Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 1167, Task ID: 4094

Task ID: 4094 Risk Level: 5

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

Processing Time: 62.47 seconds
Virtual Environment: IntelliVM

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

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

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

MD5: 9bde8983ac767c24755443627cda99bc

SHA256: ca0dcf72ce74fa1084255dae79a6a787eccf04152cfadd23f775a1671f1149cf

Description: None

Pattern Matching Results

5 Query DNS from command line 2 .NET compiled executable

4 Terminates process under Windows subfolder

4 Reads process memory

2 Resolves local hostname

Process/Thread Events

Creates process: C:\windows\temp\RajivApp1.exe ["C:\windows\temp\RajivApp1.exe"]

Creates process: C:\Windows\system32\cmd.exe ["cmd.exe"]

Creates process: \SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe

0xffffffff]

Creates process: C:\Windows\system32\nslookup.exe [nslookup WORKGROUP]
Creates process: C:\Windows\system32\nslookup.exe [nslookup _MSBROWSE_

Reads from process: PID:856 C:\Windows\System32\nslookup.exe Reads from process: PID:1592 C:\Windows\System32\nslookup.exe

Terminates process: C:\Windows\System32\nslookup.exe
Terminates process: C:\Windows\System32\cmd.exe
Terminates process: C:\Windows\System32\conhost.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \BaseNamedObjects\CorDBIPCSetupSyncEvent_3004

File System Events

Creates: C:\Users\Admin

Creates: C:\Users\Admin\AppData\Roaming

Opens: C:\Windows\Prefetch\RAJIVAPP1.EXE-4C2BBC3A.pf

Opens: C:\Windows\System32

C:\Windows\System32\mscoree.dll Opens: Opens: C:\Windows\System32\apphelp.dll Opens: C:\Windows\System32\version.dll Opens: C:\Windows\Temp\RajivApp1.exe Opens: C:\Windows\System32\ntdll.dll C:\Windows\System32\kernel32.dll Opens: C:\Windows\System32\KernelBase.dll Opens: Opens: C:\Windows\System32\msvcrt.dll

Opens: C:\Windows\apppatch\apppatch64\sysmain.sdb

Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\rpcrt4.dll
Opens: C:\Windows\System32\advapi32.dll

Opens: C:\Windows\Microsoft.NET\Framework64\v4.0.30319

Opens: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll

Opens: C:\Windows\Microsoft.NET\Framework64

 Opens:
 C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll

 Opens:
 C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll

 Opens:
 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll

Opens: C:\Windows\System32\gdi32.dl1
Opens: C:\Windows\System32\user32.dl1
Opens: C:\Windows\System32\shlwapi.dl1
Opens: C:\Windows\System32\shlwapi.dl1
Opens: C:\Windows\System32\mm32.dl1
Opens: C:\Windows\System32\msctf.dl1
Opens: C:\windows\temp\RajivApp1.exe.config
Opens:

 $\hbox{C:} \verb|Windows| \verb|WinSxS| amd 64_microsoft.vc 80.crt_1 fc 8b 3b 9a 1e 18e 3b_8.0.50727.69 10_none_88dc 8c 812 fb 1ba 3fOpens: \\$

Opens: C:\
Opens: C:\Windows

Opens: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config

Opens:

```
C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\RajivApp1.exe.log
                                                              C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\security.config
    Opens:
    Opens:
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\security.config.cch
    Opens:
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\enterprisesec.config.cch
                                                              C:\Windows\System32\combase.dll
    Opens:
                                                              C:\Windows\System32\shell32.dll
    Opens:
    Opens:
                                                              C:\Windows\System32\SHCore.dll
    Opens:
                                                              {\tt C:\Windows\Globalization\Sorting\SortDefault.nls}
    Opens:
                                                              C:\Windows\System32\profapi.dll
                                                              C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
    Opens:
Config\v2.0.50727.312\64bit\security.config
                                                              C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
    Opens:
Config\v2.0.50727.312\64bit\security.config.cch
    Opens:
                                                              C:\Windows\assembly\NativeImages_v2.0.50727_64\index21.dat
    Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\da1374321aba580a5d2ec1c436b7f627\mscorlib.ni.dll
                                                              C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0_b77a5c561934e089
    Opens:
    Opens:
                                                              C:\Windows\Temp
                                                              C:\Windows\System32\ole32.dll
    Opens:
    Opens:
                                                              C:\Windows\System32\oleaut32.dll
    Opens:
                                                              C:\Windows\System32\rpcss.dll
    Opens:
                                                              C:\Windows\System32\cryptbase.dll
                                                              C:\Windows\System32\bcryptprimitives.dll
    Opens:
    Opens:
                                                              C:\Windows\System32\uxtheme.dll
    Opens:
                                                              C:\Windows\System32\l_intl.nls
    Opens:
                                                              C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
    Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\5a205dcf58af0d8e6bf8a3cf6ca71f2d\System.ni.dll
C: \verb|Windows| assembly \verb|NativeImages_v2.0.50727_64 \verb|System.Drawing| a 97d798d61ed181a3219f67584767c5 \verb|System.Drawing.ni.dll| and the state of t
    Opens:
C: \windows \assembly \Native Images\_v2.0.50727\_64 \System. \windows. Forms \assembly \Native Images\_v2.0.50727\_64 \System. \windows. \w
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:
    Opens:
\verb|C::Windows| assembly GAC_MSIL System. Windows. Forms \\| 2.0.0.0\_b77a5c561934e089 \\| System. Windows. Forms. dll assembly GAC_MSIL \\| System. Windows. Forms \\| All assembly GAC_MSIL \\| System. Windows. Forms \\| System. Windows. Forms
                                                              C:\Windows\System32\dwmapi.dll
    Opens:
C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_72771d4ecc1c3a4d
C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_72771d4ecc1c3a4d\GdiPlus.dll
    Opens:
                                                              C:\Windows\System32\DWrite.dll
    Opens:
                                                              C:\Windows\Fonts\micross.ttf
    Opens:
                                                              C:\Windows\System32\en-US\user32.dll.mui
                                                              C:\Windows\WinSxS\amd64 microsoft.windows.common-
    Opens:
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
                                                              C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
                                                              C:\Windows\WindowsShell.Manifest
    Opens:
    Opens:
                                                              C:\Windows\system32\uxtheme.dll.Config
    Opens:
                                                              C:\Windows\System32\cmd.exe
    Opens:
                                                              C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
    Opens:
                                                              C:
    Opens:
                                                              C:\Windows\Branding
                                                              C:\Windows\Branding\Basebrd
    Opens:
    Opens:
                                                              C:\Windows\Branding\Basebrd\en-US
    Opens:
                                                              C:\Windows\Globalization
    Opens:
                                                              C:\Windows\Globalization\Sorting
    Opens:
                                                              C:\Windows\System32\en-US
    Opens:
                                                              C:\Windows\System32\wbem
                                                              C:\Windows\System32\wbem\WMIC.exe
    Opens:
    Opens:
                                                              C:\Windows\System32\locale.nls
    Opens:
                                                              C:\Windows\System32\winbrand.dll
                                                              {\tt C:\Windows\Branding\Basebrd\basebrd.dll}
    Opens:
    Opens:
                                                              C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
    Opens:
                                                              C:\Windows\System32\en-US\cmd.exe.mui
    Opens:
                                                              C:\Windows\System32\conhost.exe
                                                              C:\Windows\System32\en-US\conhost.exe.mui
    Opens:
                                                              {\tt C:\Windows\System32\cryptsp.dll}
    Opens:
    Opens:
                                                              C:\Windows\System32\rsaenh.dll
    Opens:
                                                              C:\Windows\System32\nslookup.exe
    Opens:
                                                              C:\Windows\Prefetch\NSLOOKUP.EXE-3D06E09F.pf
    Opens:
                                                              C:\Windows\System32\wsock32.dll
    Opens:
                                                              C:\Windows\System32\dnsapi.dll
    Opens:
                                                              C:\Windows\System32\mswsock.dll
    Opens:
                                                              C:\Windows\System32\nsi.dll
    Opens:
                                                              C:\Windows\System32\ws2_32.dll
    Opens:
                                                              C:\Windows\System32\en-US\nslookup.exe.mui
    Opens:
                                                              C:\Windows\System32\NapiNSP.dll
                                                              C:\Windows\System32\pnrpnsp.dll
    Opens:
    Opens:
                                                              C:\Windows\System32\nlaapi.dll
```

