Raytheon
Blackbird Technologies

20150828-269-CSIT-15079
Cozy Bear

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

28 August 2015

(U) Table of Contents

1.0 (U) Analysis Summary

(S//NF) The following report details a new round of Cozy Bear attacks identified in 2015. These attacks use a new final payload titled MiniDionis. Previous Cozy Bear campaigns were reported in CSIT-15021.

(S//NF) The Cozy Bear attacks begin with a spear fishing email containing a link to download a ZIP file. The zip file is hosted on a comprised legitimate website. The zip contains a self-extracting RAR executable with a fake PDF icon. Once executed the loader will be extracted and executed which will in turn download a second stage dropper. This second stage dropper will then extract and execute the final payload.

(S//NF) The MiniDionis Dropper contains an encrypted segment appended to the end of the file as overlay data after the .reloc section. This encrypted segment contains the file to be loaded. The dropper first decrypts the custom header stored in the first 32 bytes of this data. This header is used to determine how large the parameter section is. This section is then also decrypted. These parameters are then passed as arguments to another instance of itself.

(S//NF) Once the loader is running, the second stage downloader is retrieved and an Auto-Start Execution Point (ASEP) is installed. The loader then removes the initial dropper. A hardcoded URL is used for downloading the final payload. This payload is a valid Adobe Flash (SWF) file appended with another encrypted segment. Within the segment is an XML file containing the final payload. This payload is the MiniDionis Remote Access Tool and can be installed with or without persistence based on a configurable value. It is able to execute commands, exfiltrate files, and download additional payloads.

(S//NF) MiniDionis data is transmitted over http and https to perform C2 communications. Furthermore these communications are encrypted using a custom TrCrypt protocol. MiniDionis can be redirected to a different C2 server by using an HTTP 302 status code.

(S//NF) In conclusion, Cozy Bear campaigns using MiniDiois use well-known methods to achieve their goals. 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

5.0 (U) Configurable Parameters

(U) None

6.0 (U) Exploitation Method and Vectors

(S//NF) Cozy Bear attacks are achieved through spearfishing emails requiring user action to execute.

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.