**Post-Incident Report**

Date of investigation 11/06/2019

Date of incident 2019-01-28 21:49 UTC

Outcome True Positive - Dridex Malware Variant Found

Action Taken Identified Malware and infected host.

Advise Firewall Rules to Block Traffic from Source, and watch closely for similar activity. Advise reformatting infected computer or restoring to a backup prior to time of incident.

Reporting tool Snort

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

Source IP | 91.121.30.69

Source port 8000

Destination IP 172.17.8.109

Destination port 49207

**Narrative**

• Alerted by Snort and Suricata:

◦ “ET POLICY HTTP Request on Unusual Port Possibly Hostile

172.17.8.109 -> 91.121.30.169”

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

91.121.30.169 -> 172.17.8.109”

“ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)”

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

◦ Src/Prt: 91.121.30.169:8000

◦ Dst/Prt: 172.17.8.109:49207

**Post-Incident Report**•

Identified Hostname and MacAddress of infected computer in pacp:

◦ MAC: 14:fe:b4:d4:15:ca

Host Name: Dunn-Windows-PC

**Post-Incident Report.**

• Identified download link in pcap HTTP traffic:

◦ /91msE95B/actiV.bin

• Followed the TCP Stream and found binary downloaded:

◦ Date: Mon, 28 Jan 2019 21:49:19 GMT

**Post-Incident Report**

• Uploaded SHA256 hash to virus total for confirmation:

◦9f6e3e65aedca997c6445329663bd1d279392a34cfda7d1b56461eb41641fa08

actiV.bin

TrojanDownloader:Win32/Cridex.1726c5da

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

◦ # IPv4 destination address.

▪ iptables --append INPUT --in-interface eth0 --source 91.121.30.169/8000 --jump DROP