

Raytheon Blackbird Technologies

20150821-265-VB-Dridex-2015

Dridex

**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**

21 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	1
4.0 (U) Related Techniques.....	1
5.0 (U) Configurable Parameters	1
6.0 (U) Exploitation Method and Vectors.....	2
7.0 (U) Caveats	2
8.0 (U) Risks	2
9.0 (U) Recommendations	2

1.0 (U) Analysis Summary

(S//NF) The following report discusses Dridex, a banking Trojan descendant of the Cridex malware. Dridex is a windows executable which uploads system info to a C&C server and then downloads a DLL which acts as a Remote Access Tool (RAT) and banking Trojan. This tool does not appear to contain any worthwhile techniques besides the User Access Control bypass method which has since been patched by Microsoft.

(S//NF) Dridex is usually delivered as a Word Document with macros. This initial module downloads the main module when executed. Dridex XOR's and encrypts the C&C server URL using the aPlib algorithm. Dridex utilizes http, https, and ftp over their default ports for communication. The communications sent are encrypted.

(S//NF) Dridex uses a different method for User Access Control (UAC) bypass. Where as many pieces of malware use PlugX to achieve this bypass, Dridex uses application compatibility databases. This is a file that configures execution rules for applications that have compatibility issues in Windows. This is achieved by creating and installing a new application compatibility database file. Dridex then launches the iscsicli command, a command line tool for the iSCSI initiator. The newly installed application compatibility database file executes a batch file which then causes Dridex to execute with administrative privileges. Microsoft has released a patch for this vulnerability causing a warning message to pop up should this method be applied.

(S//NF) In conclusion, this Banking Trojan does not demonstrate any new or notable techniques besides the UAC bypass which has since been patched by Microsoft. As such no PoC is recommended.

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) Trojan, UAC Bypass

5.0 (U) Configurable Parameters

(U) None

6.0 (U) Exploitation Method and Vectors

(S//NF) This malware is delivered through malicious word documents delivered through spam email campaigns. It exploits a now patched vulnerability in application compatibility databases to bypass UAC.

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.