# 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

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: UP)

#### 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 C:\Windows\SysWOW64\KernelBase.dll Opens: Opens: C:\Windows\apppatch\sysmain.sdb Opens: C:\Windows\apppatch\AcGenral.dll C:\Windows\apppatch\AcLayers.dll Opens: Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\uxtheme.dll C:\Windows\SysWOW64\winmm.dll Opens: 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\dwmapi.dll C:\Windows\SysWOW64\winspool.drv Opens: Opens: C:\Windows\SysWOW64\mpr.dll Opens: C:\Windows\SysWOW64\winmmbase.dll C:\Windows\SysWOW64\combase.dll Opens: C:\Windows\SysWOW64\profapi.dll Opens:

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

```
C:\Windows\SysWOW64\bcryptprimitives.dll
 Opens:
                         C:\Windows\SysWOW64\cryptbase.dll
 Opens:
                         C:\Windows\SysWOW64\sspicli.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\rpcrt4.dll
 Opens:
                         C:\Windows\SysWOW64\gdi32.dll
                         C:\Windows\SysWOW64\user32.dll
 Opens:
                         C:\Windows\SysWOW64\shlwapi.dll
 Opens:
                         C:\Windows\SysWOW64\ole32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\oleaut32.dll
                         C:\Windows\SysWOW64\advapi32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\shell32.dll
 Opens:
                         C:\Windows\SysWOW64\iertutil.dll
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
                         C:\Windows\SysWOW64\urlmon.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cfgmgr32.dll
                         C:\Windows\SysWOW64\devobj.dll
 Opens:
 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
                         C:\Windows\WinSxS\x86_microsoft.windows.common-
 Opens:
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\srvcli.dll
                         C:\Windows\SysWOW64\wkscli.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
                         C:\usr\local\ssl\cert.pem
 Opens:
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
                         C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc.dll
 Opens:
                         C:\Windows\System32\Drivers\etc\hosts
 Opens:
                         C:\Windows\SysWOW64\FWPUCLNT.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
                         C:\Windows\WinSxS\x86_microsoft.windows.c...
 Opens:
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
                         C:\Windows\Fonts\micross.ttf
 Opens:
 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  $\Rightarrow$  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\policies\microsoft\windows\safer\codeidentifiers
   Opens key:
   Opens key:
                                               HKCU\software\policies\microsoft\windows\safer\codeidentifiers
   Opens kev:
                                               HKLM\system\currentcontrolset\control\nls\customlocale
                                               HKLM\system\currentcontrolset\control\nls\language
   Opens key:
   Opens key:
                                               HKLM\system\currentcontrolset\control\mui\uilanguages
   Opens key:
                                               HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
                                               HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
   Opens key:
   Opens key:
                                               HKLM\software\wow6432node\policies\microsoft\mui\settings
   Opens key:
                                               HKLM\software\policies\microsoft\mui\settings
   Opens key:
   Opens key:
                                               HKCU\control panel\desktop\muicached\machinelanguageconfiguration
   Opens key:
                                               HKLM \verb|\system| current control current control current control current control current control current control current current control current control current control current current current control current current
   Opens key:
                                               HKCU\software\policies\microsoft\control panel\desktop
                                               {\tt HKCU \backslash control\ panel \backslash desktop \backslash language configuration}
   Opens key:
   Opens key:
                                               HKCU\control panel\desktop
                                               HKCU\control panel\desktop\muicached
   Opens key:
                                               HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
   Opens kev:
   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:
Opens key:
                                               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
                                               HKLM\software\wow6432node\microsoft\windows
   Opens key:
nt\currentversion\compatibility32
                                               HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
   Opens key:
compatibility
   Opens key:
                                               HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
   Opens key:
   Opens key:
                                               HKLM\software\policies\microsoft\sqmclient\windows
   Opens key:
                                               HKLM\software\microsoft\sqmclient\windows
                                               HKLM\software\wow6432node\microsoft\ole
   Opens key:
   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 \verb|\system| current controlset \verb|\control| network provider \verb|\hworder| and the substitution of the 
   Opens key:
                                               HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
   Opens key:
                                               Opens key:
                                               HKLM\software\microsoft\windows\currentversion\setup
   Opens kev:
                                               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 kev:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
   Opens key:
                                               HKLM\system\currentcontrolset\services\crypt32
   Opens key:
                                               HKLM\system\currentcontrolset\services\winsock2\parameters
                                               \label{lem:hklm} \verb+ HKLM \system \current control \end{+} ls \end{+} sorting \verb+ ids \\
   Opens key:
   Opens key:
                                               HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\16316034
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
   Opens kev:
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\000000000006

Opens kev:

Opens key:

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ parameters \ protocol\_catalog\_entries \ protocol\_catalog \ parameters \ parameters
   Opens key:
Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 000000000011) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (catal
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
    Opens key:
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\000000000000
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
    Opens key:
Opens key:
                                                       HKCU\software\microsoft\windows\currentversion\policies\explorer
    Opens key:
                                                       HKCU\software\microsoft\windows\currentversion\policies\network
                                                       HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus comdlg 32
    Opens key:
    Opens key:
HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| explorer\\| folder descriptions
    Opens kev:
fdc1-4dc3-a9dd-070d1d495d97}
   Opens key:
fdc1-4dc3-a9dd-070d1d495d97}\propertybag
                                                       HKLM\software\wow6432node\microsoft\windows
    Opens key:
nt\currentversion\profilelist
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\profilelist
    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:
\label{thm:local_hammon_hammon} HKCU \software \microsoft \windows \current version \explorer \session in follows \current version \explorer \session \current \cur
    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\svstem\setup
    Opens key:
                                                       HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
                                                       HKLM\software\wow6432node\microsoft\rpc
    Opens key:
                                                       HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
    Opens key:
    Opens key:
                                                       HKLM\software\policies\microsoft\windows nt\rpc
                                                       HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider
    Opens key:
types\type 001
    Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
                                                       HKLM\software\policies\microsoft\cryptography
    Opens key:
    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
                                                       HKLM\system\currentcontrolset\services\winsock\setup migration\providers
    Opens kev:
    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 kev:
                                                       HKLM\svstem\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\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\software\wow6432node\policies\microsoft\windows

nt\dnsclient\dnspolicyconfig

HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig

Opens kev:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

Opens key:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-

806e6f6e6963}

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces Opens kev:

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-

25b8d56dd1d83

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\nls\locale

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

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

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

Opens kev:

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

HKLM\software\microsoft\windows Opens kev:

nt\currentversion\languagepack\datastore\_v1.0

HKLM\software\microsoft\windows Opens kev:

nt\currentversion\languagepack\surrogatefallback

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 HKLM\software\wow6432node\microsoft\ctf\ Opens key:

Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses

HKLM\software\microsoft\windows Opens kev: nt\currentversion\languagepack\surrogatefallback\ms shell dlg

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

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|$ HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries value:

Oueries 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]

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

Queries value:

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

HKCU\software\microsoft\windows Queries value:

nt\currentversion\appcompatflags[showdebuginfo]

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

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

protection[knowndlllist]

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

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

HKLM\software\microsoft\windows Oueries value: nt\currentversion\gre\_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[bb02abb18c51ee149dde9732ca8e5fae] Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

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

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

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

reporting\wmr[disable]

Oueries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Queries value:  $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \setminus current version [device path]$ 

Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-usl Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter] HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value: options\dllnxoptions[bb02abb18c51ee149dde9732ca8e5fae.exe] Oueries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version] Queries 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] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace\_callout] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num] Oueries 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\00000000001[packedcatalogitem] Oueries 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\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\000000000008[packedcatalogitem] Oueries value: 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] Queries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[displaystring])$ Oueries 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:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space \_ catalog 5 \ (catalog\_entries \ 000000000001 [supported name space]$ 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\000000000001[version] Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 1000000000001 \ [storesservice classinfo]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000002[librarypath] Queries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000002 \ [displaystring]$ Queries value: 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\0000000000002[supportednamespace] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 00000000000002 [version]$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog\_catalog\_entries \ (000000000003[library path])$ 

Queries value:

Oueries value:

Queries value:

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[storesserviceclassinfo]
  Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 0000000000003 \ [provider info] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[librarypath] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring]
   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\0000000000004[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo]
   Oueries value:
- 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]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerid]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
   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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[storesserviceclassinfo]

  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerinfo]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring]
   Oueries 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[version]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 000000000006 \ [storesserviceclassinfo] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo] Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2\_32 numhandle buckets]$

Queries value:

- $HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$
- fdc1-4dc3-a9dd-070d1d495d97}[category]

Queries value:

- $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (62ab5d82-d82-d82) \ descriptions \ (62ab5d82-d82-d82) \ descriptions \ (62ab5d82-d82) \ descriptions \ (62ab5d82-$
- fdc1-4dc3-a9dd-070d1d495d97}[name]

Queries value:

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

Queries value:

- HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
- fdc1-4dc3-a9dd-070d1d495d97}[description]

Oueries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\early folderdescriptions \end{2.0} $$ fdc1-4dc3-a9dd-070d1d495d97\[localizedname] $$$ 

Oueries value:

 $\label{thm:local-decomposition} HKLM \software \wow 6432 node \windows \current version \explorer \folder descriptions \explorer \folder descriptions \folder \folde$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (62ab 5d82-fdc1-4dc3-a9dd-070d1d495d97) [security]$ 

Oueries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder desc$ 

Queries value:

 $\label{local-software-wow6432-node-microsoft-windows-current-version-explorer-folder-descriptions-folder-description-f$ 

Oueries value:

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

Queries value:

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{limit} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescripti$ 

Queries value: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\profile| list[programdata]|$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cite{parentfolder} and the context of the c$ 

Queries value:

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

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 \wow6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \cite{Abcompart} \cite{Abcompart} \end{area} The label{lem:hklmsoftware} \end{area} The label{lem:hklmsoftware} \cite{Abcompart} \end{area} The label{lem:hklmsoftware} The label{lem:hklmsoftware} \end{area} The label{lem:hklmsoftware} \cite{Abcompart} \end{area} The label{lem:hklmsoftware} The label{lem:hklmsoftware} \end{area} The label{lem:hklmsoftware} The labe$ 

Queries value:

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

Queries value

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$ 

Queries value:

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

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]

65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[roamable]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[precreate]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[stream]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (3eb685db-10eb) \ descr$ 65f9-4cf6-a03a-e3ef65729f3d}[attributes]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{3eb685db-10explorer\} \ folder \ before \ folder \ before \ folder \ folder \ before \ folder \ fol$ 65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]

Queries value:

 $\label{thm:local_explorer_local_ex$ 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] HKLM\system\setup[oobeinprogress] Queries value:

HKLM\system\setup[systemsetupinprogress] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en]

Queries value:

HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize] HKLM\software\microsoft\rpc[idletimerwindow] Queries value:

HKLM\software\wow6432node\microsoft\cryptography\defaults\provider Queries value:

types\type 001[name]

Queries value:

HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]

 $HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic$ provider[image path]

Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Oueries value:

HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]

HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds] Oueries value:

HKLM\software\microsoft\cryptography[machineguid] Oueries value:

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Queries value:

HKLM\system\currentcontrolset\services\winsock\setup Oueries value:

migration\providers\tcpip[winsock 2.0 provider id]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

Oueries value:

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

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:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \{ parameters \setminus winsock [maxsock addrlength] \}$ 

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance] HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]

Oueries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]

Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [disables mart name resolution]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn] Oueries value: Oueries value:

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

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value:

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

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] Oueries value:

Queries value:

Queries value:

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

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

Queries value:

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

HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value:

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

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

HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value:

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update top level domain zones]$ Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries 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] Oueries 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] HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: Oueries 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] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration] Oueries value: 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] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Oueries value: Queries value:  $HKLM \ system \ current control set \ services \ tcpip \ harameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-8$ 55779daa70e9}[searchlist1 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] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registeradaptername] Oueries value: 55779daa70e9}[domain] Oueries 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: 55779daa70e9}[nameserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserver] Oueries 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]
   Oueries value:
806e6f6e6963}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
   Oueries value:
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]
   Oueries value:
55779daa70e9}[queryadaptername]
   Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ \align{tabular}{ll} HKLM \
55779daa70e9}[disableadapterdomainname]
   Queries value:
55779daa70e9}[registrationmaxaddresscount]
   Queries value:
55779daa70e9}[maxnumberofaddressestoregister]
   Queries value:
55779daa70e9}[enablemulticast]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[queryadaptername]
   Queries value:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-be62-be12e1de57-d6fa-11e1-be62-be12e1de57-d6fa-11e1-be62-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57-d6fa-11e1-be12e1de57
806e6f6e6963}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disabledynamicupdate]
   Queries value:
806e6f6e6963}[enableadapterdomainnameregistration]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationmaxaddresscount]
   Queries value:
806e6f6e6963}[maxnumberofaddressestoregister]
   Oueries 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\nls\locale[00000409]
                                             HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
   Oueries value:
                                             HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
                                             HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
   Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
                                             HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
                                             HKLM\software\microsoft\windows
   Queries value:
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]
   Oueries 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]
                                             HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
```

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

 $\verb|nt\currentversion\language| pack\surrogatefallback[plane11]|$ 

Queries value:

Queries value:

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:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer[turn off spianimations]$