Opens:

C:\Windows\System32\winrnr.dll

Opens: C:\Windows\System32\IPHLPAPI.DLL Opens: C:\Windows\System32\winnsi.dll C:\Windows\System32\dhcpcsvc6.dll Opens: Opens: C:\Windows\System32\dhcpcsvc.dll Opens: C:\Windows\Fonts\StaticCache.dat

Opens: C:\Windows\System32\en-US\KernelBase.dll.mui

Opens:

C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0_b77a5c561934e089\sorttbls.nlp

Opens:

C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0_b77a5c561934e089\sortkey.nlp

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config Reads from:

Reads from: C:\Windows\Prefetch\CMD.EXE-4A81B364.pf

Reads from: C:\Windows\Fonts\StaticCache.dat

Network Events

DNS query: 8.8.8.8.in-addr.arpa DNS query: WORKGROUP MSBROWSE DNS query: Connects to: 8.8.8.8:53 Sends data to: 8.8.8.8:53 Receives data from: 8.8.8.8:53

Windows Registry Events

Creates key: HKLM\software\microsoft\fusion\gacchangenotification\default Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens kev: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\

HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key:

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ side by side$ Opens key: HKLM\system\currentcontrolset\control\session manager

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} approximately approxima$ Opens key: Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKLM\

Opens key: HKLM\software\microsoft\.netframework\policy\ Opens key: HKLM\software\microsoft\.netframework\policy\v4.0 Opens key: HKLM\software\microsoft\.netframework Opens key: HKLM\software\policies\microsoft\sqmclient\windows Opens key: HKLM\software\microsoft\sqmclient\windows

Opens kev: HKCU\software\microsoft\.netframework

HKLM\system\currentcontrolset\control\error message instrument\ Opens key: Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ 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\.netframework\policy\standards

Opens key:

Opens key: HKLM\software\microsoft\fusion

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots HKLM\software\microsoft\.netframework\policy\apppatch Opens kev:

Opens key: HKLM\software\microsoft\.netframework\policy\apppatch\v4.0.30319.00000

Opens key:

 $HKLM \ software \ microsoft \ .net framework \ policy \ apppatch \ v4.0.30319.00000 \ mscorwks.dll$

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

options\rajivapp1.exe

Opens key: HKCU\software\microsoft\fusion

Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the$ options

HKLM\software\microsoft\.netframework\ngen\policy\v2.0 Opens kev

Opens key:

HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets

Opens key:

 $HKLM \ software \ microsoft \ . net framework \ security \ policy \ extensions \ named permission sets \ internet$ Opens key:

 $HKLM \label{lem:hklm} Which is a fixed by the second of the second of$ Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1923240461-1905901954-2556564120-1001

Opens key: HKLM\software\microsoft\ole Opens key: HKLM\software\microsoft\ole\tracing

