

**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**

*This document includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this concept. If, however, a contract is awarded to Blackbird as a result of—or in connection with—the submission of these data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in these data if they are obtained from another source without restriction.*

*This document contains commercial or financial information, or trade secrets, of Raytheon Blackbird Technologies, Inc. that are confidential and exempt from disclosure to the public under the Freedom of Information Act, 5 U.S.C. 552(b)(4), and unlawful disclosure thereof is a violation of the Trade Secrets Act, 18 U.S.C. 1905. Public disclosure of any such information or trade secrets shall not be made without the prior written permission of Raytheon Blackbird Technologies, Inc.*

## (U) Table of Contents

1.0 (U) Analysis Summary .....	1
2.0 (U) Description of the Technique .....	1
3.0 (U) Identification of Affected Applications .....	1
4.0 (U) Related Techniques .....	1
5.0 (U) Configurable Parameters .....	1
6.0 (U) Exploitation Method and Vectors.....	2
7.0 (U) Caveats .....	2
8.0 (U) Risks .....	2
9.0 (U) Recommendations .....	2

## 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.