

Raytheon Blackbird Technologies

Mimikatz Password Scanning Analysis PoC Report

**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
1.1 (U) Heading 2	Error! Bookmark not defined.
2.0 (U) Description of the Technique.....	1
2.1 (U) Heading 2	1
3.0 (U) Identification of Affected Applications	Error! Bookmark not defined.
4.0 (U) Related Techniques	Error! Bookmark not defined.
5.0 (U) Configurable Parameters.....	Error! Bookmark not defined.
6.0 (U) Exploitation Method and Vectors.....	Error! Bookmark not defined.
7.0 (U) Caveats	Error! Bookmark not defined.
8.0 (U) Risks	Error! Bookmark not defined.
9.0 (U) Recommendations.....	2

(U) List of Figures

Figure 1. (U) Figure Caption	Error! Bookmark not defined.
------------------------------------	------------------------------

(U) List of Tables

Table 1. (U) Table Caption	Error! Bookmark not defined.
----------------------------------	------------------------------

1.0 (U) Analysis Summary

(U) Mimikatz was analyzed in-depth in an attempt to isolate the techniques and subroutines used in harvesting usernames and passwords. After thorough static and dynamic analysis, the task in question was determined to exceed the scope of a traditional program-based PoC.

2.0 (U) Description of the Technique

(U) The following sections detail various highlights found during research and analysis.

2.1 (U) List of Affected Files

- kuhl_m_lsadump.c
- kuhl_m_sekurlsa.c – Place initial breakpoint in kuhl_m_sekurlsa_enum()
- kuhl_m_sekurlsa_nt6.c
- kuhl_m_sekurlsa_utils.c
- mimikatz.c

2.2 (U) Research Notes

- Frequently, switch() statements were used in the place of if() statements.
- Almost all parameters are structures. The structures typically contain multiple other user-defined structures as well as functions. For example, kuhl_m_sekurlsa!kuhl_m_sekurlsa_acquireLSA() calls initLocalLib() which is a function within the lsassLocalHelper instance of the global structure KUHL_M_SEKURLSA_LOCAL_HELPER.
- The limited documentation available online is also incomplete. For example, the code path exists to parse an LSASS minidump; however, the functionality and appropriate command syntax is not documented.
- Kuhl_m_sekurlsa!kuhl_m_sekurlsa_acquireLSA() contains most of the critical functionality.
- Kull_m_memory!kull_m_memory_search() appears to be the function that finally performs the search; however, it appears to be a recursive call. Complicating matters further, the PKULL_M_MEMORY_SEARCH structure nests an addition 6 structures. None of the field names or their associated values indicate a specific pattern to search for.
- The author removed the DEBUG build configuration. When configuring a DEBUG configuration manually, ensure that all the linker generates debugging information and all optimizations are disabled.
- The AcquireKeys() call suggests there are additional decryption / deobfuscation measures.

3.0 (U) Recommendations

(U) When balancing the complex nature of the source code style / syntax with the technique used, the benefits still outweigh the negative aspects. Mimikatz still contains a useful, valid technique