Opens key:

a03a-e3ef65729f3d}

Opens key:

```
a03a-e3ef65729f3d}\propertybag
          Opens key:
                                                                                                                                                           HKCU\software\microsoft\windows\currentversion\explorer
           Opens key:
                                                                                                                                                           HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
          Opens kev:
\label{thm:linear} HKCU \software \microsoft \windows \current version \explorer \session in folders \cite{thm:linear} and \cite{t
          Opens key:
                                                                                                                                                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
  folders
          Opens key:
                                                                                                                                                          HKLM\system\currentcontrolset\control\nls\customlocale
          Opens key:
                                                                                                                                                          HKLM\system\currentcontrolset\control\nls\extendedlocale
                                                                                                                                                          HKLM\svstem\currentcontrolset\control\nls\sorting\ids
          Opens kev:
          Opens key:
                                                                                                                                                          HKLM\software\policies\microsoft\windows\explorer
          Opens key:
                                                                                                                                                          HKCU\software\policies\microsoft\windows\explorer
          Opens key:
9afe-ea3317b67173}
         Opens key:
HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{lkklm} White \label{lkklm}
9afe-ea3317b67173}\propertybag
           Opens key:
 HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
                                                                                                                                                          HKLM\software\microsoft\.netframework\v2.0.50727\security\policy
          Opens key:
                                                                                                                                                          HKLM \verb|\software\microsoft| fusion \verb|\nativeimagesindex| v2.0.50727\_64
          Opens key:
          Opens key:
                                                                                                                                                          Opens key:
 HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus native images index \setminus v2.0.50727\_64 \setminus na
          Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus 181938c6 \setminus 181936c6 \setminus 181966c6 \setminus 181966c6 \setminus 181966c6 \setminus 181966c6 \setminus 1819
          Opens key:
Opens key:
                                                                                                                                                          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
           Opens key:
                                                                                                                                                           HKLM\system\currentcontrolset\control\lsa
          Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                                                                                                                                                          HKCU\software\microsoft\windows\currentversion\directmanipulation
          Onens key:
          Opens key:
ba85-6007caedcf9d}
          Opens key:
ba85-6007caedcf9d}\propertybag
           Opens key:
HKLM\software\microsoft\strongname
          Opens key:
          Opens key:
                                                                                                                                                           HKLM\software\microsoft\.netframework\internal\jit\perf
                                                                                                                                                          HKLM\software\microsoft\fusion\publisherpolicy\default
          Opens key:
          Opens key:
Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10
          Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 dce 10 \setminus 4000 dce 10 \cup 4000 dce 10 \setminus 4000 dce 10 \cup 4000 
          Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 19ab8d57 \ 5206cfdb \ 17abb \ 19abb \ 19abb
          Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4
          Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 424bd4d8 \ 210819fb \ 64bd4d8 \ value \ and \ and
         Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f
           Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3ced59c5 \ bd38540 \ fusion \ native images index \ native images \ native images index \ native images \ native im
         Opens key:
Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni\ 30bc7c4f\ 3f50fe4f\ 8ex \ not \
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3f50fe4f\6ff8cf57\8
         Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9
          Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus i1 \setminus 6dc7d4c0 \setminus 153b7f91 \setminus 9dc7d4c0 \setminus 153b7f91 \setminus 153b761 \setminus 15
                                                                                                                                                           HKLM\software\microsoft\.netframework\policy\aptca
           Opens key:
          Opens key:
                                                                                                                                                           HKLM\hardware\devicemap\video
          Opens key:
                                                                                                                                                          HKLM\system\currentcontrolset\control\video\{bf735b18-1b5a-4e14-b64c-
  f2223c917d28}\0000
          Opens kev
 HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
                                                                                                                                                           HKLM\system\currentcontrolset\services\fontcache\parameters
           Opens key:
          Opens key:
                                                                                                                                                           HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
          Opens key:
                                                                                                                                                          HKCU\eudc\1252
          Opens key:
                                                                                                                                                          HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
          Opens key:
                                                                                                                                                          HKLM\system\currentcontrolset\control\nls\locale
          Opens key:
                                                                                                                                                          HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
                                                                                                                                                           HKLM\system\currentcontrolset\control\nls\language groups
           Opens key:
           Opens key:
                                                                                                                                                           HKLM\system\currentcontrolset\control\cmf\config
          Opens kev:
                                                                                                                                                          HKLM\software\microsoft\windows\currentversion\policies\explorer
           Opens key:
                                                                                                                                                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ policies\+ explorer
          Opens key:
                                                                                                                                                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
```

```
options\cmd.exe
  Opens key:
                              HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:
                              HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:
                              HKLM\software\policies\microsoft\windows\appcompat
  Opens key:
                              HKCU\software\microsoft\windows nt\currentversion
  Opens key:
                              HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:
                              HKLM\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:
                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
  Opens kev:
                              HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:
                              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:
                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\conhost.exe
  Opens key:
                              HKLM\software\microsoft\oleaut
  Opens key:
                              HKLM\software\microsoft\windows nt\currentversion\console\truetypefont
  Opens key:
                              \label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\console\fullscreen} \\
  Opens key:
                              HKCU\console
  Opens key:
                              HKCU\console\
  Opens key:
                              HKLM\software\microsoft\rpc
  Opens key:
                              HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:
                              HKCU\console\%systemroot%_system32_cmd.exe
                              HKCU\console\%systemroot%\system32\cmd.exe
  Opens key:
  Opens key:
                              HKLM\system\setup
  Opens key:
                              HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:
                              HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange
  Opens key:
                              HKCU\software\classes\
  Opens key:
                              HKCU\software\classes\appid\rajivapp1.exe
  Opens key:
                              HKCR\appid\rajivapp1.exe
  Opens key:
                              HKLM\software\microsoft\ole\appcompat
  Opens key:
                              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:
                              HKCU\software\policies\microsoft\windows\system
  Opens key:
                              HKLM\software\microsoft\command processor
                              HKCU\software\microsoft\command processor
  Opens key:
  Opens key:
                              HKLM\software\policies\microsoft\cryptography
  Opens key:
                              HKLM\software\microsoft\cryptography
  Opens key:
                              HKLM\software\microsoft\cryptography\offload
  Opens key:
                              HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:
                              HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:
                              HKCR\interface\{00000134-0000-0000-c000-00000000046}
  Opens key:
                              00000000046}\proxystubclsid32
  Opens key:
                              HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32
  Opens key:
                              HKLM\software\microsoft\rpc\extensions
  Opens key:
                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\nslookup.exe
  Opens key:
                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\nslookup.exe
  Opens key:
                              HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
                              HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ 00000005
  Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries 64 \ 0000000000001
 Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ positions \ defined as the system \ protocol\_catalog \ protocol\_catal
  Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64
 Opens key:
```

