# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3314, Task ID: 766

Task ID: 766 Risk Level: 10

Date Processed: 2016-05-18 10:35:49 (UTC)

Processing Time: 80.91 seconds Virtual Environment: IntelliVM

**Execution Arguments:** "c:\windows\temp\857bd61a8241ac81385ee957d8137887.exe"

Sample ID: Type: basic Owner: admin

Label: 857bd61a8241ac81385ee957d8137887

Date Added: 2016-05-18 10:30:49 (UTC) PE32:win32:gui File Type:

File Size: 184832 bytes

857bd61a8241ac81385ee957d8137887 MD5:

efed61ac534b30cf6837dea448b72c43ec008f31273c445440a934aa5246ba2f SHA256:

Description: None

#### Pattern Matching Results

5 PE: Contains compressed section

3 HTTP connection - response code 200 (success)

10 Creates malicious events: Cycbot [Backdoor]

4 Checks whether debugger is present

3 Long sleep detected

#### Process/Thread Events

Creates process: C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe

["C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe"]

C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe Creates process: [C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe startC:\Program Files (x86)\LP\6930\027.exe%C:\Program Files (x86)\LP\6930]

Creates process: C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe

[C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe

startC:\Users\Admin\AppData\Roaming\0CE74\B5469.exe%C:\Users\Admin\AppData\Roaming\0CE74]

Terminates process: C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe

### Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects\{5D92BB9F-9A66-458f-ACA4-66172A7016D4}
Creates mutex:	\Sessions\1\BaseNamedObjects\{4D92BB9F-9A66-458f-ACA4-66172A7016D4}
Creates mutex:	\Sessions\1\BaseNamedObjects\{61B98B86-5F44-42b3-BCA1-33904B067B81}
Creates mutex:	\Sessions\1\BaseNamedObjects\{B16C7E24-B3B8-4962-BF5E-4B33FD2DFE78}
Creates mutex:	\Sessions\1\BaseNamedObjects\{B37C48AF-B05C-4520-8B38-2FE181D5DC78}
Creates mutex:	\Sessions\1\BaseNamedObjects\{OECE180F-6E9E-4FA6-A154-6876D9DB8906}
Creates mutex:	\Sessions\1\BaseNamedObjects\_!MSFTHISTORY!_
Creates mutey	ş – <u>–</u>

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!

\Sessions\1\BaseNamedObjects\WininetStartupMutex Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex Creates mutex:  $\verb|\Sessions|1| BaseNamedObjects| WininetProxyRegistryMutex|$ Creates mutex: \Sessions\1\BaseNamedObjects\4A3282FEF482C0F79E1 Creates mutex:

\Sessions\1\BaseNamedObjects\{6B985724-623F-492e-B0D6-C9715ADE853B} Creates event:

Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED \KernelObjects\MaximumCommitCondition Creates event: \BaseNamedObjects\SvcctrlStartEvent A3752DX Creates event:

\BaseNamedObjects\BFE\_Notify\_Event\_{3947d672-e600-4192-bf94-Creates event:

ce35ec765800}

## File System Events

Creates:	<pre>C:\Program Files (x86)</pre>
Creates:	C:\Program Files (x86)\74E66
Creates:	<pre>C:\Users\Admin\AppData\Roaming</pre>
Creates:	C:\Users\Admin\AppData\Roaming\0CE74
_	

C:\Users\Admin\AppData\Roaming\0CE74\4E66.CE7 Creates:

Creates: C:\Users\Admin

C:\Users\Admin\AppData\Local Creates:

C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files Creates:

Creates: C:\Program Files (x86)\LP Creates: C:\Program Files (x86)\LP\6930

```
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Creates:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Creates:
                         C:\Windows\Prefetch\857BD61A8241AC81385EE957D8137-5577336B.pf
 Opens:
 Opens:
                         C:\Windows
 Opens:
                         C:\Windows\System32\wow64.dll
 Opens:
                         C:\Windows\System32\wow64win.dll
                         C:\Windows\System32\wow64cpu.dll
 Opens:
                         C:\Windows\system32\wow64log.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64
 Opens:
                         C:\windows\temp\oleacc.dll
                         C:\Windows\SysWOW64\oleacc.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\sechost.dll
 Opens:
                         C:\windows\temp\MSIMG32.DLL
                         C:\Windows\SysWOW64\msimg32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
                         C:\windows\temp\OLEACCRC.DLL
 Opens:
                         C:\Windows\SysWOW64\oleaccrc.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\windows\temp\_CÂuVirtualProtect.DLL
                         C:\Windows\SysWOW64\_CÂuVirtualProtect.DLL
 Opens:
 Opens:
                         C:\Windows\system\_CÂuVirtualProtect.DLL
 Opens:
                         C:\Windows\_CÂuVirtualProtect.DLL
                         C:\Windows\SysWOW64\Wbem\_CÂuVirtualProtect.DLL
 Opens:
 Opens:
                         C:\Windows\SysWOW64\WindowsPowerShell\v1.0\_CÂuVirtualProtect.DLL
 Opens:
                         C:\windows\temp\apphelp.dll
                         C:\Windows\SysWOW64\apphelp.dll
 Opens:
 Opens:
                         C:\windows\temp\RASAPI32.dll
 Opens:
                         C:\Windows\SysWOW64\rasapi32.dll
 Opens:
                         C:\windows\temp\rasman.dll
 Opens:
                         C:\Windows\SysWOW64\rasman.dll
 Opens:
                         C:\windows\temp\WINHTTP.dll
 Opens:
                         C:\Windows\SysWOW64\winhttp.dll
 Opens:
                         C:\windows\temp\webio.dll
 Opens:
                         C:\Windows\SysWOW64\webio.dll
 Opens:
                         C:\
 Opens:
                         C:\Program Files (x86)
 Opens:
                         C:\Program Files (x86)\74E66
 Opens:
                         C:\Users\Admin\AppData\Roaming\0CE74
 Opens:
                         C:\Users\Admin\AppData\Roaming\0CE74\4E66.CE7
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
                         C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
                         C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe.Local\
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
 Opens:
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         C:\windows\temp\profapi.dll
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
 Opens:
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\AppData\Local
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
 Opens:
                         C:\Program Files (x86)\LP\6930
 Opens:
                         C:\Windows\Temp
                         C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wship6.dll
 Opens:
                         C:\Users\Admin\AppData\Roaming
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
                         C:\Windows\SysWOW64\rpcss.dll
                         C:\Windows\SysWOW64\uxtheme.dll
 Opens:
 Opens:
                         C:\windows\temp\DNSAPI.dll
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
                         C:\Users\Admin\AppData\Roaming\Cloud AV 2012\ahst.lni
 Opens:
 Opens:
                         C:\windows\temp\IPHLPAPI.DLL
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                         C:\windows\temp\WINNSI.DLL
 Opens:
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
                         C:\Windows\SysWOW64\FirewallAPI.dll
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens:
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
```

Opens:

C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

C:\Windows\SysWOW64\version.dll Opens: C:\windows\temp\dhcpcsvc6.DLL Opens: Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll Opens: C:\windows\temp\dhcpcsvc.DLL Opens: C:\Windows\SysWOW64\dhcpcsvc.dll Opens: C:\windows\temp\rasadhlp.dll C:\Windows\SysWOW64\rasadhlp.dll Opens: Opens: C:\Windows\System32\drivers\etc\hosts

Opens: C:\windows\temp\rtutils.dll
Opens: C:\Windows\SysWOW64\rtutils.dll

Opens: C:\Program
Opens: C:\Program.exe
Opens: C:\Program Files

Opens: C:\Program Files (x86)\LP\6930\027.exe
Opens: C:\Program Files (x86)\LP\6930\027.exe.exe
Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\

Opens: C:\Windows\SysWOW64\ras

 $\label{thm:connections} Opens: \\ C: \Users \land Admin \land AppData \land Roaming \land Microsoft \land Network \land Connections \land Pbk \\$ 

Opens: C:\windows\temp\sensapi.dll C:\Windows\SysWOW64\SensApi.dll Opens: Opens: C:\Users\Admin\AppData\Roaming\Mozilla\ Opens: C:\Users\Admin\AppData\Roaming\Opera\ Opens: C:\Windows\SysWOW64\wbem\wbemprox.dll C:\Windows\SysWOW64\wbem\wbemcomn.dll Opens: Opens: C:\Windows\SysWOW64\wbemcomn.dll Opens: C:\Windows\SysWOW64\wbem\Logs C:\windows\temp\CRYPTSP.dll Opens: Opens: C:\Windows\SysWOW64\cryptsp.dll Opens: C:\Windows\SysWOW64\rsaenh.dll Opens: C:\windows\temp\RpcRtRemote.dll Opens: C:\Windows\SysWOW64\RpcRtRemote.dll Opens: C:\Windows\SysWOW64\wbem\wbemsvc.dll Opens: C:\Windows\SysWOW64\wbem\fastprox.dll

Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL
Opens: C:\Users\Admin\AppData\Roaming\OCE74\B5469.exe
Opens: C:\Users\Admin\AppData\Roaming\OCE74\B5469.exe.exe

C:\Windows\SysWOW64\wbem\NTDSAPI.dll

C:\Windows\SysWOW64\ntdsapi.dll

Writes to: C:\Users\Admin\AppData\Roaming\OCE74\4E66.CE7
Reads from: C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe

Reads from: C:\Windows\System32\drivers\etc\hosts

#### **Network Events**

Opens:

Opens:

DNS query: cdn.adventofdeception.com DNS query: krq.enotusfed.com DNS query: jybeu.kupinosis.com DNS query: www.google.com DNS query: ncd.kupinosis.com DNS query: xprstats.com DNS guery: ocsp.verisign.com DNS response: www.google.com  $\Rightarrow$  58.26.8.109 www.google.com  $\Rightarrow$  58.26.8.99 DNS response:

www.google.com  $\Rightarrow$  58.26.8.89 DNS response: DNS response: www.google.com  $\Rightarrow$  58.26.8.94 www.google.com  $\Rightarrow$  58.26.8.103 DNS response: www.google.com  $\Rightarrow$  58.26.8.98 DNS response: DNS response: www.google.com  $\Rightarrow$  58.26.8.108 www.google.com  $\Rightarrow$  58.26.8.113 DNS response: DNS response: www.google.com  $\Rightarrow$  58.26.8.84 DNS response: www.google.com  $\Rightarrow$  58.26.8.93 www.google.com ⇒ 58.26.8.119 DNS response: DNS response: www.google.com  $\Rightarrow$  58.26.8.118 DNS response: www.google.com  $\Rightarrow$  58.26.8.104 DNS response: www.google.com  $\Rightarrow$  58.26.8.114 DNS response: www.google.com  $\Rightarrow$  58.26.8.123 DNS response: www.google.com  $\Rightarrow$  58.26.8.88

DNS response: e8218.dscb1.akamaiedge.net ⇒ 23.15.155.27

Connects to: 58.26.8.109:80
Connects to: 23.15.155.27:80
Sends data to: 8.8.8.8:53

Sends data to: www.google.com:80 (58.26.8.109)

Sends data to: e8218.dscb1.akamaiedge.net:80 (23.15.155.27)

 Sends data to:
 127.0.0.1:49162

 Sends data to:
 127.0.0.1:49164

 Receives data from:
 8.8.8.8:53

Receives data from: www.google.com:80 (58.26.8.109)

Receives data from: 127.0.0.1:49162

Receives data from: e8218.dscb1.akamaiedge.net:80 (23.15.155.27)

Receives data from: 127.0.0.1:49164

### Windows Registry Events

HKCU\software\microsoft\windows\currentversion\internet settings Creates key:

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\connections

Creates key: HKLM\software\wow6432node\microsoft\tracing

Creates kev:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385ee 957d8137887\_rasapi321ac + 12ac +$ 

Creates kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac 81385ee 957d 8137887\_rasmancs$ 

Creates kev: HKLM\software\wow6432node\microsoft\wbem\cimom

Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyoverride]

Deletes value:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ 

settings[autoconfigurl]

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

options

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

HKLM\software\microsoft\wow64 Opens kev:

Opens key:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \ nt \setminus current version \setminus image \ file$ 

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

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

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

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

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

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

Opens key: HKCU\

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

HKCU\software\policies\microsoft\control panel\desktop Opens key: Opens kev: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key:

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

Opens key:

HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre\_initialize

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

nt\currentversion\compatibility32 HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

Opens kev: compatibility

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

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

Opens key: HKLM\software\wow6432node\microsoft\ole\tracing Opens key: HKLM\software\microsoft\ole\tracing  $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| oleaut$ 

Opens kev: Opens key: HKCU\software\classes\

Opens key: HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-

00aa00389b71}\proxystubclsid32

HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-Opens key:

00aa00389b71}\proxystubclsid32

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

Opens key:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ 

settings Opens key:

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

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

settings

HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: Opens key: HKCU\software\microsoft\windows nt\currentversion\windows

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

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

Opens key: HKLM\system\setup

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

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

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

Opens key: HKLM\software\microsoft\rpc

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions$ 

Opens kev:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\}$ 

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\}\ property bag$ 

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\}$ 

Opens key:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.00} folder \color=1.00 \co$ 

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

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

Opens key:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ appid\_catalog \ 1b6cd 5d7$ 

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9

Opens key:

 $\label{lem:hklmsystem} $$HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\00000005$$ Opens key:$ 

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog 9 \setminus catalog\_entries$ 

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008 Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol\_catalog 9 \catalog\_entries \000000000010 \parameters \end{substitute} Opens key:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5
Opens kev:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 \setminus 00000028$ 

Opens key:

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

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000001

Opens key:

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

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

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

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

migration\providers\tcpip

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings

Opens key: HKLM\software\wow6432node\policies

Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer

Opens key: HKLM\software\policies\microsoft\internet explorer

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main

Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\wow6432node\policies\microsoft\internet

explorer\main\featurecontrol

Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol

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

explorer\main\featurecontrol

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

settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ f9d\}$ 

Opens key:

 $\label{thm:local-base-bound} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\eqref{352481e8-33be-4251-ba85-6007}\eqref{352481e8-33be-$ 

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders

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

folders

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

Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}$ 

Opens key:

 $\label{local-HKLM} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fifthed fib32785-6fba-4fcf-9d55-7b8e7f157091\propertybag$ 

Opens key:

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

Opens key:

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

 $Opens~key: $HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001$ 

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}$ 

Opens key:

 $\label{local-equation} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}\property\bag$ 

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

options\857bd61a8241ac81385ee957d8137887.exe

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

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

 $\verb|migration\providers\tcpip6||$ 

Opens key:

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

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

Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

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

nt\currentversion\appcompatflags

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

Opens key:

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

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

Opens key: HKLM\software\microsoft\com3

HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}

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

settings\5.0\cache\history

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

settings\5.0\cache\history

Opens key:

b784-432e-a781-5a1130a75963}

HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4} Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-Opens kev:

b913c40c9cd4}\treatas

Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\progid

Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid

HKLM\software\wow6432node\policies\microsoft\system\dnsclient Opens kev:

Opens key: HKLM\software\policies\microsoft\system\dnsclient

Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprocserver32

Opens key:

b784-432e-a781-5a1130a75963}\propertybag

HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\inprochandler32

HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\inprochandler

HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\inprochandler

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

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

settings\5.0\cache\extensible cache\feedplat HKCU\software\microsoft\windows\currentversion\internet

Opens key:

settings\5.0\cache\extensible cache\iecompat HKCU\software\microsoft\windows\currentversion\internet Opens key:

settings\5.0\cache\extensible cache\ietld

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

settings\5.0\cache\extensible cache\privacie:

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_bufferbreaking\_818408

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

explorer\main\featurecontrol\feature\_bufferbreaking\_818408 HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954

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

explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954 Opens key: HKLM\system\currentcontrolset\control\samservicelist

Opens key:

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache

Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ 

settings\5.0\cache

HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev:

settings\5.0\cache

HKCU\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289

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

explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149 HKLM\software\wow6432node\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature use cname for spn kb911149 HKCU\software\microsoft\internet

Opens key: explorer\main\featurecontrol\feature\_disable\_notify\_unverified\_spn\_kb2385266 Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature\_disable\_notify\_unverified\_spn\_kb2385266

Opens kev: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_compat\_use\_connection\_based\_negotiate\_auth\_kb2151543

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

explorer\main\featurecontrol\feature\_compat\_use\_connection\_based\_negotiate\_auth\_kb2151543

Opens key: HKCU\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names| \\$ 

```
HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens kev:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens kev:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                        HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                        HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                        HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                        HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                        HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                        HKCU\software\microsoft\windows\currentversion\internet settings\wpad
 Opens kev:
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                       HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                        HKLM\system\currentcontrolset\services\dns
                        HKLM\software\wow6432node\policies\microsoft\windows
 Opens kev:
nt\dnsclient\dnspolicyconfig
                        HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
 Opens kev:
 Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
 Opens key:
                        HKU\
                        HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens key:
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
 Opens key:
                        HKLM\software\wow6432node\microsoft\rpc\securityservice
 Opens key:
                        HKLM\software\microsoft\rpc\securityservice
 Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
 Opens key:
806e6f6e6963}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
 Opens key:
65fee5bae0b1}
 Opens key:
                        HKLM\system\currentcontrolset\services\tcpip\linkage
 Opens key:
                        HKLM\software\wow6432node\microsoft\rpc\extensions
 Opens key:
                        HKLM\software\microsoft\rpc\extensions
 Opens key:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32
 Opens key:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs
 Opens key:
                        HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
 Opens key:
                        HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
                        HKLM\software\microsoft\sqmclient\windows\disabledsessions\
 Opens key:
 Opens key:
                        HKCU \setminus software \setminus classes \setminus appid \setminus 857bd61a8241ac81385ee957d8137887. exe
                        HKCR\appid\857bd61a8241ac81385ee957d8137887.exe
 Opens key:
 Opens key:
                        HKLM\system\currentcontrolset\control\lsa
```

Opens key: 00aa004b2e24} HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas Opens key: 00aa004b2e24}\progid  $HKCR\wow6432 node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\ \ progid$ Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens key: Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid Opens key: Opens key: 00aa004b2e24}\inprocserver32 HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-Opens kev: 00aa004b2e24}\inprocserver32 Opens key: 00aa004b2e24}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-Opens kev: 00aa004b2e24}\inprochandler Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas Opens key:  $\label{locality} HKCR\wow6432 node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\ treat as }$ Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32 HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-Opens key: 00c04fb68820}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-Opens key: 00c04fb68820}\inprochandler32 Opens key:  $HKCR\wow6432 node\clsid\{8bc3f05e-d86b-11d0-a075-$ 00c04fb68820}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler Opens key: provider Opens kev: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration Opens key: HKLM\software\policies\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography Opens key:  $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| cryptography \verb|\softload||$ Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-00000000046} HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046} Opens key: Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32 HKCR\wow6432node\interface\{00000134-0000-0000-c000-Opens key: 000000000046}\proxystubclsid32 Opens kev: HKLM\svstem\currentcontrolset\services\bfe Opens key: HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820} Opens key: HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{f309 \\ ad 18 - d86 \\ a-11 \\ d0-a075 - d86 \\ a-11 \\ a-11$ Opens key: 00c04fb68820}\proxystubclsid32 HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-Opens kev: 00c04fb68820}\proxystubclsid32 Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}

Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas

Opens key: HKCP\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas

Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid Opens key:  $HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid$ HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{7c857801-7381-11cf-884d-146844-14684404-146844-146844-14684-1468444-146844-14684-14684-14684-14684-14684-14684-14684-14684-14684-$ 00aa004b2e24}\progid HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7c857801-7381-11cf-884d-11cf-8$ 00aa004b2e24}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32 Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{7c857801 - 7381 - 11cf - 884d - 11cf - 884d - 11cf - 11cf$ 00aa004b2e24}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32 Opens kev:  $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7c857801-7381-11cf-884d-1464\} \\ + 11cf-884d-1464 \\ +$ 00aa004b2e24}\inprochandler Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler Opens key: HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} Opens kev: Opens key: HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32 HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-Opens key: 930efe48a887}\proxystubclsid32 HKLM\system\currentcontrolset\control\computername Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas Opens key:  $HKCR\wow6432 node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treat as$ HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\progid  $HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid$ Opens kev: HKCU\software\classes\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: Opens key:  $HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}$ Opens key: HKCU\software\classes\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprocserver32 HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprocserver32  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{674b6698 - ee92 - 11d0 - ad71 - ad71$ Opens key: 00c04fd8fdff}\inprochandler32 HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprochandler Opens key HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler HKLM\software\wow6432node\microsoft\wbem\cimom Opens kev: Opens key: HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} Opens key: HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{9556 \\ dc99-828 \\ c-11 \\ cf-a37 \\ e-11 \\ cf-a37 \\ e-12 \\ e-12$ Opens key: 00aa003240c7}\proxystubclsid32 Opens key: HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens key: ce99a996d9ea} HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\treatas  $HKCR \setminus wow6432 node \\ clsid \\ \{d68af00a-29cb-43fa-8504-ce99a996d9ea\} \\ \setminus treatas$ Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{d68af00a-29cb-43fa-8504-468af00a-29cb-436af00a-29$ ce99a996d9ea}\progid  $HKCR\wow6432 node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\$ Opens key: Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens key: ce99a996d9ea}\progid HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprocserver32

ce99a996d9ea}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-

Opens key:

HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-

```
ce99a996d9ea}\inprochandler32
                                                                    HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
    Opens key:
 ce99a996d9ea}\inprochandler
                                                                    HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
     Opens key:
ce99a996d9ea}\inprochandler
     Opens key:
                                                                    HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{027947e1 - d731 - 11ce - a357 - d731 - 
 00000000001}
                                                                    HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-00000000001}
     Opens key:
     Opens key:
                                                                    HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-
 00000000001}\proxystubclsid32
                                                                    HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
     Opens kev:
 000000000001}\proxystubclsid32
    Opens key:
                                                                    HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
 00104b703efd}
     Opens key:
                                                                    HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
     Opens key:
                                                                    HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\treatas
     Opens key:
                                                                    HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treat as
     Opens key:
                                                                    HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
 00104b703efd}\progid
     Opens key:
                                                                    HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
                                                                    HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
     Opens key:
                                                                    HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
     Opens kev:
     Opens key:
                                                                    HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
 00104b703efd}\progid
                                                                    HKCR\clsid{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
     Opens key:
     Opens key:
                                                                    00104b703efd}\inprocserver32
                                                                    HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
     Opens kev:
 00104b703efd}\inprocserver32
    Opens key:
                                                                    HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
 00104b703efd}\inprochandler32
                                                                    HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
     Opens key:
00104b703efd}\inprochandler32
                                                                    HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
     Opens key:
 00104b703efd}\inprochandler
                                                                    HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
    Opens kev:
 00104b703efd}\inprochandler
     Opens key:
                                                                    HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{1c1c45ee-4395-11d2-b60b-432 \\ node \setminus interface \setminus \{1c1c45ee-430b-432 \\ node \setminus \{1c1c45ee-430b-4
00104b703efd}
                                                                    HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
     Opens key:
     Opens key:
                                                                    HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32
                                                                   HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
     Opens key:
 00104b703efd}\proxystubclsid32
                                                                    HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-
     Opens key:
00104b703efd}
     Opens key:
                                                                    HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
     Opens key:
                                                                    HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32
                                                                    HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-
     Opens kev:
00104b703efd}\proxystubclsid32
     Opens key:
                                                                    HKLM\software\microsoft\windows defender
                                                                    \label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ netbt \+ linkage
     Opens key:
     Oueries value:
                                                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
 options[disableusermodecallbackfilter]
                                                                    HKLM\system\currentcontrolset\control\session
     Oueries value:
manager[cwdillegalindllsearch]
                                                                    HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
     Oueries value:
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
     Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} explicitly indows \end{tabular} if it is a parentenabled \end{tabular}
                                                                    HKLM\system\currentcontrolset\control\nls\customlocale[empty]
     Queries value:
     Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                                                                    HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
     Oueries value:
                                                                    HKLM\system\currentcontrolset\control\mui\uilanguages\en-
     Queries value:
us[alternatecodepage]
     Queries value:
                                                                    HKCU\control panel\desktop[preferreduilanguages]
                                                                    HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
     Oueries value:
     Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest] \ described by the side of the sid
                                                                    HKLM\system\currentcontrolset\control\nls\sorting\versions[]
     Oueries value:
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
```

HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles] Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[857bd61a8241ac81385ee957d8137887] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\windows[loadappinit\_dlls] Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]

Queries value:

HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c00aa00389b71}\proxystubclsid32[]

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

settings[disableimprovedzonecheck]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security\_hklm\_only]

Queries value: HKLM\system\currentcontrol\scustomlocale[en-us] Queries value: HKLM\system\currentcontrol\set\control\nls\extendedlocale[en-us]

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

Queries value:

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

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

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [name]$ 

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [description]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [relative path]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [parsing name]$ 

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [infotip]$ 

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[icon]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\eqref{folderdescriptions} and the second sec$ 

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]
Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\eqref{lem:hklmsoftware} and the substitution of the substitution of$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[roamable]$ 

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[stream]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\eqno(905e63b6-c1bf-494e-b29c-65b732d3d21a)[publishexpandedpath]} \\$ 

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[attributes]}$ 

Queries value:

 $\label{thm:local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\grays\gr$ 

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [initfolder \ handler]$ 

Queries value:

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version[program files dir]|$ 

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [name]$ 

Queries value:

```
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
```

a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-descriptions\} \\ folde$ a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]

a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]

Oueries value:

a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[num\_catalog\_entries] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000002[packedcatalogitem] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 00000000000003 \ [packed catalog item]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000005[packedcatalogitem] Queries 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\00000000007[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009[packedcatalogitem] Oueries value:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 [serial\_access\_num]$ 

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[addressfamily]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[storesserviceclassinfo]
  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]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ solves \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo] Queries 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\000000000003[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]
  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\00000000003[providerinfo]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 00000000000004 [library path] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
   Oueries 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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 0000000000004 [storesservice class info] \\ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog \catalog\_entries \namespace\_catalog \catalog\_entries \catalog \catalog\_entries \catalog \catalog\_entries \catalog \cat$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 \ [address family]
   Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 [supported name space]]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000005[storesserviceclassinfo]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus mame space\_catalog \\ \setminus catalog\_entries \setminus 0000000000005[provider info]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000006[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[addressfamily]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000006 [supported name space]]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace\_catalog \\ \  \setminus catalog\_entries \setminus 0000000000006[storesserviceclass info]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus ser
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
                                            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                                            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
   Oueries value:
                                             {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ winsock \verb|\ set up | \\
migration\providers\tcpip[winsock 2.0 provider id]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
   Queries value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[fromcachetimeout]
  Queries value:
                                             \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[secureprotocols]
  Queries value:
                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[secureprotocols]
                                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[certificaterevocation]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablepassport]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[idnenabled]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                                             HKLM\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablehttp1_1]
                                             HKCU\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[enablehttp1_1]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Oueries value:
                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
   Queries value:
                                             HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablenegotiate]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
   Queries value:
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                            HKLM\software\wow6432node\microsoft\internet
   Oueries value:
```

explorer\main\featurecontrol[feature\_clientauthcertfilter]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings[clientauthbuiltinui]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[syncmode5]

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value:

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache[signature]

HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache\content[peruseritem]

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value:

settings\5.0\cache\content[peruseritem]

Queries value:

33be-4251-ba85-6007caedcf9d}[category]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]

Queries value:

33be-4251-ba85-6007caedcf9d}[parentfolder]

Queries value:

33be-4251-ba85-6007caedcf9d}[description]

Queries value:

33be-4251-ba85-6007caedcf9d}[relativepath]

Queries value:

33be-4251-ba85-6007caedcf9d}[parsingname]

Oueries value:

33be-4251-ba85-6007caedcf9d}[infotip]

Queries value:

33be-4251-ba85-6007caedcf9d}[localizedname]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-16444, \ node \$ 33be-4251-ba85-6007caedcf9d}[icon]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (352481e8-16484) \ and \ microsoft \ windows \ current \ version \ (352481e8-16484) \ and \ microsoft \ windows \ current \ version \ (352481e8-16484) \ and \ microsoft \ windows \ (352481e8-16484) \ and \ microsoft \$ 33be-4251-ba85-6007caedcf9d}[security]

Oueries value:

33be-4251-ba85-6007caedcf9d}[streamresource]

Queries value:

 $HKLM \label{lem:hklm} White the software \label{lklm} White the$ 33be-4251-ba85-6007caedcf9d}[streamresourcetype]

Oueries value:

33be-4251-ba85-6007caedcf9d}[localredirectonly] Oueries value:

33be-4251-ba85-6007caedcf9d}[roamable]

Oueries value:

33be-4251-ba85-6007caedcf9d}[precreate]

Oueries value:

33be-4251-ba85-6007caedcf9d}[stream]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-16444, \ node \$ 33be-4251-ba85-6007caedcf9d}[publishexpandedpath]

Oueries value:

33be-4251-ba85-6007caedcf9d}[attributes]

Queries value:

 $HKLM \label{lem:hklm} White the software \label{lklm} White the$ 33be-4251-ba85-6007caedcf9d}[foldertypeid]

Oueries value:

33be-4251-ba85-6007caedcf9d}[initfolderhandler]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cache]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[category]

6fba-4fcf-9d55-7b8e7f157091}[name]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[parentfolder]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[description]

6fba-4fcf-9d55-7b8e7f157091}[relativepath]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[parsingname]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[infotip]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[localizedname]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-b2785-b27864, \ b27864, \ b$ 6fba-4fcf-9d55-7b8e7f157091}[security]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[streamresource]

Queries value:

 $\label{thm:local_thm} \begin{tabular}{ll} HKLM \end{tabular} Software \wow 6432 node \microsoft \windows \current version \end{tabular} explorer \folder descriptions \end{tabular} \end{tabular} Tb 32785 - Tb$ 6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[roamable]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}[precreate]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[stream]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}[attributes]

Queries value:

6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]

Oueries value:

6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]

HKCU\software\microsoft\windows\currentversion\explorer\user shell

Oueries value:

folders[local appdata]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]

Oueries value:

Queries value:

0e22-4760-9afe-ea3317b67173}[name]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]

0e22-4760-9afe-ea3317b67173}[description]

0e22-4760-9afe-ea3317b67173}[relativepath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]

0e22-4760-9afe-ea3317b67173}[infotip]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]

0e22-4760-9afe-ea3317b67173}[icon]

Queries value:

0e22-4760-9afe-ea3317b67173}[security]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream resource]$ 

Queries value

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [local redirectonly]$ 

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [precreate]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[stream]}$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [publish \ explorer]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [attributes]$ 

Queries value:

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

Queries value:

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

Queries value:  $HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]$ 

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[cacheprefix]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[cachelimit]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[peruseritem]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[peruseritem]

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [name]$ 

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe9-4171$ 

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\c$ 

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \[relative path]\]$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [localized name]$ 

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [security]$ 

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \ \ coe9-4171-908e-08a611b84ff6 \ [stream resource type]$ 

Queries value:

 $\label{localization} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{Coe9-4171-908e-08a611b84ff6} [local redirectonly]$ 

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[roamable]}$ 

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe9-41$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [publish \ expanded \ path]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[attributes]$ 

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{$\sim$ coe9-4171-908e-08a611b84ff6} \ \mbox{$\sim$ c$ 

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

folders[cookies]

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [authenticode enabled]$ 

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

migration\providers\tcpip6[winsock 2.0 provider id]

Oueries value:

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

Queries value: |KLM\svstem\c

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock [maxsock addrlength]$ 

Queries value:

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disablelocaloverride]

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$ 

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

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

folders[appdata]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[cacheprefix]

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

HKLM\software\microsoft\com3[com+enabled] Queries value:

HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings\5.0\cache\cookies[cachelimit]

HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache\history[peruseritem]

settings\5.0\cache\history[peruseritem]

Oueries value:

b784-432e-a781-5a1130a75963}[category]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{d9dc8a3b-der \ der \$ b784-432e-a781-5a1130a75963}[name]

HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid[] Oueries value:

b784-432e-a781-5a1130a75963}[parentfolder]

b784-432e-a781-5a1130a75963}[description]

b784-432e-a781-5a1130a75963}[relativepath]

b784-432e-a781-5a1130a75963}[parsingname]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[infotip]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d9dc8a3b-delta \} \\ description \setminus \{d9dc8ab-delta \} \\ descript$ b784-432e-a781-5a1130a75963}[localizedname]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[icon] Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[security]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[streamresource]

Oueries value:

b784-432e-a781-5a1130a75963}[streamresourcetype]

HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[] Queries value:

Oueries value: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprocserver32[inprocserver32]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-descriptions\} \ description \ explorer \ folder \ descriptions \ explorer \ folder \$ b784-432e-a781-5a1130a75963}[localredirectonly]

Queries value:

 $HKLM \label{lem:hklm} White the latest and the la$ b784-432e-a781-5a1130a75963}[roamable]

Oueries value:

b784-432e-a781-5a1130a75963}[precreate]

Oueries value:

b784-432e-a781-5a1130a75963}[stream]

Oueries value:

b784-432e-a781-5a1130a75963}[publishexpandedpath]

Oueries value:

b784-432e-a781-5a1130a75963}[attributes]

Oueries value:

```
b784-432e-a781-5a1130a75963}[foldertypeid]
  Oueries value:
b784-432e-a781-5a1130a75963}[initfolderhandler]
                            HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
  Oueries value:
b913c40c9cd4}\inprocserver32[]
  Queries value:
                            HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[threadingmodel]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
                            HKLM\software\microsoft\ole[maxsxshashcount]
  Oueries value:
  Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\history[cacheprefix]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\ietld[cachepath]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  Oueries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[displayscriptdownloadfailureui]
                            HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[mbcsservername]
  Oueries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
  Queries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
                            HKLM\svstem\currentcontrolset\control\samservicelist[samservicelist]
  Oueries value:
  Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[disableworkerthreadhibernation]
                            HKLM\software\wow6432node\microsoft\windows\currentyersion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
  Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
```

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ 

settings[disablereadrange]

Queries value:

```
settings[socketsendbufferlength]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketreceivebufferlength]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Queries value:
                         settings[maxconnectionsperserver]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                         settings\5.0\cache[scavengecachefilelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[httpdefaultexpirytimesecs]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirvtimesecs]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer \verb|\main| featurecontrol| feature_disable_unicode_handle_closing_callback[857bd61a8241ac81385ee957d8137887.exe]|
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablecachingofsslpages]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[leashlegacycookies]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendextracrlf]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[wpadsearchalldomains]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttptrace]
```

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[nocheckautodialoverride] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[dontusednsloadbalancing] Queries value: settings[dontusednsloadbalancing] Queries value: settings[sharecredswithwinhttp] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[mimeexclusionlistforcache]  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings[headerexclusionlistforcache] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[dnscacheenabled] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[dnscacheentries]  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings[dnscachetimeout] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[warnonpost] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[warnalwaysonpost] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[warnonzonecrossing] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[warnonbadcertrecving] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpostredirect] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[alwaysdrainonredirect] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[warnonhttpstohttpredirect] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[tcpautotuning] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\wpad[wpadoverride] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[enableautodial] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[nonetautodial] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[globaluseroffline] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[badproxyexpirestime] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[disablebranchcache] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [domain named evolution level]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]$ Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[allowungualifiedguerv] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: 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: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns secure name query fall back]$ 

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]$ HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: Queries value: HKLM\svstem\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[registrationoverwrite] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: 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] HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Queries value:  $\label{lem:hklm} \verb+Kklm \system \current control set \services \dns cache \parameters [dnstest]$ 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: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts] Queries 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] Queries value: e1e01c1f69b5}[searchlist] Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxysettingsperuser] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[proxyenable] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyserver] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyoverride] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[autoconfigurl]  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings\connections[savedlegacysettings] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\connections[defaultconnectionsettings] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[enabledhcp] HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registrationenabled] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registeradaptername] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[domain] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpdomain] Queries value: e1e01c1f69b5}[dhcpv6domain] HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[nameserver] Oueries value: e1e01c1f69b5}[nameserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpnameserver] Oueries value:  $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee342-7039-11de-9d20-11de-9$ 806e6f6e6963}[enabledhcp] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername] 806e6f6e6963}[domain] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain] 806e6f6e6963}[nameserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[queryadaptername]

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

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-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}[disableadapterdomainname]

Queries value:

e1e01c1f69b5}[registrationmaxaddresscount]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-

