Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 1167, Task ID: 4095

Task ID: 4095 Risk Level:

2016-07-04 04:18:06 (UTC) Date Processed:

Processing Time: 61.31 seconds Virtual Environment: IntelliVM

"c:\windows\temp\RajivApp1.exe" **Execution Arguments:**

1167 Sample ID: Type: basic Owner: admin Label: RajivApp1.exe

2016-07-04 04:18:06 (UTC) Date Added: PE32:win32:gui:.net File Type: File Size: 8704 bytes

MD5: 9bde8983ac767c24755443627cda99bc

SHA256: ca0dcf72ce74fa1084255dae79a6a787eccf04152cfadd23f775a1671f1149cf

Description:

Pattern Matching Results

4 Reads process memory

2 Resolves local hostname

NET compiled executable

3 Long sleep detected

5 Query DNS from command line

4 Terminates process under Windows subfolder

Process/Thread Events

C:\WINDOWS\Temp\RajivApp1.exe ["c:\windows\temp\RajivApp1.exe"]
C:\WINDOWS\system32\cmd.exe ["cmd.exe"] Creates process:

Creates process:

Creates process: C:\WINDOWS\system32\nslookup.exe [nslookup WORKGROUP] Creates process: C:\WINDOWS\system32\nslookup.exe [nslookup __MSBROWSE_

Reads from process: PID:1600 C:\WINDOWS\system32\nslookup.exe PID:1596 C:\WINDOWS\system32\nslookup.exe Reads from process:

Terminates process: C:\WINDOWS\system32\nslookup.exe Terminates process: C:\WINDOWS\system32\cmd.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

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

1957994488-1003

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

1957994488-1003 \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-Creates mutex:

1957994488-1003

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

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003 \BaseNamedObjects\SHIMLIB_LOG_MUTEX Creates mutex:

Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.MJH \BaseNamedObjects\CorDBIPCSetupSyncEvent_360 Creates event: \BaseNamedObjects\userenv: User Profile setup event Creates event:

\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

Creates semaphore: \BaseNamedObjects\GdiplusFontCacheFileV1

File System Events

C:\WINDOWS\Prefetch\RAJIVAPP1.EXE-0FE9BC5A.pf Opens:

C:\Documents and Settings\Admin Opens: C:\WINDOWS\system32\mscoree.dll Opens: Opens: C:\WINDOWS\system32\imm32.dll C:\windows\temp\RajivApp1.exe.config Opens: Opens: C:\WINDOWS\Temp\RajivApp1.exe

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727 Opens:

Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll

Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Manifest Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Config

C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca

Opens:

C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-

ww_b80fa8ca\msvcr80.dll

Opens: C:\WINDOWS Opens:

Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config $\label{lem:config} C: \verb|\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch| config. C: \verb|\WINDOWS\Microsoft.NET\Framework\w2.0.50727\config\security.config.cch| config. C: \verb|\WINDOWS\Microsoft.NET\Framework\w2.0.50727\config\security.config.cch| config. C: \verb|\WINDOWS\Microsoft.NET\Framework\w2.0.50727\config\security.config.cch| config. C: \verb|\WINDOWS\Microsoft.NET\Framework\w2.0.50727\config\security.config.cch| config. C: \verb|\WINDOWS\Microsoft.NET\WINDOWS\WARD Washington Washingto$ Opens:

