Raytheon
Blackbird Technologies

20150807-252-MIRcon
Something About WMI

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

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 report is a slide deck of a presentation given on WMI and its use in malicious attacks. The briefing is a very good overview of what WMI is and provides some examples of how to construct WMI commands to accomplish important tasks such as target reconnaissance, pivoting, privilege escalation, persistence, and data theft.

(S//NF) Prior to getting into the examples on how to use WMI maliciously, the briefing deck provides a nice overview of what WMI is and how to interact with it.

(S//NF) This report is a very nice high-level overview of what WMI is and how to interact with it via several methods, CLI, VBS, PowerShell, and a couple of third-party tools. However, there are no techniques or methods discussed worth recommending PoCs against.

2.0 (U) Description of the Technique

(S//NF) Not applicable as no PoCs are recommended.

3.0 (U) Identification of Affected Applications

(U) Windows.

4.0 (U) Related Techniques

(S//NF) Remote administration, target reconnaissance, pivoting, privilege escalation, persistence, and data theft.

5.0 (U) Configurable Parameters

(U) Not applicable.

6.0 (U) Exploitation Method and Vectors

(S//NF) No exploitation method or attack vectors were discussed in this report.

7.0 (U) Caveats

(U) None.

8.0 (U) Risks

(S//NF) Not applicable as no PoCs are recommended from this report.

9.0 (U) Recommendations

(S//NF) No PoCs are recommended from this report.

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