Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3307, Task ID: 737

Task ID:	737
Risk Level:	10
Date Processed:	2016-05-18 10:31:53 (UTC)
Processing Time:	62.77 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"

Sample ID:	3307
Type:	basic
Owner:	admin
Label:	6b78f38317a53920e530cc1e36053242
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	407933 bytes
MD5:	6b78f38317a53920e530cc1e36053242
SHA256:	cd43eae17643cd5510d87ca5b49ddb5b45f73b83c169dcd1102b356633943046
Description:	None

Pattern Matching Results

7	Writes to memory of system processes
2	PE: Nonstandard section
10	Creates malicious mutex: Bifrost [APT, RAT, MoreInfo]
7	Attempts to connect to dynamic DNS
4	Reads process memory
5	PE: Contains compressed section
6	Creates ActiveSetup run key
6	Packer: PECompact
7	Injects thread into Windows process

Static Events

Anomaly:	PE: Contains one or more non-standard sections
Packer:	PeCompact

Process/Thread Events

Creates process:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe ["C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"]
Creates process:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe [C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe]
Creates process:	C:\Program Files\Internet Explorer\iexplore.exe ["C:\Program Files\Internet Explorer\iexplore.exe"]
Reads from process:	PID:2688 C:\Program Files\Internet Explorer\iexplore.exe
Reads from process:	PID:2720 C:\Windows\System32\calc.exe
Writes to process:	PID:2672 C:\Windows\Temp\6b78f38317a53920e530cc1e36053242.exe
Writes to process:	PID:1232 C:\Windows\explorer.exe
Writes to process:	PID:2688 C:\Program Files\Internet Explorer\iexplore.exe
Terminates process:	C:\Windows\Temp\6b78f38317a53920e530cc1e36053242.exe
Creates remote thread:	C:\Windows\explorer.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\Bif1234
Creates mutex:	\Sessions\1\BaseNamedObjects\Ook3s
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{66e58a79-7295-4530-b6c0-04ea01fb4067}

