Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	2409
Risk Level:	5
Date Processed:	2016-02-22 05:26:53 (UTC)
Processing Time:	63.31 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	

"c:\windows\temp\55885d1928d39600ce3d99617072bf3632db94352fed8032bc3dce3afe665740.exe"

Sample ID:	616
Type:	basic
Owner:	admin
Label:	55885d1928d39600ce3d99617072bf3632db94352fed8032bc3dce3afe665740
Date Added:	2016-02-22 05:26:48 (UTC)
File Type:	PE32:win32:gui
File Size:	64036 bytes
MD5:	0c921935f0880b5c2161b3905f8a3069
SHA256:	55885d1928d39600ce3d99617072bf3632db94352fed8032bc3dce3afe665740
Description:	None

Pattern Matching Results

`4` Checks whether debugger is present
`5` Accesses Filesystem keys
`5` Abnormal sleep detected

Process/Thread Events

Creates process:
C:\windows\temp\55885d1928d39600ce3d99617072bf3632db94352fed8032bc3dce3afe665740.exe
["C:\windows\temp\55885d1928d39600ce3d99617072bf3632db94352fed8032bc3dce3afe665740.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\55885D1928D39600CE3D99617072B-269DF603.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	

C:\Windows\Temp\55885d1928d39600ce3d99617072bf3632db94352fed8032bc3dce3afe665740.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\SysWOW64\odbcjt32.dll
Opens:	C:\Windows\SysWOW64\inetcomm.dll
Opens:	C:\Windows\SysWOW64\msi.dll
Opens:	C:\Windows\SysWOW64\drprov.dll
Opens:	C:\Windows\SysWOW64\msjet40.dll
Opens:	C:\Windows\SysWOW64\mswstr10.dll
Opens:	C:\Windows\SysWOW64\msoert2.dll
Opens:	C:\Windows\SysWOW64\oleacc.dll
Opens:	C:\Windows\SysWOW64\winsta.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\sechost.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\SHCore.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.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\advapi32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\comdlg32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll

```
Opens:                    C:\Windows\SysWOW64\odbcji32.dll
Opens:                    C:\Windows\SysWOW64\msjter40.dll
Opens:                    C:\Windows\SysWOW64\msjint40.dll
Opens:                    C:\Windows\WindowsShell.Manifest
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\SysWOW64\oleaccrc.dll
Opens:                    C:\Windows\SysWOW64\INETRES.dll
Opens:                    C:\Windows\SysWOW64\6flwrjmxnz27c
Opens:                    C:\Windows\SysWOW64\cmdial32.dll
Opens:                    C:\Windows\SysWOW64\cmpbk32.dll
Opens:                    C:\Windows\SysWOW64\cmutil.dll
Opens:                    C:\Windows\SysWOW64\eappcfg.dll
Opens:                    C:\Windows\SysWOW64\userenv.dll
Opens:                    C:\Windows\SysWOW64\version.dll
Opens:                    C:\Windows\SysWOW64\profapi.dll
Opens:                    C:\Windows\SysWOW64\cfgmgr32.dll
Opens:                    C:\Windows\SysWOW64\devobj.dll
Opens:                    C:\Windows\SysWOW64\setupapi.dll
Opens:                    C:\Windows\SysWOW64\en-US\setupapi.dll.mui
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\SysWOW64\mswsock.dll
Opens:                    C:\Windows\SysWOW64\NapiNSP.dll
Opens:                    C:\Windows\SysWOW64\pnrpnsp.dll
Opens:                    C:\Windows\SysWOW64\nlaapi.dll
Opens:                    C:\Windows\SysWOW64\dnsapi.dll
Opens:                    C:\Windows\SysWOW64\winrnr.dll
Opens:                    C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:                    C:\Windows\SysWOW64\winnsi.dll
Opens:                    C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens:                    C:\Windows\SysWOW64\dhcpcsvc.dll
Opens:                    C:\Windows\System32\Drivers\etc\hosts
Opens:                    C:\Windows\SysWOW64\rasadhlp.dll
Reads from:               C:\Windows\System32\Drivers\etc\hosts
```

Network Events

```
DNS query:            wowrizep.ru
DNS query:            jiwviqpa.ru
Sends data to:        0.0.0.0:53
Receives data from:   0.0.0.0:53
```

Windows Registry Events

```
Creates key:          HKLM\system\currentcontrolset\services\tcpip\parameters
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\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key:            HKLM\system\currentcontrolset\control\session manager
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
   Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
   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\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\ole
   Opens key:             HKLM\software\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:             HKCU\control panel\international\calendars\twodigityearmax
   Opens key:             HKCU\software\microsoft\internet explorer\international
   Opens key:             HKLM\system\currentcontrolset\control\filesystem
   Opens key:             HKLM\system\currentcontrolset\services\rdpnp\networkprovider
   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\microsoft\windows\currentversion\setup
   Opens key:             HKLM\software\wow6432node\microsoft\windows\currentversion
   Opens key:             HKLM\system\currentcontrolset\control\nls\extendedlocale
   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\control\nls\sorting\ids
   Opens key:             HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\128353c6
   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\services\winsock\parameters
   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\software\wow6432node\microsoft\rpc
Opens key:              HKLM\software\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\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\services\dns
Opens key:              HKLM\system\currentcontrolset\control\sqmservicelist
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\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-
25b8d56dd1d8}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
Opens key:              HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key:              HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
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\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[55885d1928d39600ce3d99617072bf3632db94352fed8032bc3dce3afe665740.exe]
Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value:          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[55885d1928d39600ce3d99617072bf3632db94352fed8032bc3dce3afe665740]
Queries value:          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value:          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value:          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value:          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value:          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value:          HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value:          HKLM\system\currentcontrolset\control\wmi\security[5d8c8d91-8f81-488d-
a278-0d06d32b39d1]
Queries value:          HKLM\system\currentcontrolset\control\wmi\security[aba7397f-f033-4c35-
9aab-6ec3322ea7a2]
Queries value:          HKCU\software\microsoft\internet
explorer\international[jp_iso_sio_control]
```

```
Queries value:              HKLM\system\currentcontrolset\control\filesystem[win31filesystem]
Queries value:              HKLM\system\currentcontrolset\services\rdpnp\networkprovider[name]
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[5f31090b-d990-4e91-
b16d-46121d0255aa]
Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
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[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]
    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\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\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\rpc[idletimerwindow]
   Queries value:                HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:                HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   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[disablesmartnameresolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize]
   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[newdhcpsrvregistration]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
    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\control\sqmservicelist[sqmservicelist]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationenabled]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[domain]
```

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]