Incident Response Report

- What activity is snort reporting on? (Provide a few alert headlines)

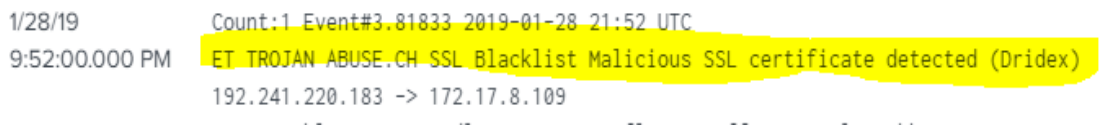
Malware download

- "ET Policy HTTP Request on Unusual Port Possibly Hostile"

- "ET POLICY HTTP Binary Download Smaller than 1MB Likely Hostile"

- This is where and when malware was downloaded.

- "ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL Certificate detected (Dridex)"



- What is the date and time of this alert?

2019-01-28 21:49 UTC

- What is the external IP address that snort is flagging for malicious activity?

91.121.30.169

- What is the internal IP address that snort is flagging for malicious activity?

172.17.8.109

- What is the source port of the activity?

Port 8000

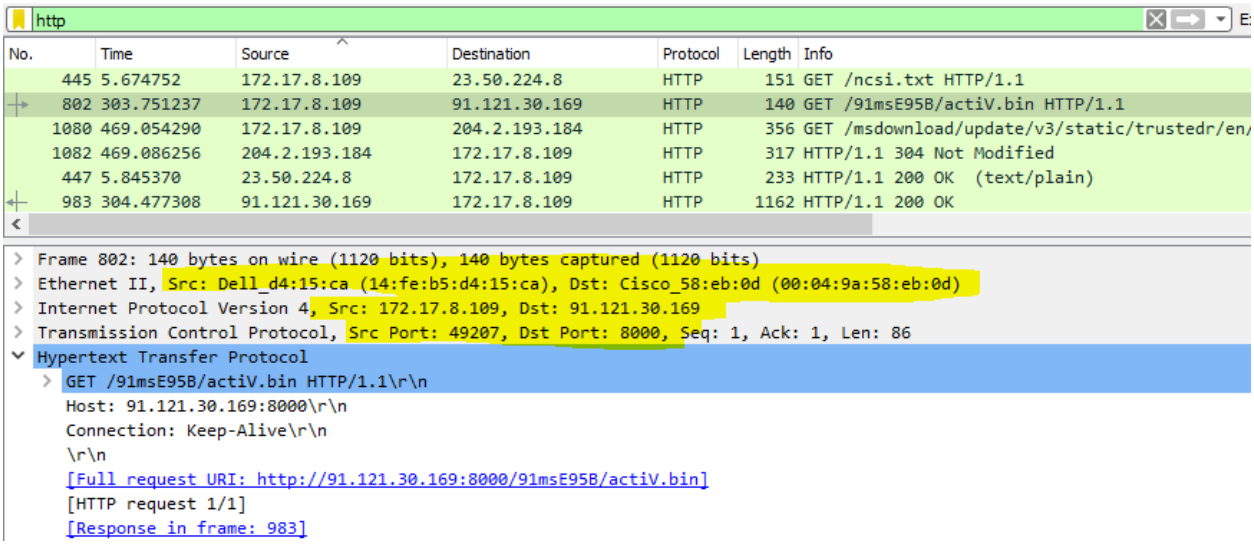
- What is the destination port of the activity?

