Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 213, Task ID: 851

Task ID:	851
Risk Level:	4
Date Processed:	2016-04-28 13:10:57 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1fb48c879fc499067455e9ad068a9718.exe"

Sample ID:	213
Type:	basic
Owner:	admin
Label:	1fb48c879fc499067455e9ad068a9718
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	223624 bytes
MD5:	1fb48c879fc499067455e9ad068a9718
SHA256:	d7e46ddf69a86609545f7ab506913fb1713cef2ea203da964b50f15e9bb50858
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\1fb48c879fc499067455e9ad068a9718.exe ["c:\windows\temp\1fb48c879fc499067455e9ad068a9718.exe"]
Creates process:	C:\PROGRA~1\Java\jre7\bin\java.exe [c:\PROGRA~1\java\jre7\bin\java.exe -version]
Terminates process:	C:\PROGRA~1\Java\jre7\bin\java.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 mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.IDH
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\c:_windows_temp_1fb48c879fc499067455e9ad068a9718.exe

File System Events

Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\e4j1.tmp
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\hsperfdata_Admin
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin\832
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin\808
Opens:	C:\WINDOWS\Prefetch\1FB48C879FC499067455E9AD068A9-23E085D3.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83

```
  Opens:                   C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
  Opens:                   C:\WINDOWS\system32\imm32.dll
  Opens:                   C:\WINDOWS\WindowsShell.Manifest
  Opens:                   C:\WINDOWS\WindowsShell.Config
  Opens:                   C:\
  Opens:                   C:\WINDOWS
  Opens:                   C:\WINDOWS\Temp\1fb48c879fc499067455e9ad068a9718.exe
  Opens:                   C:\Documents and Settings
  Opens:                   C:\Documents and Settings\Admin\Local Settings
  Opens:                   C:\WINDOWS\.install4j\pref_jre.cfg
  Opens:                   C:\windows\jre\lib\
  Opens:                   C:\windows\jre\jre\bin\
  Opens:                   C:\windows\jre\bin\
  Opens:                   C:\Program Files\Java\jre7\jre\bin\
  Opens:                   C:\Program Files\Java\jre7\bin
  Opens:                   C:\WINDOWS\Temp\dcad433b-8ba7-4ef4-9827-28862a2ed395
  Opens:                   C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:                   C:\Program Files\Java\jre7\bin\java.exe
  Opens:                   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
  Opens:                   C:\PROGRA~1\java\jre7\bin\java.exe.Manifest
  Opens:                   C:\PROGRA~1\java\jre7\bin\java.exe.Config
  Opens:                   C:\WINDOWS\Prefetch\JAVA.EXE-19AF36F7.pf
  Opens:                   C:\WINDOWS\system32\shimeng.dll
  Opens:                   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:                   C:\Program Files\Java\jre7\bin\client\jvm.dll
  Opens:                   C:\PROGRA~1\java\jre7\bin\client\jvm.dll.2.Manifest
  Opens:                   C:\PROGRA~1\java\jre7\bin\client\jvm.dll.2.Config
  Opens:                   C:\WINDOWS\system32\wsock32.dll
  Opens:                   C:\WINDOWS\system32\ws2_32.dll
  Opens:                   C:\WINDOWS\system32\ws2help.dll
  Opens:                   C:\WINDOWS\system32\winmm.dll
  Opens:                   C:\WINDOWS\system32\psapi.dll
  Opens:                   C:\Program Files\Java\jre7\bin\verify.dll
  Opens:                   C:\Program Files\Java\jre7\bin\java.dll
  Opens:                   C:.hotspotrc
  Opens:                   C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
  Opens:                   C:\Program Files\Java\jre7\bin\zip.dll
  Opens:                   C:\Program Files\Java\jre7\lib
  Opens:                   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:                   C:.hotspot_compiler
  Opens:                   C:\Program Files\Java\jre7\lib\ext\meta-index
  Opens:                   C:\Program Files\Java\jre7\lib\ext
  Opens:                   C:\Documents and Settings\Admin\Local Settings\Temp\e4j1.tmp
  Opens:                   C:\program files\java\jre7\bin\hotspot\
  Opens:                   C:\program files\java\jre7\bin\client\jvm.dll.2.Manifest
  Opens:                   C:\program files\java\jre7\bin\client\jvm.dll.2.Config
  Opens:                   C:\WINDOWS\system32\msvcr100.dll
  Opens:                   C:\WINDOWS\Temp\1fb48c879fc499067455e9ad068a9718.vmoptions
  Opens:                   C:\WINDOWS\Temp\1fb48c879fc499067455e9ad068a9718.exe.vmoptions
  Opens:                   C:\WINDOWS\.install4j\
  Opens:                   C:\WINDOWS\system32\MSCTF.dll
  Opens:                   C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                   C:\WINDOWS\system32\ole32.dll
  Opens:                  C:\WINDOWS\system32\uxtheme.dll
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\e4j1.tmp
  Reads from:             C:\WINDOWS\Temp\1fb48c879fc499067455e9ad068a9718.exe
  Reads from:             C:\Program Files\Java\jre7\lib\i386\jvm.cfg
  Reads from:             C:\Program Files\Java\jre7\lib\meta-index
  Reads from:             C:\Program Files\Java\jre7\bin\client\classes.jsa
  Reads from:             C:\Program Files\Java\jre7\lib\rt.jar
  Reads from:             C:\Program Files\Java\jre7\lib\ext\meta-index
  Reads from:             C:\Documents and Settings\Admin\Local Settings\Temp\e4j1.tmp
  Deletes:                C:\Documents and Settings\Admin\Local Settings\Temp\e4j1.tmp
```

