Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3314, Task ID: 765

Task ID: 765 Risk Level: 10

Date Processed: 2016-05-18 10:35:42 (UTC)

Processing Time: 61.78 seconds
Virtual Environment: IntelliVM

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

Sample ID: 3314
Type: basic
Owner: admin

Label: 857bd61a8241ac81385ee957d8137887

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

File Type: PE32:win32:gui File Size: 184832 bytes

MD5: 857bd61a8241ac81385ee957d8137887

SHA256: efed61ac534b30cf6837dea448b72c43ec008f31273c445440a934aa5246ba2f

Description: None

Pattern Matching Results

5 PE: Contains compressed section

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"]

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

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

Files\LP\1144\027.exe%C:\Program Files\LP\1144]

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

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

startC:\Users\Admin\AppData\Roaming\40CB9\DFC11.exe%C:\Users\Admin\AppData\Roaming\40CB9]

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\{0ECE180F-6E9E-4FA6-A154-6876D9DB8906}
Creates mutex:	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_
Creates mutex:	-

 $\label{local:microsoft:windows:temporary internet} $$ \space{-0.05\textwindows:temporary internet files:content.ie5:} $$ is $$ $$ $$ is $$ is $$ is $$ is $$ is $$ is $$ is $$ is $$ $$ is $$ $$ is $$ is $$ is $$ is $$ $$ is $$ $$ is $$ is $$ $$ is $$ $$ is $$ is $$ is $$ $$ i$

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!

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

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

Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED

Creates event: \BaseNamedObjects\BFE_Notify_Event_{a8167df2-f56a-457b-b3f6-

28b793eeb458}

Creates event: \KernelObjects\MaximumCommitCondition

File System Events

Creates: C:\Program Files
Creates: C:\Program Files\B95C1

Creates: C:\Users\Admin\AppData\Roaming
Creates: C:\Users\Admin\AppData\Roaming\40CB9

Creates: C:\Program Files\LP
Creates: C:\Program Files\LP\1144

Creates: C:\Users\Admin\AppData\Roaming\40CB9\95C1.0CB

Creates: C:\Users\Admin

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

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

```
C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Creates:
                         C:\Windows\Prefetch\857BD61A8241AC81385EE957D8137-5577336B.pf
 Opens:
 Opens:
                         C:\Windows\System32
 Opens:
                         C:\windows\temp\oleacc.dll
 Opens:
                         C:\Windows\System32\oleacc.dll
                         C:\windows\temp\MSIMG32.DLL
 Opens:
 Opens:
                         C:\Windows\System32\msimg32.dll
 Opens:
                         C:\Windows\System32\imm32.dll
 Opens:
                         C:\windows\temp\OLEACCRC.DLL
 Opens:
                         C:\Windows\System32\oleaccrc.dll
 Opens:
                         C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                         C:\windows\temp\A#â,,\cuVirtualProtect.DLL
 Opens:
                         C:\Windows\system32\A#â,,¢uVirtualProtect.DLL
 Opens:
                         C:\Windows\system\A#â,,\cuVirtualProtect.DLL
 Opens:
                         C:\Windows\A#â,,¢uVirtualProtect.DLL
 Opens:
                         C:\Windows\Svstem32\Wbem\A#â..¢uVirtualProtect.DLL
 Opens:
                         C:\Windows\System32\WindowsPowerShell\v1.0\A#â,,¢uVirtualProtect.DLL
 Opens:
                         C:\windows\temp\apphelp.dll
 Opens:
                         C:\Windows\System32\apphelp.dll
 Opens:
                         C:\Windows\System32\sechost.dll
 Opens:
                         C:\windows\temp\RASAPI32.dll
 Opens:
                         C:\Windows\System32\rasapi32.dll
 Opens:
                         C:\windows\temp\rasman.dll
 Opens:
                         C:\Windows\System32\rasman.dll
 Opens:
                         C:\windows\temp\WINHTTP.dll
 Opens:
                         C:\Windows\System32\winhttp.dll
 Opens:
                         C:\windows\temp\webio.dll
 Opens:
                         C:\Windows\System32\webio.dll
 Opens:
                         C:\
 Opens:
                         C:\Program Files
                         C:\Program Files\B95C1
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\40CB9
 Opens:
                         C:\Users\Admin\AppData\Roaming\40CB9\95C1.0CB
 Opens:
                         C:\Windows\System32\mswsock.dll
 Opens:
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
                         C:\Windows\System32\wship6.dll
 Opens:
                         C:\windows\temp\DNSAPI.dll
 Opens:
                         C:\Windows\System32\dnsapi.dll
 Opens:
                         C:\windows\temp\IPHLPAPI.DLL
                         C:\Windows\System32\IPHLPAPI.DLL
 Opens:
 Opens:
                         C:\windows\temp\WINNSI.DLL
 Opens:
                         C:\Windows\System32\winnsi.dll
                         C:\Program Files\LP\1144
 Opens:
 Opens:
                         C:\Windows\Temp
                         C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe
 Opens:
 Opens:
                         C:\windows\temp\dhcpcsvc6.DLL
 Opens:
                         C:\Windows\System32\dhcpcsvc6.dll
                         C:\Windows\System32\wininet.dll
 Opens:
                         C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe.Local\
 Opens:
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls 6595b64144ccf1df 6.0.7601.17514 none 41e6975e2bd6f2b2
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
 Opens:
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         C:\windows\temp\dhcpcsvc.DLL
 Opens:
                         C:\Windows\System32\dhcpcsvc.dll
                         C:\windows\temp\SspiCli.dll
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
 Opens:
                         C:\windows\temp\profapi.dll
 Opens:
                         C:\Windows\System32\profapi.dll
 Opens:
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 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
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
 Opens:
                         C:\windows\temp\rasadhlp.dll
 Opens:
                         C:\Windows\System32\rasadhlp.dll
                         C:\Windows\System32\drivers\etc\hosts
 Opens:
 Opens:
                         C:\windows\temp\CRYPTBASE.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
                         C:\Users\Admin\AppData\Roaming
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens:
C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini|
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
```