Opens:

```
\label{lem:c:windows} $$ C: \WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config\\ $$
      Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
                                                                                                   C:\WINDOWS\svstem32\shell32.dll
      Opens:
      Opens:
                                                                                                   C:\WINDOWS\system32\shell32.dll.124.Manifest
      Opens:
                                                                                                   C:\WINDOWS\system32\shell32.dll.124.Config
                                                                                                   C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
      Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                                                                                                  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
      Opens:
                                                                                                  C:\WINDOWS\WindowsShell.Manifest
      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
                                                                                                  {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Microsoft\CLR\ Security}
      Opens:
Config\v2.0.50727.42\security.config
                                                                                                   C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
      Opens:
Config\v2.0.50727.42\security.config.cch
                                                                                                  C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\index9c.dat
      Opens:
      Opens:
C: \verb|WINDOWS| assembly \verb|NativeImages_v2.0.50727_32 \verb|mscorlib|| 9 adb 89 fa 22 fd 5b 4 ce 43 3b 5a ca 7 fb 1b 07 \verb|mscorlib.ni.dll|| 1 for the control of the control of
      Opens:
                                                                                                   C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089
      Opens:
                                                                                                   C:\WINDOWS\Temp
      Opens:
                                                                                                   C:\WINDOWS\system32\rpcss.dll
      Opens:
                                                                                                   C:\WINDOWS\system32\MSCTF.dll
      Opens:
                                                                                                   C:\WINDOWS\system32\l_intl.nls
      Opens:
                                                                                                   C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
                                                                                                   C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll.2.Manifest
      Opens:
      Opens:
                                                                                                   C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll.2.Config
      Opens:
                                                                                                    C:\WINDOWS\assembly\pubpol1.dat
       Opens:
C: \verb|WINDOWS| assembly \verb|NativeImages_v2.0.50727_32 \\ System \\ aa7926460a336408c8041330ad90929d \\ System.ni.dll \\ above the property of the 
      Opens:
C: \windows \assembly \native Images\_v2.0.50727\_32 \system. Drawing \assembly \assem
C: \windows. Forms. \yindows. \y
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089
                                                                                                   C:\WINDOWS\assembly\GAC_MSIL\System\2.0.0.0_b77a5c561934e089
      Opens:
      Opens:
                                                                                                   \verb|C:\WINDOWS\assembly\GAC_MSIL\System.Drawing\2.0.0.0\_b03f5f7f11d50a3a| \\
      Opens:
                                                                                                   C:\WINDOWS\system32\uxtheme.dll
      Opens:
Opens:
C: \verb|WINDOWS| assembly \verb|GAC_MSIL| System. Windows. Forms \verb|| 2.0.0.0_b | 577a5c561934e089 \verb|System. Windows. Forms. dll. 101. Manifest | 10
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089\System.Windows.Forms.dll.101.Config
      Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c
      Opens:
 \verb| C: \WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.5512\_x-1.0.2600.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.551200.5512000.
ww_dfb54e0c\GdiPlus.dll
      Opens:
                                                                                                    C:\WINDOWS\system32\MSCTFIME.IME
                                                                                                    C:\Documents and Settings\Admin\Local Settings\Application
       Opens:
Data\GDIPFONTCACHEV1.DAT
      Opens:
                                                                                                   C:\WINDOWS\Fonts\micross.ttf
      Opens:
                                                                                                   C:\WINDOWS\system32\cmd.exe
      Opens:
                                                                                                   C:\WINDOWS\system32\apphelp.dll
      Opens:
                                                                                                   C:\WINDOWS\AppPatch\sysmain.sdb
      Opens:
                                                                                                    C:\WINDOWS\AppPatch\systest.sdb
      Opens:
                                                                                                   C:\WINDOWS\system32
      Opens:
                                                                                                   C:\WINDOWS\system32\cmd.exe.Manifest
      Opens:
                                                                                                   C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
      Opens:
      Opens:
                                                                                                   C:\WINDOWS\AppPatch
                                                                                                   C:\WINDOWS\system32\wbem
      Opens:
      Opens:
                                                                                                   C:\WINDOWS\WinSxS
                                                                                                   C:\WINDOWS\system32\ntdll.dll
      Opens:
      Opens:
                                                                                                   C:\WINDOWS\system32\kernel32.dll
      Opens:
                                                                                                   C:\WINDOWS\system32\unicode.nls
      Opens:
                                                                                                    C:\WINDOWS\system32\locale.nls
      Opens:
                                                                                                    C:\WINDOWS\system32\sorttbls.nls
      Opens:
                                                                                                   C:\WINDOWS\system32\msvcrt.dll
      Opens:
                                                                                                    C:\WINDOWS\system32\user32.dll
      Opens:
                                                                                                   C:\WINDOWS\system32\gdi32.dll
      Opens:
                                                                                                   C:\WINDOWS\system32\shimeng.dll
      Opens:
                                                                                                    C:\WINDOWS\AppPatch\AcGenral.dll
      Opens:
                                                                                                   C:\WINDOWS\system32\advapi32.dll
      Opens:
                                                                                                   C:\WINDOWS\system32\rpcrt4.dll
                                                                                                   C:\WINDOWS\system32\secur32.dll
      Opens:
      Opens:
                                                                                                   C:\WINDOWS\system32\winmm.dll
      Opens:
                                                                                                   C:\WINDOWS\system32\ole32.dll
       Opens:
                                                                                                    C:\WINDOWS\system32\oleaut32.dll
       Opens:
                                                                                                   C:\WINDOWS\system32\msacm32.dll
      Opens:
                                                                                                   C:\WINDOWS\svstem32\version.dll
```

Opens:

Opens:

C:\WINDOWS\system32\shlwapi.dll

C:\WINDOWS\system32\userenv.dll

Opens: C:\WINDOWS\system32\ctype.nls
Opens: C:\WINDOWS\system32\sortkey.nls
Opens: C:\WINDOWS\system32\wbem\wmic.exe

Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config

Opens: C:\WINDOWS\system32\winlogon.exe
Opens: C:\WINDOWS\system32\xpsp2res.dll
Opens: C:\Documents and Settings
Opens: C:\WINDOWS\system32\nslookup.exe

Opens: C:\WINDOWS\system32\nslookup.exe.Manifest
Opens: C:\WINDOWS\Prefetch\NSLOOKUP.EXE-160B1221.pf

Opens: C:\WINDOWS\system32\wsock32.dll Opens: C:\WINDOWS\system32\ws2_32.dll Opens: C:\WINDOWS\system32\ws2help.dll Opens: C:\WINDOWS\system32\mswsock.dll Opens: C:\WINDOWS\system32\dnsapi.dll C:\WINDOWS\system32\iphlpapi.dll Opens: Opens: C:\WINDOWS\system32\winrnr.dll Opens: C:\WINDOWS\system32\hnetcfg.dll Opens: C:\WINDOWS\system32\wshtcpip.dll C:\WINDOWS\system32\MSIMTF.dll Opens:

Reads from: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

Reads from: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

Network Events

DNS query: 8.8.8.8.in-addr.arpa

 DNS query:
 WORKGROUP

 DNS query:
 __MSBROWSE_

 Connects to:
 8.8.8.8:53

 Sends data to:
 8.8.8.8:53

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders

Creates key: HKLM\software\microsoft\fusion\gacchangenotification\default

Creates key: HKCU\software\microsoft\gdiplus

Creates key: HKCU\software\microsoft\multimedia\audio

Creates key: HKCU\software\microsoft\multimedia\audio compression manager\
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority

v4.00

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

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

Opens key: HKLI options\rajivapp1.exe

Opens key: HKLM\system\currentcontrolset\control\safeboot\option

Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\session manager

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

options\secur32.dll

Opens key:

Opens key:

Opens key: $\mbox{HKLM\software\mbox{\mbox{microsoft\windows nt\currentversion\image file execution options\script{\mbox{\m}\m}\mbox{\mbox{\m}\mbox{\mbox{\m}\m}\mbox{$

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

options\advapi32.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon

Opens key: HKLM\

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

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\mscoree.dll
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\.netframework

HKLM\software\microsoft\windows nt\currentversion\image file execution

HKLM\software\microsoft\windows nt\currentversion\image file execution

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

options\shlwapi.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\currentversion\explorer\performance

Opens key: HKCU\

```
Opens key:
                                                                                                                                                   HKCU\software\microsoft\.netframework\policy\standards
           Opens key:
                                                                                                                                                   HKLM\software\microsoft\.netframework\policy\standards
           Opens key:
                                                                                                                                                   HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727
          Opens key:
                                                                                                                                                 HKCU\software\policies\microsoft\control panel\desktop
          Opens key:
                                                                                                                                                 HKCU\control panel\desktop
          Opens key:
HKLM \ software \ microsoft \ windows \ current version \ side by side \ assembly storage roots
          Opens key:
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\msvcr80.dll
         Opens key:
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\mscorwks.dll
          Opens key:
                                                                                                                                                   HKCU\software\microsoft\.netframework
          Opens key:
                                                                                                                                                 HKLM\software\microsoft\fusion
          Opens key:
                                                                                                                                                   HKCU\software\microsoft\fusion
         Opens key:
\label{thm:local_hammon} \begin{tabular}{l} HKLM \end{tabular} Software \end{tabular} in the three \end{tabular} is a constant of the three \end{tabular} All the three \end{tabular} is a constant \end{tabular} in the three \end{tabular} All the three \end{tabular} in the three \end{tabular} All the three \end{tabular} in the three \end{tabular} in the three \end{tabular} All three \end{tabular} All three \end{tabular} All three \end{tabular} in the three \end{tabular} All three \
          Opens kev
HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet
          Opens key:
HKLM \ software \ microsoft \ .net framework \ security \ policy \ extensions \ named permission sets \ local intranet
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
         Opens key:
 1757981266-507921405-1957994488-1003
          Opens key:
                                                                                                                                                 \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
 options\shell32.dll
          Opens key:
                                                                                                                                                   HKLM\system\setup
          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\microsoft\.netframework\v2.0.50727\security\policy
          Opens key:
                                                                                                                                                   HKLM \verb|\software\microsoft\fusion\native images index \verb|\v2.0.50727_32|
          Opens key:
                                                                                                                                                 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c
          Opens kev:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus ni \setminus 181938c6 \setminus 7950e2c5
          Opens key:
Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
         Opens kev:
 options\ole32.dll
          Opens key:
                                                                                                                                                   HKLM\software\microsoft\ole
          Opens key:
                                                                                                                                                 HKCR\interface
                                                                                                                                                   HKCR\interface\{00020400-0000-0000-c000-00000000046}
          Opens key:
         Opens key:
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\mscorlib.ni.dll
          Opens key:
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
          Opens key:
                                                                                                                                                   HKLM\software\microsoft\ctf\compatibility\rajivapp1.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 \ fusion \ native images index \ v2.0.50727\_32 \ ni\ 38c56119 \ 1d3ee2d7
           Opens key:
                                                                                                                                                 HKLM\software\microsoft\net framework setup\dotnetclient\v3.5
                                                                                                                                                 HKLM\software\microsoft\strongname
           Opens kev:
          Opens key:
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorjit.dll
          Opens key:
                                                                                                                                                 HKLM\software\microsoft\fusion\publisherpolicy\default
          Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 61e7e666 \setminus c991064 \setminus 13e8 \setminus c991064 \setminus 13e
         Opens kev
HKLM \setminus software \\ \mbox{microsoft} \\ \mbox{fusion} \\ \mbox{native images index} \\ \mbox{v2.0.50727\_32} \\ \mbox{il} \\ \mbox{475dce40} \\ \mbox{3856a4e} \\ \mbox{10} \\ \mbox{10} \\ \mbox{equation} \\ \mbox{equation
          Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 19ab8d57 \ 61dc497f \ 61dc4
          Opens key:
Opens kev:
Opens key:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ il\ 41c04c7e\ 286a445d\ 24ex
          Opens key:
 Opens key:
HKLM \verb|\software\microsoft| fusion \verb|\nativeimagesindex| v2.0.50727\_32 \verb|\since| i1 \verb|\c991064| 3880e29a \verb|\since| i1 \verb|\since| i2 \verb|\since| i2 \verb|\since| i2 \verb|\since| i3 \verb|\since| i4 \verb|\since| i3 \verb|\since| i4 \verb|
          Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 7f50fe4f \ 7f50
         Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i1 \setminus 3f50fe4f \setminus 7540f5be \setminus 7540
         Opens key:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ ni\ 3cca06a0 \ 6dc7d4c0 \ 170 \ next \ ne
          Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 6dc7d4c0\ 7cd935b4 \ early \ described a software \ described \ described a software \ described \ describe
           Opens key:
                                                                                                                                                 HKLM\software\microsoft\.netframework\policy\aptca
          Opens kev:
                                                                                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
          Opens key:
                                                                                                                                                 HKCU\software\microsoft\windows\currentversion\thememanager
```

