

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 41, Task ID: 161

Task ID:	161
Risk Level:	5
Date Processed:	2016-04-28 12:51:25 (UTC)
Processing Time:	60.44 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe"
Sample ID:	41
Type:	basic
Owner:	admin
Label:	bb02abb18c51ee149dde9732ca8e5fae
Date Added:	2016-04-28 12:44:53 (UTC)
File Type:	PE32:win32:gui
File Size:	813216 bytes
MD5:	bb02abb18c51ee149dde9732ca8e5fae
SHA256:	c5c1d3d6b80fb79a451ac1b8a8dfcb5a5b20e76f38df0f6ed34dc08842a13ad1
Description:	None

## Pattern Matching Results

1	SSL traffic on standard port
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\bb02abb18c51ee149dde9732ca8e5fae.exe
["C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe" ]	

## Named Object Events

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

## 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\{6986DDDD-26A2-4827-B390-DA68F75E9541}
Creates:	C:\Users\Admin\AppData\Local\Temp\Tmp5241.tmp
Opens:	C:\Windows\Prefetch\BB02ABB18C51EE149DDE9732CA8E5-39A45309.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\bb02abb18c51ee149dde9732ca8e5fae.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\apppatch\AcGenral.dll
Opens:	C:\Windows\apppatch\AcLayers.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\Windows\SysWOW64\samcli.dll
Opens:	C:\Windows\SysWOW64\msacm32.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\userenv.dll
Opens:	C:\Windows\SysWOW64\dwmmapi.dll
Opens:	C:\Windows\SysWOW64\winspool.drv
Opens:	C:\Windows\SysWOW64\mpr.dll
Opens:	C:\Windows\SysWOW64\winmmbase.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\profapi.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\SysWOW64\sfc.dll
Opens:	C:\Windows\SysWOW64\sfc_os.dll
Opens:	C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.Config
Opens:	C:\Windows\SysWOW64\msvcrt.dll

Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\iertutil.dll
Opens:	C:\Windows\SysWOW64\wininet.dll
Opens:	C:\Windows\SysWOW64\urlmon.dll
Opens:	C:\Windows\SysWOW64\cfgmgr32.dll
Opens:	C:\Windows\SysWOW64\devobj.dll
Opens:	C:\Windows\SysWOW64\setupapi.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985	
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll	
Opens:	C:\Windows\SysWOW64\wsock32.dll
Opens:	C:\Windows\SysWOW64\comdlg32.dll
Opens:	C:\Windows\SysWOW64\msasn1.dll
Opens:	C:\Windows\SysWOW64\crypt32.dll
Opens:	C:\Windows\SysWOW64\nsi.dll
Opens:	C:\Windows\SysWOW64\ws2_32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.2.Manifest
Opens:	C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.3.Manifest
Opens:	C:\windows\temp\Log.ini
Opens:	C:\ProgramData\ZebraNetworkSystems\NeoRouter\Log.ini
Opens:	C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.1000.Manifest
Opens:	C:\dev\
Opens:	C:\Windows\SysWOW64\netapi32.dll
Opens:	C:\Windows\SysWOW64\netutils.dll
Opens:	C:\Windows\SysWOW64\svrcli.dll
Opens:	C:\Windows\SysWOW64\wksccli.dll
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\usr\local\ssl\cert.pem
Opens:	C:\Windows\SysWOW64\mswsock.dll
Opens:	C:\Windows\SysWOW64\dnsapi.dll
Opens:	C:\Windows\SysWOW64\rasadhlp.dll
Opens:	C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:	C:\Windows\SysWOW64\winnsi.dll
Opens:	C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens:	C:\Windows\SysWOW64\dhcpcsvc.dll
Opens:	C:\Windows\System32\Drivers\etc\hosts
Opens:	C:\Windows\SysWOW64\FWPULNT.DLL
Opens:	C:\usr\local\ssl\certs\
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.9200.16384_en-us_9f44aa25b2ac1b72	
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.9200.16384_en-us_9f44aa25b2ac1b72\comctl32.dll.mui	
Opens:	C:\Windows\Fonts\tahoma.ttf
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\Fonts\tahomabd.ttf
Opens:	C:\Windows\Fonts\micross.ttf
Reads from:	C:\Windows\System32\Drivers\etc\hosts
Reads from:	C:\Windows\Fonts\StaticCache.dat

