**Post-Incident Report**

Date of investigation 11/06/2019

Date of incident 2018-11-07 at 20:47 UTC

Outcome True Positive - Ursnif MalwareVariant Found

Action Taken Identified Malware and infected host.

Advise Instant quarantine of host and removal of malware. Recommend updating antivirus as most will catch and remove this before it has a chance to install.

Reporting tool Snort

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

Source IP | 46.29.160.132

Source port 80

Destination IP 10.22.15.119

Destination port 49208

**Narrative**

• Alerted by Snort and Suricata:

◦ “ETPRO CURRENT\_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24”

◦ “ET POLICY Binary Download Smaller than 1 MB Likely Hostile”

“ET POLICY PE EXE or DLL Windows file download HTTP”

• Located Source/Destination IP Addresses and timestamp from Alerts: Date/Time: 2018-11-07 20:47 UTC

◦ Src/Prt: 46.29.160.132:80

◦ Dst/Prt: 10.22.15.119:49208

**Post-Incident Report**•

Identified Hostname and MacAddress of infected computer in pacp:

◦ MAC: 00:11:2f:d1:6e:52

Host Name: Danger-Win-PC

**Post-Incident Report.**

• Identified download link in pcap HTTP traffic:

◦ shumbildac[.]com/WES/fatog.php?l=ngul5.xap

• Followed the TCP Stream and found binary downloaded:

◦ Date: 2018-11-07 20:47 UTC

**Post-Incident Report**

• Uploaded SHA256 hash to virus total for confirmation:

◦97f149f146b0ec63c32abff204ae27638f0310536172b0f718f1a91a5672fe71