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\system.ni.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\system.drawing.ni.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\system.windows.forms.ni.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\gdiplus.dll Opens key: HKLM\hardware\devicemap\video HKLM\software\microsoft\windows nt\currentversion\imm Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll Opens kev HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime HKCU\software\microsoft\ctf Opens key: ${\tt HKLM \ } software \verb|\ microsoft \verb|\ ctf \verb|\ systems \ hared$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\fonts Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink Opens key: HKCU\eudc\1252 Opens key: $\label{lem:hklmsoftware} \verb+MKLM+ software+ \verb+microsoft+ windows nt+ current version+ fontsubstitutes$ Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls 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 kev: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\cmd.exe Opens key: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus app compatflags$ 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 kev: be2efd2c1a33} Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328} Opens kev: b813f72dbb91} Opens key: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16$ 7c29ddecae3f} Opens key 085bcc18a68d} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc} Opens key: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 0 \ vert zones$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens kev 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: Opens key: $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers \verb|\software| length of the microsoft \|\software| length of the microsoft \|\soft$ 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: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 262144 \ paths$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens kev HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens key: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$ 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 \ code identifiers \ his \ paths
   Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens kev:
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
                                                \label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell} folders}
   Opens key:
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
  Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
   Opens key:
                                                {\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}
options\shimeng.dll
  Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
   Opens kev:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
   Opens key:
                                                \label{lem:hklmsoftware} $$HKLM\software\microsoft\windows nt\currentversion\image file execution $$
options\userenv.dll
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\drivers32
   Opens key:
Opens key:
                                                HKLM\software\microsoft\oleaut
   Opens key:
                                                HKLM\software\microsoft\oleaut\userera
   Opens key:
                                                HKLM\software\microsoft\audiocompressionmanager\drivercache
   Opens kev:
Opens key:
HKLM \verb|\software\m| icrosoft \verb|\audiocompression| manager \verb|\driver| cache \verb|\m| sacm. msadpcm | msadpcm
                                                HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. msg 711
   Opens key:
   Opens key:
HKLM \verb|\software\m| icrosoft\audio compression manager \verb|\drivercache\m| sacm. msgsm610
   Opens key:
                                                HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.trspch
   Opens key:
                                                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
   Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
   Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} soft \end{tabular} and \begin{tabular}{ll} soft \end{tabular} are the label{tabular} are the lab
   Opens key:
                                                HKLM \ \ software \ \ \ iac 2
   Opens key:
                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ audio compression manager\+ driver cache\+ msacm. 13 acm
   Opens key:
                                                HKLM\system\currentcontrolset\control\mediaresources\acm
   Opens key:
                                                HKLM\system\currentcontrolset\control\productoptions
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
   Opens key:
                                                HKLM\software\policies\microsoft\windows\system
                                                {\tt HKLM \ }. \\
   Opens key:
   Opens key:
                                                HKLM\software\microsoft\rpc
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\rajivapp1.exe\rpcthreadpoolthrottle
   Opens kev:
                                                HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                                HKCU\software\classes\
   Opens key:
                                                HKCU\software\classes\appid\rajivapp1.exe
   Opens key:
                                                HKCR\appid\rajivapp1.exe
   Opens key:
                                                HKLM\system\currentcontrolset\control\computername
   Opens key:
                                                HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens kev:
                                                HKLM\svstem\currentcontrolset\control\lsa
   Opens key:
                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\xpsp2res.dll
   Opens key:
                                                HKCU\software\policies\microsoft\windows\system
                                                HKLM\software\microsoft\command processor
   Opens key:
   Opens key:
                                                HKCU\software\microsoft\command processor
   Opens key:
                                                HKLM\system\currentcontrolset\control\nls\locale
                                                HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
   Opens key:
   Opens key:
                                                HKLM\system\currentcontrolset\control\nls\language groups
   Opens key:
                                                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\nslookup.exe
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\nslookup.exe
   Opens key:
                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\ws2help.dll
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Opens kev:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wsock32.dll
   Opens key:
                                                {\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}
```