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Program Files\Bifrost
Creates:	C:\Program Files\Bifrost\server.exe
Opens:	C:\Windows\Prefetch\6B78F38317A53920E530CC1E36053-7800A4C9.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\version.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens:	C:\windows\temp\winmm.dll
Opens:	C:\Windows\System32\winmm.dll
Opens:	C:\Windows\System32\imm32.dll

```
  Opens:                  C:\windows\temp\6b78f38317a53920e530cc1e36053242.ENU
  Opens:                  C:\windows\temp\6b78f38317a53920e530cc1e36053242.ENU.DLL
  Opens:                  C:\windows\temp\6b78f38317a53920e530cc1e36053242.EN
  Opens:                  C:\windows\temp\6b78f38317a53920e530cc1e36053242.EN.DLL
  Opens:                  C:\Windows\System32\uxtheme.dll
  Opens:                  C:\windows\temp\dwmapi.dll
  Opens:                  C:\Windows\System32\dwmapi.dll
  Opens:                  C:\Windows\Fonts\StaticCache.dat
  Opens:                  C:\Windows\System32\en-US\user32.dll.mui
  Opens:                  C:\Windows\Temp\6b78f38317a53920e530cc1e36053242.exe
  Opens:                  C:\Windows\System32\apphelp.dll
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\windows\temp\profapi.dll
  Opens:                  C:\Windows\System32\profapi.dll
  Opens:                  C:\Users\Admin
  Opens:                  C:\Users\Admin\AppData\Roaming
  Opens:                  C:\Windows\System32\advapi32.dll
  Opens:                  C:\Program Files\Bifrost\server.exe
  Opens:                  C:\Program Files\Bifrost\logg.dat
  Opens:                  C:\Program Files\Bifrost
  Opens:                  C:\Windows\explorer.exe
  Opens:                  C:\Program Files\Internet Explorer\iexplore.exe
  Opens:                  C:\Program Files\Internet Explorer\en-US\iexplore.exe.mui
  Opens:                  C:\Program Files\Internet Explorer\en\iexplore.exe.mui
  Opens:                  C:\Windows\Prefetch\IEXPLORE.EXE-908C99F8.pf
  Opens:                  C:
  Opens:                  C:\Program Files
  Opens:                  C:\Program Files\Common Files
  Opens:                  C:\Program Files\Common Files\Adobe
  Opens:                  C:\Program Files\Common Files\Adobe\Acrobat
  Opens:                  C:\Program Files\Common Files\Adobe\Acrobat\ActiveX
  Opens:                  C:\Program Files\Internet Explorer
  Opens:                  C:\Program Files\Internet Explorer\en-US
  Opens:                  C:\Users
  Opens:                  C:\Users\Admin\AppData
  Opens:                  C:\Users\Admin\AppData\Local
  Opens:                  C:\Users\Admin\AppData\LocalLow
  Opens:                  C:\Users\Admin\AppData\LocalLow\Sun
  Opens:                  C:\Users\Admin\AppData\LocalLow\Sun\Java
  Opens:                  C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment
  Opens:                  C:\Users\Admin\AppData\LocalLow\Sun\Java\Deployment\tmp
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:                  C:\Users\Admin\Desktop
  Opens:                  C:\Windows
  Opens:                  C:\Windows\Fonts
  Opens:                  C:\Windows\Globalization
  Opens:                  C:\Windows\Globalization\Sorting
  Opens:                  C:\Windows\System32\en-US
  Opens:                  C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
  Opens:                  C:\Windows\System32\ntdll.dll
  Opens:                  C:\Windows\System32\kernel32.dll
  Opens:                  C:\Windows\System32\apisetschema.dll
  Opens:                  C:\Windows\System32\KernelBase.dll
  Opens:                  C:\Windows\System32\locale.nls
  Opens:                  C:\Windows\System32\msvcrt.dll
  Opens:                  C:\Windows\System32\rpcrt4.dll
  Opens:                  C:\Windows\System32\user32.dll
  Opens:                  C:\Windows\System32\gdi32.dll
  Opens:                  C:\Windows\System32\lpk.dll
  Opens:                  C:\Windows\System32\usp10.dll
  Opens:                  C:\Windows\System32\shlwapi.dll
  Opens:                  C:\Windows\System32\shell32.dll
  Opens:                  C:\Windows\System32\ole32.dll
  Opens:                  C:\Windows\System32\iertutil.dll
  Opens:                  C:\Windows\System32\urlmon.dll
  Opens:                  C:\Windows\System32\wininet.dll
  Opens:                  C:\Windows\System32\oleaut32.dll
  Opens:                  C:\Windows\System32\crypt32.dll
  Opens:                  C:\Windows\System32\msasn1.dll
  Opens:                  C:\Windows\System32\msctf.dll
  Opens:                  C:\Windows\System32\ieframe.dll
  Opens:                  C:\Windows\System32\psapi.dll
  Opens:                  C:\Windows\System32\oleacc.dll
  Opens:                  C:\Windows\System32\oleaccrc.dll
  Opens:                  C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:                  C:\Windows\WindowsShell.Manifest
  Opens:                  C:\Windows\System32\comdlg32.dll
  Opens:                  C:\Windows\System32\rpcss.dll
  Opens:                  C:\Windows\System32\cryptbase.dll
  Opens:                  C:\Windows\System32\RpcRtRemote.dll
  Opens:                  C:\Program Files\Internet Explorer\sqmapi.dll
  Opens:                  C:\Windows\System32\clbcatq.dll
  Opens:                  C:\Windows\System32\propsys.dll
  Opens:                  C:\Windows\System32\ntmarta.dll
  Opens:                  C:\Windows\System32\Wldap32.dll
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
  Opens:                  C:\Users\desktop.ini
  Opens:                  C:\Users\Admin\Desktop\desktop.ini
  Opens:                  C:\Windows\System32\setupapi.dll
  Opens:                  C:\Windows\System32\cfgmgr32.dll
  Opens:                  C:\Windows\System32\devobj.dll
  Opens:                  C:\Windows\System32\en-US\setupapi.dll.mui
  Opens:                  C:\Windows\System32\cryptsp.dll
  Opens:                  C:\Windows\System32\rsaenh.dll
  Opens:                  C:\Program Files\Internet Explorer\ieproxy.dll
  Opens:                  C:\Windows\System32\sspicli.dll
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
  Opens:                  C:\Windows\System32\ws2_32.dll
  Opens:                  C:\Windows\System32\nsi.dll
  Opens:                  C:\Windows\System32\dnsapi.dll
  Opens:                  C:\Windows\System32\IPHLPAPI.DLL
  Opens:                  C:\Windows\System32\winnsi.dll
  Opens:                  C:\Windows\System32\en-US\ieframe.dll.mui
  Opens:                  C:\Windows\System32\mlang.dll
  Opens:                  C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
  Opens:                  C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
  Opens:                  C:\Windows\System32\sxs.dll
  Opens:                  C:\Windows\System32\en-US\urlmon.dll.mui
  Opens:                  C:\Windows\System32\stdole2.tlb
  Opens:                  C:\Windows\System32\url.dll
  Opens:                  C:\Windows\System32\msimg32.dll
  Opens:                  C:\Windows\Fonts\nyala.ttf
  Opens:                  C:\Program Files\Internet Explorer\avicap32.dll
  Opens:                  C:\Windows\System32\avicap32.dll
  Opens:                  C:\Program Files\Internet Explorer\WINMM.dll
  Opens:                  C:\Program Files\Internet Explorer\VERSION.dll
  Opens:                  C:\Program Files\Internet Explorer\MSVFW32.dll
  Opens:                  C:\Windows\System32\msvfw32.dll
  Opens:                  C:\Program Files\Internet Explorer\iexplore.exe.Local\
  Opens:                  C:\Windows\System32\en-US\msvfw32.dll.mui
  Opens:                  C:\Windows\System32\en-US\avicap32.dll.mui
  Opens:                  C:\Program Files\Internet Explorer\dwmapi.dll
  Opens:                  C:\Windows\System32\nlaapi.dll
  Opens:                  C:\Windows\System32\NapiNSP.dll
  Opens:                  C:\Windows\System32\pnrpnsp.dll
  Opens:                  C:\Windows\System32\mswsock.dll
  Opens:                  C:\Program Files\Internet Explorer\DNSAPI.dll
  Opens:                  C:\Windows\System32\winrnr.dll
  Opens:                  C:\Program Files\Internet Explorer\IPHLPAPI.DLL
  Opens:                  C:\Program Files\Internet Explorer\WINNSI.DLL
  Opens:                  C:\Windows\System32\calc.exe
  Opens:                  C:\
  Opens:                  C:\Program Files\Internet Explorer\dhcpcsvc6.DLL
  Opens:                  C:\Windows\System32\dhcpcsvc6.dll
  Opens:                  C:\Program Files\Internet Explorer\dhcpcsvc.DLL
  Opens:                  C:\Windows\System32\dhcpcsvc.dll
  Opens:                  C:\Windows\System32\drivers\etc\hosts
  Opens:                  C:\Program Files\Internet Explorer\CRYPTBASE.dll
  Opens:                  C:\Windows\System32\WSHTCPIP.DLL
  Opens:                  C:\Windows\System32\FWPUCLNT.DLL
  Opens:                  C:\Program Files\Internet Explorer\rasadhlp.dll
  Opens:                  C:\Windows\System32\rasadhlp.dll
  Writes to:              C:\Program Files\Bifrost\server.exe
  Reads from:             C:\Windows\Fonts\StaticCache.dat
  Reads from:             C:\Windows\Temp\6b78f38317a53920e530cc1e36053242.exe
  Reads from:             C:\Windows\System32\advapi32.dll
  Reads from:             C:\Program Files\Internet Explorer\iexplore.exe
  Reads from:             C:\Windows\Prefetch\IEXPLORE.EXE-908C99F8.pf
  Reads from:             C:\Program Files\Bifrost\server.exe
  Reads from:             C:\Windows\System32\drivers\etc\hosts
```

