Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	829
Risk Level:	10
Date Processed:	2016-05-18 10:43:22 (UTC)
Processing Time:	61.56 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1b213953a4baf79fadfe9968cf3a1446.exe"

Sample ID:	3330
Type:	basic
Owner:	admin
Label:	1b213953a4baf79fadfe9968cf3a1446
Date Added:	2016-05-18 10:30:51 (UTC)
File Type:	PE32:win32:gui
File Size:	565248 bytes
MD5:	1b213953a4baf79fadfe9968cf3a1446
SHA256:	3de393336565e1e6d500ce152e99281a2e3d785c3c41dc1a2f0c7b242c134e57
Description:	None

Pattern Matching Results

`10` Resolves malicious domain: Fosniw trojan
`1` HTTP connection - response code 404 (file not found)
`4` Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\1b213953a4baf79fadfe9968cf3a1446.exe

["C:\windows\temp\1b213953a4baf79fadfe9968cf3a1446.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{b7745c24-ab3d-40d8-b8a9-8f1c7a3c83a2}

File System Events

Opens:	C:\Windows\Prefetch\1B213953A4BAF79FADFE9968CF3A1-C996567E.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\NETAPI32.dll
Opens:	C:\Windows\System32\netapi32.dll
Opens:	C:\windows\temp\netutils.dll
Opens:	C:\Windows\System32\netutils.dll
Opens:	C:\windows\temp\srvcli.dll
Opens:	C:\Windows\System32\srvcli.dll
Opens:	C:\windows\temp\wkscli.dll
Opens:	C:\Windows\System32\wkscli.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\windows\temp\netbios.dll
Opens:	C:\Windows\System32\netbios.dll
Opens:	C:\Windows\System32\mswsock.dll
Opens:	C:\Windows\System32\WSHTCPIP.DLL
Opens:	C:\Windows\System32\nlaapi.dll
Opens:	C:\Windows\System32\NapiNSP.dll
Opens:	C:\Windows\System32\pnrpnsp.dll
Opens:	C:\windows\temp\DNSAPI.dll
Opens:	C:\Windows\System32\dnsapi.dll
Opens:	C:\Windows\System32\winrnr.dll
Opens:	C:\windows\temp\IPHLPAPI.DLL
Opens:	C:\Windows\System32\IPHLPAPI.DLL
Opens:	C:\windows\temp\WINNSI.DLL
Opens:	C:\Windows\System32\winnsi.dll
Opens:	C:\windows\temp\dhcpcsvc6.DLL
Opens:	C:\Windows\System32\dhcpcsvc6.dll
Opens:	C:\windows\temp\dhcpcsvc.DLL
Opens:	C:\Windows\System32\dhcpcsvc.dll
Opens:	C:\Windows\System32\drivers\etc\hosts
Opens:	C:\Windows\System32\FWPUCLNT.DLL
Opens:	C:\windows\temp\rasadhlp.dll
Opens:	C:\Windows\System32\rasadhlp.dll
Reads from:	C:\Windows\System32\drivers\etc\hosts