## Network Events

DNS query:	secure.neorouter.com
DNS response:	secure.neorouter.com ⇒ 72.167.40.3
Connects to:	72.167.40.3:443
Sends data to:	0.0.0.0:53
Sends data to:	secure.neorouter.com:443 (72.167.40.3)
Receives data from:	0.0.0.0:53
Receives data from:	secure.neorouter.com:443 (72.167.40.3)

## Windows Registry Events

Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers	

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers  
 Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers  
 Opens key: HKLM\system\currentcontrolset\control\nls\customlocale  
 Opens key: HKLM\system\currentcontrolset\control\nls\language  
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages  
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us  
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete  
 Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings  
 Opens key: HKLM\software\policies\microsoft\mui\settings  
 Opens key: HKCU\  
 Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration  
 Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration  
 Opens key: HKCU\software\policies\microsoft\control panel\desktop  
 Opens key: HKCU\control panel\desktop\languageconfiguration  
 Opens key: HKCU\control panel\desktop  
 Opens key: HKCU\control panel\desktop\muicached  
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside  
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog  
 Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags  
 Opens key: HKLM\system\currentcontrolset\control\session manager  
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\windows file  
 protection  
 Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\appcompatflags\disable8and16bitmitigation  
 Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy  
 Opens key: HKLM\system\currentcontrolset\control\lsa  
 Opens key:  
 HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration  
 Opens key: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\gre\_initialize  
 Opens key: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\compatibility32  
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime  
 compatibility  
 Opens key: HKLM\  
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows  
 Opens key: HKLM\software\policies\microsoft\sqlclient\windows  
 Opens key: HKLM\software\microsoft\sqlclient\windows  
 Opens key: HKLM\software\wow6432node\microsoft\ole  
 Opens key: HKLM\software\wow6432node\microsoft\ole\tracing  
 Opens key: HKLM\software\microsoft\ole\tracing  
 Opens key: HKLM\software\wow6432node\microsoft\oleaut  
 Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder  
 Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr  
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup  
 Opens key: HKLM\software\microsoft\windows\currentversion\setup  
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion  
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
 Opens key:  
 HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file  
 execution options  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\dlloptions  
 Opens key: HKLM\system\currentcontrolset\services\crypt32  
 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters  
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids  
 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\16316034  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\000000005  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000002  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006  
 Opens key:  
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000014  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005  
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006  
 Opens key: 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\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\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\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\tcpip6\parameters\winsock  
 Opens key: HKLM\system\currentcontrolset\services\winsock\setup  
 migration\providers\tcpip6  
 Opens key: HKLM\system\currentcontrolset\services\dns\parameters  
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient  
 Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient  
 Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient  
 Opens key: HKLM\software\policies\microsoft\system\dnsclient  
 Opens key: HKLM\system\currentcontrolset\services\dns  
 Opens key: HKLM\system\currentcontrolset\control\squmservicelist  
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows

```

nt\dnsclient\dnspolicyconfig
  Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
  Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-25b8d56dd1d8}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-8a6dc56e0da9}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
  Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key: HKLM\system\currentcontrolset\control\ntp\locale
  Opens key: HKLM\system\currentcontrolset\control\ntp\locale\alternate sorts
  Opens key: HKLM\system\currentcontrolset\control\ntp\language groups
  Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\bb02abb18c51ee149dde9732ca8e5fae.exe
  Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
  Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  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\ms shell dlg 2
  Opens key: HKLM\software\wow6432node\microsoft\ctf\
  Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
  Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
  Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
  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\ntp\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\ntp\language[installlanguagefallback]
  Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatencodepage]
  Queries value: HKCU\control panel\desktop[preferreduilanguages]
  Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value: HKLM\system\currentcontrolset\control\ntp\sorting\versions[]
  Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value: HKLM\software\policies\microsoft\windows nt\windows file
protection[knowndlllist]
  Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[bb02abb18c51ee149dde9732ca8e5fae]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value: HKLM\software\microsoft\vol[pageallocatorusesystemheap]
  Queries value: HKLM\software\microsoft\vol[pageallocatorusesystemheapisprivate]
  Queries value: HKLM\software\microsoft\vol[aggressivemtestesting]
  Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]

