Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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

Task ID: 645 Risk Level: 5

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

Processing Time: 61.14 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe"

Sample ID: 161
Type: basic
Owner: admin

Label: 6282b1723f3a4b0054d80aeb27c8fed5

Date Added: 2016-04-28 12:45:06 (UTC)

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

MD5: 6282b1723f3a4b0054d80aeb27c8fed5

SHA256: 63e6e2e578871b03c530a3a5d3ddd22e6a00bf9de6f167ceeb5908d5c9c56c8e

Description: None

Pattern Matching Results

2 PE: Nonstandard section

5 Packer: UPX

5 PE: Contains compressed section

4 Checks whether debugger is present

Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

Packer: UPX

Process/Thread Events

Creates process: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe

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

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

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

File System Events

Creates: C:\ProgramData\ZebraNetworkSystems

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

 $\label{lem:continuous} Creates: C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems\NeoRouter$

Creates: C:\Users\Admin\AppData\Local\Temp\{BE05233B-09BA-478E-BD53-BF105526ACA1}

Creates: C:\Users\Admin\AppData\Local\Temp\Tmp2C2B.tmp

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

Opens: C:\Windows

 Opens:
 C:\Windows\System32\wow64.dl1

 Opens:
 C:\Windows\System32\wow64win.dl1

 Opens:
 C:\Windows\System32\wow64cpu.dl1

 Opens:
 C:\Windows\system32\wow64log.dl1

 Opens:
 C:\Windows\SysWOW64

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

Opens: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.Local\

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

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

 $Opens: C: \windows \times x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2 \times comct132.dll$

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

Opens: C:\Windows\AppPatch\AcGenral.dll
Opens: C:\Windows\temp\UxTheme.dll
Opens: C:\Windows\Sys\WO\W64\uxtheme.dll
Opens: C:\Windows\temp\WINMM.dll
Opens: C:\Windows\Sys\WO\W64\winmm.dll
Opens: C:\Windows\Sys\WO\W64\winmm.dll
Opens: C:\Windows\Sys\WO\W64\samcli.dll
Opens: C:\Windows\Sys\WO\W64\samcli.dll

C:\windows\temp\MSACM32.dll Opens: 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: C:\windows\temp\USERENV.dll Opens: Opens: C:\Windows\SysWOW64\userenv.dll Opens: C:\windows\temp\profapi.dll Opens: C:\Windows\SysWOW64\profapi.dll Opens: C:\windows\temp\dwmapi.dll C:\Windows\SysWOW64\dwmapi.dll Opens: Opens: C:\windows\temp\MPR.dll Opens: C:\Windows\SysWOW64\mpr.dll

Opens: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.Config

Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\WindowsShell.Manifest

Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens: C:\Windows\Globalization\SortIng\SortDefault.nls

 Opens:
 C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.2.Manifest

 Opens:
 C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.3.Manifest

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

Opens: C:\ProgramData\ZebraNetworkSystems\NeoRouter

Opens: C:\ProgramData\ZebraNetworkSystems

Opens: C:\ProgramData

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

Opens: C:\Users\Admin\AppData\Roaming\ZebraNetworkSystems

Opens: C:\Users\Admin\AppData\Roaming

Opens: C:\Windows\Temp

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

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

Opens: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5ENU.dl1
Opens: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5LOC.dl1

Opens: C:\dev'

Opens:

Opens: C:\windows\temp\NETAPI32.DLL C:\Windows\SysWOW64\netapi32.dll Opens: 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

C:\Windows\SysWOW64\ws2_32.dll Opens: Opens: C:\Windows\SysWOW64\mswsock.dll Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL C:\Windows\SysWOW64\wship6.dll Opens: 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 Opens: C:\Windows\SysWOW64\winnsi.dll Opens: C:\windows\temp\dhcpcsvc6.DLL Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll Opens: C:\windows\temp\dhcpcsvc.DLL Opens: C:\Windows\SysWOW64\dhcpcsvc.dll Opens: C:\windows\temp\rasadhlp.dll Opens: C:\Windows\SysWOW64\rasadhlp.dll Opens: C:\Windows\System32\drivers\etc\hosts Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui

Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\windows\temp\imageres.dll
Opens: C:\Windows\SysWOW64\imageres.dll

Opens: C:\Windows\SysWOW64\en-US\imageres.dll.mui

Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\rpcss.dll

Reads from: C:\Windows\System32\drivers\etc\hosts
Reads from: C:\Windows\Fonts\StaticCache.dat