Windows Registry Events

```
  Creates key:            HKCU\software\ej-technologies\exe4j\pids\
  Creates key:            HKCU\software
  Creates key:            HKCU\software\ej-technologies
  Creates key:            HKCU\software\ej-technologies\exe4j
  Creates key:            HKCU\software\ej-technologies\exe4j\pids
  Creates key:            HKCU\software\ej-technologies\exe4j\jvms\c:/program
files/java/jre7/bin/java.exe
  Creates key:            HKCU\software\ej-technologies\exe4j\jvms
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\1fb48c879fc499067455e9ad068a9718.exe
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  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\user32.dll
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  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\shlwapi.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.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
  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\currentversion\explorer\performance
  Opens key:              HKCU\
  Opens key:              HKCU\software\policies\microsoft\control panel\desktop
  Opens key:               HKCU\control panel\desktop
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:               HKLM\software\javasoft\java development kit
  Opens key:               HKLM\software\javasoft\java runtime environment
  Opens key:               HKLM\software\javasoft\java runtime environment\1.7
  Opens key:               HKCU\software\ej-technologies\exe4j\jvms\c:/program
files/java/jre7/bin/java.exe
  Opens key:               HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:               HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  Opens key:               HKLM\system\wpa\tabletpc
  Opens key:               HKLM\system\wpa\mediacenter
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:               HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\java.exe
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:               HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key:               HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}
  Opens key:               HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  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:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  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:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  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\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\java.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
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:                HKLM\software\microsoft\windows nt\currentversion\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:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jvm.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
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
  Opens key:                HKCU\software\ej-technologies\exe4j\locatedjvms\
  Opens key:                HKLM\software\ej-technologies\exe4j\locatedjvms\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\1fb48c879fc499067455e9ad068a9718.exe
  Opens key:                 HKLM\software\microsoft\ctf\systemshared\
  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:                 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-c000-000000000046}
  Opens key:                 HKCU\software\microsoft\ctf
  Opens key:                 HKLM\software\microsoft\ctf\systemshared
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key:                 HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:                 HKCU\software\microsoft\ctf\langbaraddin\
  Opens key:                 HKLM\software\microsoft\ctf\langbaraddin\
  Queries value:             HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:             HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\compatibility32[1fb48c879fc499067455e9ad068a9718]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[1fb48c879fc499067455e9ad068a9718]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:             HKCU\control panel\desktop[multiuilanguageid]
  Queries value:             HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:             HKLM\software\javasoft\java runtime environment[currentversion]
  Queries value:             HKLM\software\javasoft\java runtime environment\1.7[javahome]
  Queries value:             HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:             HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
  Queries value:             HKLM\system\wpa\mediacenter[installed]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:             HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
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:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
  Queries value:
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]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\compatibility32[java]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[java]
```

```
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  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]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  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:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jvm.dll[checkapphelp]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
  Queries value:              HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:              HKCU\keyboard layout\toggle[language hotkey]
  Queries value:              HKCU\keyboard layout\toggle[hotkey]
  Queries value:              HKCU\keyboard layout\toggle[layout hotkey]
  Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:              HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:              HKCR\interface[interfacehelperdisableall]
  Queries value:              HKCR\interface[interfacehelperdisableallforole32]
  Queries value:              HKCR\interface[interfacehelperdisabletypelib]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:              HKCU\software\microsoft\ctf[disable thread input manager]
  Queries value:              HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:              HKCU\control panel\desktop[lamebuttontext]
  Sets/Creates value:         HKCU\software\ej-
technologies\exe4j\pids[c:\windows\temp\1fb48c879fc499067455e9ad068a9718.exe]
  Sets/Creates value:         HKCU\software\ej-technologies\exe4j\jvms\c:/program
files/java/jre7/bin/java.exe[lastwritetime]
  Sets/Creates value:         HKCU\software\ej-technologies\exe4j\jvms\c:/program
files/java/jre7/bin/java.exe[version]
  Value changes:              HKLM\software\microsoft\cryptography\rng[seed]
```