Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 41, Task ID: 164

Task ID: 164 Risk Level: 5

Date Processed: 2016-04-28 12:51:29 (UTC)

Processing Time: 61.3 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: PF32:win32:gui

File Type: PE32:win32:gui File Size: 813216 bytes

MD5: bb02abb18c51ee149dde9732ca8e5fae

SHA256: c5c1d3d6b80fb79a451ac1b8a8dfcb5a5b20e76f38df0f6ed34dc08842a13ad1

Description: None

Pattern Matching Results

2 PE: Nonstandard section

SSL traffic on standard port

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: 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

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

Creates event: \BaseNamedObjects\BFE_Notify_Event_{1b51c8aa-833c-4d8e-a6fd-

57d8d1ab2494}

Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Creates: C:\ProgramData\ZebraNetworkSystems

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

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

Creates: C:\Users\Admin\AppData\Local\Temp\{949A0C80-8A07-40DF-8C96-92C8D7E0D565}

Creates: C:\Users\Admin\AppData\Local\Temp\TmpCA93.tmp

Opens: C:\Windows\Prefetch\BB02ABB18C51EE149DDE9732CA8E5-39A45309.pf

Opens: C:\Windows

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

 Opens:
 C:\Windows\System32\wow64win.dll

 Opens:
 C:\Windows\System32\wow64cpu.dll

 Opens:
 C:\Windows\system32\wow64log.dll

Opens: C:\Windows\SysWOW64

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

Opens: C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.Local\

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

 $Opens: C: \verb|Windows| winsxs| x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\\comctl32.dll$

Opens: C:\windows\temp\WINSPOOL.DRV
Opens: C:\Windows\SysWOW64\winspool.drv
Opens: C:\windows\temp\WSOCK32.dl1
Opens: C:\Windows\SysWOW64\wsock32.dl1
Opens: C:\Windows\SysWOW64\apphelp.dl1
Opens: C:\Windows\AppPatch\sysmain.sdb

Opens: C:\Windows\Temp\bb02abb18c51ee149dde9732ca8e5fae.exe

Opens: C:\windows\temp\samcli.dll C:\Windows\SysWOW64\samcli.dll Opens: Opens: C:\windows\temp\MSACM32.dll Opens: C:\Windows\SysWOW64\msacm32.dll Opens: C:\windows\temp\VERSION.dll Opens: C:\Windows\SysWOW64\version.dll Opens: C:\windows\temp\sfc.dll Opens: C:\Windows\SysWOW64\sfc.dll Opens: C:\windows\temp\sfc_os.DLL C:\Windows\SysWOW64\sfc_os.dll Opens: Opens: C:\windows\temp\USERENV.dll Opens: C:\Windows\SysWOW64\userenv.dll C:\windows\temp\profapi.dll Opens: Opens: C:\Windows\SysWOW64\profapi.dll Opens: C:\windows\temp\dwmapi.dll Opens: C:\Windows\SysWOW64\dwmapi.dll Opens: C:\windows\temp\MPR.dll Opens: C:\Windows\SysWOW64\mpr.dll C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.Config Opens: Opens: C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\WindowsShell.Manifest Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui Opens: C:\Windows\Globalization\Sorting\SortDefault.nls Opens: C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.2.Manifest Opens: C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.3.Manifest Opens: C:\windows\temp\Log.ini Opens: C:\ProgramData\ZebraNetworkSystems\NeoRouter Opens: C:\ProgramData\ZebraNetworkSystems Opens: C:\ProgramData Opens: C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems\NeoRouter C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems Opens: Opens: C:\Users\Admin\AppData\Roaming Opens: C:\Windows\Temp Opens: C:\ProgramData\ZebraNetworkSystems\NeoRouter\Log.ini Opens: C:\windows\temp\bb02abb18c51ee149dde9732ca8e5fae.exe.1000.Manifest Opens: C:\windows\temp\bb02abb18c51ee149dde9732ca8e5faeENU.dll Opens: C:\windows\temp\bb02abb18c51ee149dde9732ca8e5faeL0C.dll Opens: C:\dev\ Opens: C:\windows\temp\NETAPI32.DLL Opens: C:\Windows\SysWOW64\netapi32.dll Opens: C:\windows\temp\netutils.dll Opens: C:\Windows\SysWOW64\netutils.dll Opens: C:\windows\temp\srvcli.dll Opens: C:\Windows\SysWOW64\srvcli.dll Opens: C:\windows\temp\wkscli.dll C:\Windows\SysWOW64\wkscli.dll Opens: Opens: C:\windows\temp\CRYPTSP.dll Opens: C:\Windows\SysWOW64\cryptsp.dll Opens: C:\Windows\SysWOW64\rsaenh.dll Opens: C:\usr\local\ssl\cert.pem Opens: C:\Users\Admin\AppData\Local\Temp Opens: C:\Windows\SysWOW64\ws2_32.dll Opens: C:\Windows\SysWOW64\mswsock.dll Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL Opens: C:\Windows\SysWOW64\wship6.dll Opens: C:\windows\temp\DNSAPI.dll Opens: C:\Windows\SysWOW64\dnsapi.dll C:\windows\temp\IPHLPAPI.DLL Opens: Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: C:\windows\temp\WINNSI.DLL C:\Windows\SysWOW64\winnsi.dll Opens: Opens: C:\windows\temp\dhcpcsvc6.DLL Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll Opens: C:\windows\temp\dhcpcsvc.DLL Opens: C:\Windows\SysWOW64\dhcpcsvc.dll Opens: C:\windows\temp\rasadhlp.dll C:\Windows\SysWOW64\rasadhlp.dll Opens: 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_6.0.7600.16385_en-us_581cd2bf5825dde9 Opens: C:\Windows\winsxs\x86_microsoft.windows.c..controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui Opens: C:\Windows\Fonts\tahoma.ttf Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui Opens: C:\Windows\Fonts\StaticCache.dat Opens: C:\Windows\Fonts\tahomabd.ttf Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\SysWOW64\rpcss.dll Reads from: C:\Windows\System32\drivers\etc\hosts

