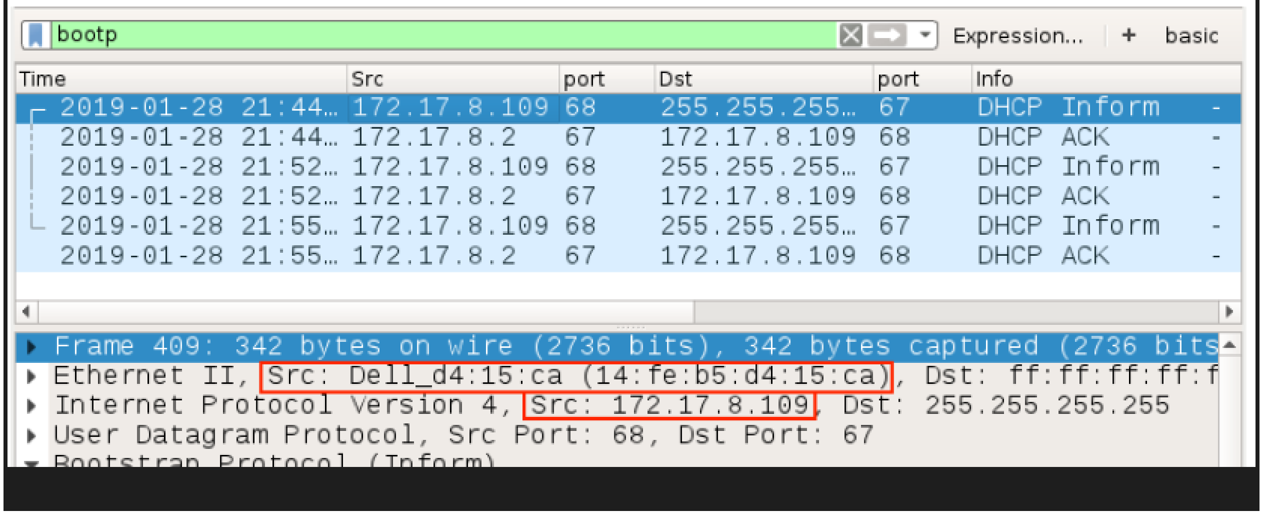
Timbershade Post-Incident Report

What activity is snort reporting on?	DHCP/NBNS traffic
What is the date and time of this alert?	January 28th, 2019 on 9:44 PM
What is the external IP address that snort is flagging for malicious activity?	255.255.255.255
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?	68
What is the destination port of the activity?	67
What are the MAC Addresses of the computers involved?	14:fe:b5:d4:15:ca (Dell_d4:15:ca
What is the host name of the internal machine?	Dunn-Windows-PC
Can you confirm the date and time this issue occurred?	Yes
How can you confirm if the snort alert is accurate?	By running a TCP.
Can you safely verify whether or not malware was downloaded?	Yes

