

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"

```
1/28/19          Count:1 Event#3.81737 2019-01-28 21:49 UTC
9:49:00.000 PM  ET POLICY HTTP Request on Unusual Port Possibly Hostile
                  172.17.8.109 -> 91.121.30.169
```

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

```
1/28/19          Count:1 Event#3.81738 2019-01-28 21:49 UTC
9:49:00.000 PM  ET POLICY Binary Download Smaller than 1 MB Likely Hostile
                  91.121.30.169 -> 172.17.8.109
```

- This is where and when malware was downloaded.

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

```
1/28/19          Count:1 Event#3.81833 2019-01-28 21:52 UTC
9:52:00.000 PM  ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
                  192.241.220.183 -> 172.17.8.109
```

- 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)

http

No.	Time	Source	Destination	Protocol	Length	Info
445	5.674752	172.17.8.109	23.50.224.8	HTTP	151	GET /ncsi.txt HTTP/1.1
802	303.751237	172.17.8.109	91.121.30.169	HTTP	140	GET /91msE95B/activ.bin HTTP/1.1
1080	469.054290	172.17.8.109	204.2.193.184	HTTP	356	GET /msdownload/update/v3/static/trustedr/en/
1082	469.086256	204.2.193.184	172.17.8.109	HTTP	317	HTTP/1.1 304 Not Modified
447	5.845370	23.50.224.8	172.17.8.109	HTTP	233	HTTP/1.1 200 OK (text/plain)
983	304.477308	91.121.30.169	172.17.8.109	HTTP	1162	HTTP/1.1 200 OK

> Frame 802: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits)
> Ethernet II, Src: Dell_d4:15:ca (14:fe:b5:d4:15:ca), Dst: Cisco_58:eb:0d (00:04:9a:58:eb:0d)
> Internet Protocol Version 4, Src: 172.17.8.109, Dst: 91.121.30.169
> Transmission Control Protocol, Src Port: 49207, Dst Port: 8000, Seq: 1, Ack: 1, Len: 86
▼ Hypertext Transfer Protocol
 > GET /91msE95B/activ.bin HTTP/1.1\r\n
 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]

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

Ethernet · 6		IPv4 · 11		IPv6	TCP · 74		UDP · 44					
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
23.50.224.8	172.17.8.109	9	778	4	399	5	379	5.499479	0.3463	9216		
91.121.30.169	172.17.8.109	187	166 k	124	162 k	63	3500	303.620071	0.8940	1455 k		
172.17.8.2	172.17.8.109	869	216 k	400	97 k	469	119 k	0.011749	697.2482	1114		
172.17.8.109	172.17.8.255	28	3164	28	3164	0	0	0.000000	698.7949	36		
172.17.8.109	224.0.0.22	8	432	8	432	0	0	2.865425	118.2323	29		
172.17.8.109	224.0.0.252	8	556	8	556	0	0	2.867322	465.9603	9		
172.17.8.109	255.255.255.255	3	1026	3	1026	0	0	2.873625	694.3859	11		
172.17.8.109	239.255.255.250	6	1050	6	1050	0	0	120.875232	6.3901	1314		
172.17.8.109	192.241.220.183	846	638 k	354	30 k	492	608 k	468.706257	11.5033	21 k		
172.17.8.109	204.2.193.184	9	1330	5	584	4	746	469.026672	11.1875	417		
172.17.8.109	216.239.94.252	1,717	1363 k	661	49 k	1,056	1314 k	697.024231	49.9689	7897		

- What is the host name of the internal machine?

Dunn-Windows-PC

> Bootp flags: 0x0000 (Unicast)
Client IP address: 172.17.8.109
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_d4:15:ca (14:fe:b5:d4:15:ca)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Inform)
> Option: (61) Client identifier
▼ Option: (12) Host Name
 Length: 15
 Host Name: Dunn-Windows-PC
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List

- 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	Count:1 Event#3.81737 2019-01-28 21:49 UTC
9:49:00.000 PM	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.....
B.....T.....text....c.....p.....
...data.....@.....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.