```
options\mswsock.dll
```

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

options\dnsapi.dll

Opens kev: HKLM\svstem\currentcontrolset\services\dnscache\parameters Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004

Opens key:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries$ Opens key:

Opens key:

Opens key:

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004

Opens key:

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000007 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000000 Opens key:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ catalog_entries \ 1000000000010$ Opens kev:

 $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol_catalog_entries \ \ 000000000011$ Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004

Opens kev:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ name space_catalog \ catalog_entries$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000 Opens key:

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

options\nslookup.exe\rpcthreadpoolthrottle Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\iphlpapi.dll

HKLM\system\currentcontrolset\services\tcpip\linkage Opens key: Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters

Opens key:

c7d49d7cecdc}

Opens key: HKLM\software\policies\microsoft\system\dnsclient

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

options\wldap32.dll

Opens key: HKLM\system\currentcontrolset\services\ldap

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

options\winrnr.dll

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file \ execution}$

options\hnetcfg.dll

Opens key: HKLM\software\microsoft\rpc\securityservice

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens kev: HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

Opens key: HKCU\software\microsoft\ctf\langbaraddin\ HKLM\software\microsoft\ctf\langbaraddin\ Opens key:

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mscoree.dll[checkapphelp]

HKLM\system\currentcontrolset\control\session Oueries value:

manager\appcompatibility[disableappcompat]

Oueries value: HKLM\software\microsoft\.netframework[installroot] Queries value: HKLM\software\microsoft\.netframework[clrloadlogdir] Queries value: HKLM\software\microsoft\.netframework[onlyuselatestclr]

HKLM\software\microsoft\windows Oueries value: nt\currentversion\gre_initialize[disablemetafiles] Queries value: HKLM\software\microsoft\windows

```
nt\currentversion\compatibility32[rajivapp1]
   Queries value:
                                               HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[rajivapp1]
   Oueries value:
                                               HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
   Oueries value:
                                               HKCU\control panel\desktop[multiuilanguageid]
   Queries value:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorwks.dll[checkapphelp]
   Queries value:
                                               HKLM\software\microsoft\.netframework[gcstressstart]
   Queries value:
                                               HKLM\software\microsoft\.netframework[gcstressstartatjit]
   Oueries value:
                                               HKLM\software\microsoft\.netframework[disableconfigcache]
   Oueries value:
                                               HKLM\software\microsoft\fusion[cachelocation]
   Oueries value:
                                               HKLM\software\microsoft\fusion[downloadcachequotainkb]
                                               HKLM\software\microsoft\fusion[enablelog]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\fusion[logginglevel]
   Queries value:
                                               HKLM\software\microsoft\fusion[forcelog]
                                               HKLM\software\microsoft\fusion[logfailures]
   Oueries value:
   Oueries value:
                                               HKLM\software\microsoft\fusion[versioninglog]
   Oueries value:
                                               HKLM\software\microsoft\fusion[logresourcebinds]
                                               HKLM\software\microsoft\fusion[uselegacyidentityformat]
   Queries value:
   Queries value:
                                               HKLM\software\microsoft\fusion[disablemsipeek]
                                               HKLM\software\microsoft\fusion[noclientchecks]
   Queries value:
   Oueries value:
                                               HKLM\system\setup[systemsetupinprogress]
   Queries value:
                                               HKCU\control panel\desktop[smoothscroll]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Queries value:
folders[appdata]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 [latest index]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ index 9c[nius agemask]
   Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\index9c[ilusagemask]
   Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[displayname]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i181938c6 \setminus 7950e2c5 \setminus 8[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\ni\181938c6\7950e2c5\8[configstring]
   Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 181938c6 \ 7950e2c5 \ 8[evalation data]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[status]
   Queries value:
HKLM \label{lem:hklm} Software \\ \mbox{microsoft} fusion \\ \mbox{native} images index \\ \mbox{v2.0.50727\_32} \\ \mbox{ni} 181938c6 \\ \mbox{7950e2c5} \\ \mbox{8[ildependencies]} \\ \mbox{microsoft} \\ \mbox
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[nidependencies]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 181938c6 \ 7950e2c5 \ 8 \ [missing dependencies]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 7950e2c5 \ 3838a3a4 \ 8 \ [display name]
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[status]
   Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il \ 7950e2c5 \ 3838a3a4 \ 8 \ [modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[sig]
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 7950e2c5 \ 3838a3a4 \ 8[last mod time]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
   Queries value:
                                               HKLM\software\microsoft\ole[rwlockresourcetimeout]
   Queries value:
                                               HKCR\interface[interfacehelperdisableall]
                                               HKCR\interface[interfacehelperdisableallforole32]
   Queries value:
   Oueries value:
                                               HKCR\interface[interfacehelperdisabletypelib]
   Oueries value:
                                               HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
                                               HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableallforole32]
                                               HKLM\software\microsoft\ctf\systemshared[cuas]
   Queries value:
                                               HKCU\keyboard layout\toggle[language hotkey]
   Oueries value:
   Oueries value:
                                               HKCU\keyboard layout\toggle[hotkey]
   Queries value:
                                               HKCU\keyboard layout\toggle[layout hotkey]
                                               HKLM\software\microsoft\ctf[enableanchorcontext]
   Queries value:
   Queries value:
                                               HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                                               HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\fusion\publisherpolicy\default[index1]
   Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \begin{tabul
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 61e7e666 \ c991064 \ 13[display name]
   Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 61e7e666 \ c991064 \ 13[configmask]
```

- Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configstring]
 Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[mvid]
 Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[evalationdata]
 Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \subseted in the lates of th$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[nidependencies] Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[missingdependencies]
 Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[displayname]
 Oueries value:
- $\label{lem:hklm} $HKLM \sim \max_{n=0} \frac{1}{475dce40 \cdot 3856a4e \cdot 10[status]}$ Oueries value:$
- $\label{local-bound} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727_32 \normalized 10 \normalize$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[sig]
 Oueries value:
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{images} index\v2.0.50727_32\il\475dce40\3856a4e\10[last mod time] \\ Queries\ value:$
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} in a tive images in dex $$\v2.0.50727_32\il\19ab8d57\61dc497f\6[status] $$ Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \end{area} Hklm \software \end{area} All 19ab8d57 \software \end{area} Oueries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[sig]
 Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-ham} HKLM \software \microsoft \sion \native images in dex \normalized by 2.0.50727_32 \normalized \normalized$
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[last mod time] \\ Oueries\ value:$
- $\label{lem:hklmsoftware} HKLM \software \mbox{\le 1.0.50727_32\il\424bd4d8\2bfe65de\5[status] } Queries \ value:$
- $\label{local-bound} HKLM\software\microsoft\fusion\native images in dex $$v2.0.50727_32\il\424bd4d8\2bfe65de\5[modules]$ Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \signature images in dex \signature \signature$
- $\label{local-bound} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_32\il\424bd4d8\2bfe65de\5[last mod time] \\ Queries value:$
- $\label{local-equation} HKLM software \mbox{$\mbox{}\mbox{$\mbox{\mbox
- $\label{local-equation} HKLM \software \microsoft \fusion \native images in dex \normalized 2.0.50727_32 \normalized 1.41 \co4c7e \normalized 2.4[status] Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \end{area} HKLM \software \end{area} Alticut \software \end{area} Alticut \software \end{area} Alticut \software \end{area} Alticut \software \software \software \end{area} Alticut \software \so$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-equation} HKLM \software \mbox{$\mbox{$\mathbb{N}$} $$ in $\mbox{$\mathbb{N}$} $$ in \mbo
- $\label{local-bound} HKLM\software\microsoft\fusion\native\magesindex\v2.0.50727_32\il\aced59c5\32e43dd1\d[displayname] Oueries\ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[status] Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_32 \il\aced59c5\32e43dd1 \d[modules] Queries value:$
- $\label{lem:hklmsoftware} HkLM \software \end{array} Hklm \software \end{array} All \software \software \end{array} All \software \software \end{array} All \software \end{array} All \software \soft$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[lastmodtime]
 Oueries value:
- $\label{local-prop} HKLM \software \end{align*} HKLM \software \end{align*} With \software \end{align*} 10.50727_32 \end$
- $\label{lem:hklmsoftware} HKLM \software \mbox{\le 10.50727_32\il\c991064\3880e29a\1d[status] } Queries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\c991064\3880e29a\1d[modules]
 Queries value:
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727_32\label{local-equation} 132\label{local-equation} In the continuous co$
- $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} irrosoft \subseted in a tive images in dex \subseted value:} \\ Queries \subseted value:$
- $\label{local-hamilton} HKLM \setminus software \setminus irrosoft \setminus fusion \setminus native images in dex \setminus v2.0.50727_32 \setminus i130bc7c4f \setminus 3f50fe4f \setminus 7[configmask]$