C:\Windows\Fonts\StaticCache.dat

C:\Windows\SysWOW64\winmm.dll

Opens:

Reads from:

Network Events

DNS query: secure.neorouter.com

secure.neorouter.com \Rightarrow 72.167.40.3 DNS response:

Connects to: 72.167.40.3:443

8.8.8.8:53 Sends data to:

Sends data to: secure.neorouter.com:443 (72.167.40.3)

Receives data from: 8.8.8.8:53

secure.neorouter.com:443 (72.167.40.3) Receives data from:

Windows Registry Events

HKLM\system\currentcontrolset\services\tcpip\parameters

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

options

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

HKLM\software\microsoft\wow64 Opens kev:

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

execution options

Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens kev:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

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

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

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

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

Opens key: HKCU\

HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

Opens key: HKCU\software\policies\microsoft\control panel\desktop ${\it HKCU} \ control\ panel\ desktop\ language configuration$ Opens key:

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

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

protection

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

HKI M\ Opens key:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows$ Opens key:

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

nt\currentversion\gre_initialize HKLM\software\wow6432node\microsoft\windows

Opens key: nt\currentversion\compatibilitv32

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

compatibility

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

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

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\software\wow6432node\microsoft\windows\currentversion\internet

settings Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \begin{tabular}{ll} policies \end{tabular} in the local policies \end{tabular} and the local policies \end{tabular$ Opens key:

settings

Opens kev: HKLM\svstem\currentcontrolset\control\cmf\config

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

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

Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder Opens kev:

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

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

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

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\16316034

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 00000000000001)
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
 Opens key:
                  HKCU\software\microsoft\windows\currentversion\policies\explorer
 Opens key:
                  HKCU\software\microsoft\windows\currentversion\policies\network
 Opens key:
                  HKCU\software\microsoft\windows\currentversion\policies\comdlg32
 Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions
 Opens kev:
fdc1-4dc3-a9dd-070d1d495d97}
 Opens kev:
fdc1-4dc3-a9dd-070d1d495d97}\propertybag
                  HKLM\software\wow6432node\microsoft\windows
 Opens kev:
nt\currentversion\profilelist
 Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
                  HKCU\software\microsoft\windows\currentversion\explorer
 Opens key:
                  HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
 Opens kev:
 Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus explorer \setminus 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
                  HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
 Opens key:
 Opens key:
                  HKLM\software\wow6432node\microsoft\rpc
 Opens key:
                  HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
 Opens key:
                  HKLM\software\policies\microsoft\windows nt\rpc
 Opens key:
                  HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001
 Opens kev:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
```

HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

Opens key: HKLM\system\currentcontrolset\control\lsa Opens key:

provider Opens key:

```
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                                                 HKLM\software\policies\microsoft\cryptography
   Opens key:
   Opens key:
                                                 HKLM\software\microsoft\cryptography
   Opens key:
                                                  HKLM\software\wow6432node\microsoft\cryptography\offload
   Opens kev:
                                                 HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\intel
hardware cryptographic service provider
                                                 HKLM\software\wow6432node\zebranetworksystems\neorouter
   Opens kev:
   Opens key:
                                                 HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
                                                  HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
   Opens key:
                                                  HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:
                                                  HKLM\system\currentcontrolset\services\winsock\setup migration\providers
   Opens key:
                                                  HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                                                 HKLM\system\currentcontrolset\services\winsock\setup
   Opens key:
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\control\sqmservicelist
   Opens key:
                                                  HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
   Opens kev:
                                                 HKLM\svstem\currentcontrolset\services\dns
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
   Opens key:
                                                  HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
   Opens key:
e1e01c1f69b5}
   Opens key:
HKLM \land system \land current control set \land services \land tcpip6 \land parameters \land table 20-1000 for the system \land tcpip6 
806e6f6e6963}
   Opens key:
806e6f6e6963}
   Opens key:
127795cce47a}
   Opens key:
65fee5bae0b1}
   Opens key:
                                                  HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens key:
                                                 HKLM\system\currentcontrolset\control\nls\locale
   Opens key:
                                                  HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
   Opens key:
                                                 HKLM\system\currentcontrolset\control\nls\language groups
   Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ bb02abb18c51ee149dde9732ca8e5fae. execond \ building \ buildin
                                                 HKLM\software\wow6432node\microsoft\windows
   Opens kev:
nt\currentversion\fontsubstitutes
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
                                                  HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
   Opens key:
   Opens key:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
   Opens key:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
                                                 HKLM\software\microsoft\windows
   Opens key:
nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2
                                                 HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
   Opens key:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
   Opens key:
                                                 HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                                 HKLM\software\wow6432node\microsoft\ctf\
   Opens key:
   Opens key:
                                                  HKLM\software\wow6432node\microsoft\ctf\knownclasses
                                                 HKLM\software\microsoft\windows
   Opens key:
nt\currentversion\languagepack\surrogatefallback\segoe ui
   Opens key:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
                                                 HKLM\software\microsoft\windows\currentversion\policies\explorer
   Opens key:
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
                                                 HKLM\system\currentcontrolset\control\session
   Queries value:
manager[cwdillegalindllsearch]
                                                 HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Oueries value:
   Queries value:
                                                 HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                 \label{lem:hklm} \verb+kklm \+ system \+ control \+ ls \+ custom \+ locale \+ [empty]
   Oueries value:
   Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
   Queries value:
                                                  HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
```

Oueries value: HKLM\system\currentcontrolset\control\mui\uilanguages\enus[alternatecodepage] Oueries value: HKCU\control panel\desktop[preferreduilanguages] HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ [prefer external manifest]$ Oueries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value: HKLM\software\policies\microsoft\windows nt\windows file

protection[knowndlllist]

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

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

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[security_hklm_only]

HKLM\system\currentcontrolset\control\cmf\config[system] Queries value: HKLM\software\wow6432node\microsoft\windows\windows error Queries value:

reporting\wmr[disable]

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ setup [source path]$ Oueries value: Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]

HKLM\software\microsoft\sqmclient\windows[ceipenable] Queries value:

Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters [winsock_registry_version]$

HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] Queries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog 9 [next_catalog_entry_id]$

HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9[num catalog entries]

Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ (000000000001[packed catalog item]) \ details \ de$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem] Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace _catalog5 \ catalog_entries \ 00000000001 [library path]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000001[displaystring]) \ descriptions and the services \ (displaystring) \ descriptions are the services \ (displaystring) \ descriptions \$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled] Queries value:

Oueries value:

- 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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- 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\0000000000004[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\000000000004[addressfamily]
 Queries 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]
 Queries value:
- 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] Oueries 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\000000000005[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\000000000006[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000006 [providerid] \ Oueries \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000000006 [address family] \\ Queries \ value:$

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000006 [supported name space]]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ set alog_entries \ (00000000000006 \ [version]) \ and \ (version) \ and \ (ve$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value:

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

Queries value:

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

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

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

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

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

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

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[icon]

Queries value:

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[streamresource]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{62ab5d82-4b14, 2444, 2$ fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]

fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly] Oueries value:

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[roamable] Queries value:

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

Oueries value:

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[attributes]

 $HKLM \label{lem:hklm} White the latest and the la$ fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ ficon 1$

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder 6569-4cf6-a03a-e3ef65729f3d \[stream resource]$

Queries value:

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

Oueries value

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

Oueries value:

 $\label{local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folder$

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[appdata]

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]

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

Queries value:

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

types\type 001[name]

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\sprovider\sprovide$

Queries value:

 $\label{lem:hklmsoft} HKLM \ software \ wow 6432 node \ icrosoft \ cryptography \ defaults \ provider \ [image path]$

Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

Queries value: HKLM\system\currentcontrol\sa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrol\sa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Oueries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography [privkey cachepurge interval seconds]$

 $\label{thm:condition} Queries \ value: \qquad \qquad \text{HKLM} \ software \ policies \ microsoft \ cryptography [privatekey lifetimes econds]$

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

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

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

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