Network Events

DNS query: secure.neorouter.com

Sends data to: 8.8.8.8:53

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options Opens key: HKLM\system\currentcontrolset\control\session manager HKLM\software\microsoft\wow64 Opens key: Opens kev: 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 key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens kev: Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings HKLM\software\policies\microsoft\mui\settings Opens key: Opens key: HKCU\ Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration Opens key: Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop\languageconfiguration Opens key: HKCU\control panel\desktop Opens key: HKCU\control panel\desktop\muicached Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside Opens kev: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$ Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \ nt \setminus windows \ file$ protection HKLM\software\policies\microsoft\windows nt\windows file protection Opens key: Opens key: HKLM∖ Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\gre_initialize HKLM\software\wow6432node\microsoft\windows Opens key: nt\currentversion\compatibility32 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility

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

Opens key: HKLM\system\currentcontrolset\services\crypt32 Opens key: HKLM\software\wow6432node\microsoft\ole Opens key: HKLM\software\wow6432node\microsoft\ole\tracing Opens kev: HKLM\software\microsoft\ole\tracing

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

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

settings Opens key:

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

settings

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

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

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

Opens key: HKLM\software\microsoft\windows\currentversion\setup Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: $\label{lem:hworder} \verb+HKLM\+ system\+ current controlset\+ control\+ network provider\+ hworder$

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

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

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

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00260bb3

Opens kev:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000

Opens key:

Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \000000000010 \parameters \end{substitute} Opens key:$

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog 5$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
Opens kev:

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:

Opens key:

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

Opens key:

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

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

nt\currentversion\profilelist

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

 $\label{thm:local-prop} \parks the local-property of the local-pr$

65f9-4cf6-a03a-e3ef65729f3d}\propertybag

Opens key: $\label{local-opens} \mbox{\sc HKCU\software\mbox{\sc microsoft\windows\currentversion\explorer}} \mbox{\sc hkCu\software\mbox{\sc microsoft\windows\currentversion\explorer}} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer} \mbox{\sc microsoft\windows\explorer}} \mbox{\sc microsoft\windows\explorer} \mbox{\sc microsoft\windows\explorer} \mbox{\sc microsoft\windows\explorer} \mbox{\sc microsoft\windows\explorer} \mbox{\sc microsoft\windows\explorer} \mbox{\sc microsoft\windows\explorer} \mbox{\s$

 $Opens\ key: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following \ for the contraction \ fo$

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \session in folders \end{tabular}$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

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

Opens key: HKLM\system\setup

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

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

Opens key: HKLM\software\policies\microsoft\windows nt\rpc

 $Opens~key: \\ HKLM\software\wow6432node\microsoft\cryptography\defaults\provider$

types\type 001

Opens key:

 $HKLM \label{lem:hklm} Which is the latest and the latest and the latest and the latest area of the latest and the latest area of the latest and the latest area of the latest area. The latest area of the latest area. The latest area of the latest area. The latest area of the latest area. The latest area of the latest area of the late$

provider

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

Opens key: HKLM\system\currentcontrol\lsa

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\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

 $\verb|migration\providers\tcpip| \\$

Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6 Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient Opens key: Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| system\\| dnsclient$ Opens key: HKLM\software\policies\microsoft\system\dnsclient HKLM\system\currentcontrolset\control\samservicelist Opens key: Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache HKLM\system\currentcontrolset\services\dns Opens key: Opens kev: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient\dnspolicyconfig Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5} Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5} Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963} Opens key: 806e6f6e6963} Opens kev: 127795cce47a} Opens key: 65fee5bae0b1} ${\tt HKLM \ } system \verb| current control set \verb| services \verb| tcpip \verb| linkage \\$ Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\locale Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens key: HKLM\system\currentcontrolset\control\nls\language groups Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0 HKLM\software\microsoft\windows Opens key: $\verb|nt\currentversion\language| pack\surrogatefall back|$ HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback\segoe ui Opens key: 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 kev: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer HKLM\software\microsoft\windows\currentversion\policies\explorer Opens kev: Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter] HKLM\system\currentcontrolset\control\session Oueries value: manager[cwdillegalindllsearch] Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Oueries value: $\label{lem:hklmsoftware belief} HKLM \software \parente abled] \\$ HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries value: Oueries 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] HKCU\control panel\desktop[preferreduilanguages] Oueries value: $\label{local-control} \mbox{ HKCU\control panel\desktop\muicached[machinepreferreduilanguages]} \\$ Queries value: Oueries value: $HKLM \label{limits} \label{limits} HKLM \label{limits} HKLM \label{limits} Which \label{lim$

Queries value: HKCU\software\microsoft\windows

nt\currentversion\appcompatflags[showdebuginfo]

