# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 161, Task ID: 642

Task ID: 642 Risk Level: 5

Date Processed: 2016-04-28 13:04:49 (UTC)

Processing Time: 61.37 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

4 Checks whether debugger is present

5 PE: Contains compressed section

### 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

# File System Events

Creates: C:\ProgramData\ZebraNetworkSystems

Creates: C:\ProgramData\ZebraNetworkSystems\NeoRouter
Creates: C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems

 $\label{lem:continuous} Creates: C: \label{lem:continuous} C: \label{lem:continuous} Admin\appData\ap$ 

Creates: C:\Users\Admin\AppData\Local\Temp\{C4F8782C-E12C-434E-8631-EBEA3E8890A1}

Creates: C:\Users\Admin\AppData\Local\Temp\Tmp41D6.tmp

Opens: C:\Windows\Prefetch\6282B1723F3A4B0054D80AEB27C8F-E920D1CA.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\apphelp.dll

Opens: C:\Windows\Temp\6282b1723f3a4b0054d80aeb27c8fed5.exe

C:\Windows\SysWOW64\ntdll.dll Opens: Opens: C:\Windows\SysWOW64\kernel32.dll C:\Windows\SysWOW64\KernelBase.dll Opens: C:\Windows\apppatch\sysmain.sdb Opens: Opens: C:\Windows\apppatch\AcGenral.dll Opens: C:\Windows\apppatch\AcLayers.dll C:\Windows\SysWOW64\sechost.dll Opens: Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\Windows\SysWOW64\winmm.dll C:\Windows\SysWOW64\samcli.dll Opens:

Opens: C:\Windows\SysWOW64\msacm32.dll Opens: C:\Windows\SysWOW64\version.dll Opens: C:\Windows\SysWOW64\userenv.dll Opens: C:\Windows\SysWOW64\dwmapi.dll Opens: C:\Windows\SysWOW64\winspool.drv C:\Windows\SysWOW64\mpr.dll Opens: Opens: C:\Windows\SysWOW64\winmmbase.dll Opens: C:\Windows\SysWOW64\combase.dll C:\Windows\SysWOW64\profapi.dll Opens:

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\6282b1723f3a4b0054d80aeb27c8fed5.exe.Config

Opens: C:\Windows\SysWOW64\msvcrt.dll

Opens: C:\Windows\SysWOW64\bcryptprimitives.dll

C:\Windows\SysWOW64\cryptbase.dll Opens: Opens: C:\Windows\SysWOW64\sspicli.dll C:\Windows\SysWOW64\rpcrt4.dll Opens: Opens: C:\Windows\SysWOW64\gdi32.dll Opens: C:\Windows\SysWOW64\user32.dll Opens: C:\Windows\SysWOW64\shlwapi.dll Opens: C:\Windows\SysWOW64\ole32.dll C:\Windows\SysWOW64\oleaut32.dll Opens: C:\Windows\SysWOW64\advapi32.dll Opens: Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\iertutil.dll Opens: C:\Windows\SysWOW64\wininet.dll Opens: C:\Windows\SysWOW64\urlmon.dll C:\Windows\SysWOW64\cfgmgr32.dll Opens: Opens: C:\Windows\SysWOW64\devobj.dll C:\Windows\SysWOW64\setupapi.dll Opens: 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

C:\Windows\WinSxS\x86\_microsoft.windows.common-Opens: controls\_6595b64144ccf1df\_6.0.9200.16384\_none\_893961408605e985\comctl32.dll

C:\Windows\SysWOW64\wsock32.dll Opens: 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\6282b1723f3a4b0054d80aeb27c8fed5.exe.2.Manifest C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.3.Manifest Opens:

Opens: C:\windows\temp\Log.ini

Opens: C:\ProgramData\ZebraNetworkSystems\NeoRouter\Log.ini

C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.1000.Manifest Opens:

Opens:

Opens: C:\Windows\SysWOW64\netapi32.dll C:\Windows\SysWOW64\netutils.dll Opens: Opens: C:\Windows\SysWOW64\srvcli.dll Opens: C:\Windows\SysWOW64\wkscli.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 C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: Opens: C:\Windows\SysWOW64\winnsi.dll Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll  ${\tt C:\Windows\SysWOW64\dhcpcsvc.dll}$ Opens: Opens: C:\Windows\System32\Drivers\etc\hosts Opens: C:\Windows\Fonts\StaticCache.dat Opens: C:\Windows\SysWOW64\imageres.dll Reads from: C:\Windows\System32\Drivers\etc\hosts

#### Network Events

Reads from:

DNS query: secure.neorouter.com

Sends data to: 0.0.0.0:53

# Windows Registry Events

HKLM\system\currentcontrolset\services\tcpip\parameters Creates kev:

C:\Windows\Fonts\StaticCache.dat

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 kev: 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

HKLM\software\policies\microsoft\mui\settings

Opens key:

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration  $HKLM \verb|\system| current controlset| control \verb|\mui| settings \verb|\language| configuration$ Opens key:

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 \ wow 6432 node \ microsoft \ windows \ current version \ side by side
 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
                      HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows nt\\| windows file
 Opens key:
protection
 Opens key:
                      HKLM\software\policies\microsoft\windows nt\windows file protection
                     HKLM\software\microsoft\windows
 Opens kev:
nt\currentversion\appcompatflags\disable8and16bitmitigation
 Opens key:
                      HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
                      HKLM\system\currentcontrolset\control\lsa
 Opens key:
 Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                     HKLM\software\wow6432node\microsoft\windows
 Opens kev:
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:
 Opens key:
                     HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
 Opens key:
                      HKLM\software\policies\microsoft\sqmclient\windows
 Opens key:
                     HKLM\software\microsoft\sqmclient\windows
 Opens key:
                     HKLM\software\wow6432node\microsoft\ole
 Opens key:
                     HKLM\software\wow6432node\microsoft\ole\tracing
                     HKLM\software\microsoft\ole\tracing
 Opens key:
 Opens key:
                     HKLM\software\wow6432node\microsoft\oleaut
 Opens key:
                     HKLM\system\currentcontrolset\control\networkprovider\hworder
                     HKLM \ software \ wow 6432 node \ microsoft \ windows \ error \ reporting \ wmr
 Opens key:
 Opens key:
                      HKLM\software\wow6432node\microsoft\windows\currentversion\setup
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\setup
                     HKLM\software\wow6432node\microsoft\windows\currentversion
 Opens key:
 Opens key:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale
 Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
                      HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
 Opens key:
execution options
 Opens key:
                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\dllnxoptions
 Opens kev:
                      HKLM\svstem\currentcontrolset\services\crvpt32
                      HKLM \verb|\system| current control set \verb|\services| winsock 2 \verb|\parameters| \\
 Opens key:
 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\00260bb3
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000003
 Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
 Opens key:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000014

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000001)$ 

Opens key:

Opens key:

Opens key:

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
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
                                HKCU\software\microsoft\windows\currentversion\policies\network
  Opens key:
  Opens key:
                                HKCU\software\microsoft\windows\currentversion\policies\comdlg32
  Opens key:
Opens key:
fdc1-4dc3-a9dd-070d1d495d97}
  Opens key:
fdc1-4dc3-a9dd-070d1d495d97}\propertybag
                                 HKLM\software\wow6432node\microsoft\windows
  Opens key:
nt\currentversion\profilelist
                                HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:
  Opens key:
65f9-4cf6-a03a-e3ef65729f3d}
  Opens key:
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
                                HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:
  Opens key:
                                 HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
  Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in folders
  Opens key:
                                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:
                                 HKLM\system\currentcontrolset\control\computername
                                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens kev:
  Opens key:
                                HKLM\system\setup
  Opens key:
                                HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
  Opens key:
                                HKLM\software\wow6432node\microsoft\rpc
  Opens key:
                                HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \ nt \setminus rpc
  Opens key:
                                 HKLM\software\policies\microsoft\windows nt\rpc
  Opens kev:
                                HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001
  Opens kev:
provider
  Opens key:
                                 HKLM\software\policies\microsoft\cryptography
                                 HKLM\software\microsoft\cryptography
  Opens key:
  Opens key:
                                HKLM\software\wow6432node\microsoft\cryptography\offload
                                 HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ intellar \ and \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ intellar \ node \ microsoft \ node \ microsoft \ node \
  Opens key:
hardware cryptographic service provider
  Opens key:
                                HKLM\software\wow6432node\zebranetworksystems\neorouter
  Opens key:
                                 \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ 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
                                HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:
  Opens key:
                                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
  Opens key:
                                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:
                                 HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
  Opens key:
                                 HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:
                                HKLM\software\wow6432node\policies\microsoft\system\dnsclient
  Opens key:
                                 HKLM\software\policies\microsoft\system\dnsclient
  Opens key:
                                 HKLM\system\currentcontrolset\services\dns
  Opens key:
                                HKLM \setminus system \setminus current control \setminus sqmservice list
  Opens key:
                                HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\|
nt\dnsclient\dnspolicyconfig
  Opens key:
                                HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens kev:
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:
806e6f6e6963}
```

Opens key:

25b8d56dd1d8}

8a6dc56e0da9}

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus interfaces \setminus \{b5105d63-74c6-4dc1-87b7-47b1-147b1$ 

55779daa70e9}

HKLM\system\currentcontrolset\services\tcpip\linkage Opens key: Opens key: HKLM\svstem\currentcontrolset\control\nls\locale

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens key: HKLM\system\currentcontrolset\control\nls\language groups

HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink Opens key:

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore\_v1.0

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\surrogatefallback

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus compatibility \setminus 6282b1723f3a4b0054d80 \\ aeb27c8fed5.exe$ 

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\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] HKLM\system\currentcontrolset\control\nls\customlocale[empty] Queries value:

Queries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Oueries value:

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-

us[alternatecodepage]

Oueries value: HKCU\control panel\desktop[preferreduilanguages]

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value:

HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value:

HKCU\software\microsoft\windows Oueries value:

 $\verb|nt\currentversion\appcompatflags[showdebuginfo]| \\$ 

HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value:

Queries value: HKLM\software\policies\microsoft\windows nt\windows file

protection[knowndlllist]

Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]

HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Oueries value:

HKLM\software\microsoft\windows Queries value:

nt\currentversion\gre\_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[6282b1723f3a4b0054d80aeb27c8fed5] HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\windows[loadappinit dlls]

HKLM\software\microsoft\sqmclient\windows[ceipenable] Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

HKLM\software\microsoft\ole[aggressivemtatesting] Oueries value:

Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

Oueries 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] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[usefilter]

 $\label{lem:hklmsoftware} \verb+ HKLM \software \microsoft \windows nt \current version \cite{lem:hklmsoftware} in the execution \cite{lem:hklmsoftware} and \cite{lem:hklmsoftware} in the execution \cite{lem:hklmsoftware} and \ci$ Oueries value:

options\dllnxoptions[6282b1723f3a4b0054d80aeb27c8fed5.exe]

HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version]

Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx] Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[namespace\_callout]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num]

Oueries value:

Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog9 [num\_catalog\_entries]$ 

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001[packedcatalogitem]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\0000000000002[packedcatalogitem]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005[packedcatalogitem]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006[packedcatalogitem] Oueries 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]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
   Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 00000000000002 [displaystring] \\ Queries \ value:$
- $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[storesserviceclassinfo]
  Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 00000000000002 [provider info] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid] Oueries value:
- $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 00000000000003 \ [address family] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version]
  Queries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerinfo]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
   Oueries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid] Oueries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[supportednamespace] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 00000000000004 \ [version] \ Oueries \ value:$ 

 $HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[librarypath]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 00000000000005 \ [displaystring] \ Queries \ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[enabled]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[storesserviceclassinfo]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[librarypath]
Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 00000000000006 \ [displaystring] \ Queries \ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[enabled]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]
Oueries value:

Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[category]

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} Whit$ 

fdc1-4dc3-a9dd-070d1d495d97[name]

Queries value:

fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{62ab5d82-d84b, 1944b, 1$ 

fdc1-4dc3-a9dd-070d1d495d97}[description]

Queries value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{62ab5d82-microsoft \setminus windows \setminus explorer \setminus explorer$ 

fdc1-4dc3-a9dd-070d1d495d97}[relativepath]

Queries value:

 $HKLM \label{lem:hklm} White the latest and the la$ 

fdc1-4dc3-a9dd-070d1d495d97}[parsingname]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} [infotip]$ 

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[icon]}$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-

fdc1-4dc3-a9dd-070d1d495d97}[security]

Queries value:

fdc1-4dc3-a9dd-070d1d495d97}[streamresource]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} [stream resource type]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} \ [local redirectonly]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} \ [roamable]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} [precreate]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} [stream]$ 

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \equal 62 ab 5d82-fdc1-4dc3-a9dd-070d1d495d97 \cite{thm:local-ham} [publish expanded path]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[attributes]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} \ [folder type id]$ 

Queries value:

 $\label{limit} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\early \cite{Cab5d82-fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]$ 

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[category]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [name]$ 

Oueries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder folder folder$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescription\folderdescri$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [relative path]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [infotip]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[localized name]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]$ 

Queries value:

 $\label{lem:hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$ 

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder 65f9-4cf6-a03a-e3ef65729f3d\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729f\folder 65f9-4cf6-a03a-e3ef65729$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1}{3} eb 685 db 65f9 - 4cf6 - a 03a - e 3ef65729 f 3d \footnote{2}{3} es the surface of the surface \colored \co$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [local redirectonly]$ 

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\roamable\

Queries value:

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\[publishexpanded\path]$ 

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[attributes] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid] Oueries value: 65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[appdata] Queries value: Queries value: HKLM\system\setup[oobeinprogress] Oueries value: HKLM\system\setup[systemsetupinprogress] HKLM\system\currentcontrolset\control\nls\customlocale[en] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en] Oueries value: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout] Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Queries value: HKLM\software\microsoft\rpc[idletimerwindow]  $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| cryptography \verb|\defaults\\| provider$ Queries value: 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] HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems] Queries value: Oueries value: HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds] Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds] HKLM\software\microsoft\cryptography[machineguid] Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Oueries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip[winsock 2.0 provider id] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping] HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6[winsock 2.0 provider id] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]  $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [prioritize record data]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]

HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\svstem\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]  $\label{lem:hklmsystem} \verb|HKLM| system| current control set | services| dnscache| parameters [use hosts file]| \\$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries 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[multicastsenderflags] Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]

Oueries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
   Oueries value:
                                                 HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
   Oueries 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]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
   Oueries value:
                                                 HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
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:
55779daa70e9}[registeradaptername]
HKLM\svstem\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[domain]
   Oueries value:
55779daa70e9}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpv6domain]
   Oueries value:
HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-
55779daa70e9}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
   Oueries value:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-
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]
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]
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]
   Oueries value:
                                                 HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[queryadaptername]
   Oueries value:
```

55779daa70e9}[disableadapterdomainname] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationmaxaddresscount] Oueries value: 55779daa70e9}[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[enablemulticast] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationmaxaddresscount] Oueries value:  $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-d$ 806e6f6e6963}[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enablemulticast] HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409] HKLM\system\currentcontrolset\control\nls\language groups[1] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore\_v1.0[disable] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\datastore\_v1.0[datafilepath] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane1] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane3] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane4] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane5] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane6] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane7] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane9] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane10] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane11] HKLM\software\microsoft\windows Queries value:  $\verb|nt\currentversion\languagepack\surrogatefallback[plane12]|$ HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane13] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane14]

Queries value:  $\begin{tabular}{ll} $HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext] \\ Queries value: \end{tabular}$ 

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

 $\verb|nt\currentversion\languagepack\surrogatefallback[plane15]|$ 

nt\currentversion\languagepack\surrogatefallback[plane16]

Queries value:

Queries value:

 $HKLM \verb|\software\microsoft| windows \verb|\currentversion| policies \verb|\explorer[turnoffspianimations]| \\$