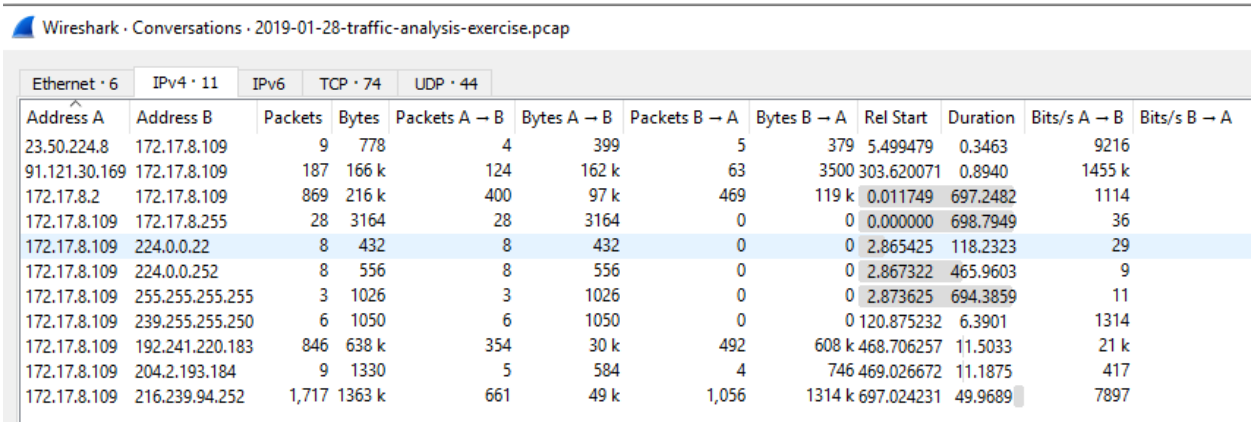
Port 49207

- What are the MAC Addresses of the computers involved?

Internal: Dell_d4:15:ca (14:fe:b5:d4:15:ca)

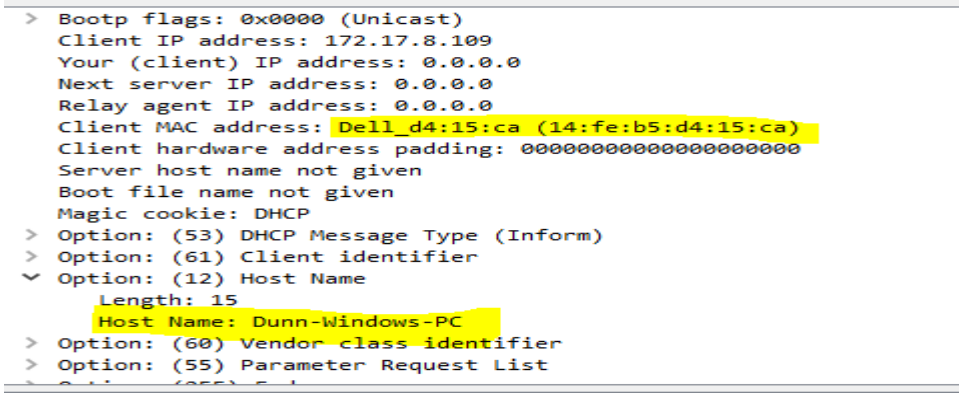
External: Cisco_58:eb:0d (00:04:9a:58:eb:0d)





- What is the host name of the internal machine?

Dunn-Windows-PC



- Can you confirm the date and time this issue occurred?

January 28, 2019 16:49:17 EST (from the SNORT file)

January 28, 2019 21:49 UTC (from the Splunk analysis of the log file)

```
Frame 802: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 28, 2019 16:49:17.801380000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1548712157.801380000 seconds
```

```
1/28/19 9:49:00.000 PM  Count:1 Event#3.81737 2019-01-28 21:49 UTC
ET POLICY HTTP Request on Unusual Port Possibly Hostile
172.17.8.109 -> 91.121.30.169
IPVer=4 hlen=5 tos=0 dlen=40 ID=462 flags=2 offset=0 ttl=128 chksum=27095
Protocol: 6 sport=49207 -> dport=8000
```

- How can you confirm if the snort alert is accurate?

