cert M3 (O CN)	1	194.28.190.26	443	172.16.137.40	49254	TCP	2a:e2:99:1f:51:69:3d:bb:ee:e1:6e:c6:e0:83:9b:c8:eb:1c:9f:a7
2015-02-08 18:32:36 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Upatre or Dyre SSL Cert Jan 22 2015	1	194.28.190.26	443	172.16.137.40	49254	TCP	2a:e2:99:1f:51:69:3d:bb:ee:e1:6e:c6:e0:83:9b:c8:eb:1c:9f:a7

Packet total says a network trojan detected with Dyre SSL cert. A quick search on Dyre SSL cert gave about Dyreza a banking malware which is downloaded to the End point by Upatre downloader trojan.

Summary:

Mike's computer is infected with Dyre or Dyreza Banking malware. This was distributed by Upatre trojan via email with an attachment. Mike opened the attachment and infected his computer.