Raytheon
Blackbird Technologies

20150807-251-Symantec ZeroAccess Indepth

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

07 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 2
4.0 (U) Related Techniques..2
5.0 (U) Configurable Parameters 2
6.0 (U) Exploitation Method and Vectors...2
7.0 (U) Caveats...2
8.0 (U) Risks...2
9.0 (U) Recommendations 2

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 2013 report covers the well-known malware sample known as ZeroAccess. The aspect of ZeroAccess that makes it most interesting is its peer-to-peer (P2P) command and control architecture, which is fairly unique in malware. ZeroAccess does not use dedicated command and control (C2) servers, rather it uses P2P to distribute its communications network. Each infected machine acts as both a client and a server. The downside of a P2P comms architecture is the relative “chattiness” of the network in updating the infected machines about the growing and ever changing IP addresses of infected machines. ZeroAccess has been observed conducting bit coin mining and click fraud.

(S//NF) There are four distinct variants of the ZeroAccess malware:

- Version 1 – Type I, II, and III
- Version 2 – Type IV

Type I dates back to early 2011 and contains a rootkit component that is installed as a device driver and used to access a hidden NTFS file system. Type I also contains a tripwire device driver that monitors the infected system for behavior indicating anti-virus applications. Specifically, the tripwire driver watches for processes with high registry access counts. If a process examines more than 50 service registry key entries in a short period, the process is suspended. We assume the report means the anti-virus process is suspended and not the malware, but it isn’t clear.

Type II first appeared in July 2012 and contains the same rootkit component as Type I but hides its files in a different directory than Type I. Type II also contains the same tripwire component as Type I.

Type III was first observed in the fall of 2012 and is identical to Type II but with the tripwire driver removed.

Type IV appeared in late 2012/early 2013 and represents a major overhaul of the ZeroAccess malware. This version ported the rootkit component to user-mode and emphasizes UDP communications instead of TCP.

(S//NF) ZeroAccess is at its core a framework used to load additional malware components. ZeroAccess can be purchased on underground gray market websites. There are different levels of support that can be procured, the top-level support costing $120K per year.

(S//NF) The most interesting aspect of this report is the described detection and defeat of anti-virus products, specifically monitoring for high counts of registry key access in a short period of time. We recommend this technique be developed as a PoC.

2.0 (U) Description of the Technique

(S//NF) The technique recommended for PoC monitors registry key access and triggers on processes with high registry key access in a short period of time. If detected, those processes are terminated.

3.0 (U) Identification of Affected Applications

(S//NF) Windows and anti-virus applications.

4.0 (U) Related Techniques

(S//NF) Anti-anti-virus.

5.0 (U) Configurable Parameters

(S//NF) Varied depending on anti-virus product targeted.

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) The risk associated with the development of the anti-anti-virus PoC is assessed to be moderate due to technical complexity. We estimate that the PoC will require two FTE weeks to complete.

9.0 (U) Recommendations

(S//NF) We recommend that the ZeroAccess technique of identifying anti-virus products (triggering on high registry key access processes) be developed as a PoC.

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