Raytheon
Blackbird Technologies

20150904-273-FireEye
Window into Russian Cyber Ops

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

04 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

Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this document.

1.0 (U) Analysis Summary

(S//NF) This FireEye report focuses on APT28, suspected Russian nation-state sponsored attacks. The report spends most of its pages on attribution, making the case that the attacks and tools used in a series of malware events starting in 2007 stem from the same Russian group. There is very little technical detail on how the malware is installed or implemented. FireEye seems to be impressed with the modular nature of the malware tools covered in this report, even though modular malware architectures have become common over the past few years. What little technical detail that is provided in this report are contained in Appendices C, D, and E.

(S//NF) The attack tools covered in this report are:

- SourFace/CoreShell – First-stage loader
- Chopstick - RAT
- OldBait – Credential harvester

(S//NF) SourFace, and its recent updated version, CoreShell is a downloader that retrieves a second stage RAT, Chopstick. CoreShell runs two threads, one thread that beacons back to the command and control (C2) server with collected information and the other thread is responsible for downloading and executing payloads from the C2 server. CoreShell uses HTTP as its communications protocol with the C2 server. The communications between CoreShell and its C2 server is Base64 encrypted. No other technical details on SourFace/CoreShell are provided.

(S//NF) Chopstick is the second stage RAT downloaded by SourFace/CoreShell. Chopstick is a modular RAT written in C++ and is capable of communicating with its C2 server either via HTTP or SMTP. When first launched, Chopstick collects basic information about its victim (Windows version, CPU architecture, Windows Firewall state, UAC configuration, IE settings, and installed PSP products). Chopsticks has been observed using the target organizations own mail servers to exfiltrate data. After collecting the initial information about the target, Chopsticks creates a hidden file for temporary storage and creates a Windows mailslot. The Windows mailslot could allow external binaries and other malware to write data to it. Chopsticks is capable of:

- Screen capture
- Capturing Windows focus events
- Keylogging
- Windows scraping

Unfortunately, no technical details on implementation of any of these capabilities is provided.

(S//NF) OldBait is a credential harvester that installs itself in **\\Application** Data\Microsoft\MediaPlayer. Credentials for the following applications are collected:

- Internet Explorer
- Firefox
- Eudora

- The Bat! (Modavian email client)
- Becky! (Japanese email client)

No technical details are provided on how OldBait implements credential harvesting but we suspect browser hooking.

(S//NF) Although this report is an interesting read on Russian malware activity, there is very little technical detail provided on implementation and therefore 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

(S//NF) Windows, Windows-based browsers (IE and Firefox), and email clients (Eudora, The Bat!, and Becky!).

4.0 (U) Related Techniques

(S//NF) Dropper, general RAT, and credential harvesting.

5.0 (U) Configurable Parameters

(U) Varied.

6.0 (U) Exploitation Method and Vectors

(S//NF) No exploitation methods were discussed. The attack vector mentioned is spear phishing.

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.