```
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configstring]
     Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 7[mvid]
     Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 7[evalation data]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus id=10.50724f \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus id=10.50727\_32 \setminus i
     Queries value:
HKLM \ software \ `microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ini \ 30bc7c4f \ 7[ildependencies]
     Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 7[nidependencies]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i \setminus 30bc7c4f \setminus 3f50fe4f \setminus 7[missing dependencies]
    Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i1 \setminus 3f50 fe4f \setminus 7f540 f5be \setminus 7[display name]
     Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 3f50fe4f\ 7540f5be\ 7[status]
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 3f50fe4f\ 7540f5be\ 7[modules]
    Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ i1\ 3f50fe4f\ 7540f5be\ 7[sig]
     Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i1 \setminus 3f50fe4f \setminus 7f540f5be \setminus 7[last modtime]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus mi \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 17[display name]
     Oueries value:
HKLM \ software \ |\ microsoft \ fusion \ |\ mative images index \ |\ v2.0.50727\_32 \ |\ mi\ account \ |\ mask] |
     Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[configstring]
      Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni\ 3cca06a0\ 6dc7d4c0\ 17[mvid]
     Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 17[evalation data]
     Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 17[status]
      Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 17[ildependencies]
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 17[nide pendencies]
      Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca 06a0 \ 6dc 7d4c0 \ 17 \ [missing dependencies]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i1 \setminus 6dc7d4c0 \setminus 7cd935b4 \setminus e[displayname]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 6dc7d4c0\ 7cd935b4 \ e[status]
     Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il \ 6dc7d4c0 \ 7cd935b4 \ e[modules]
     Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\6dc7d4c0\7cd935b4\e[sig]
     Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i1 \setminus 6dc7d4c0 \setminus 7cd935b4 \setminus e[last modtime]
HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
     Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.drawing,2.0.0.0,,b03f5f7f11d50a3a,msil]
     Oueries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} in \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Wi
     Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
HKLM\software\microsoft\fusion\gacchangenotification\default[system.configuration,2.0.0.0,,b03f5f7f11d50a3a,msil]
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchangenotification \setminus default[system.deployment, 2.0.0.0, , b03f5f7f11d50a3a, msil] + (b1) + (b2) + (b2) + (b3) +
     Queries value:
Queries value:
HKLM \label{lem:hklm} In the large of the 
    Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil]
      Oueries value:
                                                                               HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
                                                                               HKCU\control panel\desktop[lamebuttontext]
      Queries value:
      Queries value:
                                                                               HKLM\software\microsoft\.netframework[dbgjitdebuglaunchsetting]
     Queries value:
                                                                               HKLM\software\microsoft\.netframework[dbgmanageddebugger]
     Oueries value:
                                                                               HKLM\hardware\devicemap\video[maxobjectnumber]
     Oueries value:
                                                                               HKLM\hardware\devicemap\video[\device\video0]
     Queries value:
                                                                               HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
                                                                               HKCU\software\microsoft\ctf[disable thread input manager]
      Queries value:
      Queries value:
                                                                               HKCU\software\microsoft\gdiplus[fontcachepath]
```

 $Queries\ value: \\ HKLM\ software\ policies\ microsoft\ windows\ safer\ code identifiers\ 0\ paths\ \{dda3f824-d8cb-441b-834d-be2efd2c1a33\}[itemdata]$

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]

HKLM\system\currentcontrolset\control\session

HKLM\system\wpa\mediacenter[installed]

 $HKLM \verb| software \verb| policies \verb| microsoft \verb| windows \verb| safer \verb| code identifiers [authenticode enabled]|$

Queries value:

Queries value:

Oueries value:

Queries value:

manager[safeprocesssearchmode]

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834dbe2efd2c1a33}[saferflags]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemdata]

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{349d35ab-37b5-462f-9b89-4666f-9b89-46666f-9b89-4666$ edd5fbde1328}[hashalg]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemsize]

Oueries value:

edd5fbde1328}[saferflags]

Oueries value:

b813f72dbb91}[itemdata]

b813f72dbb91}[hashalg]

Oueries value:

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[saferflags]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16$ 7c29ddecae3f}[hashalg]

Oueries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16$ 7c29ddecae3f}[itemsize]

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16$ 7c29ddecae3f}[saferflags]

Oueries value:

085bcc18a68d}[itemdata]

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-8411-64e3e076-8f53-42a5-86e3e076-8f53-42a5-86e3e076-8f53-42a5-86e3e076-8f53-86e3e076-8f55-86e3e076-8f55-86e3e076-8f55-86e56-8$ 085bcc18a68d}[hashalg]

Queries value:

085bcc18a68d}[itemsize]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]

Queries value:

b91490411bfc}[itemdata]

Oueries value:

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[itemsize]

Oueries value:

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

Oueries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [default level]$

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]

HKCU\software\microsoft\windows\currentversion\explorer\shell Queries value:

folders[cache]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]

HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Oueries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Oueries value:

Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]

