Raytheon
Blackbird Technologies

20150911-280-CSIT-15085
NfLog

For

SIRIUS Task Order PIQUE

Submitted to:

U.S. Government

Submitted by:

Raytheon Blackbird Technologies, Inc.
13900 Lincoln Park Drive
Suite 400
Herndon, VA 20171

11 September 2015

(U) Table of Contents

1.0 (U) Analysis Summary

(S//NF) The following report details a new variant of the NfLog Remote Access Tool (RAT), also known as IsSpace, used by SAMURAI PANDA. This new variant is deployed using a repurposed version of the leaked Hacking Team Adobe Flash Exploit which leverages CVE-2015-5122. This new variant also incorporates the use of the Google App Engine (GAE) hosting to proxy communications to its C2 Server.

(S//NF) NfLog is a basic RAT that polls C2 servers every 6 seconds awaiting an encoded response. It uses an embedded plain text configuration file. The primary C2 server communicates over port 80. Alternate ports are configurable through the secondary C2 server variable. This RAT is also proxy aware. On older operating systems it will bind to port 1139 using a raw socket and attempt to sniff proxy credentials. On newer systems with Windows Firewall it will attempt to enumerate the basic authorization username and password used for most proxy authentications using HTTP.

(S//NF) If NfLog determines that the current user has administrative privileges it will attempt to reload itself using the elevated permissions. NfLog will use the well-known UAC bypass technique of DLL side-loading of CryptBase.dll on Windows Vista and newer operating systems to attempt UAC bypass and privilege escalation.

(S//NF) Persistence is achieved through the setting of an ASEP after the RAT has been installed to a particular folder.

(S//NF) In conclusion, NfLog is a very simple RAT. No new techniques worthy of a PoC were presented.

2.0 (U) Description of the Technique

(S//NF) No techniques are recommended for PoC development.

3.0 (U) Identification of Affected Applications

(U) Windows.

4.0 (U) Related Techniques

(S//NF) RAT and UAC Bypass.

5.0 (U) Configurable Parameters

(U) None.

6.0 (U) Exploitation Method and Vectors

(S//NF) This RAT deployed using a repurposed version of the leaked Hacking Team Adobe Flash Exploit which leverages CVE-2015-5122.

7.0 (U) Caveats

(U) None.

8.0 (U) Risks

(S//NF) Not applicable because we do not recommend any techniques for PoC development.

9.0 (U) Recommendations

(S//NF) No PoCs recommended.