Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 1247, Task ID: 4212

Task ID: 4212 Risk Level: 5

Date Processed: 2016-07-12 05:10:25 (UTC)

Processing Time: 61.24 seconds
Virtual Environment: IntelliVM

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

Sample ID: 1247
Type: basic
Owner: admin
Label: RajivApp1.exe

Labei: KajivAppi.exe

Date Added: 2016-07-12 05:10:24 (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

Terminates process under Windows subfolder

4 Reads process memory

2 Resolves local hostname

2 .NET compiled executable

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_

Creates process: C:\Windows\system32\nslookup.exe [nslookup _MSBROWSE_ Reads from process: PID:2084 C:\Windows\System32\nslookup.exe

Reads from process: PID: 2084 C: \Windows\System32\ns100kup.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_1236

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\Microsoft.NeT\Priamework64
Opens: C:\Windows\System32\gdi32.dl1
Opens: C:\Windows\System32\user32.dl1
Opens: C:\Windows\System32\shlwapi.dl1
Opens: C:\Windows\System32\imm32.dl1
Opens: C:\Windows\System32\imm32.dl1
Opens: C:\Windows\System32\immsetf.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:
                                                              C:\Windows\System32\uxtheme.dll
    Opens:
    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\cryptsp.dll
    Opens:
    Opens:
                                                              C:\Windows\System32\rsaenh.dll
                                                              C:\Windows\System32\en-US\conhost.exe.mui
    Opens:
    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

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

 $\label{lem:config} C: \verb|\windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config| and the configuration of the configurati$ 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: $\overline{\text{HKLM}\setminus \text{software}\setminus \overline{\text{microsoft}\setminus \text{fusion}\setminus \text{gacchangenotif}} ication \setminus \text{default}$ Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: 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\

Opens key ${\tt HKCU\control\ panel\desktop\muicached\machinelanguage} configuration$

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 kev: ${\tt HKCU \backslash control\ panel \backslash desktop}$

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

HKLM\ Opens key:

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 HKLM\software\microsoft\sqmclient\windows Opens key:

Opens key: HKCU\software\microsoft\.netframework

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens kev: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

HKLM\software\microsoft\windows nt\currentversion\windows Opens key: Opens key: HKLM\software\microsoft\.netframework\policy\standards

Opens key: $HKLM \ software \ `microsoft\ .net framework \ policy \ standards \ \ v2.0.50727$

Opens key: HKLM\software\microsoft\fusion

Opens key:

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus .net framework \setminus policy \setminus apppatch}$

Opens key:

Opens key:

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

options\rajivapp1.exe

Opens key: HKCU\software\microsoft\fusion

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

options

Opens key: HKLM\software\microsoft\.netframework\ngen\policy\v2.0

Opens key:

 $HKLM \verb|\software\microsoft|. net framework \verb|\security\policy\extensions| name dpermission sets$ Opens key:

HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet Opens kev $HKLM \ software \ microsoft \ .net framework \ security \ policy \ extensions \ named permission sets \ local intranet$

HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Opens key:

1923240461-1905901954-2556564120-1001 Opens key: HKLM\software\microsoft\ole Opens key: HKLM\software\microsoft\ole\tracing

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions$

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6a03a-e3ef65729f3d}

Opens key:

 $HKLM \label{lem:hklm} While the latest and the la$ a03a-e3ef65729f3d}\propertybag

Opens kev: HKCU\software\microsoft\windows\currentversion\explorer

Opens kev: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1

Opens key:

 $\label{thm:local_hammon_hammon} HKCU \software \microsoft \windows \current version \explorer \session in follows \current version \explorer \session \current version \explorer \session \current \cur$

```
Opens key:
                                                                                                                                                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
  folders
            Opens key:
                                                                                                                                                                      HKLM\system\currentcontrolset\control\nls\customlocale
                                                                                                                                                                    HKLM\svstem\currentcontrolset\control\nls\extendedlocale
           Opens key:
           Opens key:
                                                                                                                                                                      HKLM\svstem\currentcontrolset\control\nls\sorting\ids
           Opens key:
                                                                                                                                                                    HKLM\software\policies\microsoft\windows\explorer
           Opens key:
                                                                                                                                                                    HKCU\software\policies\microsoft\windows\explorer
           Opens key:
HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1000 \ 'explorer' \ 'explore
 9afe-ea3317b67173}
          Opens key:
9afe-ea3317b67173}\propertybag
           Opens key:
 HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
                                                                                                                                                                    HKLM\software\microsoft\.netframework\v2.0.50727\security\policy
           Opens key:
                                                                                                                                                                      HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64
           Opens kev:
           Opens key:
                                                                                                                                                                    HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_64 \ in dex 21
           Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 181938c6 \ 7950e2c5
           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 181938c6 \setminus 191938c6 \setminus 191936c6 \setminus 1919
           Opens key:
{\tt HKLM \ } \\ \textbf{System \ } \\ \textbf{Current control \ } \\ \textbf{Sa \ } \\ \textbf{fips algorithm policy}
            Opens key:
           Opens key:
                                                                                                                                                                    HKLM\system\currentcontrolset\control\lsa
           Opens kev:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                                                                                                                                                                    HKCU\software\microsoft\windows\currentversion\directmanipulation
           Opens key:
           Opens key:
ba85-6007caedcf9d}
           Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}\propertybag
            Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 38c56119 \ 1d3ee2d7
           Opens key:
                                                                                                                                                                    HKLM\software\microsoft\strongname
                                                                                                                                                                      HKLM\software\microsoft\.netframework\internal\jit\perf
           Opens kev:
           Opens key:
                                                                                                                                                                    HKLM\software\microsoft\fusion\publisherpolicv\default
           Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10
          Opens key:
Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid range index \setminus range index \cap r
           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 \ v2.0.50727\_64 \ il\ 424bd4d8 \ v2.0.50727\_64 \ v2.0.50727\_6
           Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f
           Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3ced59c5 \setminus bd38540 \setminus i1 \setminus 3ced59c5 \setminus 3ced59c5 \setminus i1 \setminus 3ced59c5 
          Opens kev:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ c991064 \ 34e16fb6 \ 20.50727\_64 \ il\ c991064 \ 34e16fb6 \ 34e16fb
           Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 30bc7c4f \ 3f50fe4f \ 8ex \ new \ ne
HKLM \setminus software \setminus icrosoft \setminus fusion \setminus icrosoft \setminus fusion \setminus icrosoft \setminus icroso
          Opens kev
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni\ 3cca06a0\ 6dc7d4c0\ 9dca06a0\ 9dc
           Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 6dc7d4c0\ 153b7f91\ 9dc \ and \ respectively. The software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 6dc7d4c0\ 153b7f91\ 9dc \ and \ respectively. The software \ native images index \ v2.0.50727\_64 \ il\ 6dc7d4c0\ 153b7f91\ 9dc \ and \ respectively. The software \ native images \ native imag
           Opens key:
                                                                                                                                                                    HKLM\software\microsoft\.netframework\policy\aptca
           Opens key:
                                                                                                                                                                      HKLM\hardware\devicemap\video
                                                                                                                                                                      HKLM\system\currentcontrolset\control\video\{bf735b18-1b5a-4e14-b64c-
           Opens key:
 f2223c917d28}\0000
           Opens key:
                                                                                                                                                                      HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-
 08002be10318}\0000
           Opens key:
 HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
           Opens key:
                                                                                                                                                                      HKLM\system\currentcontrolset\services\fontcache\parameters
           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 key:
                                                                                                                                                                    HKLM\software\microsoft\windows\currentversion\policies\explorer
            Opens key:
                                                                                                                                                                      HKCU\software\microsoft\windows\currentversion\policies\explorer
            Opens key:
                                                                                                                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\cmd.exe
                                                                                                                                                                      HKLM\system\currentcontrolset\control\session manager\appcertdlls
           Opens key:
```

HKLM\system\currentcontrolset\control\session manager\appcompatibility

Opens key:

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 kev: HKLM\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\cmd.exe Opens key: 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\rpc Opens key: $HKLM \verb|\system| current control \verb|\computername| active computername|$ Opens key: HKLM\svstem\setup Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKCU\software\classes\ Opens key: HKCU\software\classes\appid\rajivapp1.exe Opens key: HKCR\appid\rajivapp1.exe Opens key: HKLM\software\microsoft\ole\appcompat Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider Opens key: HKLM\software\policies\microsoft\cryptography Opens key: HKLM\software\microsoft\oleaut Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} windows $$nt\circ \end{tabular} in the console \end{tabular} The console \end{tabular} and the console \end{tabular} in the console \end{tabular} The console \end{tabular} and the console \end{tabular} and the console \end{tabular} The console \end{tabular} and the console$ Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen Opens key: HKLM\software\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography\offload Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046} HKCU\console Opens key: HKCU\console\ Opens key: Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046} HKCU\software\classes\interface\{00000134-0000-0000-c000-Opens key: 00000000046}\proxystubclsid32 Opens key: HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: HKLM\software\microsoft\rpc\extensions Opens key: HKCU\console\%systemroot%_system32_cmd.exe Opens key: HKCU\console\%systemroot%\system32\cmd.exe Opens key: $HKLM \verb|\system| current controlset| control \verb|\nls| code page \verb|\eudccoder ange| code page \verb|\eudcccoder ange| code page \verb|\eudcccoder ange| code p$ Opens key: HKCU\software\policies\microsoft\windows\system Opens key: HKLM\software\microsoft\command processor HKCU\software\microsoft\command processor Opens kev: Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr 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\svstem\currentcontrolset\services\winsock2\parameters Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2-3373a944 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2 Opens key: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005 Opens key: $HKLM \ system \ current controls et \ services \ winsock 2 \ parameter \ protocol_catalog 9 \ catalog_entries 64 \ protocol_catalog 9 \ catalog_entries 64 \ protocol_catalog 9 \ protocol_catalog 9$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000001 Opens key: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ possible \ and \ protocol_catalog_entries \ protocol_catalog \ protoc$ Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000005 Opens key: Opens key: Opens key: Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ 00000014$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64 Opens kev:

Opens key:

```
Opens key:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000006
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\winsock\parameters
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
                                                                            HKLM\system\currentcontrolset\services\winsock\setup migration\providers
     Opens kev:
     Opens key:
                                                                           HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                                                                            HKLM\system\currentcontrolset\services\tcpip\parameters
     Opens kev:
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows nt\dnsclient
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\dnscache\parameters
     Opens key:
                                                                            HKLM\software\policies\microsoft\system\dnsclient
                                                                            {\tt HKLM \ } system \verb| current control set \verb| services \verb| dns \\
     Opens kev:
     Opens key:
HKLM \ system \ current control set \ services \ typip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-8
55779daa70e9}
     Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus interfaces \setminus \{97e1de57-d6fa-11e1-be62-de1abe1\} \cap tcpip6 \setminus tcpip6 
806e6f6e6963}
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
     Opens key:
HKLM \ system \ current control set \ services \ typip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-d
806e6f6e6963}
     Opens key:
HKLM \land system \land current control set \land services \land tcpip \land parameters \land interfaces \land \{a04231f6-42eb-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b
25b8d56dd1d8}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\tcpip\linkage
     Opens key:
                                                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
                                                                           HKLM\software\microsoft\windows
    Opens kev:
nt\currentversion\languagepack\surrogatefallback
                                                                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\microsoft sans serif
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid catalog\3a41eaa2-2d47c47e
                                                                            {\tt HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus rajivapp 1.exe}
     Opens key:
     Opens key:
                                                                            HKLM\software\microsoft\ctf\
     Queries value:
                                                                            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
     Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                                            HKCU\control panel\desktop[preferreduilanguages]
     Queries value:
                                                                            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
     Queries value:
     Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
                                                                            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
     Oueries value:
                                                                            HKCU\software\microsoft\windows
     Oueries value:
nt\currentversion\appcompatflags[showdebuginfo]
                                                                            {\tt HKLM \backslash software \backslash microsoft \backslash .net framework [install root]}
     Queries value:
     Queries value:
                                                                            HKLM\software\microsoft\.netframework[clrloadlogdir]
     Queries value:
                                                                            HKLM\software\microsoft\sqmclient\windows[ceipenable]
                                                                            HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                                                           HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\compatibility32[rajivapp1]
                                                                            HKLM\software\microsoft\windows
     Queries value:
nt\currentversion\windows[loadappinit_dlls]
     Queries value:
HKLM\software\microsoft\.netframework[uselegacyv2runtimeactivationpolicydefaultvalue]
                                                                            HKLM\software\microsoft\.netframework[onlvuselatestclr]
     Oueries value:
     Oueries value:
                                                                            HKLM\software\microsoft\fusion[noclientchecks]
     Oueries value:
                                                                            HKLM\software\microsoft\.netframework[gcstressstart]
     Queries value:
                                                                            HKLM\software\microsoft\.netframework[gcstressstartatjit]
     Queries 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-
     Oueries value:
8990-d74c2e8af500]
     Queries value:
                                                                            HKLM\software\microsoft\fusion[cachelocation]
     Queries value:
                                                                            HKLM\software\microsoft\fusion[downloadcachequotainkb]
     Queries value:
                                                                            HKLM\software\microsoft\fusion[enablelog]
     Oueries value:
                                                                            HKLM\software\microsoft\fusion[logginglevel]
     Oueries value:
                                                                            HKLM\software\microsoft\fusion[forcelog]
     Oueries value:
                                                                            HKLM\software\microsoft\fusion[logfailures]
     Queries value:
                                                                            HKLM\software\microsoft\fusion[versioninglog]
     Queries value:
                                                                            HKLM\software\microsoft\fusion[logresourcebinds]
     Oueries value:
                                                                            HKLM\software\microsoft\fusion[uselegacvidentityformat]
     Oueries value:
                                                                            HKLM\software\microsoft\fusion[disablemsipeek]
```

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

options[devoverrideenable]

Queries value:

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

Queries value:

Oueries value:

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

Oueries value

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ folder descriptions \ 'all folder \ a03a-e3ef65729f3d \ `parent folder' \ a03a-e3ef65729f3d \ `parent folder' \ a03a-e3ef65729f3d \ 'parent \$

Oueries value:

 $\label{thm:local-condition} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cite{thm:local-condition} a03a-e3ef65729f3d \cite{thm:local-condition} \footnote{thm:local-condition} description \cite{thm:local-condition} \end{tikzpicture}$

Queries value:

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

Queries value:

Queries value

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

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]

ueries value:

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

Queries value:

 $\label{lem:hkkm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hkkm} a 3a-e 3e f 65 72 9f 3d \cal{lem:hkkm} [roamable]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} Hk \Label{lem:hklm} In the label{lem:hklm} Which is the label{lem:hkklm} Which is the$

 $\label{thm:constraint} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ value \\$

folders[appdata]

 Queries value:
 HKLM\system\currentcontrolset\control\nls\customlocale[en-us]

 Queries value:
 HKLM\system\currentcontrolset\control\nls\sextendedlocale[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]

are-ea331706 Oueries value:

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

Queries value:

 $\label{thm:local-prop} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}\[parentfolder]\]$

Queries value:

 $\label{thm:local-parameters} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[description]}$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [relative path]$

Queries value:

9afe-ea3317b67173}[parsingname]

Oueries value:

9afe-ea3317b67173}[infotip]

Queries value:

9afe-ea3317b67173}[localizedname]

Oueries value:

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

9afe-ea3317b67173}[security]

Oueries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (5e6c858f-0e22-4760-1000) \ model \ model \ model) \ model \ model$ 9afe-ea3317b67173}[streamresourcetype]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-164e7descriptions\} \ folder \ fold$ 9afe-ea3317b67173}[localredirectonly]

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-164e7descriptions\} \ folder \ fold$ 9afe-ea3317b67173}[precreate]

Queries value:

9afe-ea3317b67173}[stream]

Oueries value:

9afe-ea3317b67173}[publishexpandedpath]

Queries value:

9afe-ea3317b67173}[attributes1

Oueries value:

9afe-ea3317b67173}[foldertypeid]

Queries value:

9afe-ea3317b67173}[initfolderhandler]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]

Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64[latestindex]

Queries value:

 $\label{local_hamilton} HKLM \software \mbox{\sc microsoft} \sc matrive images index \sc 2.0.50727_64 \sc microsoft \sc matrixed in the local matrixed in$

Queries value:

 $HKLM \verb|\software\microsoft| fusion \verb|\nativeimagesindex| v2.0.50727_64 \verb|\index21[ilusagemask]| line for the software microsoft fusion fusion for the software microsoft fusion fusion$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[displayname] Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[configmask]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[configstring]

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[mvid]$ Queries value:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_64 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus 1[evalation data]$ Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[status]$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[ildependencies] Queries value:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_64 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus 1[nidependencies]$ Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_64 \ ni \ 181938c6 \ 7950e2c5 \ 1[missing dependencies]$

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_64 \setminus i1 \setminus 7950e2c5 \setminus 6f33d37e \setminus 1[display name]$ Queries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ il\ 7950e2c5 \ 6f33d37e \ 1[status]$ Oueries value:

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

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_64 \setminus i1 \setminus 7950e2c5 \setminus 6f33d37e \setminus 1[sig]$ Queries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ il\ 7950e2c5 \ 6f33d37e \ 1[last mod time]$ Oueries value:

HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,amd64] Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]

HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Queries value:

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251ba85-6007caedcf9d}[category]

Queries value:

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\sc Nicrosoft \windows \current version} \ensuremath{\sc Nicrosoft \current \current$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ folder\ folder \ folder \ folder \ folder \ folder \ folder \ folder \$

Oueries value:

Ouerieevelue

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{352481e8-33be-4251-ba85-6007 \ caed \ for \ folder \ for \ for \ for \ folder \ for \ for \ for \ folder \ for \ for$

Oueries value:

 $\label{thm:local-continuous} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\footing{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]$

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]

Queries value:

 $HKLM \software \mbox{$microsoft\windows\currentversion} \explorer \folder descriptions \footnote{1} \footnote{1} \footnote{2} \footno$

Queries value

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

Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]

Oueries value:

 $\label{thm:local_thm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cite{252481e8-33be-4251-ba85-6007} \cite{252481e8-33be-4251-ba85-6$

Queries value:

Oueries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ cf9d \ fstream\}$

Queries value:

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

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:

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

Queries value:

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

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

folders[cache]

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

Queries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ ni \ 61e7e666 \ c991064 \ 10[display name] \\ Oueries \ value:$

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

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

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

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

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

 $\label{lem:hklmsoftware} HKLM \software \mbox{$\sim 0.50727_64$ in $61e7e666$ c991064$ 10[ildependencies]} \\ Queries value:$

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

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

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

- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_64 \ il \ 475 dce 40 \ 6604 efc \ 3[status] \\ Oueries \ value:$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-observation} HKLM \software \microsoft \single 2.0.50727_64 \single 1.475 \single 2.0.50727_64 \sin$
- $HKLM \ software \ `microsoft \ fusion \ `native images in dex \ `v2.0.50727_64 \ 'il \ '475 dce 40 \ '6604 efc \ '3[last mod time] \\ Oueries \ value:$
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_64 \ il\ 19ab8d57 \ 5206cfdb \ 7[display name] \\ Oueries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[status]
 Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727_64 \normalized 11 \normalized 19 ab 8d 57 \sion \norm$
- $\label{local-prop} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_64\il\19ab8d57\5206cfdb\7[sig] \\ Oueries\ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[lastmodtime]
 Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \slices on \slices and \slices a like \slices of \slices \slices on \slices \slices$
- $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} in a tive images in dex $$\v2.0.50727_64$ in $\c20.6bbd663d$ 4[status] Queries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[modules]
 Queries value:
- $\label{lem:hklmsoftware} HKLM \software \microsoft \size 1.0.50727_64 \noindent \noindent\noindent \noindent \noindent \noindent \noindent \noindent \noin$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[lastmodtime]
 Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} in a tive images in dex $$\v2.0.50727_64$ in $\d424bd4d8$ \sc210819fb $$\end{\mathbb{G} display name} $$ Queries value:$
- $\label{local-bound} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_64\il\424bd4d8\210819fb\6[status] Oueries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6[modules] Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6[sig]
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f[displayname]
 Oueries value:
- $\label{local-operator} HKLM \software \microsoft \sion \native images in dex \normalized \normalized$
- $\label{local-equation} HKLM \software \mbox{$\mbox{$\mbox{w} index}$} Like \software \mbox{$\mbox{$\mbox{$w$} index}$} All \software \mbox{$\mbox{$\mbox{w} index}$} All \software \software \mbox{$\mbox{$\mbox{w} index}$} All \software \software \mbox{$\mbox{$\mbox{w} index}$} All \software \mbox{$\mbox{$\mbox{$\mbox{w} index}$} All \software \mbox{$\mbox{$\mbox{$\mbox{w} index}$} All \software \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$w$} index}$} All \software \mbox{$\mbox{\m
- $\label{lem:hklm} HKLM \software \mbox{\mathbb{N} in a tive images in dex.} $$2.0.50727_64 \il\41c04c7e\7a981124\1f[sig] $$Oueries value:$
- $\label{local-equation} HKLM \software \microsoft \fusion \native images in dex \normalized \normaliz$
- $\label{local-operator} HKLM \software \end{area} HKLM \software \end{area} IN 3ced 59c5 \bd 38540 \end{area} Oueries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3ced59c5\bd38540\f[status]
 Queries value:
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{local-hammac} HKLM\software\microsoft\fusion\native\mbox{images} index\v2.0.50727_64\il\aced59c5\bd38540\f[sig] \\ Oueries\ value:$
- $\label{lem:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \colone{lem:hklm} 1\colone{lem:hklm} ages in dex \colone{lem:hklm} 2\colone{lem:hklm} 2\colone{$
- $\label{local-bound} HKLM \software \microsoft \sin \native images in dex \v2.0.50727_64 \il\c991064 \ade 16fb6 \c90[display name] \\ Oueries \value:$
- $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex \normalized by the local example of t$
- $\label{local-bound} HKLM \software \microsoft \sion \native images in dex \slash 2.0.50727_64 \slash 1 \colone{local-bound} Cueries \slash 2.0.50727_64 \slash 2.0.5$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\c991064\34e16fb6\20[sig] Oueries value:
- $\label{local-equation} HKLM \software \sinces of this ion \native images in dex \v2.0.50727_64 \il\c991064 \addition{1}{34e16fb6 \addition{2}{20[last mod time]}} Queries value:$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{lem:hklmsoftware} HKLM\software\microsoft\fusion\native\magesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[configmask] Queries value: \\ HKLM\software\microsoft\fusion\native\magesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[configstring] \\ HKLM\software\microsoft\fusion\native\magesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[configstring] \\ HKLM\software\microsoft\fusion\native\magesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[configstring] \\ HKLM\software\microsoft\fusion\native\magesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[configstring] \\ HKLM\soft\magesindex\m$
- Queries value:

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

- $\label{lem:hklmsoftware} HKLM \software \mbox{\le 1.050727_64\ni\30bc7c4f\sf50fe4f\sf$ [ildependencies] } Queries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[nidependencies]
 Queries value:
- $\label{lem:hklmsoftware} HKLM \software \single sindex \single s$
- $\label{lem:hklmsoftware} HKLM \software \since \s$

```
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3f50 fe4 f \setminus 6ff8 cf57 \setminus 8[status]
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3f50fe4f \setminus 6ff8cf57 \setminus 8[modules]
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3f50fe4f \setminus 6ff8cf57 \setminus 8[sig]
    Queries 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[last modtime]
     Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 9[displayname]
    Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[configmask]
     Oueries value:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_64 \ ni\ 3cca06a0\ 6dc7d4c0\ 9[configstring]
    Queries 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[mvid]
    Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[evalationdata]
     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[ildependencies]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni\ 3cca06a0\ 6dc7d4c0\ 9[nidependencies]
Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 64\il\6dc7d4c0\153b7f91\9[displayname]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 6dc7d4c0 \ 153b7f91 \ v9[status]
     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[modules]
     Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 64\il\6dc7d4c0\153b7f91\9[sig]
    Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\6dc7d4c0\153b7f91\9[lastmodtime]
HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
    Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.drawing.2.0.0.0..b03f5f7f11d50a3a.msil]
    Oueries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} in \label{lem:hklm} If it is a simple state \label{lem:hklm} If it is a simple state \label{lem:hklm} If it is a simple state \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} If it is a simple state \label{lklm} If it is a simple state \label{lk
     Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
    Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} which is a considerable software \label{lem:hklm} which is a considerable software \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lklm} \label{lk
    Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[system.deployment, 2.0.0.0, , b03f5f7f11d50a3a, msil] + (b1) + (b2) 
     Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.serialization.formatters.soap,2.0.0.0,,b03f5f7f11d50a3a,msil]
    Queries value:
HKLM \ software \ microsoft \ fusion \ gacchange notification \ default [accessibility, 2.0.0.0, ,b03f5f7f11d50a3a, msil]
    Queries value:
HKLM \label{lem:hklm} Software \verb|\microsoft| fusion \| gacchange notification \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \verb|\microsoft| fusion \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the software \| default[system.security, 2.0.0.0, , b03f5f7f11d50a3a, msil] | the soft
     Queries value:
                                                                  HKLM\software\microsoft\.netframework[dbgjitdebuglaunchsetting]
     Oueries value:
                                                                  HKLM\software\microsoft\.netframework[dbgmanageddebugger]
                                                                  HKLM\hardware\devicemap\video[maxobjectnumber]
    Oueries value:
    Oueries value:
                                                                  HKLM\hardware\devicemap\video[\device\video0]
                                                                  HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-
    Queries value:
08002be10318}\0000[pruningmode]
     Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[clientcachesize]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\nls\customlocale[ko-kr]
     Oueries value:
                                                                  HKLM\svstem\currentcontrolset\control\nls\extendedlocale[ko-kr]
    Oueries value:
                                                                  HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-cn]
                                                                  HKLM\system\currentcontrolset\control\nls\customlocale[ja-jp]
    Queries value:
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\nls\extendedlocale[ja-jp]
    Queries value:
                                                                  HKLM\system\currentcontrolset\control\nls\customlocale[zh-tw]
    Oueries value:
                                                                  HKLM\svstem\currentcontrolset\control\nls\extendedlocale[zh-tw]
    Oueries value:
                                                                  HKLM\system\currentcontrolset\control\nls\customlocale[zh-hk]
    Oueries value:
                                                                  HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hk]
                                                                  HKLM\system\currentcontrolset\control\nls\locale[00000409]
     Queries value:
     Queries value:
                                                                  HKLM\system\currentcontrolset\control\nls\language groups[1]
                                                                  HKLM\system\currentcontrolset\control\cmf\config[system]
    Queries value:
    Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
     Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
                                                                 HKCU\software\microsoft\windows\currentversion\explorer\shell
    Queries value:
 folders[cache]
     Oueries value:
                                                                  HKLM\software\microsoft\rpc[maxrpcsize]
    Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
     Queries value:
                                                                  HKLM\system\setup[oobeinprogress]
     Queries value:
                                                                  HKLM\system\setup[systemsetupinprogress]
     Oueries value:
                                                                  HKLM\software\microsoft\rpc[idletimerwindow]
     Oueries value:
                                                                  HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
```

HKLM\software\microsoft\ole[defaultaccesspermission]

```
{\tt HKLM \ } system \verb| current control \verb| lsa[everyone includes a nonymous]|
  Queries value:
  Queries value:
                                      HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
                                      \label{thm:local_hammon} $HKLM\software\microsoft\cryptography\defaults\provider\microsoft\ strong
  Oueries value:
cryptographic provider[image path]
  Queries value:
                                      HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
  Queries value:
                                      HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constraint \end{tabular} in the c
                                      HKLM \verb|\software\policies\microsoft\cryptography[privatekeylifetimeseconds]|
  Oueries value:
  Oueries value:
                                      HKLM\software\microsoft\cryptography[machineguid]
  Oueries value:
                                      HKCU\console[screencolors]
  Queries value:
                                      HKCU\console[popupcolors]
  Queries value:
                                      HKCU\console[insertmode]
  Oueries value:
                                      HKCU\console[quickedit]
                                      HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
  Oueries value:
  Oueries value:
                                      HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                                      HKCU\console[codepage]
  Queries value:
                                      HKCU\console[screenbuffersize]
  Queries value:
                                      HKCU\console[windowsize]
  Oueries value:
                                      HKCU\console[windowposition]
  Oueries value:
                                      HKCU\console[fontsize]
  Queries value:
                                      HKCU\console[fontfamily]
  Queries value:
                                      HKCU\console[fontweight]
  Queries value:
                                      HKCU\console[facename]
  Oueries value:
                                      HKCU\console[cursorsize]
  Oueries value:
                                      HKCU\console[historybuffersize]
  Queries value:
                                      HKCU\console[numberofhistorybuffers]
  Queries value:
                                      HKCU\console[historynodup]
  Queries value:
                                      HKCU\console[colortable00]
  Oueries value:
                                      HKCU\console[colortable01]
  Oueries value:
                                      HKCU\console[colortable021
  Oueries value:
                                      HKCU\console[colortable031
  Queries value:
                                      HKCU\console[colortable04]
  Queries value:
                                      HKCU\console[colortable05]
  Queries value:
                                      HKCU\console[colortable06]
  Queries value:
                                      HKCU\console[colortable07]
  Oueries value:
                                      HKCU\console[colortable081
  Oueries value:
                                      HKCU\console[colortable091
  Queries value:
                                      HKCU\console[colortable10]
  Queries value:
                                      HKCU\console[colortable11]
  Queries value:
                                      HKCU\console[colortable12]
  Queries value:
                                      HKCU\console[colortable13]
  Oueries value:
                                      HKCU\console[colortable141
  Oueries value:
                                      HKCU\console[colortable15]
  Oueries value:
                                      HKCU\console[loadconime]
  Queries value:
                                      HKCU\console[extendededitkey]
  Oueries value:
                                      HKCU\console[extendededitkeycustom]
  Queries value:
                                      HKCU\console[worddelimiters]
  Queries value:
                                      HKCU\console[trimleadingzeros]
                                      HKCU\console[enablecolorselection]
  Queries value:
  Queries value:
                                      HKCU\console[scrollscale]
  Queries value:
                                      HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                      HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
  Oueries value:
  Oueries value:
                                      HKLM\software\microsoft\command processor[disableunccheck]
  Queries value:
                                      {\tt HKLM \setminus software \setminus microsoft \setminus command processor[enable extensions]}
  Queries value:
                                      HKLM\software\microsoft\command processor[delayedexpansion]
                                      HKLM\software\microsoft\command processor[defaultcolor]
  Queries value:
  Oueries value:
                                      HKLM\software\microsoft\command processor[completionchar]
  Queries value:
                                      HKLM\software\microsoft\command processor[pathcompletionchar]
                                      HKLM\software\microsoft\command processor[autorun]
  Oueries value:
  Oueries value:
                                      HKCU\software\microsoft\command processor[disableunccheck]
  Queries value:
                                      HKCU\software\microsoft\command processor[enableextensions]
                                      {\tt HKCU \setminus software \setminus microsoft \setminus command processor[delayed expansion]}
  Queries value:
  Queries value:
                                      HKCU\software\microsoft\command processor[defaultcolor]
  Queries value:
                                      HKCU\software\microsoft\command processor[completionchar]
  Oueries value:
                                      HKCU\software\microsoft\command processor[pathcompletionchar]
  Oueries value:
                                      HKCU\software\microsoft\command processor[autorun]
  Oueries value:
                                      HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
                                      HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\compatibility32[nslookup]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries64]
HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol\_catalog9 \ \ catalog\_entries 64 \ \ 00000000001 \ [packed catalogitem]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries 64 \ 000000000002 \ [packed catalog item]
```

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
 Oueries value:
- $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries 64 \ \ 000000000006 \ [packed catalog item]$ Queries value:
- $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries 64 \ \ 000000000007 \ [packed catalog item]$ Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
 Queries value:
- $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries 64 \ \ 000000000010 \ [packed catalog item]$ 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:
- $HKLM\system\current control set\services\winsock 2\parameters\namespace_catalog 5\catalog_entries 64\00000000001[library path]\ Queries\ value:$
- $HKLM\system\current control set\services\winsock 2\parameters\namespace_catalog 5\catalog_entries 64\00000000001[displaystring] \\ Queries\ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[providerid]
 Queries value:
- $HKLM\system\current control set\services\winsock 2\parameters\namespace_catalog 5\catalog_entries 64\00000000001 [address family] Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[storesserviceclassinfo] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries 64 \ 0000000000001 \ [providerinfo] \ Queries \ value:$
- $HKLM\system\current control set\services\winsock 2\parameters\namespace_catalog 5\catalog_entries 64\000000000002[library path]\\ Queries\ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[addressfamily]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries 64 \ 0000000000002 \ [supported namespace]$ Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[enabled]
 Oueries 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\000000000002[storesserviceclassinfo] Queries value:
- Queries value:

 HKI M\system\currentcontrolset\services\winsock2\narameters\namesnace_catalog5\catalog_entries64\00000000000003[disnlaystring
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries 64 \ 0000000000003 \ [displaystring] \\ Oueries \ value:$
- $HKLM\system\current control set\services\winsock 2\parameters\namespace_catalog 5\catalog_entries 64\000000000003[providerid]\ Queries\ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries 64 \ 0000000000003 \ [address family] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[supportednamespace]

 Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries 64 \0000000000003 \[enabled] \queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[version]
 Oueries value:
- $\label{local-bound} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[storesserviceclassinfo]\ Queries\ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerinfo]
 Oueries value:
- $HKLM\system\current controls et\services\winsock 2\parameters\namespace_catalog5\catalog_entries 64\0000000000001[library path]\\ Queries\ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004[providerid]
 Oueries value:
- $HKLM\system\current control set\services\winsock 2\parameters\namespace_catalog 5\catalog_entries 64\00000000004 [address family] \\ Queries\ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004[supportednamespace] Oueries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[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\00000000005[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]
Oueries 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\000000000005[storesserviceclassinfo]

Oueries value:

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

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

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

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

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

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

Queries value:

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

Queries value:

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]

Queries value:

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

Queries value:

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

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

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

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

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

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Oueries 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[appendtomultilabelname]

 $\label{lem:parameters} Queries \ value: \\ HKLM\ system\ current controls et\ services\ dns cache\ parameters\ [screen badtlds]$

 $\label{lem:queries} Queries \ value: \\ HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] \\$

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

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

```
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Oueries value:
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[directaccessguervorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prefer local overlower binding dns]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [disables martprotocol reordering]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register reverse lookup]
 Queries value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
 Oueries value:
HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[register wanadapters]|
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
 Queries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use compartments]
 Oueries value:
```

Queries value:

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

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

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

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

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

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

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

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

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

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

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

Queries value:

 $HKLM \ system \ \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-55779 \ daa70e9\} \ [searchlist]$

Queries value:

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hkklmsystem} HKLM \system \current controls et \end{to} $$ HKLM \system \current controls et \end{to} $$ 105d63-74c6-4dc1-87b7-55779 \daa 70e9 \end{to} $$ [domain] $$$

Queries value:

Queries value:

 $\label{thm:local-bound} $HKLM \simeq \operatorname{local-bound} $HKLM \simeq \operatorname{local-bou$

Queries value:

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

Queries value:

 $\label{thm:local-bound} $HKLM \simeq \max_{b=105d63-74c6-4dc1-87b7-55779daa70e9} [names erver] $$$

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationenabled] Oueries value:

 $\label{thm:local-be62-be66666963} However the definition of the decomposition of the decomp$

Queries value:

Queries value:

 $\label{thm:local-be} HKLM \system \current controls et \ensuremath{\sim} \ensuremath{\\sim$} \ensuremath{$\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$} \ensuremath{\\sim$}$

Queries value:

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

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:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \time faces \b5105d63-74c6-4dc1-87b7-55779 \parameters \time faces \end{substitute} \end{substitute} \end{substitute} In the face \system \sys$

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hammeters} HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9\}\ [maxnumber of address storegister]$

Queries value:

 $\label{thm:local-bound} HKLM \system \current controls et \services \tcpip \parameters \ \footnote{thm:local-bound} for all the substitutions of the substitution of$

Oueries value:

```
806e6f6e6963}[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disableadapterdomainname]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disabledynamicupdate]
    Queries value:
HKLM \ system \ current control set \ services \ trpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-d
806e6f6e6963}[enableadapterdomainnameregistration]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationmaxaddresscount]
HKLM \ system \ current control set \ services \ trpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-be62-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-defa-11e1-d
806e6f6e6963}[maxnumberofaddressestoregister]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enablemulticast]
    Queries value:
                                                            HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\datastore_v1.0[disable]|\\
                                                            HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
    Queries value:
                                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
    Queries value:
                                                           HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane2]|
                                                            HKLM\software\microsoft\windows
    Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|
    Queries value:
                                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                                                             HKLM\software\microsoft\windows
    Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane5]|
                                                            HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
                                                             HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
   Queries value:
                                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
                                                            HKLM\software\microsoft\windows
   Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
                                                             HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
                                                            HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
    Queries value:
                                                             HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane12]|
    Queries value:
                                                            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                                                            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[plane16]
                                                             HKLM\software\microsoft\ctf[enableanchorcontext]
    Oueries value:
```