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies

Creates:

```
Files\Content.IE5\index.dat
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
 Opens:
                         C:\Windows\System32\FWPUCLNT.DLL
 Opens:
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
 Opens:
                         C:\Users\Admin\AppData\Roaming\Cloud AV 2012\ahst.lni
 Opens:
                         C:\Windows\System32\rpcss.dll
 Opens:
                         C:\Windows\System32\uxtheme.dll
 Opens:
                         C:\Windows\System32\FirewallAPI.dll
 Opens:
                         C:\Windows\System32\version.dll
 Opens:
                         C:\windows\temp\ntmarta.dll
 Opens:
                         C:\Windows\System32\ntmarta.dll
 Opens:
                         C:\Windows\System32\wbem\wbemprox.dll
 Opens:
                         C:\Windows\system32\wbem\wbemcomn.dll
                         C:\Windows\System32\wbemcomn.dll
 Opens:
 Opens:
                         C:\Windows\System32\wbem\Logs
 Opens:
                         C:\windows\temp\CRYPTSP.dll
 Opens:
                         C:\Windows\System32\cryptsp.dll
 Opens:
                         C:\Windows\System32\rsaenh.dll
                         C:\windows\temp\RpcRtRemote.dll
 Opens:
 Opens:
                         C:\Windows\System32\RpcRtRemote.dll
 Opens:
                         C:\windows\temp\rtutils.dll
 Opens:
                         C:\Windows\System32\rtutils.dll
 Opens:
                         C:\ProgramData\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\Windows\System32\ras
                         C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
 Opens:
 Opens:
                         C:\windows\temp\sensapi.dll
 Opens:
                         C:\Windows\System32\SensApi.dll
                         C:\Program
 Opens:
 Opens:
                         C:\Program.exe
 Opens:
                         C:\Program Files\LP\1144\027.exe
 Opens:
                         C:\Program Files\LP\1144\027.exe.exe
 Opens:
                         C:\Windows\System32\wbem\wbemsvc.dll
 Opens:
                         C:\Windows\System32\wbem\fastprox.dll
                         C:\Windows\system32\wbem\NTDSAPI.dll
 Opens:
 Opens:
                         C:\Windows\System32\ntdsapi.dll
 Opens:
                         C:\Users\Admin\AppData\Roaming\Mozilla\
                         C:\Users\Admin\AppData\Roaming\Opera\
 Opens:
 Opens:
                         C:\Windows\System32\nlaapi.dll
                         C:\Windows\System32\NapiNSP.dll
 Opens:
 Opens:
                         C:\Windows\System32\pnrpnsp.dll
 Opens:
                         C:\Windows\System32\winrnr.dll
 Opens:
                         C:\Users\Admin\AppData\Roaming\40CB9\DFC11.exe
                         C:\Users\Admin\AppData\Roaming\40CB9\DFC11.exe.exe
 Opens:
 Writes to:
                         C:\Users\Admin\AppData\Roaming\40CB9\95C1.0CB
 Reads from:
                         C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe
 Reads from:
                         C:\Windows\System32\drivers\etc\hosts
```

