

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 161, Task ID: 645

Task ID:	645
Risk Level:	5
Date Processed:	2016-04-28 13:04:49 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe"
Sample ID:	161
Type:	basic
Owner:	admin
Label:	6282b1723f3a4b0054d80aeb27c8fed5
Date Added:	2016-04-28 12:45:06 (UTC)
File Type:	PE32:win32:gui
File Size:	813216 bytes
MD5:	6282b1723f3a4b0054d80aeb27c8fed5
SHA256:	63e6e2e578871b03c530a3a5d3ddd22e6a00bf9de6f167ceeb5908d5c9c56c8e
Description:	None

Pattern Matching Results

2	PE: Nonstandard section
5	Packer: UPX
5	PE: Contains compressed section
4	Checks whether debugger is present

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe
["C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe"]	

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Creates:	C:\ProgramData\ZebraNetworkSystems
Creates:	C:\ProgramData\ZebraNetworkSystems\NeoRouter
Creates:	C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems
Creates:	C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems\NeoRouter
Creates:	C:\Users\Admin\AppData\Local\Temp\{BE05233B-09BA-478E-BD53-BF105526ACA1}
Creates:	C:\Users\Admin\AppData\Local\Temp\Tmp2C2B.tmp
Opens:	C:\Windows\Prefetch\6282B1723F3A4B0054D80AEB27C8F-E920D1CA.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens:	C:\windows\temp\WINSPOOL.DRV
Opens:	C:\Windows\SysWOW64\winspool.drv
Opens:	C:\windows\temp\WSOCK32.dll
Opens:	C:\Windows\SysWOW64\wsock32.dll
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\AppPatch\sysmain.sdb
Opens:	C:\Windows\Temp\6282b1723f3a4b0054d80aeb27c8fed5.exe
Opens:	C:\Windows\AppPatch\AcGenral.dll
Opens:	C:\windows\temp\UxTheme.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\windows\temp\WINMM.dll
Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\windows\temp\samcli.dll
Opens:	C:\Windows\SysWOW64\samcli.dll

Opens:	C:\windows\temp\MSACM32.dll
Opens:	C:\Windows\SysWOW64\msacm32.dll
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\windows\temp\sfc.dll
Opens:	C:\Windows\SysWOW64\sfc.dll
Opens:	C:\windows\temp\sfc_os.DLL
Opens:	C:\Windows\SysWOW64\sfc_os.dll
Opens:	C:\windows\temp\USERENV.dll
Opens:	C:\Windows\SysWOW64\userenv.dll
Opens:	C:\windows\temp\profapi.dll
Opens:	C:\Windows\SysWOW64\profapi.dll
Opens:	C:\windows\temp\dwmmapi.dll
Opens:	C:\Windows\SysWOW64\dwmmapi.dll
Opens:	C:\windows\temp\MPR.dll
Opens:	C:\Windows\SysWOW64\mpr.dll
Opens:	C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.Config
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.2.Manifest
Opens:	C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.3.Manifest
Opens:	C:\windows\temp\Log.ini
Opens:	C:\ProgramData\ZebraNetworkSystems\NeoRouter
Opens:	C:\ProgramData\ZebraNetworkSystems
Opens:	C:\ProgramData
Opens:	C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems\NeoRouter
Opens:	C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems
Opens:	C:\Users\Admin\AppData\Roaming
Opens:	C:\Windows\Temp
Opens:	C:\ProgramData\ZebraNetworkSystems\NeoRouter\Log.ini
Opens:	C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.1000.Manifest
Opens:	C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5ENU.dll
Opens:	C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5LOC.dll
Opens:	C:\dev\
Opens:	C:\windows\temp\NETAPI32.DLL
Opens:	C:\Windows\SysWOW64\netapi32.dll
Opens:	C:\windows\temp\netutils.dll
Opens:	C:\Windows\SysWOW64\netutils.dll
Opens:	C:\windows\temp\srvccli.dll
Opens:	C:\Windows\SysWOW64\srvccli.dll
Opens:	C:\windows\temp\wksccli.dll
Opens:	C:\Windows\SysWOW64\wksccli.dll
Opens:	C:\windows\temp\CRYPTSP.dll
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\usr\local\ssl\cert.pem
Opens:	C:\Users\Admin\AppData\Local\Temp
Opens:	C:\Windows\SysWOW64\ws2_32.dll
Opens:	C:\Windows\SysWOW64\mswsock.dll
Opens:	C:\Windows\SysWOW64\WSH_TCPIP.DLL
Opens:	C:\Windows\SysWOW64\wship6.dll
Opens:	C:\windows\temp\DNSAPI.dll
Opens:	C:\Windows\SysWOW64\dnsapi.dll
Opens:	C:\windows\temp\IPHLPAPI.DLL
Opens:	C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:	C:\windows\temp\WINNSI.DLL
Opens:	C:\Windows\SysWOW64\winnsi.dll
Opens:	C:\windows\temp\dhcpcsvc6.DLL
Opens:	C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens:	C:\windows\temp\dhcpcsvc.DLL
Opens:	C:\Windows\SysWOW64\dhcpcsvc.dll
Opens:	C:\windows\temp\rasadhlp.dll
Opens:	C:\Windows\SysWOW64\rasadhlp.dll
Opens:	C:\Windows\System32\drivers\etc\hosts
Opens:	C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\windows\temp\imageres.dll
Opens:	C:\Windows\SysWOW64\imageres.dll
Opens:	C:\Windows\SysWOW64\en-US\imageres.dll.mui
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\rpcss.dll
Reads from:	C:\Windows\System32\drivers\etc\hosts
Reads from:	C:\Windows\Fonts\StaticCache.dat

Network Events

DNS query:	secure.neorouter.com
Sends data to:	8.8.8.8:53

Windows Registry Events

Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
--------------	---

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options

Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\software\microsoft\wow64

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options

Opens key: HKLM\system\currentcontrolset\control\terminal server

Opens key: HKLM\system\currentcontrolset\control\safeboot\option

Opens key: HKLM\system\currentcontrolset\control\srp\gp\ddl

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\system\currentcontrolset\control\locale\customlocale

Opens key: HKLM\system\currentcontrolset\control\locale\language

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

Opens key: HKCU\software\policies\microsoft\control panel\desktop

Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKLM\system\currentcontrolset\control\locale\sorting\versions

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\windows file protection

Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection

Opens key: HKLM\

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows

Opens key: HKLM\system\currentcontrolset\services\crypt32

Opens key: HKLM\software\wow6432node\microsoft\ole

Opens key: HKLM\software\wow6432node\microsoft\ole\tracing

Opens key: HKLM\software\microsoft\ole\tracing

Opens key: HKLM\software\wow6432node\microsoft\oleaut

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings

Opens key: HKLM\system\currentcontrolset\control\cmf\config

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup

Opens key: HKLM\software\microsoft\windows\currentversion\setup

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion

Opens key: HKLM\system\currentcontrolset\control\locale\extendedlocale

Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder

Opens key: HKLM\software\policies\microsoft\sqlclient\windows

Opens key: HKLM\software\microsoft\sqlclient\windows

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00260bb3

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\network
Opens key: HKCU\software\microsoft\windows\currentversion\policies\cmdlg32
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key:
HKLM\software\wow6432node\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\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\intel
hardware cryptographic service provider
Opens key: HKLM\software\wow6432node\zebranetworksystems\neorouter
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip

Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
Opens key: HKLM\system\currentcontrolset\services\dns\cache\parameters
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\system\currentcontrolset\services\dns\cache\parameters\dns\cache
Opens key: HKLM\system\currentcontrolset\services\dns
Opens key: HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dns\policyconfig
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dns\policyconfig
Opens key:
HKLM\system\currentcontrolset\services\dns\cache\parameters\dns\policyconfig
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-127795cce47a}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-65fee5bae0b1}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\6282b1723f3a4b0054d80aeb27c8fed5.exe
Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\wow6432node\microsoft\ctf\
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\software\policies\microsoft\windows nt\windows file
protection[knowndlllist]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[6282b1723f3a4b0054d80aeb27c8fed5]

Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
Queries value: HKLM\system\currentcontrolset\control\cmf\config\system]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storeresserviceclassinfo]
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]

[illegible]

fdc1-4dc3-a9dd-070d1d495d97}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-

65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\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\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup\systemsetupinprogress]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001[name]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography\privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography\privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography\privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\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\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\system\currentcontrolset\control\squmservicelist[squmservicelist]
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[prioritizecorddata]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizecorddata]
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[screndefaultservers]
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[usedns]
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[disablewanddynamicupdate]
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[maxnumberofaddressesstoregister]
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[updateopleveldomainzones]
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[adapertimeoutlimit]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[serverprioritytimelimit]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachedsockets]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[enablemulticast]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastresponderflags]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsenderflags]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[usecompartments]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[cacheallcompartments]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[usenewregistration]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistration]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistrationonly]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquickquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[searchlist]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enabledhcp]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationenabled]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registeradaptername]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[domain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpdomain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpv6domain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpnameserver]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enabledhcp]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[maxnumberofaddresstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disablenameresolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[maxnumberofaddresstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value: HKLM\system\currentcontrolset\control\ntp\parameters[ntpserver]
Queries value: HKLM\system\currentcontrolset\control\ntp\parameters[ntpserverlist]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]

Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]