Network Events

DNS query:	probook.zapto.org
DNS response:	probook.zapto.org ⇒ 5.15.116.86
Connects to:	5.15.116.86:1800
Sends data to:	8.8.8.8:53
Receives data from:	8.8.8.8:53

Windows Registry Events

Creates key:	HKLM\software\microsoft\windows\currentversion
Creates key:	HKLM\software\microsoft\active setup\installed components\{9d71d88c-c598-4935-c5d1-43aa4db90836}
Creates key:	HKLM\software\bifrost
Creates key:	HKCU\software\bifrost
Creates key:	HKLM\system\currentcontrolset\control\mediaresources\msvideo
Creates key:	HKLM\system
Creates key:	HKLM\system\currentcontrolset
Creates key:	HKLM\system\currentcontrolset\control
Creates key:	HKLM\system\currentcontrolset\control\mediaresources
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:	HKLM\system\currentcontrolset\control\session manager
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\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\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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\software\microsoft\oleaut
Opens key:	HKCU\software\borland\locales
Opens key:	HKLM\software\borland\locales
Opens key:	HKCU\software\borland\delphi\locales
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:	HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:	HKLM\system\currentcontrolset\control\nls\locale
Opens key:	HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key:	HKLM\system\currentcontrolset\control\nls\language groups
Opens key:	HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
Opens key:	HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0
Opens key:	HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback
Opens key:	HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key:	HKLM\system\currentcontrolset\control\cmf\config
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\6b78f38317a53920e530cc1e36053242.exe
Opens key:	HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key:	HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key:	HKLM\software\policies\microsoft\windows\appcompat
Opens key:	HKCU\software\microsoft\windows nt\currentversion
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key:	HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:	HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\6b78f38317a53920e530cc1e36053242.exe
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\services\crypt32
Opens key:	HKLM\software\microsoft\windows\currentversion\internet settings
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet settings

```
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKLM\software\policies\microsoft\windows\explorer
  Opens key:                HKCU\software\policies\microsoft\windows\explorer
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key:                HKLM\software\microsoft\active setup\installed components
  Opens key:                HKLM\software\microsoft\active setup\installed components\>{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}
  Opens key:                HKLM\software\microsoft\active setup\installed components\>{26923b43-
4d38-484f-9b9e-de460746276c}
  Opens key:                HKLM\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{08b0e5c0-
4fcb-11cf-aaa5-00401c608500}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{2c7339cf-
2b09-4501-b3f3-f3508c9228ed}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{3af36230-
a269-11d1-b5bf-0000f8051515}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{44bba840-
cc51-11cf-aafa-00aa00b6015c}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{44bba855-
cc51-11cf-aafa-00aa00b6015f}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{45ea75a0-
a269-11d1-b5bf-0000f8051515}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{4f645220-
306d-11d2-995d-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{5fd399c0-
a70a-11d1-9948-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{630b1da0-
b465-11d1-9948-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{6bf52a52-
394a-11d3-b153-00c04f79faa6}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{6fab99d0-
bab8-11d1-994a-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{7c028af8-
f614-47b3-82da-ba94e41b1089}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4340}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4383}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{89b4c1cd-
b018-4511-b0a1-5476dbf70820}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{9381d8f2-
0288-11d0-9501-00aa00b911a5}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{c9e9a340-
d1f1-11d0-821e-444553540600}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{de5aed00-
a4bf-11d1-9948-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{e92b03ab-
b707-11d2-9cbd-0000f87a369e}
  Opens key:                HKCU\software\microsoft\active setup\installed components\{9d71d88c-
c598-4935-c5d1-43aa4db90836}
  Opens key:                HKLM\software\policies\microsoft\windows\system
  Opens key:                HKCR\http\shell\open\command
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iexplore.exe
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\iexplore.exe
```

```
  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\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\vfw
  Opens key:                HKLM\system\currentcontrolset\control\mediaresources\msvideo
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\drivers32
  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\29bc6c5a
  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:                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:                HKCU\software\classes\applications\calc.exe
  Opens key:                HKCR\applications\calc.exe
  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
  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
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            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[6b78f38317a53920e530cc1e36053242]
  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\control\nls\customlocale[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:            HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  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\system\currentcontrolset\control\cmf\config[system]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value:              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[initfolderhandler]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:
```

