Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 1167, Task ID: 4097

Task ID: 4097 Risk Level:

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

61.29 seconds Processing Time: Virtual Environment: IntelliVM

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

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

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

MD5: 9bde8983ac767c24755443627cda99bc

SHA256: ca0dcf72ce74fa1084255dae79a6a787eccf04152cfadd23f775a1671f1149cf

Description:

Pattern Matching Results

4 Reads process memory

2 Resolves local hostname

NET compiled executable

3 Long sleep detected

5 Query DNS from command line

4 Terminates process under Windows subfolder

Process/Thread Events

C:\windows\temp\RajivApp1.exe ["C:\windows\temp\RajivApp1.exe"]
C:\Windows\system32\cmd.exe ["cmd.exe"] Creates process:

Creates process:

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

Reads from process: PID:2932 C:\Windows\System32\nslookup.exe PID:3008 C:\Windows\System32\nslookup.exe Reads from process:

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

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1

\BaseNamedObjects\CorDBIPCSetupSyncEvent_2804 Creates event:

Creates event: \KernelObjects\LowMemoryCondition

Creates event: \BaseNamedObjects\ConsoleEvent-0x0000000000000B58 Creates event: \BaseNamedObjects\ConsoleEvent-0x0000000000000BAC Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1 Creates semaphore: \Sessions\1\BaseNamedObjects\GdiplusFontCacheFileV1

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

Opens: C:\Windows\System32\mscoree.dll Opens: C:\windows\temp\VERSION.dll Opens: C:\Windows\System32\version.dll Opens: C:\Windows\System32\sechost.dll Opens: C:\Windows\SYSTEM32\MSCOREE.DLL.local

Opens: C:\Windows\Microsoft.NET\Framework64\v2.0.50727 $C: \verb|\windows\Microsoft.NET\Framework64\Upgrades.2.0.50727\\|$ Opens:

Opens: C:\Windows\System32\imm32.dll Opens: C:\windows\temp\RajivApp1.exe.config Opens: C:\Windows\Temp\RajivApp1.exe

 $\label{lem:c:windows} \textbf{Microsoft.NET} \\ \textbf{Framework64} \\ \textbf{v2.0.50727} \\ \textbf{mscorwks.dll} \\ \textbf{model} \\ \textbf{mod$ Opens:

Opens: C:\windows\temp\RajivApp1.exe.Local\

Opens:

 $C: \verb|Windows| winsxs| amd 64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6| windows winsxs| amd 64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6| windows winsxs| amd 64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6| windows winsxs| amd 64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6| windows winsxs| windows wi$ Opens:

C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll Opens:

C:\Windows Opens:

Opens: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config Opens: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\fusion.localgac Opens: $\label{lem:c:windowsMicrosoft.NET\Framework64\v2.0.50727\config\security.config\energy} C: \Windows\Microsoft.NET\Framework64\v2.0.50727\config\security.con$

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\security.config.cch Opens:

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

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\enterprisesec.config.cch

```
C:\Windows\Globalization\Sorting\SortDefault.nls
   Opens:
   Opens:
                                                 C:\windows\temp\profapi.dll
   Opens:
                                                 C:\Windows\System32\profapi.dll
   Opens:
                                                 C:\Users\Admin
   Opens:
                                                 C:\Users\Admin\AppData\Roaming
   Opens:
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\64bit\security.config
                                                 C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\64bit\security.config.cch
                                                 C:\Windows\assembly\NativeImages_v2.0.50727_64\index143.dat
   Opens:
   Opens:
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0_b77a5c561934e089
   Opens:
   Opens:
                                                 C:\Windows\Temp
   Opens:
                                                 C:\Windows\Microsoft.NET\Framework64\v2.0.50727\ole32.dll
   Opens:
                                                 C:\Windows\System32\rpcss.dll
   Opens:
                                                 C:\windows\temp\CRYPTBASE.dll
   Opens:
                                                 C:\Windows\System32\cryptbase.dll
   Opens:
                                                 C:\Windows\System32\uxtheme.dll
   Opens:
                                                 C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
                                                 C:\windows\temp\RajivApp1.config
   Opens:
   Opens:
                                                 C:\Windows\System32\l_intl.nls
   Opens:
                                                 C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
   Opens:
                                                 C:\Windows\assembly\pubpol4.dat
   Opens:
                                                 C:\Windows\assembly\GAC\PublisherPolicy.tme
   Opens:
C: \verb|Windows| assembly \verb|NativeImages_v2.0.50727_64| System | adff7dd9fe8e541775c46b6363401b22| System.ni.dll | additional temperature of the state of the stat
C: \windows\assembly\NativeImages\_v2.0.50727\_64\System.Drawing\5910828a337dbe848dc90c7ae0a7dee2\System.Drawing.ni.dll
   Opens:
C: \windows \assembly \Native Images\_v2.0.50727\_64 \System. \Windows. Forms \assembly \Native Images\_v2.0.50727\_64 \System. \Windows. Forms \assembly \Ass
   Opens:
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089
                                                 \label{lem:c:windows} C: \windows \assembly \GAC\_MSIL \System \2.0.0.0\_b77a5c561934e089
   Opens:
   Opens:
                                                 C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0_b03f5f7f11d50a3a
   Opens:
{\tt C:\windows\assembly\GAC\_MSIL\System.Windows.Forms\2.0.0.0\_b77a5c561934e089\uxtheme.dll}
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089\System.Windows.Forms.dll
                                                 C:\Windows\Globalization\en-us.nlp
   Opens:
                                                 C: \verb|\Windows\Microsoft.NET\Framework64\v2.0.50727\Gdiplus.dll|
   Opens:
   Opens:
C:\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a
   Opens:
C:\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\GdiPlus.dll
                                                 {\tt C:\Users\Admin\AppData\Local\GDIPFONTCACHEV1.DAT}
   Opens:
   Opens:
                                                 C:\Windows\Fonts\ahronbd.ttf
   Opens:
                                                 C:\Windows\Fonts\tahoma.ttf
   Opens:
                                                 C:\Windows\Fonts\msjh.ttf
   Opens:
                                                 C:\Windows\Fonts\msyh.ttf
   Opens:
                                                 C:\Windows\Fonts\malgun.ttf
   Opens:
                                                 C:\Windows\Fonts\micross.ttf
   Opens:
                                                 C:\Windows\Fonts\segoeui.ttf
   Opens:
                                                 C:\windows\temp\dwmapi.dll
   Opens:
                                                 C:\Windows\System32\dwmapi.dll
   Opens:
                                                 C:\Windows\Fonts\StaticCache.dat
   Opens:
                                                 C:\Windows\System32\en-US\user32.dll.mui
                                                 C:\Windows\winsxs\amd64_microsoft.windows.common-
   Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac
                                                 C:\Windows\winsxs\amd64_microsoft.windows.common-
   Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac\comctl32.dll
   Opens:
                                                 C:\Windows\WindowsShell.Manifest
   Opens:
                                                 C:\Windows\system32\uxtheme.dll.Config
   Opens:
                                                 C:\windows\temp\cmd.exe
   Opens:
                                                 C:\Windows\System32\cmd.exe
   Opens:
                                                 C:\Windows\System32\apphelp.dll
                                                 C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
   Opens:
   Opens:
                                                 C:\windows\temp\CRYPTSP.dll
   Opens:
                                                 C:\Windows\System32\cryptsp.dll
   Opens:
                                                 C:\Windows\System32\rsaenh.dll
   Opens:
                                                 C:\Windows\System32\winbrand.dll
   Opens:
                                                 C:\windows\temp\RpcRtRemote.dll
   Opens:
                                                 C:\Windows\System32\RpcRtRemote.dll
   Opens:
                                                 C:\Windows\System32\en-US\cmd.exe.mui
                                                 C:\Windows\system32\Branding\Basebrd\Basebrd.dll
   Opens:
                                                 {\tt C:\Windows\Branding\Basebrd\basebrd.dll}
   Opens:
   Opens:
                                                 C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
   Opens:
                                                 C:\Windows\System32\nslookup.exe
   Opens:
                                                 C:\Windows\AppPatch\AppPatch64\sysmain.sdb
   Opens:
                                                 C:\Windows\Prefetch\NSLOOKUP.EXE-3D06E09F.pf
   Opens:
                                                 C:\Windows\System32\wsock32.dll
   Opens:
                                                 C:\Windows\System32\mswsock.dll
   Opens:
                                                 C:\Windows\System32\dnsapi.dll
   Opens:
                                                 C:\Windows\System32\en-US\nslookup.exe.mui
   Opens:
                                                 C:\Windows\System32\WSHTCPIP.DLL
                                                 C:\Windows\System32\nlaapi.dll
   Opens:
   Opens:
                                                 C:\Windows\System32\NapiNSP.dll
```

Opens:

C:\Windows\System32\pnrpnsp.dll

C:\Windows\System32\winrnr.dll Opens: C:\Windows\System32\IPHLPAPI.DLL Opens: Opens: C:\Windows\System32\winnsi.dll Opens: C:\Windows\System32\dhcpcsvc6.dll Opens: C:\Windows\System32\dhcpcsvc.dll

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

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

Network Events

8.8.8.8.in-addr.arpa DNS query:

WORKGROUP DNS query: MSBROWSE DNS query: 8.8.8.8:53 Connects to: Sends data to: 8.8.8.8:53 Receives data from: 8.8.8.8:53

Windows Registry Events

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

Creates key: HKCU\software\microsoft\gdiplus

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

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

options

Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\svstem\currentcontrolset\control\nls\sorting\versions Opens kev: HKLM\svstem\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

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

Opens key: HKCU\

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

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside

Opens key: HKLM\

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

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

Opens key: HKLM\software\microsoft\.netframework

HKLM\software\microsoft\.netframework\policy\standards Opens key: Opens key: HKLM\software\microsoft\.netframework\policy\upgrades Opens key: HKLM\software\microsoft\.netframework\policy\apppatch

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 kev: HKLM\software\microsoft\windows nt\currentversion\compatibilitv32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: ${\tt HKCU \ } software \verb|\ microsoft \verb|\ .net framework \verb|\ policy \verb|\ standards$

Opens key: HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots

Opens key: HKCU\software\microsoft\.netframework Opens key: HKLM\software\microsoft\fusion

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

options\rajivapp1.exe

Opens key: HKCU\software\microsoft\fusion

Opens key:

Opens key:

 $HKLM \verb|\software\microsoft|. net framework \verb|\security\policy| extensions \verb|\namedpermissionsets\| internet | for the property of the proper$ Opens key:

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

980053277-1733835069-2361817685-1001

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions

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

Opens key:

a03a-e3ef65729f3d}

Opens key:

a03a-e3ef65729f3d}\propertybag

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

Opens key: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following \ description \ for the constraint \ description \ for the const$

Opens key:

 $\label{thm:local_hammon} HKCU \software \microsoft \windows \current version \explorer \session in folders \current \c$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders

HKLM\svstem\currentcontrolset\control\nls\customlocale Opens kev: Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\software\policies\microsoft\windows\explorer

```
Opens key:
                                                                                                           HKCU\software\policies\microsoft\windows\explorer
       Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
       Opens key:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-164e7descriptions\} \ for the software \ microsoft \ windows \ for the software \ microsoft \ micr
9afe-ea3317b67173}\propertybag
        Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
                                                                                                          HKLM\software\microsoft\.netframework\v2.0.50727\securitv\policv
       Opens kev:
       Opens key:
                                                                                                          HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64
       Opens key:
                                                                                                          HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_64 \ in dex 143
       Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 181938c6 \ 7950e2c5
      Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\82
       Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus i1 \setminus 7950e2c5 \setminus 19b8f67f \setminus 8200e2c5 \setminus 19b8f67f \setminus 19b8f67f \setminus 8200e2c5 \setminus 19b8f67f \setminus 19b8
ba85-6007caedcf9d}
       Opens key:
ba85-6007caedcf9d}\propertybag
       Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 38c56119 \ 1d3ee2d7
       Opens kev:
                                                                                                          HKLM\software\microsoft\strongname
                                                                                                          HKLM\software\microsoft\.netframework\internal\iit\perf
       Opens key:
       Opens key:
                                                                                                          HKLM\software\microsoft\fusion\publisherpolicy\default
       Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default \setminus policy. 2.0. system. windows. forms \underline{\phantom{}}b77a5c561934e089
       Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 64\ni\61e7e666\c991064
      Opens kev
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\83
        Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\2d382ce6\8d
      Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\1bd7b0d8\8f
      Opens kev
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_64 \ il\ 2dd6ac50 \ 163e1f5e \ 8acconstructions \ described by the software \ before the software \ microsoft \ fusion \ native images \ in dex \ v2.0.50727\_64 \ il\ 2dd6ac50 \ 163e1f5e \ 8acconstructions \ described by the software \ described \ described by the software \ described by the software \ described \ 
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7f3b6ac4\80
       Opens key
Opens key:
Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus mi \setminus 30bc7c4f \setminus 3f50fe4f \setminus 90bc7c4f \setminus 90bc
      Opens key:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_64 \ il\ 3f50 fe4f \ bf1 da7aa \ bg1 \ bg2 \ 
       Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\84
       Opens key:
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.drawing_b03f5f7f11d50a3a
        Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system_b77a5c561934e089
      Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. \ system. \ xml\_b77a5c561934e089
      Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. system. configuration \underline{\ b03f5f7f11d50a3a}
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.deployment__b03f5f7f11d50a3a
      Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default \setminus policy. 2.0. system. runtime. serialization. for matters. so ap\_b03f5f7f11d50a3a
       Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.accessibility_b03f5f7f11d50a3a
        Opens key:
HKLM \label{lem:hklm} Which is a fixed by the second of 
                                                                                                          HKLM\software\microsoft\.netframework\policy\aptca
       Opens key:
       Opens key:
                                                                                                           HKLM\hardware\devicemap\video
                                                                                                          Opens kev
 1e1a187c13e9}\0000
       Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\fonts
       Opens key:
       Opens key:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
       Opens key:
                                                                                                          HKCU\eudc\1252
       Opens key:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
        Opens key:
                                                                                                           HKLM\system\currentcontrolset\control\nls\locale
       Opens key:
                                                                                                           HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
       Opens kev:
                                                                                                          HKLM\system\currentcontrolset\control\nls\language groups
                                                                                                          HKLM\software\microsoft\windows
```

Opens key:

nt\currentversion\languagepack\datastore_v1.0

```
HKLM\software\microsoft\windows
      Opens key:
nt\currentversion\languagepack\surrogatefallback
     Opens key:
                                                                              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
     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
     Opens kev:
                                                                               HKLM\system\currentcontrolset\control\session manager\appcertdlls
     Opens key:
                                                                              HKLM\system\currentcontrolset\control\session manager\appcompatibility
     Opens key:
                                                                               HKLM\software\policies\microsoft\windows\appcompat
     Opens key:
                                                                              HKCU\software\microsoft\windows nt\currentversion
     Opens key:
                                                                               \label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current\version\app compatflags\layers} \\
     Opens key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\appcompatflags
     Opens key:
                                                                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
      Opens kev:
                                                                              HKLM\software\microsoft\rpc
      Opens key:
                                                                              HKLM\system\currentcontrolset\control\computername\activecomputername
     Opens key:
                                                                              HKLM\system\setup
     Opens key:
                                                                              HKLM\software\policies\microsoft\windows nt\rpc
     Opens key:
                                                                               HKLM\software\policies\microsoft\sqmclient\windows
                                                                              HKLM\software\microsoft\sqmclient\windows
     Opens key:
     Opens key:
                                                                               HKCU\software\classes\
                                                                              HKCU\software\classes\appid\rajivapp1.exe
     Opens key:
     Opens key:
                                                                               HKCR\appid\rajivapp1.exe
     Opens key:
                                                                               HKLM\software\microsoft\ole\appcompat
     Opens kev:
                                                                              HKLM\system\currentcontrolset\control\lsa
     Opens key:
                                                                              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 cryptographic provider
                                                                               HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
      Opens key:
      Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                                                                              HKLM\software\policies\microsoft\cryptography
     Opens kev:
     Opens key:
                                                                              HKLM\software\microsoft\cryptography
     Opens key:
                                                                               {\tt HKLM \ } software \verb|\ microsoft \verb|\ cryptography \verb|\ offload|
      Opens key:
                                                                              \label{local-cond} \mbox{HKCU\software\classes\interface} \ \{00000134-0000-0000-c000-000000000046\} \ \mbox{HKCU\software\classes\second} \ \ \mbox{HKCU\software\classes\secon
     Opens key:
                                                                              HKCR\interface\{00000134-0000-0000-c000-00000000046}
     Opens key:
                                                                              HKCU\software\classes\interface\{00000134-0000-0000-c000-
00000000046}\proxystubclsid32
      Opens key:
                                                                              Opens key:
                                                                              HKLM\software\microsoft\rpc\extensions
      Opens key:
                                                                              HKLM\system\currentcontrolset\services\bfe
     Opens key:
                                                                               HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
     Opens key:
                                                                              HKLM\software\microsoft\sqmclient\windows\disabledsessions\
     Opens key:
                                                                               HKCU\software\policies\microsoft\windows\system
     Opens key:
                                                                              HKLM\software\microsoft\command processor
     Opens key:
                                                                               HKCU\software\microsoft\command processor
      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:
                                                                              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell} folders}
      Opens key:
                                                                              \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \en
     Opens key:
                                                                              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\nslookup.exe
     Opens key:
                                                                              HKLM\system\currentcontrolset\services\winsock2\parameters
     Opens kev:
                                                                              HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
     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:
\label{local-proposed} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ is $i$ and $i$
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64
    Opens key:
HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol\_catalog\_entries 64 \ \ 0000000000001
     Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ possible \ and \ protocol\_catalog\_entries \ protocol\_catalog \ protoc
     Opens key:
Opens key:
Opens kev
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ possible \ and \ protocol\_catalog\_entries \ protocol\_catalog \ protoc
     Opens key:
Opens key:
Opens key:
```

Opens kev:

```
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
  Opens kev:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries 64
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000001
  Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000003
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000005
  Opens key:
Opens kev:
                                 HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:
                                 HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:
                                 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:
                                 HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:
                                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:
                                 HKLM\system\currentcontrolset\services\tcpip\parameters
  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
  Opens key:
                                 HKLM\system\currentcontrolset\services\dns
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
  Opens key:
                                 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
  Opens kev:
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5bae0b1}
  Opens key:
                                 HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:
                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\microsoft sans serif
  Opens key:
Opens key:
                                 HKLM\software\microsoft\ctf\compatibility\rajivapp1.exe
  Opens key:
                                 HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:
                                 HKLM\software\microsoft\ctf\
                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
  Oueries value:
options[disableusermodecallbackfilter]
  Queries value:
                                 HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Oueries value:
                                 HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Oueries value:
                                 HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
                                 HKCU\control panel\desktop[preferreduilanguages]
  Queries value:
                                 HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
                                 HKLM\software\microsoft\.netframework[installroot]
  Oueries value:
                                 HKLM\software\microsoft\.netframework[clrloadlogdir]
  Oueries value:
  Oueries value:
                                 HKLM\software\microsoft\.netframework[onlyuselatestclr]
                                 HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
                                 HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\compatibility32[rajivapp1]
                                 HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\windows[loadappinit_dlls]
                                 HKLM\software\microsoft\.netframework[gcstressstart]
  Queries value:
  Queries value:
                                 HKLM\software\microsoft\.netframework[gcstressstartatjit]
                                 HKLM\software\microsoft\.netframework[disableconfigcache]
  Queries value:
  Oueries value:
                                 HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-
931b-d9cc2eee27e41
  Oueries value:
                                 HKLM\system\currentcontrolset\control\wmi\security[cc2bcbba-16b6-4cf3-
8990-d74c2e8af500]
  Queries value:
                                 HKLM\software\microsoft\fusion[cachelocation]
                                 HKLM\software\microsoft\fusion[downloadcachequotainkb]
  Oueries value:
                                 HKLM\software\microsoft\fusion[enablelog]
  Oueries value:
```

HKLM\software\microsoft\fusion[logginglevel]

Oueries value:

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

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

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

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

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

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

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

options[devoverrideenable]

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \category\cite{Mklmsoftware} \cite{Mklmsoftware} \cite{Mklmsoftware}$

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \end{substitute} $$4.6569-4cf6-a03a-e3ef65729f3d \cal{lem:hklmsoftware} $$1.6569-4cf6-a03a-e3ef65729f3d \cal{lem:hklmsoftware} $$1.6569-4cf6-a03a-e3ef6572$

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value

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

Queries value:

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

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

folders[appdata]

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[relativepath]
  Queries value:
9afe-ea3317b67173}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localizedname]
  Queries value:
9afe-ea3317b67173}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[security]
  Oueries value:
9afe-ea3317b67173}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresourcetype]
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localredirectonly]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[roamable]
  Queries value:
9afe-ea3317b67173}[precreate]
  Oueries value:
9afe-ea3317b67173}[stream]
  Queries value:
9afe-ea3317b67173}[publishexpandedpath]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[attributes]
  Queries value:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-164e7descriptions\} \ for the software \ microsoft \ windows \ for the software \ microsoft \ micr
9afe-ea3317b67173}[foldertypeid]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[initfolderhandler]
                                   HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001[profileimagepath]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 64[latestindex]
  Queries value:
HKLM \verb|\software\microsoft\fusion\native images index \verb|\v2.0.50727_64\| index 143[nius age mask]|
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\index143[ilusagemask]
  Oueries value:
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\82[configmask]
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 181938c6 \ 7950e2c5 \ 82[configstring]
  Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 181938c6 \ 7950e2c5 \ 82[mvid]
  Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 181938c6 \ 7950e2c5 \ 82[evalation data]
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\82[status]
  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 82[ildependencies]
  Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 181938c6 \ 7950e2c5 \ 82[nidependencies]
HKLM \setminus software \setminus icrosoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus initial 1938c6 \setminus 7950e2c5 \setminus 82[missing dependencies]
  Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 7950e2c5 \ 19b8f67f\ 82[displayname]
  Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 7950e2c5 \ 19b8f67f\ 82[status]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 7950e2c5 \setminus 19b8f67f \setminus 82[modules]
  Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 7950e2c5 \ 19b8f67f \ 82[sig]
  Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\19b8f67f\82[lastmodtime]
```

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[mscorlib, 2.0.0.0, ,b77a5c561934e089, amd64]$

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-

Oueries value:

ba85-6007caedcf9d}[category]

Oueries value:

 $\label{thm:local-problem} HKLM \software \ensuremath{\sc Nicrosoft} windows \current version \ensuremath{\sc Nicrosoft} explorer \folder descriptions \folder \folde$

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:

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

Ouerieevelue

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

Oueries value:

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

Queries value:

Queries value:

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

Queries value

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

Oueries value:

Queries value:

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

Oueries value:

Queries value:

Oueries value:

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

Queries value:

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

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:

Queries value:

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

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] Queries value: HKLM\software\microsoft\.netframework[pinvokeinline] 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] HKLM\software\microsoft\fusion\publisherpolicy\default[index4] Queries value:

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default[legacypolicy timestamp]$

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \subseted in the label l$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\83[configmask]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\83[configstring]
 Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\83[mvid] Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\83[evalationdata]
Queries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted in a tive images in a tive images in dex $$\subseted vol. 0.50727_64 \mbox{\mathbb{N} icrosoft \subseted vol. 0.50727_64 \mbox{$$

 $\label{lem:hklm} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_64\ni\61e7e666\c991064\83[il dependencies] Queries value: \\ HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_64\ni\61e7e666\c991064\83[nide pendencies] \\ HKLM\soft\fusion\native images in dex \c901064\83[nide pendenc$

Queries value:

- Queries value:
- $\label{lem:hklmsoftware} HKLM \software \subseted in the limit of th$
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{lem:hklmsoftware} HKLM \software \end{substrate} HKLM \software \end{substrate} Nucries value: \\ Oueries value:$
- $\label{lem:hklmsoftware} HkLM \software \subseted in the limit of th$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\1bd7b0d8\8f[displayname]
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\1bd7b0d8\8f[status] Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\1bd7b0d8\8f[modules]
 Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\1bd7b0d8\8f[sig] Oueries value:
- $\label{lem:hklmsoftware} HkLM \software \sinces of this ion\native images in dex \v2.0.50727_64 \il\nabel{lem:hklmsoftware} \label{lem:hklmsoftware} Queries \ value:$
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727_64\mbox{\sl}\sl 2dd6ac50\mbox{\sl}\sl 63e1f5e\8a[displayname] Queries\ value:$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized a constraint \normalized \nor$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\163e1f5e\8a[sig]
 Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\1c83327b\8e[displayname]
 Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \mbox{\sim11424bd4d81c83327b8e[status] Queries value:}$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\1c83327b\8e[sig] Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \sinces of this ion \sinces in dex \sinces of the last model in the last model$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-prop} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_64 \label{local-prop} 11\times \times \v2.0.50727_64 \label{local-prop} 11\times \v2.0.50727_64 \label{local-prop} 12\times \v2.0.50727_64 \label{local$
- $\label{lem:hklm} $HKLM \setminus software \ensuremath{\mbox{\mbox{\times}} \ensuremath{\mbox{\times}} \ensuremath{$
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_64\il\41c04c7e\7f3b6ac4\80[last mod time] \\ Queries\ value:$
- $\label{lem:hklmsoftwaremicrosoft} HKLM \software \since \since$
- $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_64\il\aced59c5\lb2590b1\85[status] Queries\ value:$
- $\label{lem:hklmsoftware} HkLM \software \end{area} Hklm \software \end{area} In $$ 1.50727_64 \il\aced59c5 \begin{area} 1.3ced59c5 \begin{area} 1.3c$
- $\label{lem:hklmsoftware} $$HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_64\mbox{il}\aced59c5\nb2590b1\85[sig] Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \sinces of this ion \sinces in dex \sinces value: \\ Queries \sinces value:$
- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_64 \ il\ c991064 \ 2bd33e1c\ 81[display name] \\ Oueries\ value:$
- $\label{local-equation} HKLM \software \mbox{\le index$ \le 0.50727_64$ il $<$ 991064$ \ge d33e1c$ \le Queries value:$
- $\label{local-bound} HKLM \software \microsoft \sion \native images in dex \v2.0.50727_64 \il\c991064 \2bd33e1c\81 \ [modules] \\ Oueries \ value:$
- $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex\v2.0.50727_64\il\c991064\2bd33e1c\81[sig] \\ Oueries\ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\c991064\2bd33e1c\81[lastmodtime]
 Queries value:
- $\label{local-equation} HKLM \software \microsoft \fusion \native images in dex \normalises 2.0.50727_64 \ni\30bc7c4f \3f50fe4f \90[display name] \\ Queries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\90[configmask] Queries value:
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \sion 2.0.50727_64 \ni\30bc7c4f\3f50fe4f\90[configstring] Queries value:$
- $\label{lem:hklmsoftware} HkLM \software \end{subarray} HkLM \software \end{subarray} $$\text{Min} \array \end{subarray} $$\text{Mi$
- $\label{localization} HKLM\software\microsoft\fusion\native images in dex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\90[evalation data] \\ Queries\ value:$
- $\label{local-observative} HKLM \software \mbox{$\mbox{$\mbox{\sim}}$ index \scales. } 2.0.50727_64 \mbox{$\mbox{$\sim$}} 130bc7c4f \scales. \\ Queries value:$
- $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\90[ildependencies] Queries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\90[nidependencies]
 Oueries value:

```
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3f50fe4f\6f1da7aa\90[displayname]
    Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 3f50fe4f\ 6f1da7aa\ 90[status]
    Oueries value:
Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_64 \setminus i1 \setminus 3f50fe4f \setminus 6f1da7aa \setminus 90[sig]
    Queries value:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_64 \ il\ 3f50fe4f \ 6f1da7aa \ 90[last mod time]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni\ 3cca06a0\ 6dc7d4c0\ 84[displayname]
\label{locality} HKLM \software \microsoft \fusion \native images in dex \normality of the local transfer of
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\84[configstring]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni\ 3cca06a0\ 6dc7d4c0\ 84[mvid]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus ni \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 84[evalation data]
    Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 64\ni\3cca06a0\6dc7d4c0\84[status]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ ni \ 3cca 06a0 \ 6dc 7d4c0 \ 84[ildependencies]
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus ni \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 84[nidependencies]
    Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 64\ni\3cca06a0\6dc7d4c0\84[missingdependencies]
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 6dc7d4c0 \setminus a5cd4db \setminus 87[displayname]
    Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 6dc7d4c0\ a5cd4db\ 87[status]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 6dc7d4c0\ a5cd4db\ 87[modules]
    Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_64 \ il\ 6dc7d4c0\ a5cd4db\ 87[sig]
    Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_64 \setminus i1 \setminus 6dc7d4c0 \setminus a5cd4db \setminus 87[lastmodtime]
   Oueries value:
HKLM \setminus software \setminus icrosoft \setminus fusion \setminus gacchangenotification \setminus default[system.windows.forms, 2.0.0.0, , b77a5c561934e089, msil]
    Queries value:
HKLM \label{lem:hklm} Which is a few and in the latest and the l
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default [system, 2.0.0.0, , b77a5c561934e089, msil]
    Oueries value:
HKLM \ software \ microsoft \ fusion \ vacchange notification \ default [system.xml, 2.0.0.0, ,b77a5c561934e089, msil] \ default [system.xml, 2.0.0.0, ,b77a5c561934e089, msil] \ default \ fusion \ vacchange notification \ default \ fusion \ vacchange \ notified \ noti
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default [system.configuration, 2.0.0.0, ,b03f5f7f11d50a3a, msil] \\
    Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.deployment,2.0.0.0,,b03f5f7f11d50a3a,msil]
    Queries value:
Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default[accessibility, 2.0.0.0, ,b03f5f7f11d50a3a, msil]
    Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil]
                                                          HKLM\software\microsoft\.netframework[dbgjitdebuglaunchsetting]
    Oueries value:
                                                          HKLM\software\microsoft\.netframework[dbgmanageddebugger]
    Queries value:
    Queries value:
                                                          HKLM\hardware\devicemap\video[maxobjectnumber]
                                                          HKLM\hardware\devicemap\video[\device\video3]
    Queries value:
                                                          Oueries value:
1e1a187c13e9}\0000[pruningmode]
                                                          HKCU\software\microsoft\gdiplus[fontcachepath]
    Oueries value:
                                                          Oueries value:
    Queries value:
                                                          HKLM\system\currentcontrolset\control\nls\language groups[1]
                                                          HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                                                          HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
    Oueries value:
                                                          HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane1]|
                                                          HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
                                                          HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|
    Oueries value:
                                                          HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane4]|
    Queries value:
                                                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
    Queries value:
                                                          HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane6]|
    Queries value:
                                                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
                                                          HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
    Oueries value:
                                                         HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
```

HKLM\software\microsoft\windows

```
HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                                                      HKLM\software\microsoft\windows
   Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane12]|
   Queries value:
                                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
   Queries value:
                                                      HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane14]|
   Oueries value:
                                                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
                                                      HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
    Queries value:
                                                      HKLM\system\currentcontrolset\control\cmf\config[system]
   Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]|
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
   Queries value:
                                                      HKLM\software\microsoft\rpc[maxrpcsize]
    Oueries value:
HKLM \verb| system| current control \verb| scomputername| active computername| | com
    Queries value:
                                                      HKLM\system\setup[oobeinprogress]
    Queries value:
                                                      HKLM\system\setup[systemsetupinprogress]
    Queries value:
                                                      HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Oueries value:
                                                      HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
                                                      HKLM \setminus software \setminus microsoft \setminus ole[defaultaccess permission]
   Oueries value:
   Queries value:
                                                      HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
   Queries value:
                                                      HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
    Queries value:
                                                      HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
                                                      HKLM\system\currentcontrolset\control\session
   Oueries value:
manager[safeprocesssearchmode]
    Queries value:
                                                      HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
    Queries value:
                                                      HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
   Queries value:
                                                      HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
   Oueries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constraint of the constrain
    Queries value:
                                                      HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography [privatekey lifetimeseconds] \\
    Queries value:
                                                      HKLM\software\microsoft\cryptography[machineguid]
                                                      Queries value:
    Queries value:
                                                      HKLM\software\microsoft\rpc\extensions[ndroleextdll]
                                                      HKLM\software\microsoft\rpc\extensions[remoterpcdll1]
   Oueries value:
    Queries value:
                                                      HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
    Oueries value:
                                                      HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes \cite{Months} \cite{Months}
    Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
   Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
                                                      HKLM\software\microsoft\command processor[disableunccheck]
    Oueries value:
    Queries value:
                                                      HKLM\software\microsoft\command processor[enableextensions]
    Queries value:
                                                      HKLM\software\microsoft\command processor[delayedexpansion]
    Oueries value:
                                                      HKLM\software\microsoft\command processor[defaultcolor]
    Queries value:
                                                      HKLM\software\microsoft\command processor[completionchar]
   Oueries value:
                                                      HKLM\software\microsoft\command processor[pathcompletionchar]
   Queries value:
                                                      {\tt HKLM \setminus software \setminus microsoft \setminus command processor[autorun]}
   Queries value:
                                                      HKCU\software\microsoft\command processor[disableunccheck]
    Queries value:
                                                      HKCU\software\microsoft\command processor[enableextensions]
    Oueries value:
                                                      HKCU\software\microsoft\command processor[delayedexpansion]
    Queries value:
                                                      HKCU\software\microsoft\command processor[defaultcolor]
    Oueries value:
                                                      \label{lem:hkcu} \verb+KKCU\+ software \verb+\microsoft \verb+\command processor[completionchar]+ \\
   Oueries value:
                                                      {\tt HKCU \setminus software \setminus microsoft \setminus command processor[pathcompletion char]}
    Queries value:
                                                      HKCU\software\microsoft\command processor[autorun]
                                                      HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
    Queries value:
    Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
                                                      HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\compatibility32[nslookup]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace callout]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameter \ protocol\_catalog 9 \ [num\_catalog\_entries 64]
   Oueries value:
Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameter \ protocol\_catalog9 \ catalog\_entries 64 \ 000000000002 \ [packed catalog item]
    Queries value:
HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol\_catalog9 \ (catalog\_entries 64 \ 000000000003 \ [packed catalog item]
   Oueries value:
```

nt\currentversion\languagepack\surrogatefallback[plane10]

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\00000000007[packedcatalogitem]
 Oueries value:
- $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries 64 \ \ 000000000008 \ [packed catalog item]$ Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\00000000010[packedcatalogitem]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries64]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[librarypath]
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries 64 \ 0000000000001 \ [displaystring] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[supportednamespace]

 Oueries value:
- 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:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[addressfamily] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerinfo]
 Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries 64 \ 00000000000001 \ library path] \\ Oueries \ value:$
- $\label{lem:hklm/system/current} HKLM\system\current\controlset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004[displaystring] \\ Queries\value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004[providerid]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries 64 \ 0000000000004 \ [address family] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\0000000000004[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[storesserviceclassinfo]
 Oueries value:
- $HKLM \label{lem:hklk} Whish system \current controls et \services \winsock 2 \parameters \names pace_catalog_entries 64 \0000000000004 \[providerinfo]$

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

 $HKLM \ system \ current controls et \ services \ \ win sock 2 \ parameters \ names pace_catalog5 \ catalog_entries 64 \ \ 000000000005 \ [displaystring]$ Oueries value:

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

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

 $HKLM \ system \ current control set \ services \ \ winsock 2 \ parameters \ namespace_catalog5 \ \ catalog_entries 64 \ \ 000000000005 \ [supported namespace]$ Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries 64 \ 0000000000005 \ [version]$ Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries 64 \ 000000000005 \ [storesserviceclassinfo]$ Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries 64 \ 0000000000006 [library path]$ Queries value:

 $HKLM \ system \ current controls et \ services \ \ win sock 2 \ parameters \ names pace_catalog5 \ catalog_entries 64 \ \ 000000000006 \ [displaystring]$ Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries 64 \ 0000000000006 \ [providerid]$

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

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries 64 \ 0000000000006 \ [supported namespace]$ Oueries value:

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

Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog_entries 64 \ 000000000006 [storesservice class info]$ Queries value:

Queries value:

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

Oueries value:

HKLM\svstem\currentcontrolset\services\winsock2\parameters[ws2 32spincount1

Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock \setminus parameters [transports]$

Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

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

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

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters| winsock [used elayed acceptance] |$

Queries value:

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

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnslookuporder] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain] Queries value: $\label{local-operator} $$HKLM \simeq \operatorname{local-operator-operat$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpsearchlist] HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: Oueries value:

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

Oueries value:

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

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

Queries value:

 $HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[used omain name devolution]| \\$

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

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

Queries value:

 $\label{local-operator-operat$

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]

Oueries value:

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

Oueries value:

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

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

Oueries value:

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries 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[registrationenabled] HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: $HKLM \setminus system \setminus current controls et \setminus services \setminus tcpip \setminus parameters [disable wandynamic update]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Queries value: Queries value: Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [maxnumber of addresses to register]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries 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\svstem\currentcontrolset\services\dnscache\parameters[registrationoverwrite] HKLM\svstem\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]

 $\label{lem:hkkm} HKL\dot{M}\xspace \xspace \xsp$

Oueries value:

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

Oueries value:

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

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]$

Queries value:

Queries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enabledhcp]$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \end{22873b3e-c4d3-495a-8165-e1e01c1f69b5} \[registration enabled]$

Queries value:

 $HKLM \system \current controls et \services \tcpip \parameters \time faces \equiv 22873b3e-c4d3-495a-8165-e1e01c1f69b5 \[register adapter name \]$

Oueries value:

 $\label{thm:local-services} HKLM \system \current controls et \end{22873b3} e-c4d3-495a-8165-e1e01c1f69b5 \[[domain] \]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \es \tcpip \parameters \ (22873b3e-c4d3-495a-8165-e1e01c1f69b5) \ [dhcpdomain]$

Queries value:

Oueries value:

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \es \tcpip \parameters \time faces \espace{22873b3e-c4d3-495a-8165-e1e01c1f69b5} \ [names erver]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\}[dhcpnameserver]$

Queries value:

 $\label{thm:local-bound} HKLM \system \current controls et \services \tcpip \parameters \ interfaces \ \{846ee 342-7039-11de-9d 20-806e 6f 6e 69 63\} \ [enabled \htmle help]$

Oueries value:

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [register adapter name]$

Queries value:

Queries value:

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \end{4.846} \end{4.846} and \system \current controls et \system \current \system \current \system \current \system \current \system \current \system \sys$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]

 $Queries \ value: \\ HKLM\system\current controls et\services\tcpip\linkage[bind]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \ (22873b3e-c4d3-495a-8165-e1e01c1f69b5) \ [queryadaptername]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{22873b3e-c4d3-495a-8165-e1e01c1f69b5} \ [disable adapter domain name]$

Queries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration maxaddress count]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[maxnumberofaddressestoregister]

Queries value:

 $\label{local-equ$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \time faces \end{4.846} \end{4.846} and \system \syste$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'topip \ 'parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963}[disable adapter domain name]$

Queries value:

Queries value:

 $\label{lem:hkkm} HKLM \system \current controls et \services \tcpip \parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6 666963\} \ [enable adapter domain name registration]$

Queries value:

 $\label{thm:local-bound} HKLM \system \current controls et \services \tcpip \parameters \ interfaces \ \{846ee 342-7039-11de-9d 20-806e 6f 6e 69 63\} \ [registration max address count]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee342-7039-11de-9d20-11de-9$ 806e6f6e6963}[maxnumberofaddressestoregister]

Queries value:

806e6f6e6963}[enablemulticast]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be070fb58b01c4a4}\languageprofile\0xx0000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]

HKLM\software\microsoft\ctf[enableanchorcontext]