Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 203, Task ID: 813

Task ID: 813 Risk Level: 3

Date Processed: 2016-04-28 13:09:53 (UTC)

Processing Time: 61.16 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\9a992314512bbc93b07328b3941fe048.exe"

Sample ID: 203 Type: basic Owner: admin

Label: 9a992314512bbc93b07328b3941fe048

Date Added: 2016-04-28 12:45:11 (UTC)

File Type: PE32:win32:gui File Size: 925112 bytes

MD5: 9a992314512bbc93b07328b3941fe048

SHA256: 72668272001346e2deb5d2f4ff6836f7a6a613a25dfcf456c61ed1adc3ef03ef

Description: None

Pattern Matching Results

3 Writes to a log file [Info]

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\9a992314512bbc93b07328b3941fe048.exe

["C:\windows\temp\9a992314512bbc93b07328b3941fe048.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\DirectSound DllMain mutex (0x0000021C)

Creates mutex: \BaseNamedObjects\RCPHost_Instance_Mutex
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED

Creates event: \Sessions\1\BaseNamedObjects\EClientDisconnect84500
Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

Creates event: \BaseNamedObjects\BFE_Notify_Event_{47ffaf7e-4003-4331-9f85-

b0689690ca53}

Creates event: \Sessions\1\BaseNamedObjects\DINPUTWINMM

File System Events

Creates: C:\ProgramData

Creates: C:\ProgramData\Remote Control PC

Creates: C:\ProgramData\Remote Control PC\apc-host.log
Creates: C:\ProgramData\Remote Control PC\hostaccount.ini
Creates: C:\ProgramData\Remote Control PC\hoststate.dat

Opens: C:\Windows\Prefetch\9A992314512BBC93B07328B3941FE-B154F679.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\System32\wow64log.dll

Opens: C:\Windows\SysW0W64

Opens: C:\windows\temp\9a992314512bbc93b07328b3941fe048.exe.Local\

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

C:\windows\temp\winmm.dll Opens: Opens: C:\Windows\SysWOW64\winmm.dll Opens: C:\windows\temp\dsound.dll Opens: C:\Windows\SysWOW64\dsound.dll C:\windows\temp\POWRPROF.dll Opens: Opens: C:\Windows\SysWOW64\powrprof.dll Opens: C:\windows\temp\wsock32.dll C:\Windows\SysWOW64\wsock32.dll Opens: C:\windows\temp\IPHLPAPI.DLL Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: Opens: C:\windows\temp\WINNSI.DLL C:\Windows\SysWOW64\winnsi.dll Opens: C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\WindowsShell.Manifest Opens:

C:\Windows\SysWOW64\en-US\setupapi.dll.mui Opens:

Opens: C:\windows\temp\9a992314512bbc93b07328b3941fe048.ENU Opens: C:\windows\temp\9a992314512bbc93b07328b3941fe048.ENU.DLL Opens: C:\windows\temp\9a992314512bbc93b07328b3941fe048.EN Opens: C:\windows\temp\9a992314512bbc93b07328b3941fe048.EN.DLL

Opens: C:\windows\temp\profapi.dll C:\Windows\SysWOW64\profapi.dll Opens:

Opens: C:\ProgramData

C:\ProgramData\Remote Control PC\ Opens: Opens: C:\ProgramData\Remote Control PC Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\windows\temp\dwmapi.dll Opens: C:\Windows\SysWOW64\dwmapi.dll Opens: C:\Windows\Fonts\StaticCache.dat Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui

Opens: C:\Windows\Temp

Opens: C:\

Opens: C:\ProgramData\Remote Control PC\apc-host.log Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

C:\Windows\SysWOW64\mswsock.dll Opens: Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL C:\Windows\SysWOW64\nlaapi.dll Opens: C:\Windows\SysWOW64\NapiNSP.dll Opens: Opens: C:\Windows\SysWOW64\pnrpnsp.dll Opens: C:\windows\temp\DNSAPI.dll C:\Windows\SysWOW64\dnsapi.dll Opens: Opens: C:\Windows\SysWOW64\winrnr.dll Opens: C:\windows\temp\dhcpcsvc6.DLL C:\Windows\SysWOW64\dhcpcsvc6.dll Opens: Opens: C:\windows\temp\dhcpcsvc.DLL Opens: C:\Windows\SysWOW64\dhcpcsvc.dll Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL Opens: C:\windows\temp\rasadhlp.dll Opens: C:\Windows\SysWOW64\rasadhlp.dll

Opens: C:\Windows\Temp\9a992314512bbc93b07328b3941fe048.exe

Opens: C:\windows\temp\MMDevAPI.DLL Opens: C:\Windows\SysWOW64\MMDevAPI.dll Opens: C:\windows\temp\PROPSYS.dll Opens: C:\Windows\SysWOW64\propsys.dll Opens: C:\windows\temp\libspeex.dll

