Resurgo
Cyber Threat Alert Summaries

Hi All,

Between July and August 2017 the DSS was made aware of Credential Stealing Campaigns through the use of Harvesting sites. Be aware of the following domains listed. If there is a URL or link which uses the following domains, do not click and inform the DSS or US-CERT at https://www.us-cert.gov/report-phishing

Here is the listing of domains:

Domain	IP	URI	HTTP Method
whitewillowdental.in	67.225.129.238	/jama/scan.html	GET
reflection.com.pk	192.185.190.24	/alan.scan.html	GET

For a Suricata/Snort or Yara rules, contact me at ryan.ito@resurgo.net.

Additionally, the FBI and DHS have released Joint Analysis and Reporting on Advanced Persistent Threat actors have targeted computer networks of government entities and organizations in the energy, water, aviation, nuclear, and critical manufacturing sectors since at least May 2017.

The malicious actors have employed a variety of techniques to harvest credentials including the following:

- Open source reconnaissance
- Use of control-systems-themed spear-phishing emails
- Use of watering hole domains
- Host-based exploitation
- Ongoing credential gathering
- Remote access through web shells

Although this activity is still under investigation, DHS and FBI are sharing this information to assist in detecting potential compromises.

For more info on the cyber-attack tactics, techniques listed above contact me at ryan.ito@resurgo.net

Notice

These flagged IPs and domains are not a definitive black list, but a recommendation and advisement provided by the DSS, FBI and DHS. It is up to the recipients of this information to decide how, when and where to use the information contained in these summaries.