Raytheon
Blackbird Technologies

McAfee DLL Hijack 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

28 August 2015

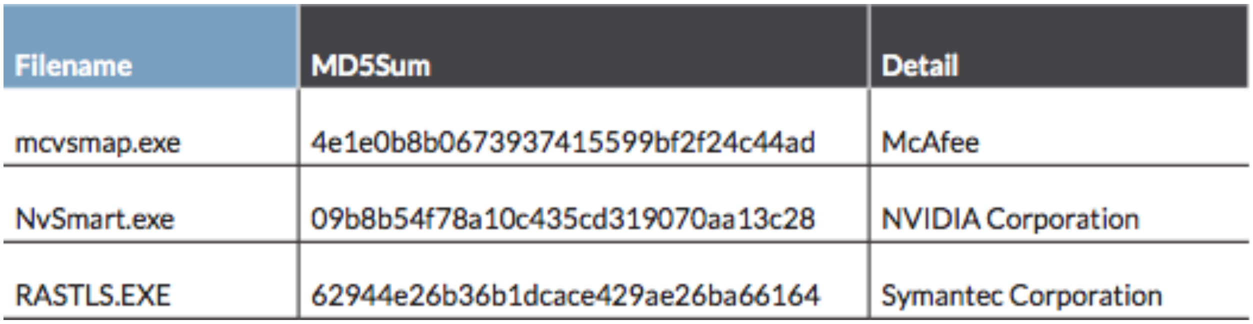
This document includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this concept. If, however, a contract is awarded to Blackbird as a result of—or in connection with—the submission of 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

(U) List of Figures

1.0 (U) Analysis Summary

(U) The PlugX Remote Access Tool (RAT) contains functionality to perform a DLL Hijack against a few targets. Further research into PlugX included the following additional EXEs that unsafely load DLLs.



Filename	MD5Sum	Detail
mcvsmap.exe	4e1e0b8b0673937415599bf2f24c44ad	McAfee
NvSmart.exe	09b8b54f78a10c435cd319070aa13c28	NVIDIA Corporation
RASTLS.EXE	62944e26b36b1dcace429ae26ba66164	Symantec Corporation

(U) Figure 1: Additional susceptible DLLs

(U) In each of these instances, the executable attempts to load a DLL after downloading without verifying its integrity (e.g., via signing).

(U) Ultimately, we found the McAfee technique to be invalid for loading mcutil.dll. The directories that contain mcutil.dll appear to have protection above the standard Windows Access Control Lists (ACLs) that protect other directories. These additional techniques prevent the replacement of mcutil.dll. Even after lifting the filter on the directories, none of the executables tested loaded mcvsmap.exe.

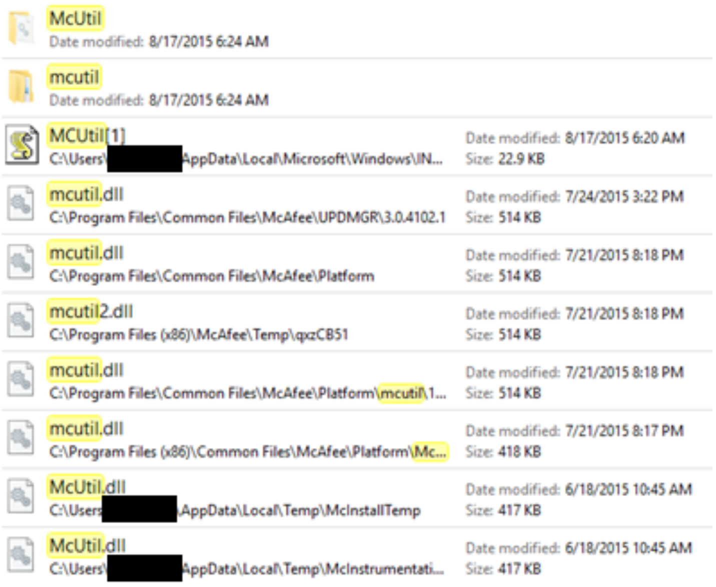
(U) With respect to RASTLS.exe, we were not only unable to find a Symantec-attributed EXE with this name, but we were unable to find any EXE on the system with this name. A DLL with this name was found in the C:\Windows\SysWOW64 directory, but we are uncertain what its purpose is.

(U) The latest Nvidia Graphics Driver was downloaded and extracted, but did not contain the NvSmart.exe file.

2.0 (U) Description of the Technique

2.1 McAfee

(U) After running a search for the affected DLL (`mcutil.dll`), the follow locations were found to contain the file.



```
McUtil
Date modified: 8/17/2015 6:24 AM

mcutil
Date modified: 8/17/2015 6:24 AM

MCUtil[1]                                                     Date modified: 8/17/2015 6:20 AM
C:\Users\[redacted]AppData\Local\Microsoft\Windows\IN...      Size: 22.9 KB

mcutil.dll                                                    Date modified: 7/24/2015 3:22 PM
C:\Program Files\Common Files\McAfee\UPDMGR\3.0.4102.1        Size: 514 KB

mcutil.dll                                                    Date modified: 7/21/2015 8:18 PM
C:\Program Files\Common Files\McAfee\Platform                 Size: 514 KB

mcutil2.dll                                                   Date modified: 7/21/2015 8:18 PM
C:\Program Files (x86)\McAfee\Temp\qxzCB51                    Size: 514 KB

mcutil.dll                                                    Date modified: 7/21/2015 8:18 PM
C:\Program Files\Common Files\McAfee\Platform\mcutil\1...     Size: 514 KB

mcutil.dll                                                    Date modified: 7/21/2015 8:17 PM
C:\Program Files (x86)\Common Files\McAfee\Platform\Mc...     Size: 418 KB

McUtil.dll                                                    Date modified: 6/18/2015 10:45 AM
C:\Users[redacted]AppData\Local\Temp\McInstallTemp            Size: 417 KB

McUtil.dll                                                    Date modified: 6/18/2015 10:45 AM
C:\Users\[redacted]AppData\Local\Temp\McInstrumentati...      Size: 417 KB
```

(U) Figure 2: Locations containing `mcutil.dll`

(U) Non temp directories were chosen first; however, a copy of mcutil.dll was copied to all directories.

(U) Attempting to copy the file to any of these locations requires Elevated Permissions; however, after granting elevated permissions, access to modify the files is still denied. In an effort to rule out any ACLs or DACLs from limiting our access, we took ownership of the folder, broke inheritance, granted our user account full access, and stripped all accesses from all other users. Despite these efforts, the same error was present when attempting to modify, add, or remove anything in any of those directories.

(U) The presence of this protection suggests (though we did not confirm) that McAfee has registered an Early Launch Anti-Malware (ELAM) filter driver that effectively prevents modification of any DLLs it considers critical. Unfortunately, the presence of something over and above ACLs effectively nullifies this technique.

(U) After disabling file system protections, we were able to copy files to the directory. McVsMap.exe was launched after each copy of mcutil.dll was moved into place, but it never appeared to load even when placing McUtil.dll in the same directory.

2.2 Symantec

(U) The file in question, RASTLS.exe was not found related to Symantec in any capacity during testing.

2.3 Nvidia

(U) The latest Nvidia Graphics Driver was downloaded and extracted, but did not contain the NvSmart.exe file.

3.0 (U) Recommendations

(U) After testing, none of the techniques were found to be valid. We do not recommend any further research or development.