Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 205, Task ID: 819

Task ID: 819

Risk Level:

Date Processed: 2016-04-28 13:09:58 (UTC)

Processing Time: 7.01 seconds IntelliVM Virtual Environment:

"c:\windows\temp\7fb29afcdb4ab59eea2314061136ed82.exe" **Execution Arguments:**

205 Sample ID: basic Type: Owner: admin

7fb29afcdb4ab59eea2314061136ed82 Label:

Date Added: 2016-04-28 12:45:11 (UTC) File Type: PE32:win32:gui 146944 bytes File Size:

MD5: 7fb29afcdb4ab59eea2314061136ed82

f53388af47c8e24680dedebc4c5d2eb6434fdf5d4bb3c1efb0a41c8e4a22b771 SHA256:

Description:

Pattern Matching Results

2 Terminates third-party processes

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\WINDOWS\Temp\7fb29afcdb4ab59eea2314061136ed82.exe

["c:\windows\temp\7fb29afcdb4ab59eea2314061136ed82.exe"]

C:\Program Files\Java\jre7\launch4j

tmp\7fb29afcdb4ab59eea2314061136ed82.exe ["C:\Program Files\Java\jre7\launch4j-

tmp\7fb29afcdb4ab59eea2314061136ed82.exe" -Xmx512M -Xss5M -classpath

 $"lib\RationalPlan.jar; lib\RationalPlan.jar; lib\RationalPlan.ja$

i18n.jar;lib\jlfgr

1_0.jar;lib\looks.jar;lib\itext.jar;lib\jxl.jar;lib\AppleJavaExtensions.jar;lib\mpxj.jar;lib\mail.jar;lib\activation.jar;lib\ical4j.jar;lib\commons-

logging.jar;lib\commons-lang.jar;lib\poi.jar;lib\quaqua.jar;lib\jaxb-api.jar;lib\jaxb-impl.jar;lib\jsr173_1.0_api.jar;lib\spring.jar;lib\spring-webmvc.jar;lib\swing-worker-

1.2.jar;lib\jasperreports.jar;lib\jasperreports-fonts-4.0.1.jar;lib\groovy-all.jar;lib\commons-collections-3.2.1.jar;lib\commons-digester-

2.1.jar;lib\SHEF.jar;lib\sam.jar;lib\jtidy.jar;lib\novaworx-

syntax.jar;lib\jna.jar;lib\jayatana.jar;lib\dropbox-java-

sdk.jar;lib\httpmime.jar;lib\httpclient.jar;lib\httpcore.jar;lib\json_simple.jar;lib\google-api-

client.jar;lib\google-api-services-drive.jar;lib\google-http-client.jar;lib\google-oauth-

client.jar;lib\guava.jar;lib\jackson-core-asl.jar;lib\resources" com.sbs.jpm.Main]

C:\Program Files\Java\jre7\launch4j-Terminates process:

tmp\7fb29afcdb4ab59eea2314061136ed82.exe

Terminates process: C:\WINDOWS\Temp\7fb29afcdb4ab59eea2314061136ed82.exe

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003 Creates mutex:

\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates C:\Program Files\Java\jre7\launch4j-tmp

Creates: C:\Program Files\Java\jre7\launch4j

tmp\7fb29afcdb4ab59eea2314061136ed82.exe

Creates: $C: \DOCUME \sim 1 \land Admin \land LOCALS \sim 1 \land Temp \land sperfdata_Admin$

Creates: C:\Documents and Settings\Admin\Local

Settings\Temp\hsperfdata_Admin\1408

Opens: C:\WINDOWS\Prefetch\7FB29AFCDB4AB59EEA2314061136E-0144CE91.pf

C:\Documents and Settings\Admin Opens: C:\WINDOWS\system32\imm32.dll Opens: C:\WINDOWS\system32\shell32.dll Opens:

C:\WINDOWS\system32\SHELL32.DLL.124.Manifest Opens: C:\WINDOWS\system32\SHELL32.DLL.124.Config Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-

Opens: Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83

C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Opens: Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll

C:\WINDOWS\WindowsShell.Manifest Opens: Opens: C:\WINDOWS\WindowsShell.Config

Opens: C:\WINDOWS\system32\comctl32.dll Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest Opens: C:\WINDOWS\system32\comctl32.dll.124.Config

