Badbundt Analysis

Executive Summary:
On 2019-08-20 19:31 UTC, a Windows device operated by Reginald.chandler was infected with Ursnif malware.

Victim details:
IP: 10.8.20.101
Host name: Tampa-office-pc
MAC address: 00:18:f3:a6:01:92
User: reginald.chandler

IoC's:
94.103.87.160 port 80 bh79sbu.com
- GET /qtra/ttqr.php?l=csuv3.j12 (MALICIOUS)
    - Contains Ursnif malware

172.217.6.174 port 80 google.com
- GET /images/wf_2BKr4G...
- Decoy URL

94.103.86.146 port 80 hne53brianaea.com
- GET /images/h653rH6w...
- GET /images/favicon.ico
- GET /images/uZD5Vn6...
- GET /images/jBs054...
- Trojan downloaded, Ursnif

185.193.141.166 port 49217 kjoanaxbrennan.top
- Encrypted Ursnif traffic

191.37.181.152 port 49222 no domain
- Trojan, Trickbot

89.105.203.184 port 49224 no domain
- Trojan, Abuse.ch SSL cert detected

185.183.98.232 port 49238 hostsailor.com
- GET /samerton.png
- GET /tableone.png
- GET /wredneg2.png
-
- Trickbot malware, executables

170.238.117.187 port 49241 no domain

- Post request for chrome passwords