Turkey and Defense Post-Incident Report

|  |  |
| --- | --- |
| Date of investigation | 2019/09/23 |
| Date of incident | 2018-11-07 at 20:47 UTC |
| Outcome | True Positive - Ursnif or Gozi/IFSB found |
| 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 took | Wireshark |
| Attack vector | Windows malware download from shumbildac[.]com/WES/fatog.php?l=ngul5.xap |
| Source IP/email | 10.22.15.119 |
| Source port | 68 |
| Destination IP/email | 10.22.15.255 |
| Destination port | 67 |

Narrative

• Date/Time malicious activity started: 2018-11-07 at 20:47 UTC

• MAC address of the infected Windows: 00:11:2f:d1:6e:52

• Host name of the infected Windows host: Danger-Win-PC

• User account name on the infected Windows host: carlos.danger

• URL that returned an EXE: shumbildac[.]com/WES/fatog.php?l=ngul5.xap

• Size of the EXE: 439,808 bytes

• SHA256 hash of the EXE: 97f149f146b0ec63c32abff204ae27638f0310536172

b0f718f1a91a5672fe71

• Type of malware: Ursnif or Gozi/IFSB





