**Post-Incident Report**

|  |  |
| --- | --- |
| Date of investigation | Nov 26, 2019 |
| Date of incident | 08/11-05:20:50 UTC |
| Outcome | True Positive - trojan downloader & malware files |
| Action Taken | Identified Malware and infected host.  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 | 149.129.222.112 / mikhail.petrov@sputnikhouse.org |
| Source port | 80 |
| Destination IP/email | 192.168.1.95 |
| Destination port | 49335 |

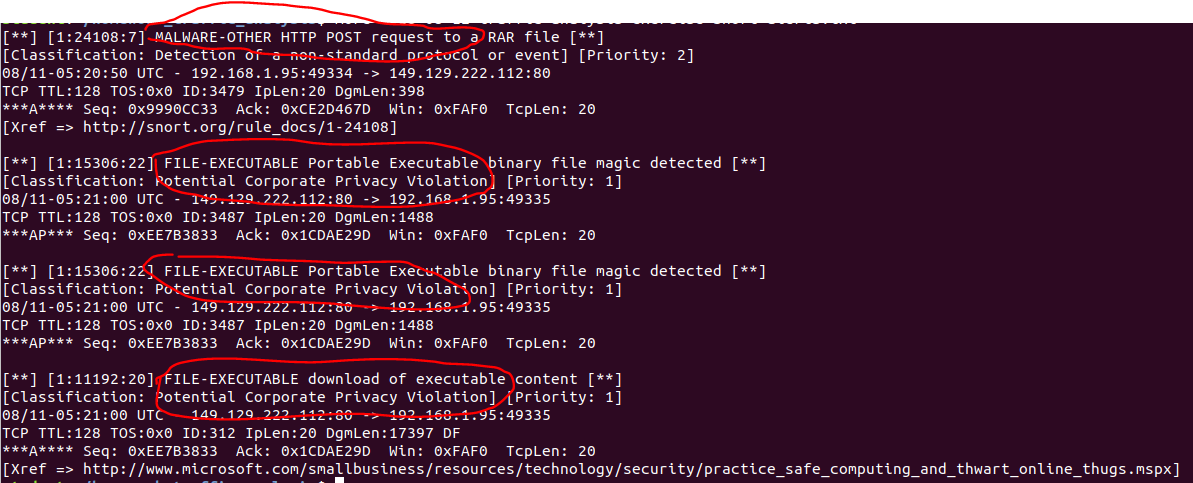
**Narrative**

• Alerted by Snort and Suricata:

◦ “MALWARE-OTHER HTTP POST request to a RAR file”

◦ “FILE-EXECUTABLE Portable Executable binary file magic detected”

◦ “FILE-EXECUTABLE download of executable content”



• Located Source/Destination IP Addresses and timestamp from Alerts:

◦ Src/Prt: 149.129.222.112:80

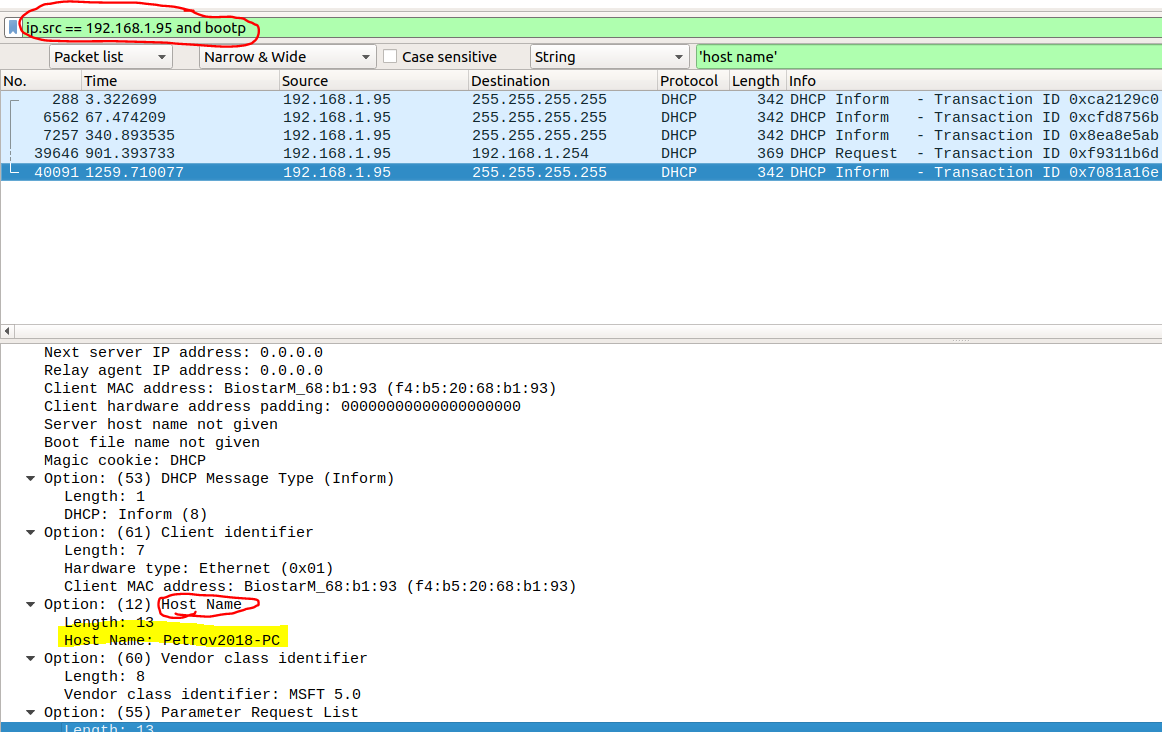
◦ Dst/Prt: 192.168.1.95:49335

◦ Time Stamp: 08/11-05:21:00 UTC

Identified Hostname and MacAddress of Potential Corporate Privacy Violation PC:

◦ MAC: f4:b5:20:68:b1:93

◦ Host Name: Petrov2018-PC

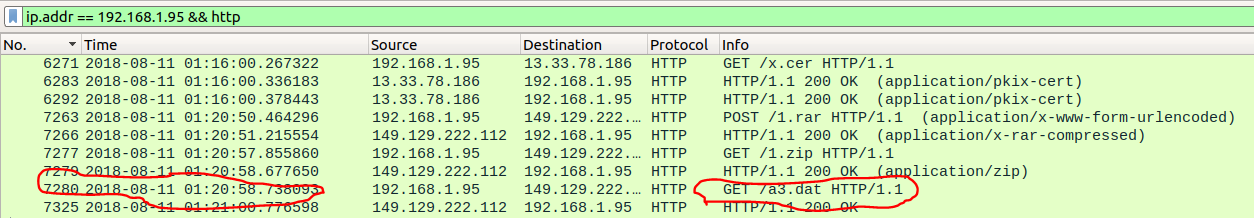


# 

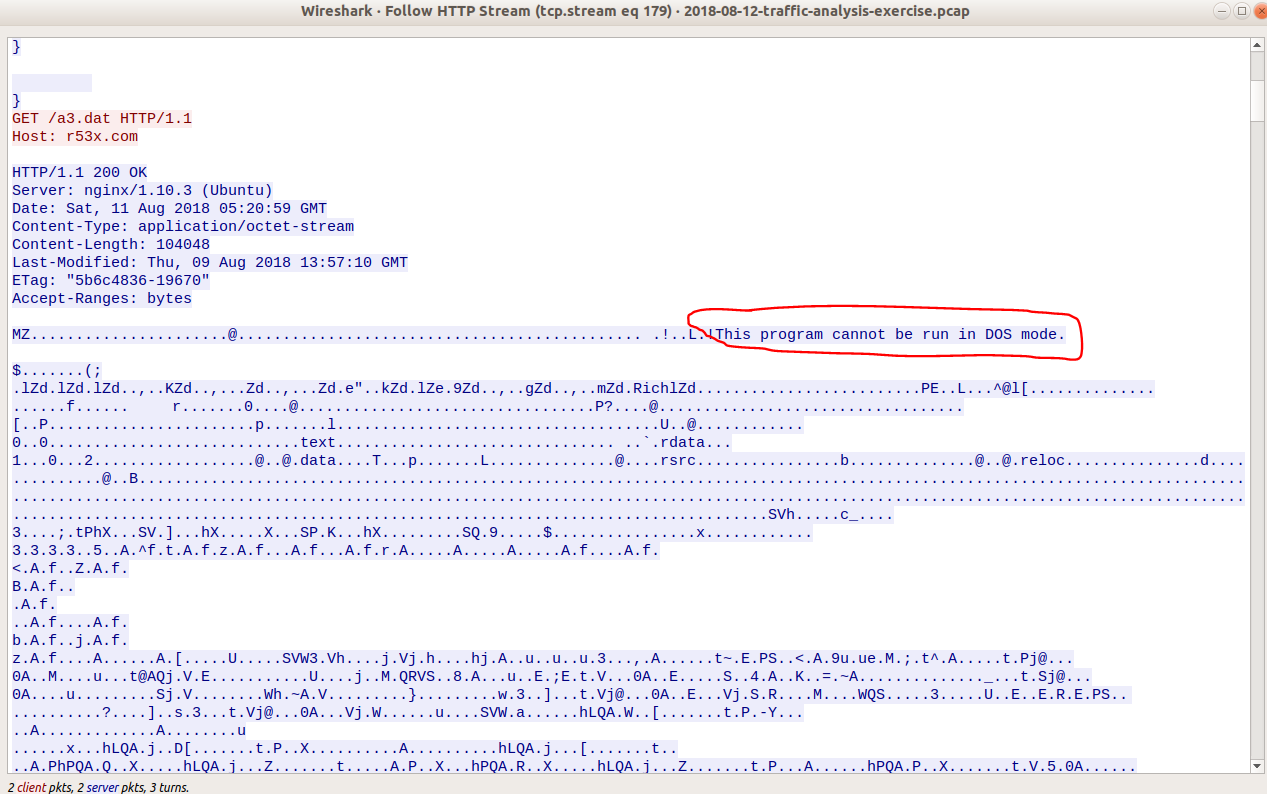
**Post-Incident Report**

**Re**: “MALWARE-OTHER HTTP POST request to a RAR file”

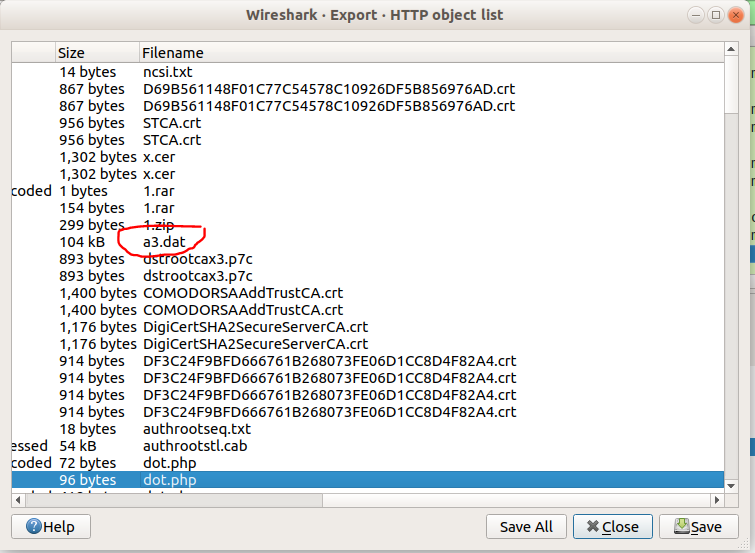
* Located pcap log entry as referenced in Snort Alert using timestamp and alert message info



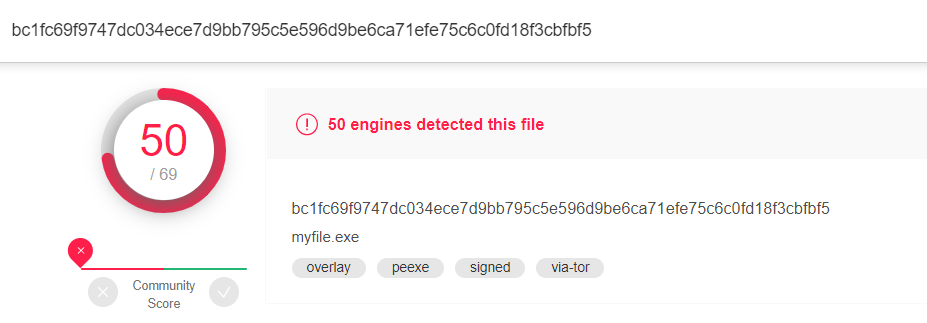
* Found unusual binary code in packet (executable)



* Downloaded file for inspection



* Using md5sum to hash the a3.dat file and VirusTotal.com there is a high probability this is a Malware file



**Conclusion**: TRUE positive, files in emails were identified as Malware

**Re**: “Potential Corporate Privacy Violation”

• Identified files in email

◦ AWB RECEIPTS\_PDF.rar

◦ PIC35793.iqy

◦ PO.doc

◦ 1.rar

• examined files using VirusTotal.exe

◦ PO.doc - 40 engines detected this file

◦ PIC35793.iqy - 33 engines detected this file

◦ AWB RECEIPTS\_PDF.rar - 27 engines detected this file

◦ 1.rar -m- 17 engines detected this file

**Conclusion**: TRUE positive, files in emails were identified as Malware