Opens: C:\WINDOWS\Temp

Opens: C:\Program Files\Java\jre7\bin C:\Program Files\Java\jre7 Opens:

```
Opens:
                                      C:\Program Files\Java\jre7\bin\javaw.exe
  Opens:
                                      {\tt C:\Program\ Files\Java\jre7\launch4j-tmp}
                                      C:\windows\temp\7fb29afcdb4ab59eea2314061136ed82.l4j.ini
  Opens:
                                      C:\WINDOWS\system32\MSCTF.dll
  Opens:
                                      C:\WINDOWS\system32\MSCTFIME.IME
  Opens:
                                      C:\WINDOWS\system32\ole32.dll
  Opens:
  Opens:
                                      C:\Program Files\Java\jre7\launch4j-
tmp\7fb29afcdb4ab59eea2314061136ed82.exe
                                      C:\WINDOWS\system32\apphelp.dll
  Opens:
                                      C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:
                                      C:\WINDOWS\AppPatch\systest.sdb
  Opens:
                                      C:\Program Files
  Opens:
                                      C:\Program Files\Java
  Opens:
                                      C:\Program Files\Java\jre7\launch4j-
  Opens:
tmp\7fb29afcdb4ab59eea2314061136ed82.exe.Manifest
  Opens:
                                      C:\Program Files\Java\jre7\launch4j-
tmp\7fb29afcdb4ab59eea2314061136ed82.exe.Config
Opens: C:\WINDOWS\Prefetch\7FB29AFCDB4AB59EEA2314061136E-0732A99E.pf
                                      C:\Program Files\Java\jre7\lib\i386\jvm.cfg
  Opens:
                                      C:\Program Files\Java\jre7\bin\client
  Opens:
                                      C:\Program Files\Java\jre7\bin\msvcr100.dll
  Opens:
  Opens:
                                      C:\Program Files\Java\jre7\bin\client\jvm.dll
                                      C:\Program Files\Java\jre7\bin\client\jvm.dll.2.Manifest
  Opens:
  Opens:
                                      C:\Program Files\Java\jre7\bin\client\jvm.dll.2.Config
  Opens:
                                      C:\WINDOWS\system32\wsock32.dll
                                      C:\WINDOWS\system32\ws2_32.dll
  Opens:
  Opens:
                                      C:\WINDOWS\system32\ws2help.dll
  Opens:
                                      C:\WINDOWS\system32\winmm.dll
                                      C:\WINDOWS\system32\psapi.dll
  Opens:
  Opens:
                                      C:\Program Files\Java\jre7\bin\verify.dll
  Opens:
                                      C:\Program Files\Java\jre7\bin\java.dll
  Opens:
                                      C:.hotspotrc
  Opens:
                                      C:\
                                      C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
  Opens:
                                      C:\Program Files\Java\jre7\bin\zip.dll
  Opens:
  Opens:
                                      C:\Program Files\Java\jre7\lib
                                      C:\Program Files\Java\jre7\lib\meta-index
  Opens:
                                      C:\Program Files\Java\jre7\bin\client\classes.jsa
  Opens:
                                      C:\Program Files\Java\jre7\lib\rt.jar
  Opens:
  Opens:
                                      C:.hotspot_compiler
                                      C:\Program Files\Java\jre7\lib\ext\meta-index
  Opens:
  Opens:
                                      C:\Program Files\Java\jre7\lib\ext
                                      C:\WINDOWS
  Opens:
  Writes to:
                                      C:\Program Files\Java\jre7\launch4j-
tmp\7fb29afcdb4ab59eea2314061136ed82.exe
  Reads from:
                                      C:\Program Files\Java\jre7\lib\i386\jvm.cfg
  Reads from:
                                      C:\Program Files\Java\jre7\lib\meta-index
                                     C:\Program Files\Java\jre7\bin\client\classes.jsa
  Reads from:
  Reads from:
                                      C:\Program Files\Java\jre7\lib\rt.jar
                                     C:\Program Files\Java\jre7\lib\ext\meta-index
  Reads from:
Windows Registry Events
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\7fb29afcdb4ab59eea2314061136ed82.exe
  Opens key:
                                      HKLM\system\currentcontrolset\control\terminal server
  Opens key:
                                      \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
options\secur32.dll
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
Opens key: options\advapi32.dll
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:
                                      HKLM\
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:
                                      HKLM\system\currentcontrolset\control\session manager
  Opens key:
                                      HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:
                                      \label{lem:hklmsoftware bolicies microsoft windows safer code identifiers \\
  Opens key:
                                      HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
Opens key: options\ntdll.dll
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
Opens key:
options\kernel32.dll
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:
                                      HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:
                                      HKLM\system\currentcontrolset\control\error message instrument
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\windows
```