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries 64 \ 0000000000001$

```
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000000
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000006
 Opens key:
                   HKLM\svstem\currentcontrolset\services\winsock\parameters
 Opens key:
                   HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
 Opens key:
                   HKLM\system\currentcontrolset\services\winsock\setup migration\providers
                   HKLM\system\currentcontrolset\services\winsock\setup
```

Opens key: migration\providers\tcpip

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

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

Opens key:

55779daa70e9} Opens key:

806e6f6e6963}

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces

Opens kev:

Opens key:

806e6f6e6963}

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-

25b8d56dd1d8} Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-

8a6dc56e0da9}

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

55779daa70e9}

Opens kev: HKLM\system\currentcontrolset\services\tcpip\linkage

Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash windows}$

nt\currentversion\languagepack\datastore_v1.0

HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\surrogatefallback\microsoft sans serif

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2-2d47c47e

Opens key: HKLM\software\microsoft\ctf\compatibility\rajivapp1.exe

Opens key: HKLM\software\microsoft\ctf\

HKLM\software\rajivapp1\rajivapp1\1.0.0.0 Opens key:

 $\label{lem:hklmsystem} \\ \textbf{HKLM} \\ \textbf{System} \\ \textbf{current control } \\ \textbf{nls} \\ \textbf{sorting} \\ \textbf{versions} []$ Queries value:

Queries value:

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

Oueries value: HKCU\control panel\desktop[preferreduilanguages] Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Oueries value: HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

HKCU\software\microsoft\windows Queries value:

nt\currentversion\appcompatflags[showdebuginfo]

Queries value: HKLM\software\microsoft\.netframework[installroot] Oueries value: HKLM\software\microsoft\.netframework[clrloadlogdir] HKLM\software\microsoft\sqmclient\windows[ceipenable] Oueries value:

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

nt\currentversion\compatibility32[rajivapp1]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\windows[loadappinit_dlls]

Oueries value:

 $HKLM \verb|\software\microsoft|. net framework [uselegacyv2runtimeactivation policy default value]|$ HKLM\software\microsoft\.netframework[onlyuselatestclr] Queries value:

Queries value: HKLM\software\microsoft\fusion[noclientchecks] HKLM\software\microsoft\.netframework[gcstressstart] Oueries value: Queries value: HKLM\software\microsoft\.netframework[gcstressstartatjit] Oueries value: HKLM\software\microsoft\.netframework[disableconfigcache]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-

931b-d9cc2eee27e4]

HKLM\system\currentcontrolset\control\wmi\security[cc2bcbba-16b6-4cf3-Queries value:

8990-d74c2e8af5001

Oueries value: HKLM\software\microsoft\fusion[cachelocation]

Oueries value: HKLM\software\microsoft\fusion[downloadcachequotainkb]

Queries value: HKLM\software\microsoft\fusion[enablelog] Oueries value: HKLM\software\microsoft\fusion[logginglevel] HKLM\software\microsoft\fusion[forcelog] Oueries value: Oueries value: HKLM\software\microsoft\fusion[logfailures] Oueries value: HKLM\software\microsoft\fusion[versioninglog] Queries value: HKLM\software\microsoft\fusion[logresourcebinds]

Queries value: HKLM\software\microsoft\fusion[uselegacyidentityformat]

Queries value: HKLM\software\microsoft\fusion[disablemsipeek]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[devoverrideenable]

Queries value:

HKLM\software\microsoft\.netframework\ngen\policy\v2.0[optimizeusedbinaries]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]

Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]

Oueries value:

 $\label{lem:hklmsoftware} HkLM \software \ensuremath{\mbox{\mbox{1}} eb685db-65f9-4cf6-a03a-e3ef65729f3d} [category]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [name]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\mbox{\mbox{1}} eb685db-65f9-4cf6-a03a-e3ef65729f3d} \cite{100} [parentfolder]$

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \ a03a-e3ef65729f3d \cal{lem:hklmsoftware} \footnote{\coloredge} \ description \cal{lem:hklmsoftware} \ a03a-e3ef65729f3d \cal{lem:hklmsoftware} \ a03$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \end{substitute} $$4.6579-4cf6-a03a-e3ef65729f3d \cal{lem:hklmsoftware} $$[relative path]$$

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \ensuremath{\sc Number \sc Number \$

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \ensuremath{\mbox{\mbox{1}} eb685db-65f9-4cf6-a03a-e3ef65729f3d} [infotip]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [localized name]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \ \footnote{1.00} \ \fo$

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\[security\]$

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \end{a} e3ef65729f3d \subseteq \subseteq \subseteq \subseteq \end{a} e3ef65729f3d \subseteq \s$

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \ensuremath{\sc Number \sc Number \$

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\mbox{\mbox{1}} eb685db-65f9-4cf6-a03a-e3ef65729f3d} \ensuremath{\mbox{1}} \ensuremath{\mbox{1}} each \ensuremath{\mbox{2}} each$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[precreate]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \footnote{Action} \ acts \colored \colore$

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cite{lem:hklmsoftware} a03a-e3ef65729f3d \cite{lem:hklmsoftware} [attributes]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cite{lem:hklmsoftware} a03a-e3ef65729f3d \cite{lem:hklmsoftware} [folder type id]$

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-

a03a-e3ef65729f3d}[initfolderhandler]

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

folders[appdata]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[category]

Queries value:

 $\label{limits} $HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[name]}$

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \f$

Queries value:

 $HKLM \label{lem:hklm} Which is the latest and the$

9afe-ea3317b67173}[description] Queries value: 9afe-ea3317b67173}[relativepath] Oueries value: $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-164e7descriptions\} \ folder \ fold$ 9afe-ea3317b67173}[parsingname] Queries value: 9afe-ea3317b67173}[infotip] Oueries value: 9afe-ea3317b67173}[localizedname] Queries value: 9afe-ea3317b67173}[icon] Oueries value: 9afe-ea3317b67173}[security] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource] Oueries value: 9afe-ea3317b67173}[streamresourcetype] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate] Queries value: 9afe-ea3317b67173}[stream] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ (5e6c858f-0e22-4760-1000) \ model \ model \ model) \ model \ model$ 9afe-ea3317b67173}[attributes] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid] Oueries value: 9afe-ea3317b67173}[initfolderhandler] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Queries value: 1923240461-1905901954-2556564120-1001[profileimagepath] Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_64 [latest index]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\index21[niusagemask] Oueries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_64 \setminus index 21[ilus agemask]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[displayname] $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[configmask]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[configstring]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[mvid]$ $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_64 \setminus i181938c6 \setminus 7950e2c5 \setminus 1[evalation data]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_64 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus 1[status]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[ildependencies]$ $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_64 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus 1[nidependencies]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[missing dependencies]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ il\ 7950e2c5 \ 6f33d37e \ 1[display name]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_64 \setminus i1 \setminus 7950e2c5 \setminus 6f33d37e \setminus 1[status]$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[status]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[modules]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[sig]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[lastmodtime]
Queries value:

HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,amd64]
Queries value:

HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]

Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category]
Oueries value:

 $HKLM\software\mbox{\tt hkLM}\software\mbox{\tt hkLM}\software\mbox{\tt$

Queries value:

Queries value:

Queries value:

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cite{252481e8-33be-4251-ba85-6007} \cite{252481e8-33be-4251-ba8$

Queries value:

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\{352481e8-33be-4251-ba85-6007 \ caedcf9d\}[localized name]$

Queries value:

Queries value:

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{352481e8-33be-4251-ba85-6007 \ caed \ cf9d\} \ [stream resource]$

Queries value:

 $\label{thm:hklm} HKL^{M} software \ensuremath{\mbox{\mbox{1}}} windows \ensuremath{\mbox{\mbox{1}}} explorer \ensuremath{\mbox{\mbox{1}}} explorer \ensuremath{\mbox{1}} explorer \ensuremat$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caedcf9d\} \ [local redirectonly]$

Queries value:

 $\label{thm:hklm} HKL^M\software\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{352481e8-33be-4251-ba85-6007} caedcf9d\columnwerf{1}{907} [roamable]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \end{subarray} $$152481e8-33be-4251-ba85-6007 \caedcf9d \cal{lem:hklmsoftware} \cal{lem:hklmsoftware} $$152481e8-33be-4251-ba85-6007 \caedcf9d \cal{lem:hklmsoftware} \cal{lem:hklmsoftware} $$152481e8-33be-4251-ba85-6007 \caedcf9d \cal{lem:hklmsoftware} \cal{lem:hklmsoftware} $$152481e8-33be-4251-ba85-6007 \caedcf9d \cal{lem:hklmsoftware} \cal{lem:hklmsoftware} $$152481e8-33be-4251-ba85-6007 \caedcf9d \caedcf9d$

Queries value:

 $\label{thm:hkm} \begin{tabular}{l} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1.5} $1.52481e8-33be-4251-ba85-6007caedcf9d\footnote{1.5} $1.5481e8-33be-4251-ba85-6007caedcf9d\footnote{1.5} $1.5481e8-33be-4251-ba85-6007caedcf9d\footnote{$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \footnote{1} descriptions \footnote{1}$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cite{252481e8-33be-4251-ba85-6007} \cite{252481e8-33be-4251-ba8$

Queries value: KLM\software

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \explorer \folder \folde$

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

folders[cache]

Queries value: HKLM\software\microsoft\.netframework[cseon] Queries value: HKLM\software\microsoft\.netframework[tailcallopt] HKLM\software\microsoft\.netframework[pinvokeinline] Queries value: Queries value: HKLM\software\microsoft\.netframework[pinvokecalliopt] HKLM\software\microsoft\.netframework[newgccalc] Queries value: Oueries value: HKLM\software\microsoft\.netframework[turnoffdebuginfo] Oueries value: HKLM\software\microsoft\.netframework[disablehotcold] Oueries value: HKLM\software\microsoft\fusion\publisherpolicy\default[latest]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[displayname] Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[configmask]
Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{$\mbox{$\mbox{\sim}}$ index \scales} 2.0.50727_64 \mbox{$\mbox{$\sim$}} 161e7e666 \scales \scales$

 $\label{lem:hklmsoftware} HkLM \software \sinces of this ion \sinces will be a single sindex \sinces of the latest and the la$

 $\label{local-equality} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727_64\ni\61e7e666\c991064\10\end{10} [evalation data] Queries value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[status]
Oueries value:

 $\label{local-bound} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \ni\61e7e666 \c991064 \10[ildependencies] \\ Queries value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[nidependencies]
Queries value:

```
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[missingdependencies] Oueries value:
```

 $\label{lem:hklmsoftware} HKLM \software \microsoft \sin \native images in dex \sin 2.0.50727_64 \sin 1475 dce 40 \sin 6604 efc \sin 2 display name] Oueries value:$

 $\label{local-operator} HKLM \software \end{area} HKLM \software \end{area} A til \475 dce 40 \604 efc \3 [status] Oueries value:$

 $\label{lem:hklmsoftware} HKLM \software \since \s$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\6604efc\3[sig]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\6604efc\3[lastmodtime]
 Oueries value:

 $\label{lem:hklmsoftware} HkLM \software \slices on \slices and \slices value: \\ Oueries \slices value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[status]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[modules]
Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \end{array} HKLM \software \end{array} 10.50727_64 \end{arra$