C:\ProgramData\Remote Control PC\libspeex.dll Opens:

Opens: C:\windows\temp\libspeexdsp.dll

Opens: C:\ProgramData\Remote Control PC\libspeexdsp.dll C:\ProgramData\Remote Control PC\hostaccount.ini Opens: Writes to: C:\ProgramData\Remote Control PC\apc-host.log Writes to: C:\ProgramData\Remote Control PC\hostaccount.ini Writes to: C:\ProgramData\Remote Control PC\hoststate.dat

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

Reads from: C:\ProgramData\Remote Control PC\hostaccount.ini

Windows Registry Events

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

Opens key: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant of the constan$

options

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

HKLM\software\microsoft\wow64 Opens kev:

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options

Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

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

Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

HKLM\software\policies\microsoft\mui\settings

Opens key:

Opens key:

 $\label{thm:local_machine} \begin{tabular}{ll} HKCU \control panel \desktop \muicached \machine \label{thm:local_machine} anguage \configuration \end{tabular}$ Opens key: $HKLM \verb|\system| current controlset| control \verb|\mui| settings \verb|\language| configuration$ Opens key:

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: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side$

Opens key:

```
Opens key:
                         HKLM\system\currentcontrolset\control\nls\sorting\versions
 Opens key:
                         HKLM\
 Opens key:
                         HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
                         HKLM\software\wow6432node\microsoft\windows
 Opens kev:
nt\currentversion\gre_initialize
 Opens key:
                         HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
 Opens key:
                         HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
                         HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
 Opens key:
 Opens key:
                         HKLM\software\wow6432node\microsoft\ole
 Opens key:
                         HKLM\software\wow6432node\microsoft\ole\tracing
                         HKLM\software\microsoft\ole\tracing
 Opens key:
 Opens key:
                         HKLM\software\wow6432node\microsoft\oleaut
 Opens key:
                         HKLM\system\currentcontrolset\control\cmf\config
```

Opens kev: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup Opens key: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version$ Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key: HKCU\software\borland\locales

Opens key: HKLM\software\wow6432node\borland\locales Opens kev: HKCU\software\borland\delphi\locales Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions$

Opens key:

fdc1-4dc3-a9dd-070d1d495d97}

Opens kev:

fdc1-4dc3-a9dd-070d1d495d97}\propertybag

HKLM\software\wow6432node\microsoft\windows Opens key:

nt\currentversion\profilelist

Opens key:

Opens key: HKLM\system\currentcontrolset\control\nls\locale

HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens kev:

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink

Opens key: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\languagepack\datastore_v1.0|$

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\software\wow6432node\microsoft\rpc

Opens key: ${\tt HKLM \ } system \verb|\ current control \ \\ computer name \verb|\ active computer name \ \\$

Opens key: HKLM\system\setup

HKLM\software\wow6432node\policies\microsoft\windows nt\rpc Opens kev:

Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\software\policies\microsoft\sqmclient\windows Opens key:

HKLM\software\microsoft\samclient\windows Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\146b8021

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens key:

Opens key:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 0000000000001) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (cata$ Opens key:

Opens key:

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 000000000011) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (catal$ Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
 Opens key:
Opens key:
                   HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key:
                   HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key:
                   HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus 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\dnscache\parameters
 Opens key:
                   HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
 Opens key:
                   HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens key:
                   HKLM\software\wow6432node\policies\microsoft\system\dnsclient
 Opens key:
                   HKLM\software\policies\microsoft\system\dnsclient
                   HKLM\system\currentcontrolset\control\sqmservicelist
 Opens key:
 Opens key:
                   HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
 Opens key:
                   HKLM\system\currentcontrolset\services\dns
                   HKLM\software\wow6432node\policies\microsoft\windows
 Opens key:
nt\dnsclient\dnspolicyconfig
 Opens key:
                   HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
 Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
 Opens kev:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
 Opens key:
                   HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens key:
e1e01c1f69b5}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
 Opens key:
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 kev:
a0fb-4bfc-874a-c0f2e0b9fa8e}
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
 Opens key:
b2f1-4857-a4ce-a8e7c6ea7d27}
b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag
 Opens key:
1d43-42f2-9305-67de0b28fc23}
1d43-42f2-9305-67de0b28fc23}\propertybag
 Opens key:
                   Opens kev:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ multimedia\+ midimap
 Opens key:
 Oueries value:
                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
 Queries value:
                   HKLM\system\currentcontrolset\control\session
```

HKLM\system\currentcontrolset\control\terminal server[tsappcompat]

manager[cwdillegalindllsearch]

Queries value:

Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]

Oueries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]

Oueries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-

us[alternatecodepage]

Queries value: HKCU\control panel\desktop[preferreduilanguages]

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest] \ described by the side of the sid$

Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\gre_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\compatibility32[9a992314512bbc93b07328b3941fe048] HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\windows[loadappinit_dlls]

HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: HKLM\system\currentcontrolset\control\cmf\config[system] Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-Oueries value:

bc58-54c27d745f8f1

fdc1-4dc3-a9dd-070d1d495d97}[category]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[name]

fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[description]

fdc1-4dc3-a9dd-070d1d495d97}[relativepath]

fdc1-4dc3-a9dd-070d1d495d97}[parsingname]

fdc1-4dc3-a9dd-070d1d495d97}[infotip]

fdc1-4dc3-a9dd-070d1d495d97}[localizedname]

Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[icon]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[security]

fdc1-4dc3-a9dd-070d1d495d97}[streamresource]

 $HKLM \label{limits} \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{limits} HKLM \label{limits} HKLM \label{limits} \label{limits} \label{limits} \label{limits} HKLM \label{limits} \label{limits} HKLM \label{limits} \labell{limits} \label{limits} \labell{limits} \labell{limits} \labe$ fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]

fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]

fdc1-4dc3-a9dd-070d1d495d97}[roamable]

Queries value:

fdc1-4dc3-a9dd-070d1d495d97}[precreate]

fdc1-4dc3-a9dd-070d1d495d97}[stream]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{62ab5d82-day \ day \$ fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]

```
Oueries value:
HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[attributes]
fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
 Oueries value:
fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
 Oueries value:
                     HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\language groups[1]
 Oueries value:
                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                     HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
 Queries value:
                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                    HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane6]|
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
 Queries value:
                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
 Oueries value:
                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                    HKLM\software\microsoft\windows
 Queries value:
nt\current version \verb|\languagepack\surrogatefallback[plane12]|
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
 Queries value:
                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                    HKLM\software\microsoft\windows
 Queries value:
nt\current version \verb|\languagepack\surrogatefallback[plane15]|
                    HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
 Queries value:
                    HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
HKLM\svstem\currentcontrolset\computername\activecomputername[computername]
 Queries value:
                    HKLM\system\setup[oobeinprogress]
 Queries value:
                     HKLM\system\setup[systemsetupinprogress]
                    HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace callout]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Oueries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
```

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog \catalog_entries \namespace_catalog \catalog_entries \catalog \catalog_entries \catalog \catalog_entries \catalog \cat$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000002 [address family] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 00000000000003 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [provider info] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000004 \ [providerid] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 00000000000005 \ [displaystring] \ Queries \ value:$

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog \\ \setminus catalog_entries \setminus 0000000000005 [version]$

Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000005 \ [storesserviceclassinfo] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
 Oueries value:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]

Oueries value:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[storesserviceclassinfo] Queries value:

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

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

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

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

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

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

Queries value:

Queries value:

Queries value:

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

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

 Queries value:
 HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

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

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

Queries value:

Oueries value:

 $\label{lem:hklm} \verb+KLM\+ system \verb+ current control set \verb+ services \verb+ dns cache \verb+ parameters [usedomain name devolution]$

Queries value:

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

Queries value:

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

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

 $\label{lem:queries} Queries \ value: $$HKLM \simeq \colored \ \colore$

CLM\system\c Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen unreachable servers]$

Queries value:

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

Queries value:

 $\label{local-parameters} $$HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]$$$

Queries value:

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

Queries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
 Oueries 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]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus topip \setminus parameters [disable reverse address registrations]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [multicasts enderflags]
 Oueries 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:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Queries value:
```

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

Queries value:

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

Queries value:

Queries value:

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

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [search list]$

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [domain]$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [dhcpdomain]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [dhcpv6domain]$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ for a control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ for a control set \ services \ tcpip \ parameters \ interfaces \ for a control set \ services \ tcpip \ parameters \ interfaces \ for a control set \ services \ for \ services \ for a control set \ services \ for a control set \ services \ for \$

Queries value:

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

Queries value:

Queries value:

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

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

Queries value:

 $\label{lem:hklm} HKLM \ system \ `current controlset \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [queryadaptername]$

Queries value:

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

Queries value

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

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [maxnumber of addresses to register]$

Queries value:

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

Queries value:

Queries value:

 $HKLM \system \current controls et \services \tcpip \parameters \interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [disable adapter domain name]$

Queries value:

 $\label{lem:hklm} HKLM \system \current controlset \services \true \parameters \end{supplies} 11 de-9d20-806e6f6e6963 \end{supplies} 12 disable dynamic update \end{supplies}$

