**Post-Incident Report**

Date of investigation 11/06/2019

Date of incident 2018-08-11 05:21 UTC

Outcome True Positive - **Trojan**:**Win32**/**Vigorf.A**

Action Taken Identified Ransomware and infected host.

Update Anitvirus to prevent the download of this ransomware(Microsoft’s built in one works fine for this specific one) Recommened: Use this guide to remove it <https://howtoremove.guide/vigorf-a-trojan-virus-win-removal/>

Reporting tool Snort

Attack vector (Web, Email, Network, etc.) Web Ransomware Download

Source IP | 149.129.222.112

Source port 80

Destination IP 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”

“ETPRO TROJAN Common Downloader Header Pattern H”

**Post-Incident Report**•

Identified Hostname and MacAddress of infected computer in pacp:

◦ MAC: 20:e5:2a:b6:93:f1

Host Name: Petrov2018-PC

**Post-Incident Report.**

• Identified download link in pcap HTTP traffic:

◦ http://r53x.com/1.rar

• Followed the TCP Stream and found binary downloaded:

◦ Date: Sat, 11 Aug 2018 05:20:59 GMT