HKLM\software\microsoft\windows\currentversion\explorer\performance

HKCU\software\policies\microsoft\control panel\desktop

HKLM\system\setup

HKCU\

Opens key:

Opens key:

Opens key:

Opens key:

Opens key: HKCU\control panel\desktop

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\comctl32.dll

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack

Opens key: HKLM\software\javasoft\java runtime environment Opens key: HKLM\software\javasoft\java development kit

Opens key: HKLM\software\javasoft\java runtime environment\1.7.0_02

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctf.dll

Opens key:

 $\label{lem:hklm} \begin{tabular}{ll} HKLM \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{tabular} which is a function of the compatibility \end{tabular} \begin{tabular}{ll} False \end{ta$

HKLM\software\microsoft\ctf\systemshared\ Opens key:

Opens key: HKCU\keyboard layout\toggle Opens key: HKLM\software\microsoft\ctf\

Opens key: HKLM\software\microsoft\windows nt\currentversion\imm

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\version.dll

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctfime.ime

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ole32.dll

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046}

Opens key: HKCU\software\microsoft\ctf

Opens key: HKLM\software\microsoft\ctf\systemshared

Opens key: Opens key: ${\tt HKLM \backslash system \backslash current control \backslash session \ manager \backslash app compatibility}$ Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the$

options\apphelp.dll

Opens key: HKLM\system\wpa\tabletpc Opens key: HKLM\system\wpa\mediacenter

 $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \label{lem:hklmsoftware} In the constant of the constant o$ Opens key:

HKLM\software\microsoft\windows Opens key:

nt\currentversion\appcompatflags\custom\7fb29afcdb4ab59eea2314061136ed82.exe

HKLM\software\policies\microsoft\windows\safer\levelobjects Opens key:

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens key:

 $\label{twarelook} HKLM \software \policies \microsoft \windows \safer \code identifiers \normalfootnote{\code} Add-tware \policies \microsoft \windows \safer \code identifiers \normalfootnote{\code} Add-tware \policies \microsoft \windows \safer \code identifiers \normalfootnote{\code} Add-tware \normalfootnote{\code} Add-twar$

be2efd2c1a33}

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key:

Opens key:

edd5fbde1328}

Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{7fb9cd2e-3076-4df9-a57b-4df9-a57$ b813f72dbb91}

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f} Opens key:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-1444, \ name \ na$

085bcc18a68d} Opens key:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc}

Opens key:

Opens key:

 $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths$ Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes

Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones$

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus has hes$

Opens key:

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens key: $\label{thm:condition} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \node \node\$ Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalfootnotes \normalfootnotes$

Opens key:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \addle \paths \end{tabular} \label{lem:hkcu}$