By following the TCP stream and see the binary download starting with 'MZ' and '!This program cannot be run in DOS mode.' The GET request ends in `/actiV.bin`.

```
Hypertext Transfer Protocol
  GET /91msE95B/actiV.bin HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /91msE95B/actiV.bin HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /91msE95B/actiV.bin
    Request Version: HTTP/1.1
  Host: 91.121.30.169:8000\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://91.121.30.169:8000/91msE95B/actiV.bin]
  [HTTP request 1/1]
  [Response in frame: 983]
```

```
MZ.....@.....  .!..L.!This program cannot be run
in DOS mode.

$.......PE..L...,AN\.....p.....p/.....`.....S...@....
.....T.....@.....P.....
8.....T.....text....c.....p.....
..... ..`.data.....0.....@....idata...
.....@..@CODE.....q.....@....rsrc.....@.....@.....@
..@.reloc.....P.....P.....@..B.....
```

- Can you safely verify whether or not malware was downloaded?

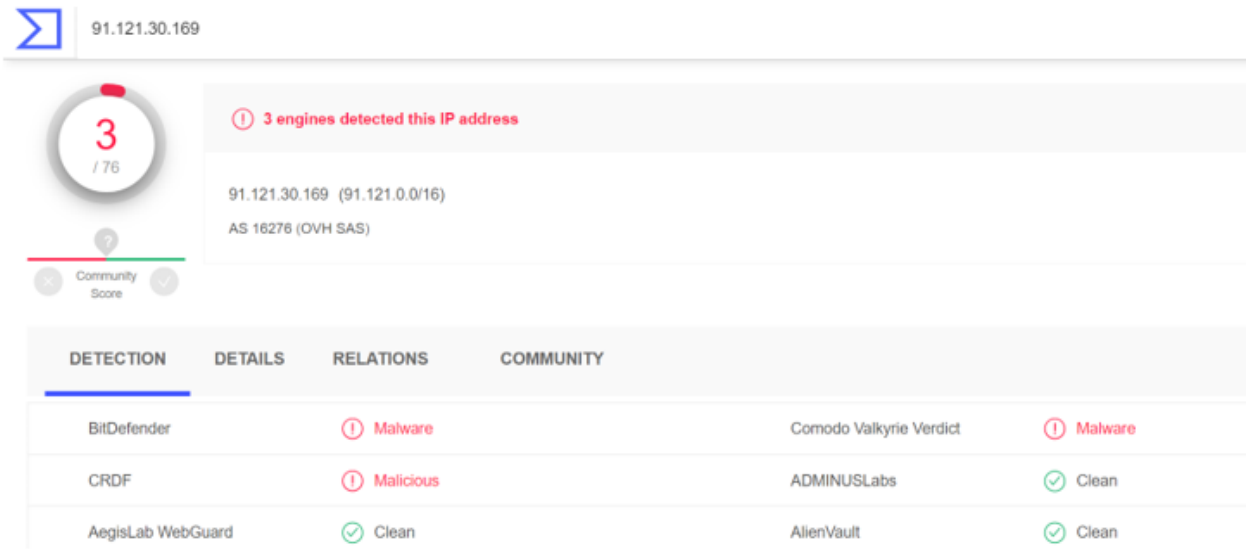
The screenshot below shows that that download was 100% complete

Wireshark · Requests · 2019-01-28-traffic-analysis-exercise.pcap

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
HTTP Requests by HTTP Host	9				0.0000	100%	0.0100	5.675
www.msftncsi.com	1				0.0000	11.11%	0.0100	5.675
/ncsi.txt	1				0.0000	100.00%	0.0100	5.675
www.download.windowsupdate.com	1				0.0000	11.11%	0.0100	469.054
/msdownload/update/v3/static/trustedr/en/authrootstl.cab	1				0.0000	100.00%	0.0100	469.054
91.121.30.169:8000	1				0.0000	11.11%	0.0100	303.751
/91msE95B/actiV.bin	1				0.0000	100.00%	0.0100	303.751
239.255.255.250:1900	6				0.0000	66.67%	0.0100	120.875
*	6				0.0000	100.00%	0.0100	120.875

- Would you categorize this alert as a `False Positive` or a `True Positive`?

This is a True Positive as we can see that 3 engines have flagged this as Malware.