```

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\dlloptions[usefilter]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\dlloptions[bb02abb18c51ee149dde9732ca8e5fae.exe]  
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace\_callout]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[next\_catalog\_entry\_id]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[num\_catalog\_entries]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000002[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[librarypath]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[displaystring]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerid]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[addressfamily]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[enabled]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[version]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[storiesserviceclassinfo]  
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[storiesserviceclassinfo]  
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:

[illegible]

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\locale\customlocale[en]  
Queries value: HKLM\system\currentcontrolset\control\locale\extendedlocale[en]  
Queries value:  
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]  
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]  
Queries value: HKLM\software\microsoft\rpc[idletimerwindow]  
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\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\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\tcpip6\parameters\winsock[mapping]  
Queries value: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip6[winsock 2.0 provider id]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]  
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[queryadaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[usedomainnamedevolution]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[domainnamedevolutionlevel]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[prioritizerecorddata]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[allowunqualifiedquery]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[appendtomultilabelname]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[screenbadtlds]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[screenunreachableservers]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[screendefaultservers]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[dynamicserverqueryorder]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[filterclusterip]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[waitfornameerroronall]  
Queries value: HKLM\system\currentcontrolset\services\dns\parameters[usedns]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[dnssecurenamequeryfallback]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[enabledaforallnetworks]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[directaccessqueryorder]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[queryipmatching]  
Queries value: HKLM\system\currentcontrolset\services\dns\parameters[usehostsfile]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[addrconfigcontrol]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[disablesmartnameresolution]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[preferlocaloverlowerbindingdns]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[querynetbtfqdn]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[disablesmartprotocolreordering]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[udprecvbuffersize]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[registrationenabled]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[registerprimaryname]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[registeradaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[registerreverselookup]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[registerwanadapters]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[registrationttl]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[registrationrefreshinterval]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[registrationmaxaddresscount]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressesstoregister]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\parameters[updatesecuritylevel]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\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[adaptimeoutlimit]  
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[newdhcprvregistration]  
Queries value:

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

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

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

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

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

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

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

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[searchlist]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enabledhcp]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationenabled]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registeradaptername]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[domain]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdomain]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpv6domain]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserver]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationenabled]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registeradaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[domain]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpdomain]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[nameserver]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpnameserver]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[queryadaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[disableadapterdomainname]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationmaxaddresscount]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[maxnumberofaddresstoregister]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[enablemulticast]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[queryadaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disableadapterdomainname]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disablenameregistration]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enableadapterdomainnameregistration]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationmaxaddresscount]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[maxnumberofaddresstoregister]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enablemulticast]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]  
Queries value: HKLM\system\currentcontrolset\control\locale[00000409]  
Queries value: HKLM\system\currentcontrolset\control\language groups[1]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms  
shell dlg 2]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\datastore\_v1.0[disable]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\datastore\_v1.0[datafilepath]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane1]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane2]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane3]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane4]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane5]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane6]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane7]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane8]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane9]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane10]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane11]  
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane12]  
 Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane13]  
 Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane14]  
 Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane15]  
 Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane16]  
 Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]  
 Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]