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

protection[knowndlllist]

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

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

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

Oueries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls] Oueries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: settings[disableimprovedzonecheck] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[security_hklm_only] Queries value: HKLM\system\currentcontrolset\control\cmf\config[system] Oueries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries 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] Oueries value: HKLM\software\microsoft\samclient\windows[ceipenable] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem] Oueries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ (0000000000006 [packed catalog item]) \ details \$ Queries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000008 \ [packed catalog item]$ Queries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ (000000000009[packed catalog item]) \ details \ de$ Queries value: Queries 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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid] Oueries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space _ catalog 5 \ (catalog_entries \ 000000000001 [supported name space]$ 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\00000000001[storesserviceclassinfo] Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath] HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value: 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]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ name space_catalog \ nam$

Oueries value:

Oueries value:

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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version] Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000003 [storesservice class info] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 00000000000004 [providerid] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Queries 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\000000000005[librarypath]
 Oueries 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\00000000005[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[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]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000006 [library path] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000006 \ [storesservice class in fo] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \end{2.5} $\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[attributes] $$$

Queries value:

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

Queries value:

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

Queries value: HKLM\software\microsoft\windows

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

Oueries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\category\cite{Control of the control of the cont$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ between the sum of the$

```
65f9-4cf6-a03a-e3ef65729f3d}[icon]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[security]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[roamable]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[precreate]
 Queries value:
65f9-4cf6-a03a-e3ef65729f3d}[stream]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
 Queries value:
65f9-4cf6-a03a-e3ef65729f3d}[attributes]
 Oueries value:
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
 Queries value:
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
               HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[appdata]
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
               HKLM\system\setup[oobeinprogress]
 Queries value:
               HKLM\system\setup[systemsetupinprogress]
               Queries value:
               HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
 Oueries value:
               HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value:
               HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001[name]
 Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
 Oueries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
 Queries value:
               HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
 Queries value:
               HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
```

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

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

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

Queries value:

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

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

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

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

Queries value:

HKLM\system\currentcontrolset\services\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]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]$

Queries value:

Queries value:

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

Queries value:

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

migration\providers\tcpip6[winsock 2.0 provider id]

Queries value:

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

Queries value:

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

Queries value:

```
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
  Queries value:
                                     HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
                                     HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [prioritize record data]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dynamicser verquery order]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:
                                     \label{lem:hklm} \verb+kklm \system \current control set \services \dns cache \parameters [useed ns]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[dnssecurenamequervfallback]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
  Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[guervipmatching]
  Queries value:
                                     HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Queries value:
\label{thm:local_hammeters} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} set \end{tabular} and \end{tabular} are the label \end{tabular} are the label \end{tabular} system \end{tabular} are the label \end{tabular} are the label \end{tabular} are the label \end{tabular} system \end{tabular} are the label \end{tabular} are the label \end{tabular} are the label \end{tabular} are the label \end{tabular} system \end{tabular} are the label \e
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [enable adapter domain name registration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  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]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicasts endermax time out]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns query time outs]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[searchlist]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enabledhcp1
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationenabled]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registeradaptername]
 Oueries value:
e1e01c1f69b5}[domain]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpdomain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpv6domain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[nameserver]
 Queries value:
e1e01c1f69b5}[nameserver]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpnameserver]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enabledhcp]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationenabled]
 Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[domain]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[dhcpdomain]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[nameserver]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[dhcpnameserver]
 Queries value:
                      HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
 Oueries value:
e1e01c1f69b5}[queryadaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[disableadapterdomainname]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationmaxaddresscount]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enablemulticast]
 Oueries value:
806e6f6e6963}[queryadaptername]
 Queries value:
806e6f6e6963}[disableadapterdomainname]
 Oueries value:
806e6f6e6963}[disabledynamicupdate]
 Queries value:
806e6f6e6963}[enableadapterdomainnameregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationmaxaddresscount]
 Queries value:
806e6f6e6963}[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enablemulticast]
                      HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Oueries value:
 Queries value:
                      HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
                      HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Queries value:
                      HKLM \ system \ current controls et \ \ control \ \ language \ groups [1]
 Oueries value:
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                      HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane1]|
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
                      HKLM\software\microsoft\windows
 Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane4]|
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
                      HKLM\software\microsoft\windows
 Oueries value:
\verb| nt\currentversion \ | \ anguage pack \ | \ surrogatefall \ back[plane 7]|
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
```

HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane12]

Oueries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane13] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane14] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane15] Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane16]

Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable] Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]

Queries value:

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