```
migration\providers\tcpip[winsock 2.0 provider id]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM\svstem\currentcontrolset\services\tcpip6\parameters\winsock[usedelavedacceptance]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
                          HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Queries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowungualifiedguery]
 Queries 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]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamegueryfallback]
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                          HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [addrconfig control]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Queries 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]
 Queries 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]
```

Queries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
                       HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
                       HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
\label{local-parameters} $$HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]$
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Queries value:
\label{lem:hklm} \verb+Kklm \system \current control set \services \label{lem:hklm} \verb+ dn scache \parameters [multicastresponder flags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
 Queries value:
                       HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Queries value:
\label{lem:hklm} \verb+Kklm \ system \ current control set \ \verb+services \ \verb+dns \ cache \ \verb+parameters \ [dnsquick query time outs]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[searchlist]
e1e01c1f69b5}[enabledhcp]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationenabled]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registeradaptername]
 Queries value:
e1e01c1f69b5}[domain]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpdomain]
 Queries value:
e1e01c1f69b5}[dhcpv6domain]
```

Oueries value:

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

Oueries value

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [names erver]$

Oueries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [dhcpnameserver]$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \true \normaliset \system \current control set \services \true \normaliset \system \syste$

Queries value:

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

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [register adapter name]$

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [domain]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [dhcpdomain]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ 'parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [nameserver]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [dhcpnameserver]$

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [queryadaptername]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [disable adapter domain name]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration maxaddress count]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [maxnumber of addresses to register]$

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\}[enable multicast]$

Queries value:

 $\label{thm:local-bound} HKLM \system \current control set \services \tcpip\parameters \interfaces \end{4846ee} 42-7039-11de-9d20-806e6f6e6963 \[query adapter name \]$

Queries value:

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

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6 16e6 963\} \ [disable dynamic update]$

Queries value:

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

Queries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'tcpip \ parameters \ 'interfaces \ '\{846ee342-7039-11de-9d20-806e6f6e6963\} \ [registration max address count]$

Queries value:

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

Queries value:

 $\label{thm:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [enable multicast]$

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdl]]

Queries value: HKLM\system\currentcontrol\st\control\nls\locale[00000409]

Queries value: HKLM\system\currentcontrol\st\control\nls\language groups[1]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms

shell dlg 2]
 Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]

Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0[datafilepath] Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane2]
Oueries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane3]

```
HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
                         HKLM\software\microsoft\windows
 Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane6]|
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
 Oueries value:
                         HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
 Queries value:
                         HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane10]|
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
 Queries value:
                         HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane13]|
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                         HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane16]|
 Queries value:
                         Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
                         HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| ctf[enablean chorcontext]
 Oueries value:
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
```