 $\label{local-equation} HKLM \software \microsoft \sion \native images in dex \v2.0.50727_64 \il\nabel{local-equation} 19ab8d57 \sion \native images in dex \v2.0.50727_64 \il\nabel{local-equation} 20ab8d57 \sion \native images in dex \v2.0.50727_64 \il\nabel{local-equation} 20ab8d57 \sion \native images in dex \v2.0.50727_64 \il\nabel{local-equation} 19ab8d57 \sion \native images in dex \v2.0.50727_64 \il\nabel{local-equation} 19ab8d57 \sion \native images in dex \v2.0.50727_64 \il\nabel{local-equation} 20ab8d57 \sion \native images in dex \v2.0.50727_64 \sion \native images i$

 $\label{lem:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \il\2dd6 ac50 \6bbd663d \4[display name] \\ Queries \value:$

 $\label{lem:hklmsoftware} HKLM \software \since \s$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[modules]
Oueries value:

 $\label{lem:hklmsoftware} HkLM \software \since \s$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[lastmodtime]
 Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \subseted in the lambda of the$

 $\label{lem:hklmsoftware} $$HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6[status] Queries value:$

 $\label{local-observation} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \il\424bd4d8 \210819fb \6 [modules] Queries value:$

 $\label{lem:hklm} HKLM \software \microsoft \signature images in dex \signature \signat$

 $\label{local-equation} HKLM \software \mbox{$\mbox{}\mbox{$\mbox{\mbo

 $\label{thm:local-condition} HKLM \software \mbox{\le index$$\$ \$ 2.0.50727_64$$ il \41c04c7e \7a981124$$ lightharmoon gueries value: }$

 $\label{thm:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \il\41c04c7e \7a981124 \1f[status] \noindent \$

 $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex $$ v2.0.50727_64\il\41c04c7e\7a981124\1f[modules] Queries value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f[sig] Oueries value:

 $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727_64\il\41c04c7e\7a981124\1f[lastmodtime] \\ Oueries\ value:$

 $\label{lem:hklmsoftware} HKLM \software \microsoft \sinon \native images in dex \normalized 50.50727_64 \normalized 59c5 \bd38540 \f[display name] Queries value:$

 $\label{local-observation} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \colone{1} \align{ Action} 13ced 59c5 \bd38540 \f[status] Queries value: \end{ Action}$

 $\label{lem:hklm} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727_64\mbox{il}\aced59c5\bd38540\f[modules] Queries value: \\ HKLM\software\mbox{microsoft}\fusion\native\mbox{imagesindex}\sl 2.0.50727_64\mbox{il}\aced59c5\bd38540\f[sig]]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \sin \native images in dex \sin 2.0.50727_64 \sin 3.50727_64 \sin 3.50727$

 $\label{local-observation} HKLM\software\mbox{\setminusv2.0.50727_64\il\c991064\34e16fb6\20[status]$} Queries\ value:$

 $\label{local-bound} HKLM\software\microsoft\fusion\native images in dex $$\v2.0.50727_64\il\c991064\34e16fb6\20[modules]$$ Queries value:$

 $\label{local-bound} HKLM \software \end{array} HKLM \software \end{array} 10.50727_64 \end{array} 10$

 $\label{local-equation} HKLM \software \mbox{$\mbox{$\mathbb{N}$} $ in\adverses index \scales. } 20.50727_64 \scales. \\ Queries value:$

 $\label{local-bound} HKLM \software \microsoft \sion \native images in dex \v2.0.50727_64 \ni\30bc7c4f\3f50fe4f\8[display name] \\ Queries value:$

 $\label{lem:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \ni\30bc7c4f\3f50fe4f\8[configmask] Queries value:$

 $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[configstring] \\ Queries\ value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[mvid]
Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \ni\30bc7c4f\3f50fe4f\8 [evalation data] \\ Queries value:$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[status]
Queries value:

 $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[nidependencies] Queries value:$

```
Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3f50fe4f \setminus 6ff8cf57 \setminus 8[displayname]
   Oueries value:
HKLM \setminus Software \setminus irrosoft \setminus fusion \setminus irrosoft \setminus software \setminus irrosoft \setminus fusion \setminus irrosoft \setminus software \setminus irrosoft \setminus fusion \setminus irrosoft \setminus irrosoft \setminus irrosoft \setminus fusion \setminus irrosoft \setminus fusion \setminus irrosoft \setminus fusion \setminus irrosoft \setminus irrosoft \setminus fusion \setminus fus
   Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3f50fe4f \setminus ff8cf57 \setminus 8[modules]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3f50fe4f\ 6ff8cf57\ 8[sig]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3f50 fe4f \setminus 6ff8cf57 \setminus 8[last modtime]
   Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni\ 3cca06a0\ 6dc7d4c0\ 9[displayname]
   Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 9[configmask]
   Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[configstring]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus ni \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 9[mvid]
   Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus ni \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 9[evalation data]
   Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 9[status]
Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 64\ni\3cca06a0\6dc7d4c0\9[nidependencies]
   Oueries value:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_64 \ ni\ 3cca06a0\ 6dc7d4c0\ 9 \ [missing dependencies]
   Queries value:
\label{local-ham} HKLM \setminus software \setminus irrosoft \setminus fusion \setminus ative images in dex \ \ v2.0.50727\_64 \ \ il \setminus 6dc7d4c0 \setminus 153b7f91 \setminus 9[display name]
   Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 64\il\6dc7d4c0\153b7f91\9[status]
   Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\6dc7d4c0\153b7f91\9[modules]
\label{locality} HKLM \software \microsoft \fusion \native images index \v2.0.50727\_64 \il\ 6dc7d4c0 \153b7f91 \9 [sig] \label{locality}
   Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 6dc7d4c0 \setminus 153b7f91 \setminus 9[last modtime]
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[system.windows.forms, 2.0.0.0, , b77a5c561934e089, msil]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[system.drawing, 2.0.0.0, ,b03f5f7f11d50a3a, msil]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system,2.0.0.0,,b77a5c561934e089,msil]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.configuration,2.0.0.0,,b03f5f7f11d50a3a,msil]
   Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[system.deployment, 2.0.0.0, ,b03f5f7f11d50a3a, msil]
   Queries value:
Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[accessibility, 2.0.0.0, ,b03f5f7f11d50a3a, msil]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil]
   Queries value:
                                              HKLM\software\microsoft\.netframework[dbgjitdebuglaunchsetting]
   Queries value:
                                              HKLM\software\microsoft\.netframework[dbgmanageddebugger]
                                              HKLM\hardware\devicemap\video[maxobjectnumber]
   Queries value:
   Oueries value:
                                              HKLM\hardware\devicemap\video[\device\video0]
                                              HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-
   Queries value:
08002be10318}\0000[pruningmode]
   Oueries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[clientcachesize]
                                              HKLM\system\currentcontrolset\control\nls\customlocale[ko-kr]
   Queries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale[ko-kr]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn]
   Oueries value:
                                              HKLM\svstem\currentcontrolset\control\nls\extendedlocale[zh-cn]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\customlocale[ja-jp]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale[ja-jp]
                                              HKLM\system\currentcontrolset\control\nls\customlocale[zh-tw]
   Queries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-tw]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\customlocale[zh-hk]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hk]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
                                              HKLM\system\currentcontrolset\control\cmf\config[system]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
   Oueries value:
HKLM \verb|\software\policies\microsoft\windows\safer\code identifiers[authenticode enabled]|
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\compatibilitv32[conhost]
```