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[category]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[name]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parentfolder]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[description]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[relativepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parsingname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[infotip]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localizedname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[icon]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[security]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresource]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresourcetype]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localredirectonly]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[roamable]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[precreate]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[stream]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[publishexpandedpath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[attributes]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[foldertypeid]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[initfolderhandler]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002[profileimagepath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\>{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\>{26923b43-
4d38-484f-9b9e-de460746276c}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\{08b0e5c0-
4fcb-11cf-aaa5-00401c608500}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\{2c7339cf-
2b09-4501-b3f3-f3508c9228ed}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\{3af36230-
a269-11d1-b5bf-0000f8051515}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\{44bba840-
cc51-11cf-aafa-00aa00b6015c}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\{44bba855-
cc51-11cf-aafa-00aa00b6015f}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\{45ea75a0-
a269-11d1-b5bf-0000f8051515}[stubpath]
   Queries value:            HKLM\software\microsoft\active setup\installed components\{4f645220-
306d-11d2-995d-00c04f98bbc9}[stubpath]
```

```
  Queries value:              HKLM\software\microsoft\active setup\installed components\{5fd399c0-
a70a-11d1-9948-00c04f98bbc9}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{630b1da0-
b465-11d1-9948-00c04f98bbc9}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{6bf52a52-
394a-11d3-b153-00c04f79faa6}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{6fab99d0-
bab8-11d1-994a-00c04f98bbc9}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{7c028af8-
f614-47b3-82da-ba94e41b1089}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4340}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4383}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{89b4c1cd-
b018-4511-b0a1-5476dbf70820}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{9381d8f2-
0288-11d0-9501-00aa00b911a5}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{c9e9a340-
d1f1-11d0-821e-444553540600}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{de5aed00-
a4bf-11d1-9948-00c04f98bbc9}[stubpath]
  Queries value:              HKLM\software\microsoft\active setup\installed components\{e92b03ab-
b707-11d2-9cbd-0000f87a369e}[stubpath]
  Queries value:              HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
  Queries value:              HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
  Queries value:              HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
  Queries value:              HKLM\software\bifrost[nck]
  Queries value:              HKCR\http\shell\open\command[]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[iexplore]
  Queries value:              HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:              HKLM\system\setup[oobeinprogress]
  Queries value:              HKLM\system\setup[systemsetupinprogress]
  Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:              HKCU\software\bifrost[plg1]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo1]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo2]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo3]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo4]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo5]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo6]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo7]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo8]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo9]
  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\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:             HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
   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\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\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Sets/Creates value:       HKLM\software\microsoft\active setup\installed components\{9d71d88c-
c598-4935-c5d1-43aa4db90836}[stubpath]
  Sets/Creates value:       HKLM\software\bifrost[nck]
  Sets/Creates value:       HKCU\software\bifrost[klg]
  Value changes:            HKLM\software\microsoft\active setup\installed components\{9d71d88c-
c598-4935-c5d1-43aa4db90836}[stubpath]
```