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus hashes$

Opens key:

```
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
    Opens key:
\label{thm:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalle 131072 \hashes \end{tabular}
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
    Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus has hes
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                                        HKCU\software\microsoft\windows\currentversion\explorer\shell folders
    Opens key:
                                                        \label{thm:local_hammon} \mbox{HKLM} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$}\mbox{$\mbox{$\mbox{$}\mbox{$\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbo
    Opens key:
options\msvcr100.dll
   Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
   Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
   Opens key:
                                                        \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/current/version/image file execution
options\wsock32.dll
    Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
    Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\drivers32
    Opens key:
Opens key:
                                                        \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
options\psapi.dll
   Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jvm.dll
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\verify.dll
   Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\java.dll
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\zip.dll
    Queries value:
                                                        HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
    Queries value:
                                                        HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
    Oueries value:
                                                        HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
    Oueries value:
                                                        HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                       HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
   Oueries value:
                                                       HKLM\software\microsoft\windows
nt\currentversion\compatibility32[7fb29afcdb4ab59eea2314061136ed82]
   Oueries value:
                                                       HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[7fb29afcdb4ab59eea2314061136ed82]
    Oueries value:
                                                        HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
    Queries value:
                                                        HKLM\system\setup[systemsetupinprogress]
                                                        HKCU\control panel\desktop[multiuilanguageid]
    Oueries value:
                                                        HKCU\control panel\desktop[smoothscroll]
    Queries value:
    Queries value:
Queries value:
                                                        HKLM \setminus software \setminus javas oft \setminus java \ runtime \ environment \setminus 1.7.0\_02[javahome]
    Oueries value:
                                                        HKLM\software\microsoft\ctf\systemshared[cuas]
    Oueries value:
                                                        HKCU\keyboard layout\toggle[language hotkey]
    Oueries value:
                                                        HKCU\keyboard layout\toggle[hotkey]
    Oueries value:
                                                        HKCU\keyboard layout\toggle[layout hotkey]
    Oueries value:
                                                        HKLM\software\microsoft\ctf[enableanchorcontext]
                                                        HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
    Oueries value:
                                                        HKLM\system\currentcontrolset\control\session
    Oueries value:
manager[criticalsectiontimeout]
    Queries value:
                                                        HKLM\software\microsoft\ole[rwlockresourcetimeout]
    Queries value:
                                                        HKCR\interface[interfacehelperdisableall]
    Queries value:
                                                        HKCR\interface[interfacehelperdisableallforole32]
                                                        HKCR\interface[interfacehelperdisabletypelib]
    Oueries value:
                                                        HKCR\interface\{00020400-0000-0000-c000-
    Oueries value:
000000000046}[interfacehelperdisableall]
                                                       HKCR\interface\{00020400-0000-0000-c000-
    Queries value:
00000000046}[interfacehelperdisableallforole32]
    Oueries value:
                                                        HKCU\software\microsoft\ctf[disable thread input manager]
    Queries value:
                                                        manager[safeprocesssearchmode]
                                                       {\tt HKLM \ } system \verb|\  current control set \verb|\  control \ \rangle session
   Oueries value:
manager\appcompatibility[disableappcompat]
                                                       HKLM\system\wpa\mediacenter[installed]
    Oueries value:
    Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [authenticode enabled]
    Queries value:
                                                        HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
    Queries value:
be2efd2c1a33}[itemdata]
    Queries value:
HKLM \ software \ \verb|voices| microsoft| windows \ safer \ \verb|code| identifiers \ \verb|voices| windows \ safer| \ s
be2efd2c1a33}[saferflags]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
```

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones$

Opens kev:

```
edd5fbde1328}[itemdata]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666
edd5fbde1328}[itemsize]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
    Queries value:
b813f72dbb91}[itemdata]
    Queries value
b813f72dbb91}[hashalg]
    Queries value:
b813f72dbb91}[itemsize]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
    Queries value:
7c29ddecae3f}[hashalg]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
    Queries value:
7c29ddecae3f}[saferflags]
    Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus (94e3e076-8f53-42a5-8411-144) + (14e3e076-8f53-42a5-8411-144) + (14e3e076-8f53-8411-144) + (14e3e076-8f53-8611-144) + (14
085bcc18a68d}[itemdata]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
    Oueries value:
085bcc18a68d}[itemsize]
    Queries value
085bcc18a68d}[saferflags]
    Oueries value:
b91490411bfc}[itemdata]
    Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus (dc971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-44eb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4c971ee5-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4-ae2e-4deb-4fe4
b91490411bfc}[hashalg]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
    Queries value:
b91490411bfc}[saferflags]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
    Queries value:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\shell
 folders[cache]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
    Oueries value:
                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
    Oueries value:
    Oueries value:
                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
    Oueries value:
                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
    Oueries value:
```

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Oueries value: $\label{lem:hklmsoftware} \verb+microsoft\+windows nt\-currentversion\+drivers32[midi3]$ Oueries value: $HKLM \backslash software \backslash microsoft \backslash windows \ nt \backslash current version \backslash drivers 32 [midi4]$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Queries value: $\label{lem:hklm} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\drivers32[aux6]} \\$

 $\label{lem:hklm} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\drivers32[aux7]} \\$

 $\label{lem:hklm} \mbox{ HKLM\software\mbox{\swindows} nt\currentversion\drivers32[aux8]} \\$

Queries value:

Oueries value:

Queries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 9] \\$ Queries value: Queries value: $\label{lem:hklmsoftware} \verb+MKLM\+ software \verb+\microsoft\+ windows nt\+ current version \verb+\drivers32[mixer]$ HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Queries value: $\label{lem:hklmsoftware} \mbox{\tt HKLM\software\mbox{\tt microsoft\windows}\ nt\current version\space{\tt version\mbox{\tt mage}\ file\ execution} \\$ options\jvm.dll[checkapphelp] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[desktop]

HKLM\software\microsoft\cryptography\rng[seed] Value changes: