Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 161, Task ID: 644

Task ID: 644 Risk Level: 5

Date Processed: 2016-04-28 13:04:50 (UTC)

Processing Time: 61.23 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

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\{E5C0BA6D-0AD9-4F3B-B984-56F456B41B25}

Creates: C:\Users\Admin\AppData\Local\Temp\TmpB5DC.tmp

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

Opens: C:\Windows\System32

Opens: C:\Windows\System32\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\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

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

Opens: C:\Windows\Temp\6282b1723f3a4b00
Opens: C:\Windows\AppPatch\AcGenral.dll
Opens: C:\windows\temp\SspiCli.dll
Opens: C:\Windows\System32\sspicli.dll
Opens: C:\windows\temp\UxTheme.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Windows\temp\WINMM.dll
Opens: C:\Windows\System32\winmm.dll

Opens: C:\windows\temp\samcli.dll
Opens: C:\Windows\System32\samcli.dll
Opens: C:\windows\temp\MSACM32.dll
Opens: C:\Windows\System32\msacm32.dll
Opens: C:\windows\temp\VERSION.dll

C:\Windows\System32\version.dll Opens: Opens: C:\windows\temp\sfc.dll Opens: C:\Windows\System32\sfc.dll Opens: C:\windows\temp\sfc_os.DLL Opens: C:\Windows\System32\sfc_os.dll Opens: C:\windows\temp\USERENV.dll Opens: C:\Windows\System32\userenv.dll Opens: C:\windows\temp\profapi.dll Opens: C:\Windows\System32\profapi.dll Opens: C:\windows\temp\dwmapi.dll Opens: C:\Windows\Svstem32\dwmapi.dll Opens: C:\windows\temp\MPR.dll

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

Opens: C:\Windows\System32\imm32.dll
Opens: C:\Windows\WindowsShell.Manifest

Opens: C:\Windows\System32\en-US\setupapi.dll.mui

Opens: C:\Windows\System32\en-US\setupapi.dl1.mui
Opens: C:\Windows\Globalization\SortIng\SortDefault.nls

C:\Windows\System32\mpr.dll

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

C:\Users\Admin\AppData\Roaming

Opens: C:\Windows\Temp

Opens:

Opens:

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

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

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

Opens: C:\dev\

Opens: C:\windows\temp\NETAPI32.DLL C:\Windows\System32\netapi32.dll Opens: Opens: C:\windows\temp\netutils.dll Opens: C:\Windows\System32\netutils.dll Opens: C:\windows\temp\srvcli.dll Opens: C:\Windows\System32\srvcli.dll Opens: C:\windows\temp\wkscli.dll C:\Windows\System32\wkscli.dll Opens: Opens: C:\windows\temp\CRYPTSP.dll Opens: C:\Windows\System32\cryptsp.dll C:\Windows\System32\rsaenh.dll Opens: Opens: C:\windows\temp\CRYPTBASE.dll Opens: C:\Windows\System32\cryptbase.dll Opens: C:\usr\local\ssl\cert.pem

Opens: C:\Users\Admin\AppData\Local\Temp Opens: C:\Windows\System32\mswsock.dll Opens: C:\Windows\System32\WSHTCPIP.DLL Opens: C:\Windows\System32\wship6.dll Opens: C:\windows\temp\DNSAPI.dll Opens: C:\Windows\System32\dnsapi.dll Opens: C:\windows\temp\IPHLPAPI.DLL Opens: C:\Windows\System32\IPHLPAPI.DLL Opens: C:\windows\temp\WINNSI.DLL Opens: C:\Windows\System32\winnsi.dll Opens: C:\windows\temp\dhcpcsvc6.DLL C:\Windows\System32\dhcpcsvc6.dll Opens: Opens: C:\windows\temp\dhcpcsvc.DLL Opens: C:\Windows\System32\dhcpcsvc.dll Opens: C:\windows\temp\rasadhlp.dll Opens: C:\Windows\System32\rasadhlp.dll Opens: C:\Windows\System32\drivers\etc\hosts

Opens: C:\Windows\System32\en-US\imageres.dll.mui

C:\Windows\System32\en-US\KernelBase.dll.mui

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

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

Network Events

Opens:

DNS query: secure.neorouter.com

Sends data to: 8.8.8.8:53

Windows Registry Events

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option

```
Opens key:
                                                         HKLM\system\currentcontrolset\control\srp\gp\dll
    Opens key:
                                                         HKLM\software\policies\microsoft\windows\safer\codeidentifiers
    Opens key:
                                                         HKCU\software\policies\microsoft\windows\safer\codeidentifiers
    Opens key:
    Opens key:
                                                         HKCU\control panel\desktop\muicached\machinelanguageconfiguration
    Opens key:
                                                         HKLM\software\policies\microsoft\mui\settings
                                                         HKCU\software\policies\microsoft\control panel\desktop
    Opens key:
                                                         {\tt HKCU \backslash control\ panel \backslash desktop \backslash language configuration}
    Opens key:
    Opens key:
                                                         HKCU\control panel\desktop
                                                         HKCU\control panel\desktop\muicached
    Opens key:
                                                         \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constraint of the
    Opens key:
    Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
    Opens key:
                                                         HKCU\software\microsoft\windows nt\currentversion\appcompatflags
    Opens key:
                                                         HKLM\system\currentcontrolset\control\nls\sorting\versions
    Opens key:
                                                         HKLM\software\policies\microsoft\windows nt\windows file protection
                                                         HKLM\
    Opens kev:
    Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\diagnostics
    Opens key:
                                                         HKLM\system\currentcontrolset\control\error message instrument\
    Opens key:
                                                         HKLM\system\currentcontrolset\control\error message instrument
    Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\gre_initialize
    Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\compatibility32
    Opens kev:
                                                         HKLM\software\microsoft\windows nt\currentversion\ime compatibility
    Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\windows
    Opens key:
                                                         HKLM\system\currentcontrolset\services\crypt32
    Opens key:
                                                         HKLM\software\microsoft\ole
    Opens key:
                                                         HKLM\software\microsoft\ole\tracing
    Opens key:
                                                         HKLM\software\microsoft\oleaut
    Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\internet settings
    Opens key:
                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings
                                                         HKLM\system\currentcontrolset\control\cmf\config
    Opens key:
    Opens key:
                                                         HKLM\software\microsoft\windows\windows error reporting\wmr
    Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\setup
                                                         HKLM\software\microsoft\windows\currentversion
    Opens key:
    Opens key:
                                                         Opens key:
                                                         HKLM\system\currentcontrolset\control\nls\extendedlocale
    Opens key:
                                                         HKLM\system\currentcontrolset\control\networkprovider\hworder
    Opens key:
                                                         HKLM\software\policies\microsoft\sqmclient\windows
    Opens key:
                                                         HKLM\software\microsoft\sqmclient\windows
                                                         HKLM\system\currentcontrolset\services\winsock2\parameters
    Opens key:
    Opens key:
                                                         HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
    Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00260bb3
    Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
    Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9 \setminus 00000019
   Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
    Opens kev:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col\_catalog \\ \setminus catalog \\ \setminus
    Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
    Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
    Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000008
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
```

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000012

Opens key:

 $HKLM \ system \ control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 000000000013$ Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000014 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000015 Opens key:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 000000000016) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (catal$ Opens key:

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000017) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (cata
     Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries \ 000000000018
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
     Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 00000000000001) \ (catalog\_entries \ name space\_catalog 5 \ (catalog\_entries \ 
     Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
     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 \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions
HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \{62ab5d82-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-
a9dd-070d1d495d97}
     Opens key:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{62ab5d82 - fdc1 - 4dc3 - fdc1 - fd
a9dd-070d1d495d97}\propertybag
                                                                            HKLM\software\microsoft\windows nt\currentversion\profilelist
     Opens key:
     Opens key:
a03a-e3ef65729f3d}
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
                                                                            HKCU\software\microsoft\windows\currentversion\explorer
     Opens key:
     Opens key:
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
     Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus explorer \setminus session in fo \setminus 1 \setminus known folders
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
     Opens key:
 folders
     Opens key:
                                                                            HKLM\system\currentcontrolset\control\computername
     Opens key:
                                                                           HKLM\system\currentcontrolset\control\computername\activecomputername
     Opens key:
                                                                            HKLM\system\setup
     Opens kev:
                                                                            HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
     Opens key:
                                                                           HKLM\software\microsoft\rpc
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows nt\rpc
                                                                           HKLM\software\microsoft\cryptography\defaults\provider types\type 001
     Opens key:
     Opens key:
                                                                           HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 cryptographic provider
                                                                            HKLM\svstem\currentcontrolset\control\lsa\fipsalgorithmpolicv
     Opens key:
     Opens key:
                                                                            HKLM\system\currentcontrolset\control\lsa
     Opens kev:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                                                                            HKLM\software\policies\microsoft\cryptography
     Opens key:
                                                                            HKLM\software\microsoft\cryptography
     Opens key:
     Opens key:
                                                                            HKLM\software\microsoft\cryptography\offload
     Opens key:
                                                                           cryptographic service provider
     Opens kev:
                                                                           HKLM\software\zebranetworksvstems\neorouter
                                                                           HKLM\system\currentcontrolset\services\winsock\parameters
     Opens key:
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\psched\parameters\winsock
     Opens key:
                                                                            \label{lem:hklm} \verb+Kklm \system \current control set \services \swinsock \setup migration \space{2mm} providers
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
```

HKLM\system\currentcontrolset\services\winsock\setup Opens key:

migration\providers\tcpip

HKLM\system\currentcontrolset\services\winsock\setup Opens key:

migration\providers\tcpip6

Opens kev: HKLM\svstem\currentcontrolset\services\dnscache\parameters Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: HKLM\software\policies\microsoft\system\dnsclient Opens key: HKLM\system\currentcontrolset\control\samservicelist

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

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

Opens key:

```
c19ce8a73253}
                                     HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens kev:
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens kev:
806e6f6e6963}
  Opens key:
1709a0196aed}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
  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\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens kev:
                                    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\segoe ui
  Opens kev:
HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus 6282b1723f3a4b0054d80aeb27c8fed5.exe
                                    HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
  Opens kev:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                     HKLM\software\microsoft\ctf\
  Opens key:
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\policies\explorer
                                    HKLM\system\currentcontrolset\control\session
  Oueries value:
manager[cwdillegalindllsearch]
                                    HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Oueries value:
                                    \label{lem:hklmsystem} \verb| HKLM \rangle is the label{lem:hklmsystem} and the label{lem:hklmsystem} is the label{lem:hklmsystem} and the label{lem:hklmsystem} is the l
  Oueries value:
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                     {\tt HKCU \backslash control\ panel \backslash desktop[preferreduilanguages]}
  Oueries value:
                                     HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
  Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]
                                    HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
                                    HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:
  Queries value:
                                    HKLM\software\policies\microsoft\windows nt\windows file
protection[knowndlllist]
  Queries value:
                                    HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\compatibility32[6282b1723f3a4b0054d80aeb27c8fed5]
  Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
                                    HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:
                                    HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Oueries value:
                                    HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disableimprovedzonecheck]
  Oueries value:
                                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
                                    HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion[devicepath]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:
                                     HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Oueries 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]
  Oueries value:
HKLM\system\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\000000000005[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Queries value:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
- Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000014[packedcatalogitem]
- Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Queries 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\000000000002[displaystring]
- 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\000000000002[supportednamespace]
- 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[displaystring]
 Queries 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:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[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] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Queries 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\00000000005[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005[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\00000000005[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
 Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Oueries value:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
 Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 numbandle buckets]$

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[category]

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} [parent folder]$

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[description]}$

Queries value:

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

Queries value:

a9dd-070d1d495d97}[parsingname]

Queries value:

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

Queries value:

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

Oueries value:

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[roamable]}$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (62ab5d82-fdc1-4dc3-a9dd-070d1d495d97) \ [precreate]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[stream]}$

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} \ fattributes \ label{eq:helmonoper}$

Queries value:

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

Queries value:

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hkkm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \folder$

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

a03a-e3ef65729f3d}[localredirectonly] Oueries value: a03a-e3ef65729f3d}[roamable] Oueries value: a03a-e3ef65729f3d}[precreate] Oueries value: a03a-e3ef65729f3d}[stream] Oueries value: a03a-e3ef65729f3d}[publishexpandedpath] Oueries value: a03a-e3ef65729f3d}[attributes] Oueries value: a03a-e3ef65729f3d}[foldertypeid] Queries value: a03a-e3ef65729f3d}[initfolderhandler] $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell$ Oueries value: folders[appdata] Queries value: HKLM\system\setup[oobeinprogress] Queries value: HKLM\system\setup[systemsetupinprogress] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[en] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en] Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Queries value: Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type 001[name] Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type] $HKLM \ software \ microsoft \ strong$ Queries value: cryptographic provider[image path] HKLM\system\currentcontrolset\control\session Queries value: manager[safeprocesssearchmode] HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Oueries value: Oueries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems] HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds] Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds] Queries value: HKLM\software\microsoft\cryptography[machineguid] Oueries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping] Oueries value: HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping] Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\psched[winsock 2.0 provider id] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] ${\tt HKLM \ } system \ \verb| current control set \ \verb| services \ \verb| winsock \ \verb| setup \ |$ Oueries value: migration\providers\tcpip[winsock 2.0 provider id] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] HKLM\system\currentcontrolset\services\winsock\setup Queries value: migration\providers\tcpip6[winsock 2.0 provider id] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance] Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
Queries 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] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Queries 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: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Queries value: Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration refreshinterval]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Queries value:

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

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

Queries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: Queries value: 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] Queries value: 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: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[searchlist] Queries value: c19ce8a73253}[enabledhcp] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[registrationenabled] Queries value: c19ce8a73253}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[domain] Oueries value: c19ce8a73253}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[dhcpv6domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[nameserver] Queries value: c19ce8a73253}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[dhcpnameserver] Queries value: 806e6f6e6963}[enabledhcp] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationenabled] Oueries value: 806e6f6e6963}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[dhcpdomain] Oueries value:

```
806e6f6e6963}[nameserver]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpnameserver]
                       HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[quervadaptername]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[disableadapterdomainname]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationmaxaddresscount]
 Queries value:
c19ce8a73253}[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enablemulticast]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[queryadaptername]
 Queries value:
806e6f6e6963}[disableadapterdomainname]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disabledynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enableadapterdomainnameregistration]
806e6f6e6963}[registrationmaxaddresscount]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[maxnumberofaddressestoregister]
806e6f6e6963}[enablemulticast]
                       HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Queries value:
 Oueries value:
                       HKLM\svstem\currentcontrolset\services\winsock2\parameters[autodialdll]
 Queries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00000409]
                       HKLM\system\currentcontrolset\control\nls\language groups[1]
 Oueries value:
 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]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
                       HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                       HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane6]|
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
 Oueries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
 Oueries value:
                       HKLM\software\microsoft\windows
\verb|nt\currentversion\language| pack\surrogatefallback[plane15]|
 Oueries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                       HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 Oueries value:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
```

Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]