91.121.30.169

3
/ 76

3 engines detected this IP address

91.121.30.169 (91.121.0.0/16)
AS 16276 (OVH SAS)

Community Score

DETECTION

DETAILS

RELATIONS

COMMUNITY

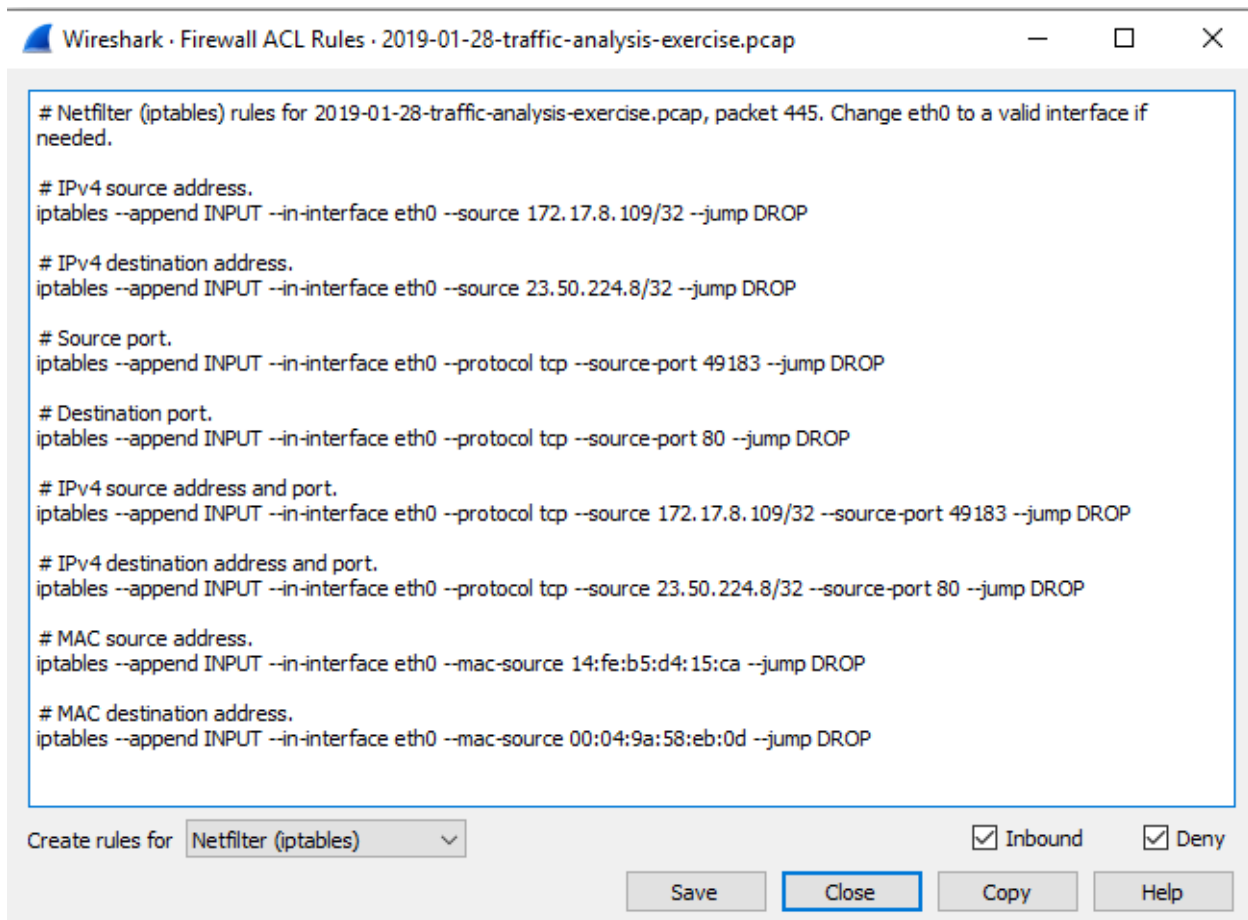
BitDefender	Malware	Comodo Valkyrie Verdict	Malware
CRDF	Malicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AlienVault	Clean

- 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.