

Raytheon Blackbird Technologies

20150807-255-SY-2015

Butterfly Attackers

**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**

7 August 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 discusses activities by a group of hackers known as the Butterfly attackers. These attackers used a zero day exploit that targeted CVE-2013-0422 titled Oracle Java Runtime Environment Multiple Remote Code Execution Vulnerabilities. This vulnerability was patched on January 31st, 2013. The attackers also used a Windows and Mac backdoor named OSX.Pintsized and Backdoor.Jiripbot as the payloads.

(S//NF) The attackers used a watering-hole attack to compromise a mobile phone developer website to deliver the Java exploit. In one case a fully up to date version of Internet Explorer 10 was exploiting indicating that a zero-day for this browser may have been used. No further information on this exploit was provided.

(S//NF) In some cases the attackers spread using a Citrix profile management application to create a back door on the infected system. In another instance the attackers used TeamViewer to create copies of the backdoor.

(S//NF) Various tools used by the hackers were discussed in this report and include:

- OSX.Pintsized: A well-documented modification of OpenSSH
- Backdoor.Jiripbot: Primary back door tool with fallback domain generation algorithm
- Hackertool.Bannerjack: used to receive default messages issued by Telnet, HTTP, and general TCP servers
- Hackertool.Multipurpose: Assists in spreading across network and cleaning up log files
- Hackertool.Eventlog: Event log parser
- Hacktool.Proxy.A: Creates a Proxy connection to route traffic through intermediary node

(S//NF) In conclusion, this report details attacks using a since patched vulnerability and other well-known tools. As such no PoC is recommended.

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) Backdoor

5.0 (U) Configurable Parameters

(U) None

6.0 (U) Exploitation Method and Vectors

(S//NF) These attacks exploited the known and patched vulnerability, CVE-2013-042 and possibly and unspecified zero day vulnerability in Internet Explorer 10.

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.