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

(U) Table of Contents

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.