```
Queries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
      Queries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
      Oueries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
      Oueries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
      Queries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
      Queries value:
      Queries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
      Queries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
      Oueries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
      Oueries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
      Oueries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
      Oueries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
      Queries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
      Queries value:
      Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
      Oueries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
      Queries value:
      Queries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
      Queries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
      Oueries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
      Oueries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
      Queries value:
      Queries value:
                                                                                       HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 7]
      Queries value:
                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
      Oueries value:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
                                                                                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ multimedia\+ audio\+ [system for mats]
      Oueries value:
      Queries value:
                                                                                       HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
      Queries value:
HKLM \verb|\software| microsoft| audio compression manager \verb|\driver| cache| msacm.ima adpcm[a for mattag cache] and the sacm of the sacm of
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
                                                                                       HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\drivers32[msacm.msadpcm]
      Queries value:
HKLM \label{lem:hklm} \\ HKLM \label{lem:hklm} HKLM \label{lem:hklm} \\ HKLM \label{lem:hkklm} \\ HKLM \label{lem:h
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
      Oueries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. msadpcm[cfilter tags]
      Oueries value:
                                                                                       HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
      Oueries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. msg711[aformattagcache]
      Oueries value:
Queries value:
                                                                                       HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msgsm610]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
      Oueries value:
HKLM \label{lem:hkkm} \label{lem:hkkm} HKLM \label{lem:hkkm} White \label{lem:hkkm} White \label{lem:hkkm} White \label{lem:hkkm} White \label{lem:hkkm} White \label{lem:hkkm} White \label{lem:hkkm} \label{lem:hkkm} \label{lem:hkkm} HKLM \label{lem:hkkm} White \labellh{lem:hkkm} Wh
      Queries value:
HKLM \verb|\software\microsoft| audio compression manager \verb|\drivercache| msgsm610[a for mattag cache]| and the same msgsm610[a formattag cache]| and the same
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
                                                                                       HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\drivers32[msacm.trspch]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
      Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} which is a constraint of the lemma substitution of the lemm
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
      Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.trspch[cfiltertags]
                                                                                       HKLM\software\microsoft\windows
      Queries value:
nt\currentversion\drivers32[msacm.msg723]
      Oueries value:
HKLM \verb|\software\microsoft\audiocompression| manager \verb|\drivercache\msacm.msg723[fdwsupport]| \\
      Oueries value:
HKLM \verb|\software\microsoft\audiocompression manager\driver cache \verb|\msg723[cformattags]| \\
      Oueries value:
HKLM \verb|\software\microsoft\audiocompression| manager \verb|\driver| cache \verb|\msacm.msg723[aformattagcache]| and the substitution of the substitution
      Oueries value:
```

 $HKLM \verb|\software\microsoft| audio compression manager \verb|\drivercache\msacm.msg723[cfiltertags]| and the first constant of the firs$

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]

Queries value:

