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

Et Policy Pe EXE or DLL Windows file download HTTP

ET Policy Binary download smaller than 1 MB likely Hostile

ET INFO Exeuctable Retrieved with Minimal HTTP Headers - Potential Second Stage download

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?  
8000

What is the destination port of the activity?  
49207

What are the MAC Addresses of the computers involved?  
(14:fe:b5:d4:15:ca

What is the host name of the internal machine?  
DUNN-WINDOWS-PC<00>

Can you confirm the date and time this issue occurred?

How can you confirm if the snort alert is accurate?

Can you safely verify whether or not malware was downloaded?  
search the offending IP address at Virus Total.

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

If this issue needs to be mitigated, what steps should be taken with the infected machine?  
The machine should be restored to a backup prior to this infection.

What steps should be taken in regards to network security?  
iptables --append INPUT --in-interface eth0 --source 91.121.30.169 --jump DROP

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

Email attack