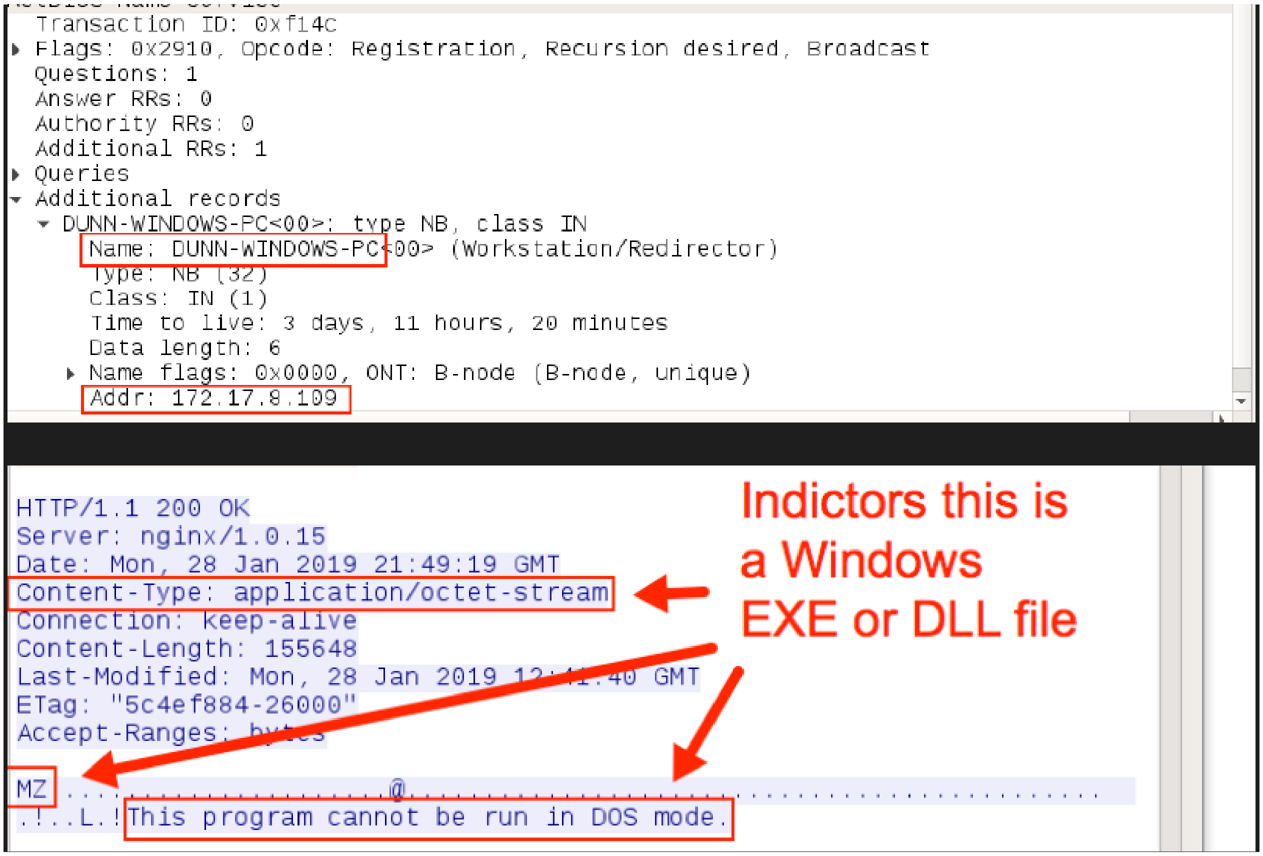
Would you categorize this alert as a False Positive or a True Positive?	False Positive
If this issue needs to be mitigated, what steps should be taken with the infected machine?	Filtering packets
What steps should be taken in regard to network security?	Default steps to network traffic blocking
Would you categorize this issue as a Web, Email or Network attack?	Network attack

Narrative



```
Time                    Src           port  Dst              port  Info
2019-01-28 21:44…   172.17.8.109  68    255.255.255…     67    DHCP Inform  -
2019-01-28 21:44…   172.17.8.2    67    172.17.8.109     68    DHCP ACK     -
2019-01-28 21:52…   172.17.8.109  68    255.255.255…     67    DHCP Inform  -
2019-01-28 21:52…   172.17.8.2    67    172.17.8.109     68    DHCP ACK     -
2019-01-28 21:55…   172.17.8.109  68    255.255.255…     67    DHCP Inform  -
2019-01-28 21:55…   172.17.8.2    67    172.17.8.109     68    DHCP ACK     -
```

```
▸ Frame 409: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits
▸ Ethernet II, Src: Dell_d4:15:ca (14:fe:b5:d4:15:ca), Dst: ff:ff:ff:ff:f
▸ Internet Protocol Version 4, Src: 172.17.8.109, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Bootstrap Protocol (Inform)
```



```
  Transaction ID: 0xf14c
▸ Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
▸ Queries
▾ Additional records
  ▾ DUNN-WINDOWS-PC<00>: type NB, class IN
      Name: DUNN-WINDOWS-PC<00> (Workstation/Redirector)
      Type: NB (32)
      Class: IN (1)
      Time to live: 3 days, 11 hours, 20 minutes
      Data length: 6
    ▸ Name flags: 0x0000, ONT: B-node (B-node, unique)
      Addr: 172.17.8.109
```

```
HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Mon, 28 Jan 2019 21:49:19 GMT
Content-Type: application/octet-stream
Connection: keep-alive
Content-Length: 155648
Last-Modified: Mon, 28 Jan 2019 12:41:40 GMT
ETag: "5c4ef884-26000"
Accept-Ranges: bytes

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

Indictors this is a Windows EXE or DLL file