Oueries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d 20-806e6 f 6e 6963\} \ [enable adapter domain name registration]$

Oueries value

 $\label{thm:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [registration max address count]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [maxnumber of addresses to register]$

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [enable multicast]$

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value:

 $\label{lem:hklm} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{100} a 0fb-4bfc-874a-c0f2e0b9fa8e\footnote{100} [category]$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ [parent folder]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [description]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [relative path]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [parsing name]$

Oueries value

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\}[infotip]$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ [localized name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [icon]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [stream resource]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$

VIM) seftware

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ [local redirectonly]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\folderdes$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\}[precreate]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\}[stream]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Queries value:

 $\label{limit} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fold$

Queries value:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version[program files dir]|$

Queries value:

 $\label{local-bound} HKLM \software \wow 6432 node \windows \current version \explorer \folder descriptions \deformance \folder descriptions \deformance \folder \deformance \folder \deformance \folder \deformance \deformance \folder \folder \deformance \folder \folder\$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} \ [name]$

Queries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[parentfolder]

Oueries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[description]

Queries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[relativepath]

Oueries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[parsingname]

b2f1-4857-a4ce-a8e7c6ea7d27}[infotip]

Queries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[localizedname]

b2f1-4857-a4ce-a8e7c6ea7d27}[icon]

b2f1-4857-a4ce-a8e7c6ea7d27}[security]

b2f1-4857-a4ce-a8e7c6ea7d27}[streamresource]

b2f1-4857-a4ce-a8e7c6ea7d27}[streamresourcetype]

b2f1-4857-a4ce-a8e7c6ea7d27}[localredirectonly]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d65231b0-description\} \\ (d65231b0-description) \\ (d6523$ b2f1-4857-a4ce-a8e7c6ea7d27}[roamable]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[precreate]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d65231b0-description\} \\ (d65231b0-description) \\ (d6523$ b2f1-4857-a4ce-a8e7c6ea7d27}[stream]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[publishexpandedpath]

Oueries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d65231b0-description\} \\ (d65231b0-description) \\ (d6523$ b2f1-4857-a4ce-a8e7c6ea7d27}[attributes]

b2f1-4857-a4ce-a8e7c6ea7d27}[foldertypeid]

Oueries value:

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[initfolderhandler]

1d43-42f2-9305-67de0b28fc23}[category]

Oueries value:

1d43-42f2-9305-67de0b28fc23}[name]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[parentfolder]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[description]

1d43-42f2-9305-67de0b28fc23}[relativepath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[parsingname]

1d43-42f2-9305-67de0b28fc23}[infotip]

Queries value:

1d43-42f2-9305-67de0b28fc23}[localizedname]

Oueries value:

1d43-42f2-9305-67de0b28fc23}[icon]

Queries value:

1d43-42f2-9305-67de0b28fc23}[security]

Oueries value:

1d43-42f2-9305-67de0b28fc23}[streamresource]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f38bf404-f18bf404$ 1d43-42f2-9305-67de0b28fc23}[streamresourcetype]

Oueries value:

1d43-42f2-9305-67de0b28fc23}[localredirectonly]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f38bf404-f18bf404$ 1d43-42f2-9305-67de0b28fc23}[roamable]

Queries value:

1d43-42f2-9305-67de0b28fc23}[precreate]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[stream]

Queries value:

 $\label{thm:local_thm} \begin{tabular}{ll} HKLM \end{tabular} Software \wow 6432 node \microsoft \windows \current version \end{tabular} explorer \folder descriptions \end{tabular} folder descriptions \end{tabular} on the local description \end{tabula$ 1d43-42f2-9305-67de0b28fc23}[publishexpandedpath]

Oueries value:

1d43-42f2-9305-67de0b28fc23}[attributes]

Queries value:

1d43-42f2-9305-67de0b28fc23}[foldertypeid]

Queries value:

1d43-42f2-9305-67de0b28fc23}[initfolderhandler]

HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\drivers32[wave]

HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\drivers32[wave1]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[wave2]

HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\drivers32[wave3]

HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\drivers32[wave4]

Queries value: $HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| windows$

nt\currentversion\drivers32[wave5] HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\drivers32[wave6]

Oueries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[wave7]

Queries value:

HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32[wave8]

HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\drivers32[wave9]

Oueries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[midi] HKLM\software\wow6432node\microsoft\windows

Queries value:

nt\currentversion\drivers32[midi1] HKLM\software\wow6432node\microsoft\windows Oueries value:

nt\currentversion\drivers32[midi2]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[midi3]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[midi4]

HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\drivers32[midi5]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[midi6]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[midi7]

HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\drivers32[midi8]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\drivers32[midi9]

Queries value:

HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]