Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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\SysWOW64`
Opens:	`C:\Windows\SysWOW64\sechost.dll`
Opens:	`C:\windows\temp\version.dll`
Opens:	`C:\Windows\SysWOW64\version.dll`
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`
Opens:	`C:\windows\temp\winmm.dll`
Opens:	`C:\Windows\SysWOW64\winmm.dll`
Opens:	`C:\windows\temp\dsound.dll`
Opens:	`C:\Windows\SysWOW64\dsound.dll`
Opens:	`C:\windows\temp\POWRPROF.dll`
Opens:	`C:\Windows\SysWOW64\powrprof.dll`
Opens:	`C:\windows\temp\wsock32.dll`
Opens:	`C:\Windows\SysWOW64\wsock32.dll`
Opens:	`C:\windows\temp\IPHLPAPI.DLL`
Opens:	`C:\Windows\SysWOW64\IPHLPAPI.DLL`
Opens:	`C:\windows\temp\WINNSI.DLL`
Opens:	`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:              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
Opens:              C:\Windows\SysWOW64\profapi.dll
Opens:              C:\ProgramData
Opens:              C:\ProgramData\Remote Control PC\
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
Opens:              C:\Windows\SysWOW64\mswsock.dll
Opens:              C:\Windows\SysWOW64\WSHTCPIP.DLL
Opens:              C:\Windows\SysWOW64\nlaapi.dll
Opens:              C:\Windows\SysWOW64\NapiNSP.dll
Opens:              C:\Windows\SysWOW64\pnrpnsp.dll
Opens:              C:\windows\temp\DNSAPI.dll
Opens:              C:\Windows\SysWOW64\dnsapi.dll
Opens:              C:\Windows\SysWOW64\winrnr.dll
Opens:              C:\windows\temp\dhcpcsvc6.DLL
Opens:              C:\Windows\SysWOW64\dhcpcsvc6.dll
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
Opens:              C:\ProgramData\Remote Control PC\libspeex.dll
Opens:              C:\windows\temp\libspeexdsp.dll
Opens:              C:\ProgramData\Remote Control PC\libspeexdsp.dll
Opens:              C:\ProgramData\Remote Control PC\hostaccount.ini
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:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options
Opens key:          HKLM\system\currentcontrolset\control\session manager
Opens key:          HKLM\software\microsoft\wow64
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
Opens key:          HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:          HKLM\system\currentcontrolset\control\nls\customlocale
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
Opens key:          HKLM\software\policies\microsoft\mui\settings
Opens key:          HKCU\
Opens key:          HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:          HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
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\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
```

```
Opens key:            HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:            HKLM\
Opens key:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
Opens key:            HKLM\software\wow6432node\microsoft\windows
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
Opens key:            HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key:            HKLM\software\wow6432node\microsoft\ole
Opens key:            HKLM\software\wow6432node\microsoft\ole\tracing
Opens key:            HKLM\software\microsoft\ole\tracing
Opens key:            HKLM\software\wow6432node\microsoft\oleaut
Opens key:            HKLM\system\currentcontrolset\control\cmf\config
Opens key:            HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key:            HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key:            HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:            HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:            HKCU\software\borland\locales
Opens key:            HKLM\software\wow6432node\borland\locales
Opens key:            HKCU\software\borland\delphi\locales
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}\propertybag
Opens key:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key:            HKLM\system\currentcontrolset\control\nls\locale
Opens key:            HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
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
nt\currentversion\languagepack\datastore_v1.0
Opens key:            HKLM\software\microsoft\windows
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:            HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key:            HKLM\system\setup
Opens key:            HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key:            HKLM\software\policies\microsoft\windows nt\rpc
Opens key:            HKLM\software\policies\microsoft\sqmclient\windows
Opens key:            HKLM\software\microsoft\sqmclient\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:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
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 key:
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\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
    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\000000000002
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
    Opens key: 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\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
    Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
    Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
    Opens key: HKLM\system\currentcontrolset\services\dns
    Opens key: HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
    Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
    Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
    Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
    Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
    Opens key:
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 key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}\propertybag
    Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32
    Opens key:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
    Opens key: HKCU\software\microsoft\windows\currentversion\multimedia\midimap
    Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
    Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
    Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]

      Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
      Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
      Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
      Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
      Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
      Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
      Queries value: HKCU\control panel\desktop[preferreduilanguages]
      Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
      Queries 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]
      Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[9a992314512bbc93b07328b3941fe048]
      Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
      Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
      Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
      Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
      Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
      Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
      Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
      Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
      Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
      Queries value: HKLM\system\currentcontrolset\control\wmi\security[12e1ddac-7ebb-434f-
bc58-54c27d745f8f]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[category]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[name]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[description]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[parsingname]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[infotip]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[icon]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[security]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[roamable]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[precreate]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[stream]
      Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]

    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
    Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
    Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
    Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
    Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
    Queries value: HKLM\system\setup[oobeinprogress]
    Queries value: HKLM\system\setup[systemsetupinprogress]
    Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
        Queries 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]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[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]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
        Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
        Queries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
    Queries 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]
    Queries 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]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
    Queries 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\000000000006[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
    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\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
    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:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
    Queries value:
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]
  Queries 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]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
  Queries 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]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries 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\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  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]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries 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]
  Queries 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:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[searchlist]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enabledhcp]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationenabled]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registeradaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[domain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpdomain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpv6domain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[nameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[nameserver]
    Queries 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]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationenabled]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registeradaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[domain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[dhcpdomain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[nameserver]
    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:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[disableadapterdomainname]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[maxnumberofaddressestoregister]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enablemulticast]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disableadapterdomainname]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disabledynamicupdate]
```

```
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enableadapterdomainnameregistration]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[maxnumberofaddressestoregister]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enablemulticast]
    Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
    Queries value:            HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[name]
    Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-
b2f1-4857-a4ce-a8e7c6ea7d27}[initfolderhandler]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[name]
    Queries value:
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]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[security]
```

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[initfolderhandler]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave1]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave2]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave3]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave4]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave5]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave6]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave7]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave8]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave9]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi1]
    Queries value: HKLM\software\wow6432node\microsoft\windows
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]
    Queries value: HKLM\software\wow6432node\microsoft\windows
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]
    Queries value: HKLM\software\wow6432node\microsoft\windows
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]