# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

| | |
|---|---|
| Task ID: | 189 |
| Risk Level: | 1 |
| Date Processed: | 2016-04-28 12:52:22 (UTC) |
| Processing Time: | 63.43 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe" |
| | |
| Sample ID: | 48 |
| Type: | basic |
| Owner: | admin |
| Label: | 9d240291c8dc756bfafe75a7e60099cc |
| Date Added: | 2016-04-28 12:44:54 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 321536 bytes |
| MD5: | 9d240291c8dc756bfafe75a7e60099cc |
| SHA256: | 7c7b5307cc803bb037226eee0eca8b0a6f1d79d3d9d96755b29208442847466a |
| Description: | None |

## Pattern Matching Results

## Static Events

| | |
|---|---|
| Anomaly: | PE: Contains a virtual section |

## Process/Thread Events

| | |
|---|---|
| Creates process: | C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe |

["C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe" ]

## Named Object Events

| | |
|---|---|
| Creates mutex: | \Sessions\1\BaseNamedObjects\DBWinMutex |

## File System Events

| | |
|---|---|
| Opens: | C:\Windows\Prefetch\9D240291C8DC756BFAFE75A7E6009-B6910FBA.pf |
| Opens: | C:\Windows |
| Opens: | C:\Windows\System32\wow64.dll |
| Opens: | C:\Windows\SysWOW64 |
| Opens: | C:\Windows\SysWOW64\apphelp.dll |
| Opens: | C:\Windows\Temp\9d240291c8dc756bfafe75a7e60099cc.exe |
| Opens: | C:\Windows\SysWOW64\ntdll.dll |
| Opens: | C:\Windows\SysWOW64\kernel32.dll |
| Opens: | C:\Windows\SysWOW64\KernelBase.dll |
| Opens: | C:\Windows\apppatch\sysmain.sdb |
| Opens: | C:\Windows\apppatch\AcGenral.dll |
| Opens: | C:\Windows\apppatch\AcLayers.dll |
| Opens: | C:\Windows\SysWOW64\sechost.dll |
| Opens: | C:\Windows\SysWOW64\uxtheme.dll |
| Opens: | C:\Windows\SysWOW64\winmm.dll |
| Opens: | C:\Windows\SysWOW64\samcli.dll |
| Opens: | C:\Windows\SysWOW64\msacm32.dll |
| Opens: | C:\Windows\SysWOW64\version.dll |
| Opens: | C:\Windows\SysWOW64\userenv.dll |
| Opens: | C:\Windows\SysWOW64\dwmapi.dll |
| Opens: | C:\Windows\SysWOW64\winspool.drv |
| Opens: | C:\Windows\SysWOW64\mpr.dll |
| Opens: | C:\Windows\SysWOW64\winmmbase.dll |
| Opens: | C:\Windows\SysWOW64\combase.dll |
| Opens: | C:\Windows\SysWOW64\profapi.dll |
| Opens: | C:\Windows\SysWOW64\SHCore.dll |
| Opens: | C:\Windows\SysWOW64\sfc.dll |
| Opens: | C:\Windows\SysWOW64\sfc_os.dll |
| Opens: | C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe.Manifest |
| Opens: | C:\Windows\SysWOW64\msvcrt.dll |
| Opens: | C:\Windows\SysWOW64\bcryptprimitives.dll |
| Opens: | C:\Windows\SysWOW64\cryptbase.dll |
| Opens: | C:\Windows\SysWOW64\sspicli.dll |
| Opens: | C:\Windows\SysWOW64\rpcrt4.dll |
| Opens: | C:\Windows\SysWOW64\gdi32.dll |
| Opens: | C:\Windows\SysWOW64\user32.dll |
| Opens: | C:\Windows\SysWOW64\shlwapi.dll |
| Opens: | C:\Windows\SysWOW64\ole32.dll |
| Opens: | C:\Windows\SysWOW64\oleaut32.dll |
| Opens: | C:\Windows\SysWOW64\advapi32.dll |
| Opens: | C:\Windows\SysWOW64\shell32.dll |
| Opens: | C:\Windows\SysWOW64\iertutil.dll |
| Opens: | C:\Windows\SysWOW64\wininet.dll |

```
Opens:                  C:\Windows\SysWOW64\urlmon.dll
Opens:                  C:\Windows\SysWOW64\cfgmgr32.dll
Opens:                  C:\Windows\SysWOW64\devobj.dll
Opens:                  C:\Windows\SysWOW64\setupapi.dll
Opens:                  C:\Windows\SysWOW64\imm32.dll
Opens:                  C:\Windows\SysWOW64\msctf.dll
Opens:                  C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
Opens:                  C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens:                  C:\Windows\SysWOW64\wsock32.dll
Opens:                  C:\Windows\SysWOW64\nsi.dll
Opens:                  C:\Windows\SysWOW64\ws2_32.dll
Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:                  C:\Windows\Fonts\sserife.fon
Opens:                  C:\Windows\SysWOW64\UxTheme.dll.Config
Opens:                  C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens:                  C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
Opens:                  C:\Windows\WindowsShell.Manifest
Opens:                  C:\Windows\Fonts\StaticCache.dat
Opens:                  C:\windows\temp\updatewizard.ini
Reads from:             C:\Windows\Fonts\StaticCache.dat
```

# Windows Registry Events

```
Opens key:              HKLM\software\microsoft\wow64
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\system\currentcontrolset\control\nls\sorting\versions
Opens key:              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key:              HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:              HKLM\system\currentcontrolset\control\session manager
Opens key:              HKLM\software\wow6432node\policies\microsoft\windows nt\windows file
protection
Opens key:              HKLM\software\policies\microsoft\windows nt\windows file protection
Opens key:              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key:              HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
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\
Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key:              HKLM\software\policies\microsoft\sqmclient\windows
Opens key:              HKLM\software\microsoft\sqmclient\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\networkprovider\hworder
Opens key:              HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key:              HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key:              HKLM\software\microsoft\windows\currentversion\setup
Opens key:              HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
```

```
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
   Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
   Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
   Opens key:              HKCU\software\borland\delphi\locales
   Opens key:              HKLM\system\currentcontrolset\control\nls\sorting\ids
   Opens key:              HKCU\software\microsoft\windows\currentversion\directmanipulation
   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\1ab01ca8
   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\00000014
   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\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\languagepack\datastore_v1.0
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms sans serif
   Opens key:              HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
   Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\9d240291c8dc756bfafe75a7e60099cc.exe
   Opens key:              HKLM\software\wow6432node\microsoft\ctf\
   Opens key:              HKLM\software\wow6432node\microsoft\ctf\knownclasses
   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:                HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
Queries value:                HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:                HKLM\software\policies\microsoft\windows nt\windows file
protection[knowndlllist]
Queries value:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value:                HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[9d240291c8dc756bfafe75a7e60099cc]
Queries value:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value:                HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value:                HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value:                HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value:                HKLM\software\microsoft\ole[aggressivemtatesting]
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\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[9d240291c8dc756bfafe75a7e60099cc.exe]
Queries value:                HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value:                HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value:                HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
Queries value:
HKLM\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]
    Queries value:
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]
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\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\wow6432node\microsoft\ctf[enableanchorcontext]
```