

**Raytheon**  
**Blackbird Technologies**

**20150911-279-CSIT-15083**  
**HTTPBrowser**

**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

**11 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

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.....	1
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 details a new variant of the HTTPBrowser Remote Access Tool (RAT) used by EMISSARY PANDA. This new variant was built in March of 2015 and is deployed through an unknown initial attack vector.

(S//NF) The dropper consists of a self-extracting zip file containing three files. One of the files is a legitimate executable associated with a Citrix Single Sign-On product which will side-load the attackers initial DLL. This will XOR decode and load API's and the HTTPBrowser RAT.

(S//NF) Persistence is achieved copying itself to an install location and setting an Auto-Start Execution Point (ASEP) for the HTTPBrowser executable. The RAT is then restarted from this location with the C2 server address, port, and default sleep time as variables.

(S//NF) This RAT captures keystrokes using the standard RegisterRawInputDevice() and GetRawInput() APIs and writes the captured keystrokes to a file. The RAT continuously attempts to contact the C2 Server for tasking and sleeping the set number of seconds. These communications are in clear text, which speaks to the low level of sophistication of this RAT.

(S//NF) In conclusion, HTTPBrowser is a very simple RAT. 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) Exploitation is achieved by using a legitimate executable to perform DLL side-loading.

## **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.