Network Events

DNS query:	appx.koreasys1.com
DNS query:	appx.koreasys2.com
DNS query:	appx.koreasys3.com
DNS query:	appx.koreasys4.com
DNS query:	appx.koreasys5.com
DNS query:	appx.koreasys6.com
DNS query:	appx.koreasys7.com
DNS query:	appx.koreasys8.com
DNS query:	appx.koreasys9.com
DNS query:	appx.koreasys10.com
DNS query:	appx.koreasys11.com
DNS query:	appx.koreasys12.com
DNS query:	appx.koreasys13.com
DNS query:	appx.koreasys14.com
DNS query:	appx.koreasys15.com
DNS query:	appx.koreasys16.com
DNS query:	appx.koreasys17.com
DNS query:	appx.koreasys18.com
DNS query:	appx.koreasys19.com
DNS query:	appx.koreasys20.com
DNS query:	appx.koreasys21.com
DNS query:	appx.koreasys22.com
DNS query:	appx.koreasys23.com
DNS query:	appx.koreasys24.com
DNS query:	appx.koreasys25.com
DNS query:	appx.koreasys26.com
DNS query:	appx.koreasys27.com
DNS query:	appx.koreasys28.com
DNS query:	appx.koreasys29.com
DNS query:	appx.koreasys30.com
DNS query:	appx.koreasys31.com
DNS query:	appx.koreasys32.com
DNS query:	appx.koreasys33.com
DNS query:	appx.koreasys34.com
DNS query:	appx.koreasys35.com
DNS query:	appx.koreasys36.com
DNS query:	appx.koreasys37.com
DNS query:	appx.koreasys38.com
DNS query:	appx.koreasys39.com
DNS query:	appx.koreasys40.com
DNS query:	appx.koreasys41.com
DNS query:	appx.koreasys42.com
DNS query:	appx.koreasys43.com
DNS query:	appx.koreasys44.com
DNS query:	appx.koreasys45.com
DNS query:	appx.koreasys46.com
DNS query:	appx.koreasys47.com
DNS query:	appx.koreasys48.com
DNS response:	appx.koreasys1.com ⇒ 208.100.26.234
DNS response:	appx.koreasys3.com ⇒ 109.74.196.143
DNS response:	appx.koreasys4.com ⇒ 192.155.89.148
Connects to:	208.100.26.234:80
Connects to:	0.0.0.0:80
Connects to:	109.74.196.143:80
Connects to:	192.155.89.148:80
Sends data to:	8.8.8.8:53
Sends data to:	appx.koreasys1.com:80 (208.100.26.234)
Sends data to:	appx.koreasys3.com:80 (109.74.196.143)
Sends data to:	appx.koreasys4.com:80 (192.155.89.148)
Receives data from:	8.8.8.8:53
Receives data from:	appx.koreasys1.com:80 (208.100.26.234)

Windows Registry Events

Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop\languageconfiguration
Opens key:	HKCU\control panel\desktop
Opens key:	HKCU\control panel\desktop\muicached
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\system\currentcontrolset\control\error message instrument\
Opens key:	HKLM\system\currentcontrolset\control\error message instrument

```
Opens key:              HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:              HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key:              HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key:              HKLM\
Opens key:              HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:              HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:              HKLM\software\microsoft\ole
Opens key:              HKLM\software\microsoft\ole\tracing
Opens key:              HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
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\customlocale
Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:              HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\043dd211
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
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\protocol_catalog9\catalog_entries\000000000011
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
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:              HKCU\software\d3dbfc041acf
Opens key:              HKLM\system\currentcontrolset\services\winsock\parameters
Opens key:              HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key:              HKLM\system\currentcontrolset\services\psched\parameters\winsock
Opens key:              HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key:              HKLM\system\currentcontrolset\services\winsock\setup
```

```
migration\providers\psched
   Opens key:               HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:               HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
   Opens key:               HKLM\software\microsoft\rpc
   Opens key:               HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens key:               HKLM\system\setup
   Opens key:               HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:               HKLM\system\currentcontrolset\services\dnscache\parameters
   Opens key:               HKLM\software\policies\microsoft\windows nt\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\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
   Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
   Opens key:               HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-
1709a0196aed}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
   Opens key:               HKLM\system\currentcontrolset\services\tcpip\linkage
   Queries value:           HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Queries value:           HKCU\control panel\desktop[preferreduilanguages]
   Queries value:           HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Queries value:
HKLM\software\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\microsoft\windows
nt\currentversion\compatibility32[1b213953a4baf79fadfe9968cf3a1446]
   Queries value:           HKLM\software\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\services\lanmanworkstation\parameters[rpccachetimeout]
   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\customlocale[en-us]
   Queries value:           HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   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\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[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\winsock2\parameters[ws2_32spincount]
   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\psched\parameters\winsock[mapping]
   Queries value:             HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
   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\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\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\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enabledhcp]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationenabled]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registeradaptername]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[domain]
        Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
```

806e6f6e6963}[dhcpdomain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[nameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[dhcpnameserver]
    Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[disableadapterdomainname]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[maxnumberofaddressestoregister]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[enablemulticast]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disableadapterdomainname]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disabledynamicupdate]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enableadapterdomainnameregistration]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[maxnumberofaddressestoregister]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enablemulticast]
    Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
    Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]