Oueries value:

Oueries value:

HKCU\console[screencolors]

HKCU\console[popupcolors]

```
HKCU\console[insertmode]
  Queries value:
  Queries value:
                           HKCU\console[quickedit]
  Queries value:
                           HKCU\console[codepage]
  Oueries value:
                           HKCU\console[screenbuffersize]
  Oueries value:
                           HKCU\console[windowsize]
 Oueries value:
                           HKCU\console[windowposition]
  Queries value:
                           HKCU\console[fontsize]
  Queries value:
                           HKCU\console[fontfamily]
  Queries value:
                           HKCU\console[fontweight]
  Oueries value:
                           HKCU\console[facename]
  Oueries value:
                           HKCU\console[cursorsize]
  Oueries value:
                           HKCU\console[historybuffersize]
                           HKCU\console[numberofhistorybuffers]
  Oueries value:
  Queries value:
                           HKCU\console[historynodup]
  Queries value:
                           HKCU\console[colortable00]
  Oueries value:
                           HKCU\console[colortable01]
  Oueries value:
                           HKCU\console[colortable02]
  Oueries value:
                          HKCU\console[colortable03]
                           HKCU\console[colortable04]
  Queries value:
  Queries value:
                           HKCU\console[colortable05]
  Queries value:
                           HKCU\console[colortable06]
  Oueries value:
                           HKCU\console[colortable07]
 Oueries value:
                           HKCU\console[colortable08]
  Queries value:
                           HKCU\console[colortable09]
  Queries value:
                           HKCU\console[colortable10]
  Queries value:
                           HKCU\console[colortable11]
  Oueries value:
                           HKCU\console[colortable121
  Oueries value:
                           HKCU\console[colortable13]
  Queries value:
                           HKCU\console[colortable14]
  Queries value:
                           HKCU\console[colortable15]
  Queries value:
                           HKCU\console[loadconime]
  Oueries value:
                           HKCU\console[extendededitkey]
  Oueries value:
                           HKCU\console[extendededitkevcustom]
  Oueries value:
                           HKCU\console[worddelimiters]
  Oueries value:
                           HKCU\console[trimleadingzeros]
  Queries value:
                           HKCU\console[enablecolorselection]
  Queries value:
                           HKCU\console[scrollscale]
  Queries value:
                           HKLM\software\microsoft\rpc[maxrpcsize]
  Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername\computername\
  Queries value:
                          {\it HKLM \ } system \verb|\ current control set \verb|\ control \ \\ session
manager[safeprocesssearchmode]
                          HKLM\system\setup[oobeinprogress]
  Queries value:
  Queries value:
                           HKLM\system\setup[systemsetupinprogress]
                          HKLM\software\microsoft\rpc[idletimerwindow]
 Oueries value:
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
  Oueries value:
                          \label{lem:hklm} \verb+Kklm \+ software \+ microsoft \+ ole \+ app compat \+ [raise default authnlevel]
  Queries value:
                           HKLM\software\microsoft\ole[defaultaccesspermission]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:
                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
                          HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong
  Queries value:
cryptographic provider[image path]
  Queries value:
                          HKLM\software\microsoft\command processor[disableunccheck]
  Oueries value:
                           HKLM\software\microsoft\command processor[enableextensions]
  Queries value:
                           HKLM\software\microsoft\command processor[delayedexpansion]
  Oueries value:
                          HKLM\software\microsoft\command processor[defaultcolor]
  Queries value:
                           {\tt HKLM \setminus software \setminus microsoft \setminus command processor[completion char]}
 Queries value:
                          HKLM\software\microsoft\command processor[pathcompletionchar]
                           HKLM\software\microsoft\command processor[autorun]
  Queries value:
  Oueries value:
                           HKCU\software\microsoft\command processor[disableunccheck]
  Queries value:
                           HKCU\software\microsoft\command processor[enableextensions]
  Oueries value:
                           HKCU\software\microsoft\command processor[delayedexpansion]
  Oueries value:
                           HKCU\software\microsoft\command processor[defaultcolor]
  Queries value:
                           HKCU\software\microsoft\command processor[completionchar]
                          HKCU\software\microsoft\command processor[pathcompletionchar]
  Queries value:
  Queries value:
                           HKCU\software\microsoft\command processor[autorun]
  Queries value:
                           HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Oueries value:
\label{lem:hklm} \verb+KLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]+ \\
  Oueries value:
                          HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                           HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
                           HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
  Queries value:
  Oueries value:
                           HKLM\software\microsoft\rpc\extensions[ndroleextdll]
 Oueries value:
                          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[nslookup]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace callout]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ [next\_catalog\_entry\_id]
 Oueries value:
Oueries value:
```

