

Raytheon
Blackbird Technologies

20150814-257-CSIT-15016

Elirks RAT

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

14 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 Summary1
2.0 (U) Description of the Technique1
3.0 (U) Identification of Affected Applications1
4.0 (U) Related Techniques1
5.0 (U) Configurable Parameters1
6.0 (U) Exploitation Method and Vectors.....1
7.0 (U) Caveats1
8.0 (U) Risks1
9.0 (U) Recommendations2

1.0 (U) Analysis Summary

(S//NF) This Crowdstrike Tipper report (brief single subject report) focuses on the Elirks RAT used by the Chinese bad actor known as Stalker Panda. While this Tipper report provides more details about the Elirks RAT, the detail provided is primarily about its multi-stage command and control (C2) infrastructure that includes social media and blog sites as a first stage. The additional information provided focuses on the URLs and IPs of these first stage sites.

(S//NF) That said, there was additional detail on Elirks' startup routine. As its first step, the RAT prepares a window with a window name and a class name that are loaded from string resources. The window icon is copied from the Windows media player (mplayer2.exe). Its only purpose is to wait until all other threads of the malware process have terminated. It was speculated that the purpose of creating this 'fake' window is to cover the fact it is running a process not associated with a window, which may be seen as suspicious.

(S//NF) Again, most of the added details on the Elirks RAT provided in this Tipper report relate details of the multi-stage C2 infrastructure and as such, no PoCs are recommended.

2.0 (U) Description of the Technique

(S//NF) Not applicable as no PoCs are recommended.

3.0 (U) Identification of Affected Applications

(U) Windows.

4.0 (U) Related Techniques

(S//NF) RAT command and control.

5.0 (U) Configurable Parameters

(S//NF) Varied depending on the social media and blog sites used as first-stage C2 points.

6.0 (U) Exploitation Method and Vectors

(S//NF) No exploitation methods or attack vectors were discussed in this report.

7.0 (U) Caveats

(U) None.

8.0 (U) Risks

(S//NF) Not applicable as no PoCs are recommended.

9.0 (U) Recommendations

(S//NF) No PoCs are recommended.