```
e1e01c1f69b5}[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enablemulticast]
 Oueries value:
806e6f6e6963}[queryadaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disableadapterdomainname]
 Oueries value:
806e6f6e6963}[disabledynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enableadapterdomainnameregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationmaxaddresscount]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enablemulticast]
                         HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Queries value:
                         HKLM\software\microsoft\rpc\extensions[ndroleextdll]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
 Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enablefiletracing]
 Queries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385ee 957d8137887\_rasapi 32[file tracing mask]
 Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac81385ee 957d8137887\_rasapi 32 [enable consolet racing]
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[consoletracingmask]
 Oueries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[maxfilesize]
 Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac81385ee 957d8137887\_rasapi 32[filedirectory]
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[enablefiletracing]
 Queries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385ee 957d8137887\_rasmancs[filetracing mask]
 Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac81385ee 957d8137887\_ras mancs \ [enable consolet racing]
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[consoletracingmask]
 Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[maxfilesize]
 Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac81385ee 957d8137887\_rasmancs [filedirectory]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
 Queries value:
                         HKLM\software\microsoft\sqmclient\windows\disabledprocesses[fbac773d]
 Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
 Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
                         HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
 Queries value:
 Oueries value:
                         HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
                         HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
 Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
 Oueries value:
00aa004b2e24}\inprocserver32[]
                         HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
 Queries value:
00aa004b2e24}\inprocserver32[threadingmodel]
 Queries value:
                         HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| wbem \verb|\cimom[logging directory]|
                         HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
 Oueries value:
 Queries value:
                         HKLM\software\wow6432node\microsoft\wbem\cimom[log file max size]
                         HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
 Oueries value:
 Oueries 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]
                         Oueries value:
manager[safeprocesssearchmode]
 Queries value:
                         HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
                         HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
 Oueries value:
```

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

Queries value:

```
Oueries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Oueries value:
                                     HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                                     HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
                                     HKCR\wow6432node\interface\{00000134-0000-0000-c000-
  Oueries value:
00000000046}\proxystubclsid32[]
  Queries value:
                                     HKLM\software\microsoft\rpc\extensions[remoterpcdll]
                                     HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Oueries value:
  Oueries value:
                                     HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32[]
                                     HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
  Oueries value:
  Queries value:
                                     HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[]
  Queries value:
                                     HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
                                     HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
  Queries value:
930efe48a887}\proxystubclsid32[]
  Oueries value:
                                     HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[]
  Queries value:
                                     HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
  Oueries value:
00c04fd8fdff}\inprocserver32[]
                                    HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
  Queries value:
00c04fd8fdff}\inprocserver32[threadingmodel]
                                     HKLM\software\wow6432node\microsoft\wbem\cimom[processid]
  Queries value:
  Queries value:
                                     HKLM\software\wow6432node\microsoft\wbem\cimom[enableprivateobjectheap]
  Oueries value:
                                     HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\wbem\cimom[identifierlimit]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\customlocale[en]
                                     HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Queries value:
  Queries value:
                                     HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32[]
                                     HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
  Queries value:
                                     HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
  Oueries value:
ce99a996d9ea}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
  Queries value:
ce99a996d9ea}\inprocserver32[]
                                     HKCR\wow6432 node\clsid\{d68af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-43fa-8504-468af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb-436af00a-29cb
  Queries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
                                     HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
  Oueries value:
000000000001}\proxystubclsid32[]
                                     HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
  Oueries value:
                                     HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
  Queries value:
00104b703efd}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[]
  Queries value:
                                     HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
                                     HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
  Oueries value:
00104b703efd}\proxystubclsid32[]
  Queries value:
                                    HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32[]
  Queries value:
                                    HKLM\software\microsoft\windows defender[disableantispyware]
  Queries value:
                                     HKLM\system\currentcontrolset\services\netbt\linkage[export]
  Sets/Creates value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enablefiletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enableconsoletracing]
  Sets/Creates value:
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac81385ee 957d8137887\_rasapi 32[file tracing mask]
  Sets/Creates value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385 ee 957d8137887\_rasapi 32[consoletracing mask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[maxfilesize]
  Sets/Creates value:
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac81385ee 957d8137887\_rasapi 32 [filedirectory]
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857 bd 61a8241 ac 81385 ee 957 d8137887\_rasmancs [enable file tracing]
  Sets/Creates value:
Sets/Creates value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857 bd 61a8241ac81385 ee 957 d8137887\_rasmancs [file tracing mask]
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[consoletracingmask]
  Sets/Creates value:
HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus 857bd61a8241ac81385ee957d8137887\_rasmancs [maxfilesize]
  Sets/Creates value:
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac81385ee 957d8137887\_rasmancs \ [filedirectory]
```

Value changes: HKLM\software\microsoft\rpc[uuidsequencenumber]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\connections[defaultconnectionsettings]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyenable]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\connections[savedlegacysettings]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]