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\00000000001[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
 Oueries value:
- $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries 64 \ \ 0000000000004 \ [packed catalog item]$ Oueries value:
- $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries 64 \ \ 000000000005 \ [packed catalog item]$ Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\00000000010[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries64]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[librarypath]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries 64 \ 0000000000001 [displaystring] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[enabled]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries 64 \ 0000000000001 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[librarypath]
 Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries 64 \ 0000000000002 \ [displaystring] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[supportednamespace] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries 64 \0000000000002 \cite{lem:hklmsystem}. \\$ Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[librarypath] Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries 64 \ 0000000000003 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[supportednamespace]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004[providerid]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries 64 \ 0000000000004 \ [address family] \ Queries \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries 64 \ 00000000000004 \ [supported namespace]$ Queries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[enabled]
Oueries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[displaystring]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[addressfamily] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[supportednamespace]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[version]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000005[storesserviceclassinfo] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries 64 \ 0000000000005 \ [providerinfo] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[librarypath] Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog \catalog_entries 64 \noone00000000006 \[displaystring] \queries \value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[addressfamily]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[supportednamespace]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[enabled]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[storesserviceclassinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value:

 $\label{thm:current} Queries \ value: \\ HKLM\system\currentcontrolset\services\winsock\setup \\$

 $\label{lem:migration} \verb|migration|| providers \verb|\tcpip|| winsock 2.0 provider id]$

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]$

Queries value:

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

Queries value:

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

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\parameters[hostname]

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} and $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of the control set \end{tabular} $$ is a constant of \end{ta$

Queries value: HKLM\system\cu Oueries value:

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

Queries value:

WKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Oueries value:

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

HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
 Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
Oueries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Queries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamegueryfallback]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
 Oueries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Queries value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters[disabledvnamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Queries value:
HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[register adapter name]|
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register reverse look up]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Queries value:
HKLM \setminus system \setminus current controls et \setminus services \setminus tcpip \setminus parameters [disable wandynamic update]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
 Oueries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Oueries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
 Queries value:
                      HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
```

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]

 $\label{thm:parameters} Queries \ value: $$HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]$$$

HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
 Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]

HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Oueries value:

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

Queries value:

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

 $Queries\ value: \\ HKLM\ system\ current control set\ services\ tcpip6\ parameters\ interfaces\ \{b5105d63-74c6-4dc1-87b7-4c6-4d$

55779daa70e9}[searchlist]
Queries value:

 $\label{thm:hkm} HKLM \system \current controls et \services \tcpip \parameters \ \ \{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [enabledhcp]$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \b5105d63-74c6-4dc1-87b7-55779 \parameters \time faces \end{substitute} \end{substitute} \end{substitute}$

Queries value:

 $\label{lem:hkklmsystem} HKLM \system \current controls et \services \tcpip \parameters \ \ \ \{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [register adapter name]$

Oueries value:

Queries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip6 \ parameters \ 'interfaces \ 'b5105d63-74c6-4dc1-87b7-55779 \ daa70e9 \ [dhcpv6domain]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip6 \ parameters \ 'interfaces \ 'b5105d63-74c6-4dc1-87b7-55779 \ daa70e9 \ [nameserver]$

Queries value:

 $\label{lem:hklmsystem} HkLM \system \current control set \services \tcpip \parameters \time faces \b5105d63-74c6-4dc1-87b7-55779 \parameters \end{array}.$

Queries value:

 $\label{lem:hammeters} HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\b5105d63-74c6-4dc1-87b7-55779daa70e9\\[1mm] [dhcpnameserver]$

Queries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'topip \ 'parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} [registration enabled]$

Queries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ 'parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [domain]$

Queries value:

 $\label{thm:local-be62-be64} HKLM \system \current controls et \end{area} $$HKLM \system \current controls et \end{area} $$1e1-be62-806e6f6e6963 \[dhcpdomain]$

Queries value:

 $\label{lem:hkkm} HKLM \system \current controls et \services \tcpip \parameters \ \ \{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [nameserver]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{97e1de57-d6fa-11e1-be62-806e6f6e6963\} \ [dhcpnameserver]$

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

Queries value:

 $\label{lem:hkklmsystem} HKLM \system \current controls et \services \tcpip \parameters \ \ \ \{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [queryadaptername]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \b5105d63-74c6-4dc1-87b7-55779 \parameters \parame$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{b5105d63-74c6-4dc1-87b7-55779daa70e9\} \ [registration maxaddress count]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[maxnumberofaddressestoregister]

Queries value:

55779daa70e9}[enablemulticast] Queries value: $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-defa-11e1-defa-11$ 806e6f6e6963}[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disabledynamicupdate] Oueries value: $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-defa-11e1-defa-11$ 806e6f6e6963}[enableadapterdomainnameregistration] Queries value: 806e6f6e6963}[registrationmaxaddresscount] Queries value: $HKLM \ system \ current control set \ services \ typip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-defa-11e1-defa-11e1-d$ 806e6f6e6963}[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enablemulticast] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0[disable] Queries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\languagepack\datastore_v1.0[datafilepath]|\\$ HKLM\software\microsoft\windows Oueries value: $\verb|nt\currentversion\languagepack\surrogatefallback[plane1]|$ Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2] Oueries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane4] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane5] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane6] HKLM\software\microsoft\windows Oueries value: $\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|$ HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane8] HKLM\software\microsoft\windows Queries value: $\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|$ Queries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\language| pack\surrogatefallback[plane10]|$ Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane11] HKLM\software\microsoft\windows Queries value:

nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane12]

nt\currentversion\languagepack\surrogatefallback[plane13]

Queries value:

Queries value:

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows