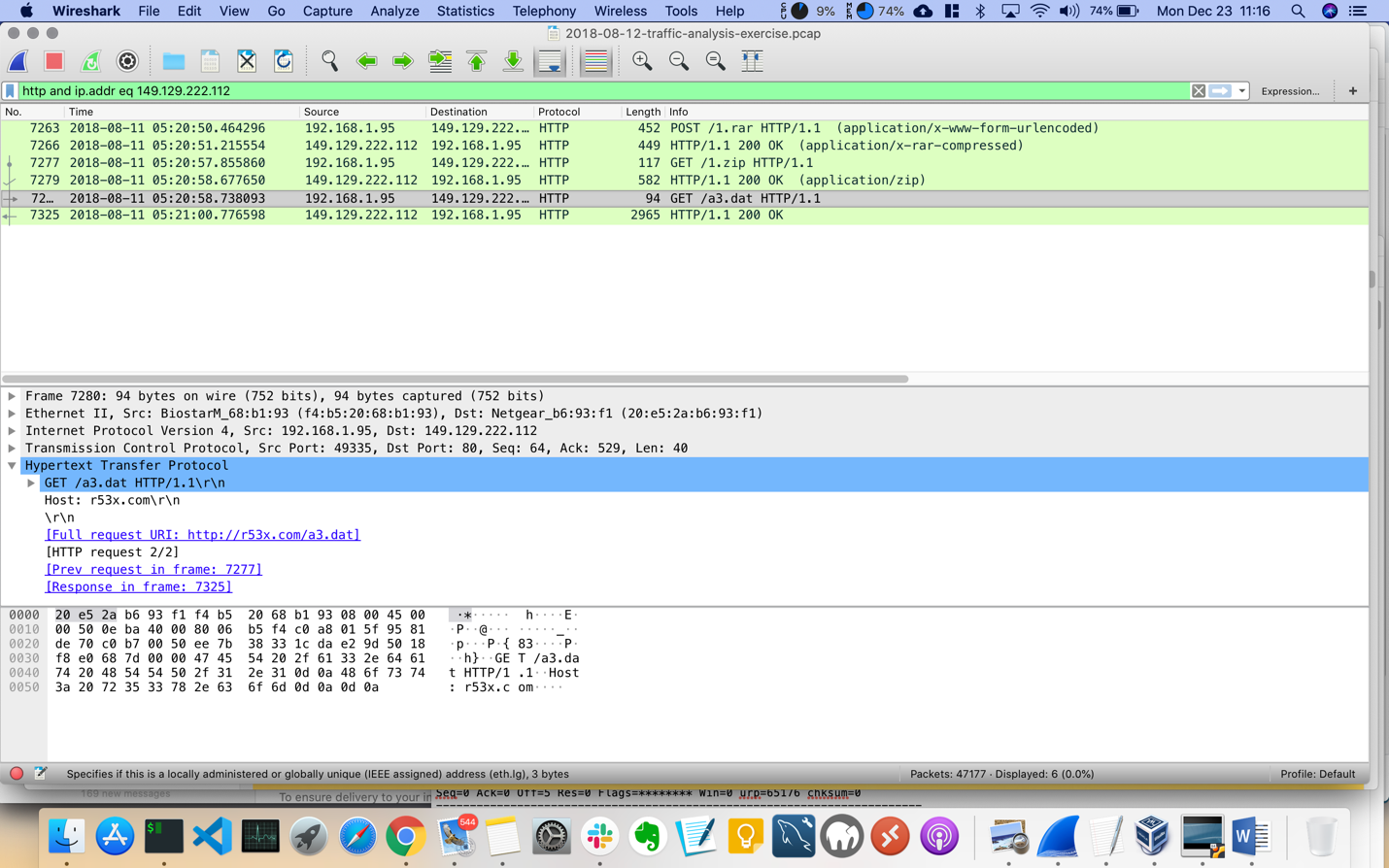
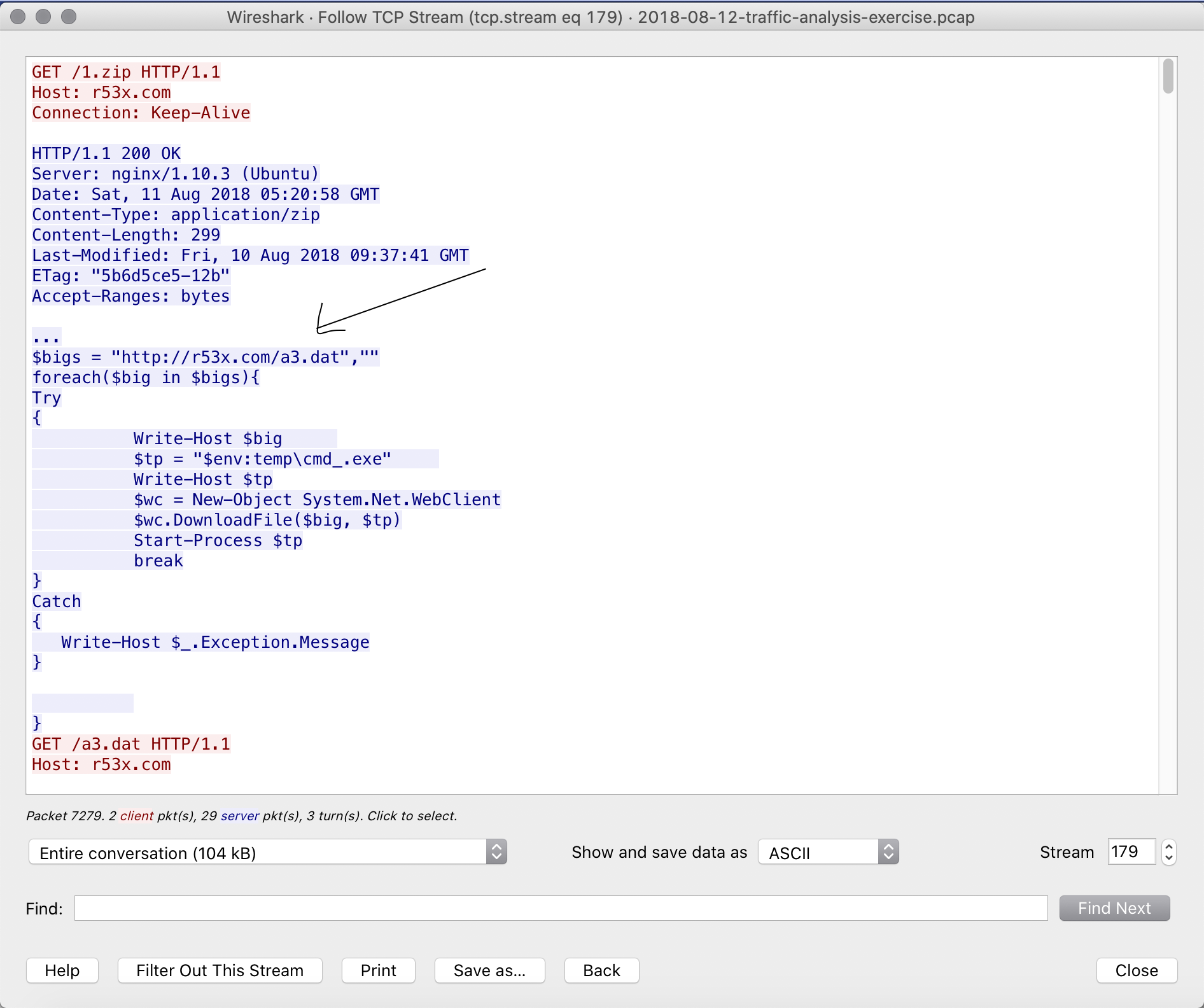
|  |  |
| --- | --- |
| **Post Incident Report** | |
|  |  |
| **Date of investigation** | 12/22/2019 |
| **Date of incident** | 2018-08-11 at 5:21 UTC |
| **Outcome** |  |
| **Action Taken** | Identified Malware and infected host. Advise Firewall Rules to Block Traffic from Source. Advise reformatting infected computer or restoring to a backup prior to time of incident. |
| **Reporting tool** | Snort and Suratica Alerts |
| **Attack vector (Web, Email, Network, etc.)** | Web Malware Download |
| **Source IP/email** | 185.68.93.18 |
| **Source port** | 80 |
| **Destination IP/email** | 149.129.222.112 |
| **Destination port** | 80 |
|  |  |
|  |  |
| **Narrative** | |
| ● Alerted by Snort and Suricata: |  |
| [\*\*] [1:15306:22] FILE-EXECUTABLE Portable Executable binary file magic detected [\*\*]  [Classification: Potential Corporate Privacy Violation] [Priority: 1]  08/11-05:21:00 UTC - 149.129.222.112:80 -> 192.168.1.95:49335  TCP TTL:128 TOS:0x0 ID:3487 IpLen:20 DgmLen:1488  \*\*\*AP\*\*\* Seq: 0xEE7B3833 Ack: 0x1CDAE29D Win: 0xFAF0 TcpLen: 20  ● Located Source/Destination IP Addresses and timestamp from Alerts: | |
| 08/11-05:20:50 UTC - 192.168.1.95:49334 -> 149.129.222.112:80 |  |
|  |  |

**Post-Incident Report**

● Identified download link of Pushdo in pcap HTTP traffic:

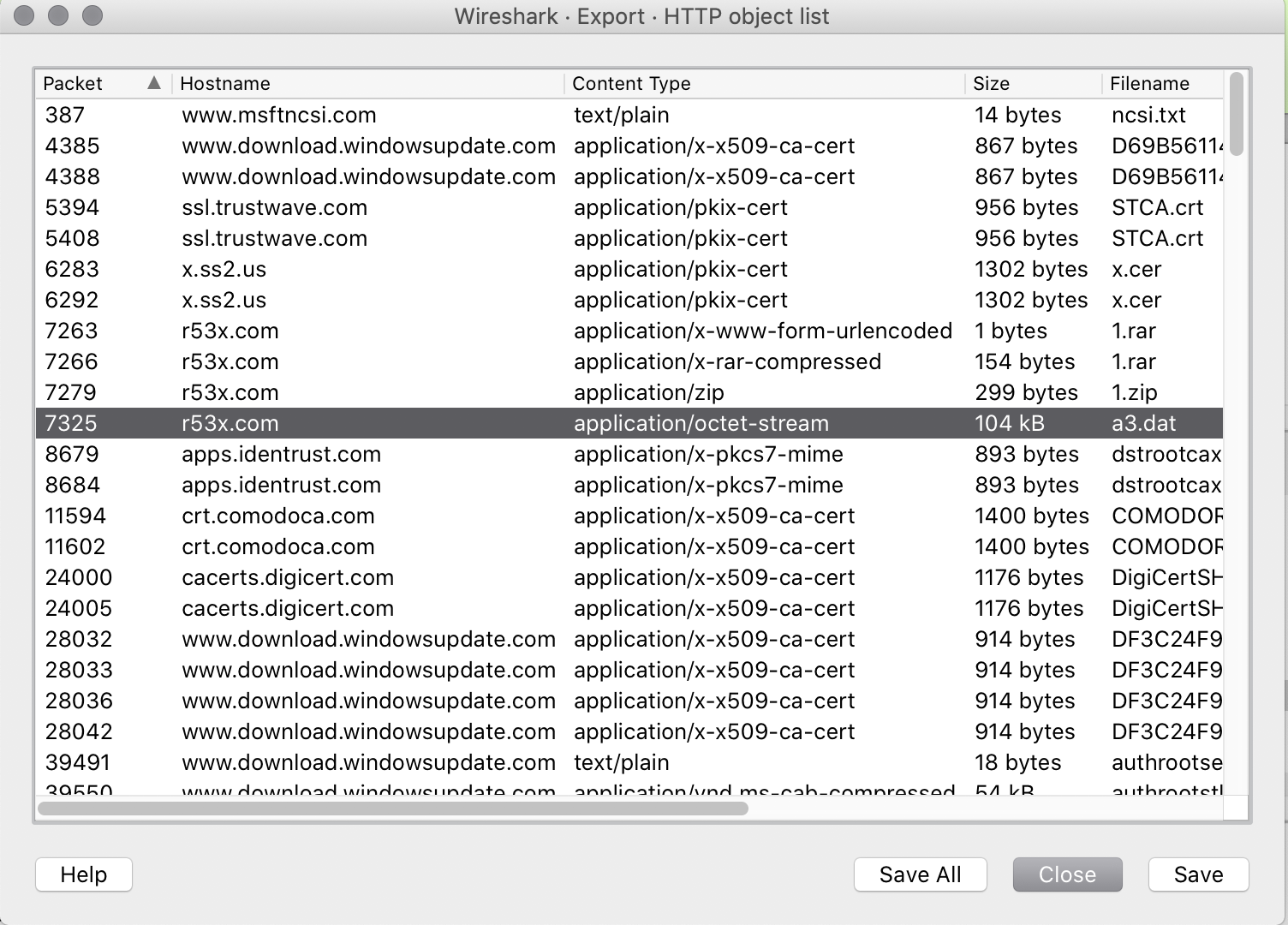


● Followed the TCP Stream and found binary downloaded:

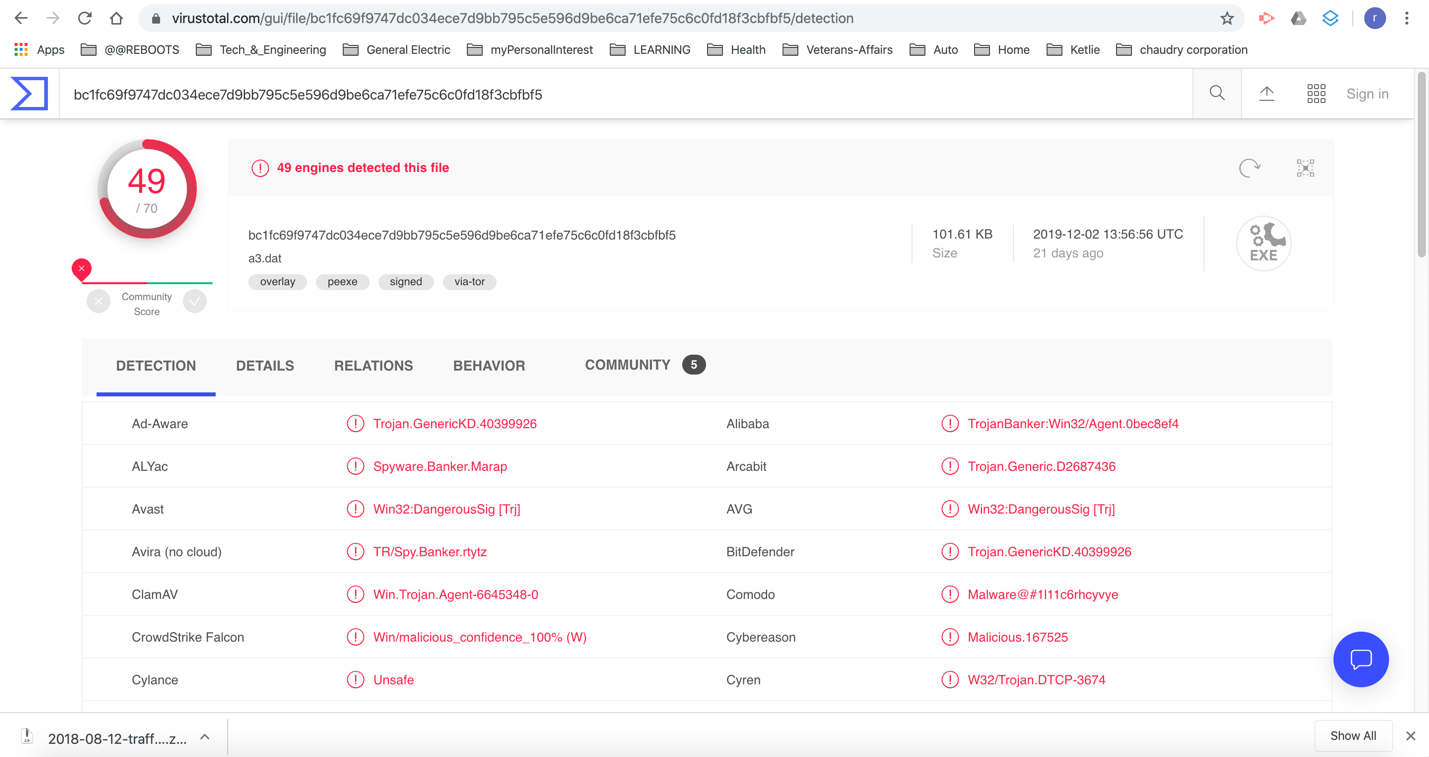


● Exported HTTP objects and found more malware downloaded:

◌ a3.dat



● Uploaded MD5 hashes to virus total for confirmation:



● 5473299167525c8d0addb8248900606a a3.dat

◌ Used Wireshark to identify possible iptables rules to block traffic from source:

# Netfilter (iptables) rules for 2018-08-12-traffic-analysis-exercise.pcap, packet 7325. Change eth0 to a valid interface if needed.

# IPv4 source address.

iptables --append INPUT --in-interface eth0 --source 149.129.222.112/32 --jump DROP

# IPv4 destination address.

iptables --append INPUT --in-interface eth0 --source 192.168.1.95/32 --jump DROP

# Source port.

iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 80 --jump DROP

# Destination port.

iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 49335 --jump DROP

# IPv4 source address and port.

iptables --append INPUT --in-interface eth0 --protocol tcp --source 149.129.222.112/32 --source-port 80 --jump DROP

# IPv4 destination address and port.

iptables --append INPUT --in-interface eth0 --protocol tcp --source 192.168.1.95/32 --source-port 49335 --jump DROP

# MAC source address.

iptables --append INPUT --in-interface eth0 --mac-source 20:e5:2a:b6:93:f1 --jump DROP

# MAC destination address.

iptables --append INPUT --in-interface eth0 --mac-source f4:b5:20:68:b1:93 --jump DROP

|  |
| --- |
| 1. What activity is snort reporting on? (Provide a few alert headlines) |
| This was a Malware attack via email |
| 1. What is the date and time of this alert? |
| 8/11/2018 at ~ 5:21 UTC |
| 1. What is the external IP address that snort is flagging for malicious activity? |
| 185.68.93.18 |
| 1. What is the internal IP address that snort is flagging for malicious activity? |
| 149.129.222.112 |
| 1. What is the source port of the activity? |
| Source port was 80 |
| 1. What is the destination port of the activity? |
| 80 |
| 1. What are the MAC Addresses of the computers involved? |
| MAC address of the infected machine is f4:b5:20:68:b1:93 |
| 1. What is the host name of the internal machine? |
| Hostname of the infected machine is Petrov2018-PC |
| 1. Can you confirm the date and time this issue occurred? |
| Yes. 8/11/2018 at ~ 5:21 UTC |
| 1. How can you confirm if the snort alert is accurate? |
|  |
| 1. Can you safely verify whether or not malware was downloaded? |
| Yes. A file named a3.dat has been identified as a threat |
|  |
| 1. Would you categorize this alert as a False Positive or a True Positive? |
| True Positive |
| 1. If this issue needs to be mitigated, what steps should be taken with the infected machine? |
| * Isolated the infected host from the network * Educate the users to not click on links sent from unknown and suspicious sources. * Sanitize the infected machine and ensure it has the the most up to date antivirus application. |
| 1. What steps should be taken in regards to network security?   Firewall rules should be implemented to prevent harmful malware from being downloaded |
|  |
| 1. Would you categorize this issue as a Web, Email or Network attack?   This is a web malware attack delivered via email |