Financial Sector
Cyber Intelligence Group

CIG Circular 44 – HTTP POST Request Used for Implant Communications

Date: 09/03/2015

TRAFFIC LIGHT PROTOCOL (TLP): GREEN – RECIPIENTS MAY SHARE TLP: GREEN INFORMATION WITH PEERS, TRUSTED GOVERNMENT AND CRITICAL INFRASTRUCTURE PARTNER ORGANIZATIONS, AND SERVICE PROVIDERS WITH WHOM THEY HAVE A CONTRACTUAL RELATIONSHIP, BUT NOT VIA PUBLICLY ACCESSIBLE CHANNELS.

Purpose:
This circular is intended to inform network security specialists of cyber actors' tactics, techniques, procedures (TTPs) and associated indicators, to assist in network defense capabilities and planning.

Summary:
This circular provides a sample HTTP POST request related to malware used in recent spear-phishing campaigns by an APT actor that has previously targeted the U.S. financial sector.

Details:
As of July 2015, an APT actor that has previously targeted the U.S. financial sector used an implant to provide command and control (C2), according to credible reporting. Implant communications were observed between administrative infrastructure and known malware C2 nodes used in spear-phishing campaigns in July 2015. The communication from administrative infrastructure was an HTTP POST request. The file name, content-length, and host associated with the request varied. A sample of the HTTP POST request is provided below:

```
POST /style.php HTTP/1.1
Accept-Encoding: identity
Content-Length: 272
Host: [HOST]
Content-Type: multipart/form-data;
boundary=127.0.1.1.1000.30750.1438176080.790.4968
Connection: close
User-Agent: Python-urllib/2.7
--127.0.1.1.1000.30750.1438176080.790.4968
Content-Disposition: form-data; name="action"
getAll --127.0.1.1.1000.30750.1438176080.790.4968
Content-Disposition: form-data; name="type"
87ce1fb4267221e03c8694bc17d17640
--127.0.1.1.1000.30750.1438176080.790.4968--
```

The actor also obfuscated executable files by Base64 encoding the files to appear as SSL certificates.

The Financial Sector Cyber Intelligence Group (CIG) was established within the Department of the Treasury, Office of Critical Infrastructure Protection and Compliance Policy in 2013. The CIG monitors and analyzes all-source intelligence on cyber threats to the financial sector; provides timely, actionable cyber threat information to the sector; and solicits feedback and information requirements from the sector. Please take a moment to let us know:

Does this Circular provide information that is not available to you elsewhere?
Is the information provided actionable?
Is the level of context appropriate?

Please direct any comments or questions to CIG@Treasury.gov.

Eligible stakeholders can download CIG Circulars and other relevant government information from the DHS Homeland Security Information Network (HSIN) Financial Services Portal. For information on membership, download the quick guide from: http://go.usa.gov/3YH45