```
Queries value:
                                                        HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
   Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cformattags]
    Queries value:
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
   Oueries value:
                                                        HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl_anet]
HKLM \label{lem:hklm} \\ HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} \\ White \label{lem:hkklm} HKLM \label{lem:hkklm} \\ White \label{lem:hkklm} White \label{lem:hkklm} \\ White \label{lem:hkklm} HKLM \label{lem:hkklm} \\ White \label{lem:hkklm} White \label{lkklm} \\ White \label{lkklm} \\ White \label{lkklm} White \label{lkklm} \\ W
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
    Oueries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} which is a more achieved and incompression manager \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lkm} \label{
                                                        HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
   Queries value:
   Oueries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
   Oueries value:
HKLM \verb|\software\microsoft| audio compression manager \verb|\drivercache\msacm.iac2[cfiltertags]| \\
    Queries value:
                                                         HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
    Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. 13 acm [cformattags]
   Queries value:
HKLM \verb|\software\microsoft\audiocompression manager\driver cache\mbox{|} msacm. 13 acm [a formattag cache] and the sack of t
    Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
                                                        HKCU\software\microsoft\multimedia\audio compression
   Oueries value:
manager\msacm[nopcmconverter]
   Queries value:
                                                        \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+multimedia \verb+audio compression manager \verb+\priority+ \\
v4.00[priority1]
                                                        HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\winlogon[userenvdebuglevel]
                                                        HKLM\software\microsoft\windows
   Oueries value:
\verb|nt\current| version \verb|winlogon[chkaccdebuglevel]|
    Queries value:
                                                        {\tt HKLM \ } system \verb| current control set \verb| control \ | product options[product type]|
    Queries value:
                                                        HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
                                                        HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Queries value:
folders[local settings]
                                                        HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\winlogon[rsopdebuglevel]
    Queries value:
                                                        HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
    Oueries value:
                                                        HKLM\software\microsoft\rpc[maxrpcsize]
                                                        HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Oueries value:
   Oueries value:
                                                        HKLM\software\microsoft\ole[defaultaccesspermission]
   Queries value:
{\tt HKLM \ } system \verb| current control \verb| lsa[every one includes a nonymous] \\
    Queries value:
    Oueries value:
                                                        HKLM\software\microsoft\command processor[disableunccheck]
   Queries value:
                                                        HKLM\software\microsoft\command processor[enableextensions]
   Oueries value:
                                                        HKLM\software\microsoft\command processor[delayedexpansion]
   Oueries value:
                                                        HKLM\software\microsoft\command processor[defaultcolor]
   Queries value:
                                                         HKLM\software\microsoft\command processor[completionchar]
                                                        {\tt HKLM \setminus software \setminus microsoft \setminus command processor[pathcompletion char]}
    Queries value:
    Queries value:
                                                         HKLM\software\microsoft\command processor[autorun]
    Queries value:
                                                         HKCU\software\microsoft\command processor[disableunccheck]
    Oueries value:
                                                         HKCU\software\microsoft\command processor[enableextensions]
    Oueries value:
                                                         HKCU\software\microsoft\command processor[delayedexpansion]
    Oueries value:
                                                        HKCU\software\microsoft\command processor[defaultcolor]
                                                         HKCU\software\microsoft\command processor[completionchar]
    Queries value:
    Queries value:
                                                         HKCU\software\microsoft\command processor[pathcompletionchar]
                                                         HKCU\software\microsoft\command processor[autorun]
   Queries value:
    Oueries value:
                                                         HKLM\system\currentcontrolset\control\nls\locale[00000409]
    Oueries value:
                                                        HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
                                                        HKLM\software\microsoft\windows
nt\currentversion\compatibility32[nslookup]
                                                        HKLM\software\microsoft\windows nt\currentversion\ime
   Queries value:
compatibility[nslookup]
   Oueries value:
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable adapter domain name]
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [used omain named evolution]
   Oueries value:
```

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [updatezone exclude file]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version] $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 [serial_access_num]$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Queries value:
- $HKLM \ system \ current controls et \ excises \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 00000000000007 \ [packed catalog item] \\ Queries \ value:$
- $\label{lem:hklmsystem} HKLM \end{substitute} Hklm \end{substitute} A log-entries \end{substitute} O log-entries \end{subst$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog \shape \current \shape \shape$
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 000000000001 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog \ services \ value;$ Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 000000000001 [supported name space] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[dnslookuporder]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[domain]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpsearchlist]

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc\censbledbcnl

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[leaseobtainedtime]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[leaseterminatestime]

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpserver]

. HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[queryadaptername]

Queries value:

c7d49d7cecdc}[disableadapterdomainname]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationenabled]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registeradaptername]

Oueries value:

c7d49d7cecdc}[registrationmaxaddresscount]

Queries value:

c7d49d7cecdc}[maxnumberofaddressestoregister]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[domain]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpdomain]

Queries value:

c7d49d7cecdc}[ipautoconfigurationenabled]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[addresstvpe]

Queries value:

c7d49d7cecdc}[nameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpnameserver]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]

Oueries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity] Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]

Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]

HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes:

folders[appdata]

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

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]