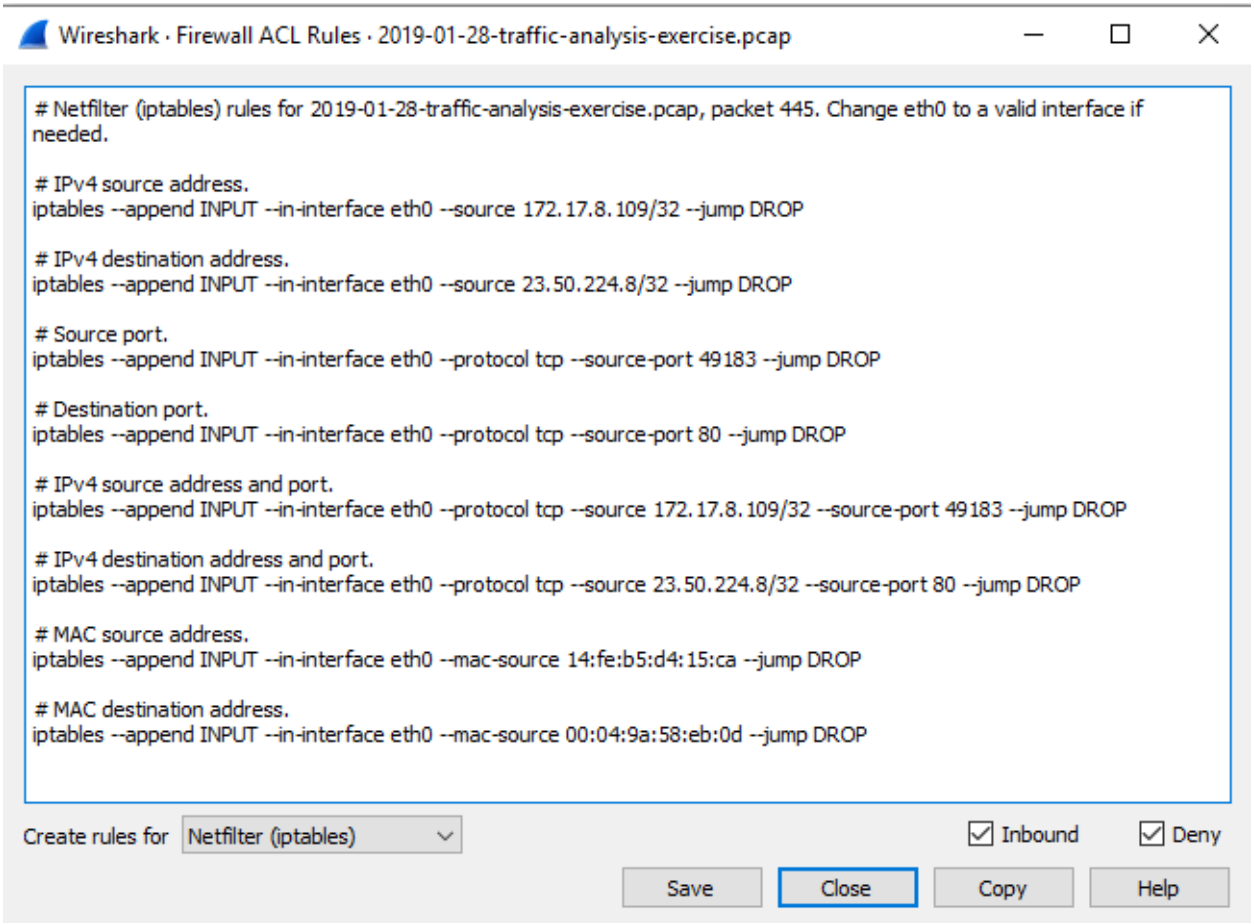


- If this issue needs to be mitigated, what steps should be taken with the infected machine?

The hard drive on the infected computer can be wiped and re-imaged with an OS and software that has not been compromised by this attack. Another alternative would be to restore the computer to a known working configuration prior to the attack occurring (if a backup was done and is available).

- What steps should be taken in regards to network security?

Using ACL Rules from the Wireshark Tools, the rule for the offending IP can be modified.



- Would you categorize this issue as a Web, Email or Network attack?

This would be classified as a Web attack.