Network Events		
DNS query:	jointhenewworldorder.com	_
DNS query:	v67.dudlik-munik.com	
DNS query:	1fx7.dudlik-munik.com	
DNS query:	ocsp.verisign.com	
DNS query:	xprstats.com	
DNS query:	www.google.com	
DNS query:	alleducationalsoftware.com	
DNS query:	tzky6yv.kupinosis.com	
DNS query:	binghamtonschools.org	
DNS response:	jointhenewworldorder.com ⇒ 208.73.211.70	
DNS response:	v67.dudlik-munik.com ⇒ 173.230.133.99	
DNS response:	1fx7.dudlik-munik.com ⇒ 173.230.133.99	
DNS response:	e8218.dscb1.akamaiedge.net \Rightarrow 23.15.155.27	
DNS response:	www.google.com \Rightarrow 58.26.8.109	
DNS response:	www.google.com \Rightarrow 58.26.8.99	
DNS response:	www.google.com \Rightarrow 58.26.8.89	
DNS response:	www.google.com \Rightarrow 58.26.8.94	
DNS response:	www.google.com \Rightarrow 58.26.8.103	
DNS response:	www.google.com \Rightarrow 58.26.8.98	
DNS response:	www.google.com \Rightarrow 58.26.8.108	
DNS response:	www.google.com \Rightarrow 58.26.8.113	
DNS response:	www.google.com \Rightarrow 58.26.8.84	
DNS response:	www.google.com ⇒ 58.26.8.93	
DNS response:	www.google.com \Rightarrow 58.26.8.119	
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:	alleducationalsoftware.com ⇒ 66.218.72.112	
DNS response:	alleducationalsoftware.com ⇒ 98.136.241.156	
DNS response:	binghamtonschools.org ⇒ 174.129.25.170	
Connects to:	208.73.211.70:80	

 Connects to:
 173.230.133.99:80

 Connects to:
 23.15.155.27:80

 Connects to:
 58.26.8.109:80

 Connects to:
 66.218.72.112:80

 Connects to:
 174.129.25.170:80

 Sends data to:
 8.8.8.8:53

 Sends data to:
 jointhenewworldorder.com:80 (208.73.211.70)

 Sends data to:
 1fx7.dudlik-munik.com:80 (173.230.133.99)

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

 Sends data to:
 127.0.0.1:49163

 Sends data to:
 127.0.0.1:49165

 Sends data to:
 127.0.0.1:49168

 Sends data to:
 127.0.0.1:49170

 Sends data to:
 127.0.0.1:49172

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

Sends data to: alleducationalsoftware.com:80 (66.218.72.112)
Sends data to: binghamtonschools.org:80 (174.129.25.170)

Receives data from: 8.8.8.8:53

Receives data from: jointhenewworldorder.com:80 (208.73.211.70)

Receives data from: 127.0.0.1:49163

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

 Receives data from:
 127.0.0.1:49165

 Receives data from:
 127.0.0.1:49168

 Receives data from:
 127.0.0.1:49170

 Receives data from:
 127.0.0.1:49172

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

Receives data from: alleducationalsoftware.com:80 (66.218.72.112)
Receives data from: binghamtonschools.org:80 (174.129.25.170)

Windows Registry Events

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

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

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

settings\connections

Creates key: HKLM\software\microsoft\wbem\cimom HKLM\software\microsoft\tracing

Creates key: HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32

Creates key:

 $HKLM \backslash software \backslash microsoft \backslash tracing \backslash 857bd61a8241ac81385ee957d8137887_rasmancs$

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

 $\label{lem:continuous} Opens \ key: $$ HKLM\software\policies\microsoft\windows\safer\codeidentifiers $$ Opens \ key: $$ HKCU\software\policies\microsoft\windows\safer\codeidentifiers $$ Opens \ key: $$ O$

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\

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

Opens key: HKLM\software\microsoft\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKCU\software\classes\

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

00aa00389b71}\proxystubclsid32

Opens key: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32

Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash windows\ nt \backslash current version \backslash diagnostics}$

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

 $\label{lem:constant} \mbox{ Opens key:} & \mbox{ HKLM\software\mbox{\mbox{microsoft\windows\currentversion\internet }} \\ \mbox{ Opens key:} & \mbox{ HKLM\software\policies\mbox{\mbox{\mbox{microsoft\windows\currentversion\internet}}} \\ \mbox{ } \mbox{$

settings

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

Opens key: HKLM\software\microsoft\rpc

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

Opens key: HKLM\svstem\setup

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

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

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions

Opens key:

b29c-65b732d3d21a}

Opens kev:

b29c-65b732d3d21a}\propertybag

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

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings

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

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1b6cd5d7

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev:

Opens kev:

Opens key:

Opens key:

Opens kev:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000012 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000013 Opens key:

Opens kev:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000016 Opens key:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ (catalog_entries \ 0000000000017) \ (catalog_entries \ (catalog \ (catalog_entries \ (catalog \ (cata$ Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000

Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006

Opens key: $\label{lem:hklm} \verb+Kklm \system \current control set \services \swinsock \space{2mm} parameters$ HKLM\svstem\currentcontrolset\services\tcpip6\parameters\winsock Opens kev: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers

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

migration\providers\psched

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

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

migration\providers\tcpip

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

migration\providers\tcpip6

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

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

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

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

Opens key:

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

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:

c19ce8a73253}

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\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKLM\software\microsoft\windows

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

options Opens key:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus side by side \setminus assembly storage roots$

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

settings

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

Opens key: HKLM\software\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software

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

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

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-

c19ce8a73253}

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\microsoft\internet explorer\main\featurecontrol

Opens key: $\label{lem:hklmsoftwaremicrosoftwindows\currentversion\internet} \begin{tabular}{ll} HKLM\software\microsoft\windows\currentversion\label{lem:hklmsoftware} \\ \end{tabular}$

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

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

settings\5.0\cache\content

Opens key:

 $HKLM \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{352481e8-33be-4251-4681e8-4681e8$

ba85-6007caedcf9d}

Opens key:

 $ba85-6007 caedcf9d \} \verb|\property| bag$

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

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

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follows folders$

 $Opens\ key: \\ \hspace{1.5cm} \text{HKCU} software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\user| shell \\$

folders

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

Opens key:

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

Opens key:

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

Opens key:

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

Opens key:

```
HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '5e6c858f-0e22-4760-1000' \ 'explorer' \ 'folder \ 'folder
9afe-ea3317b67173}\propertybag
       Opens key:
                                                                                                   HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus profile list \setminus s-1-5-21-1 = (a. 1) + (b. 1) + 
2160590473-689474908-1361669368-1002
      Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
 806e6f6e6963}
       Opens kev:
1709a0196aed}
       Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
       Opens kev:
                                                                                                   HKLM\svstem\currentcontrolset\services\tcpip\linkage
       Opens key:
                                                                                                   HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\cookies
                                                                                                  HKLM\software\microsoft\windows\currentversion\internet
      Opens key:
 settings\5.0\cache\cookies
       Opens key:
908e-08a611b84ff6}
      Opens key:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-b046464, b046464, b04646, b04
908e-08a611b84ff6}\propertybag
       Opens key:
a03a-e3ef65729f3d}
      Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
      Opens key:
                                                                                                   HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\history
                                                                                                   HKLM\software\microsoft\windows\currentversion\internet
       Opens key:
 settings\5.0\cache\history
      Opens key:
HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\{d9dc8a3b-b784-432e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d742e-d
a781-5a1130a75963}
       Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}\propertybag
                                                                                                   \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}.
      Opens key:
 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
      Opens key:
                                                                                                  HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\iecompat
                                                                                                  HKCU\software\microsoft\windows\currentversion\internet
      Opens kev:
 settings\5.0\cache\extensible cache\ietld
      Opens key:
                                                                                                  HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\privacie:
       Opens key:
                                                                                                  HKCU\software\microsoft\internet
```

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

Opens key: HKLM\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\retry_header on ly post_on connection reset|\\$

Opens key: HKLM\software\microsoft\com3

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

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

b913c40c9cd4}\treatas

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

b913c40c9cd4}\progid

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954 Opens key: HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprocserver32

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32 Opens kev:

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

b913c40c9cd4}\inprochandler32

HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32 Opens key:

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

```
b913c40c9cd4}\inprochandler
                          HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
 Opens kev:
 Opens key:
                          HKLM\software\microsoft\rpc\securityservice
 Opens key:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\5.0\cache
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                          HKLM\software\microsoft\internet
 Opens key:
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\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                          HKLM\software\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\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                          HKLM\software\microsoft\internet
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\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens key:
                         HKLM\system\currentcontrolset\control\lsa\accessproviders
 Opens key:
                          HKLM\system\currentcontrolset\services\ldap
 Opens key:
                          HKCU\software\microsoft\windows\currentversion\internet settings\wpad
                          HKLM\software\microsoft\rpc\extensions
 Opens key:
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                          HKU\
 Opens kev:
                          HKCU\software\classes\appid\857bd61a8241ac81385ee957d8137887.exe
 Opens key:
 Opens key:
                          HKCR\appid\857bd61a8241ac81385ee957d8137887.exe
 Opens key:
                          HKLM\system\currentcontrolset\control\lsa
                          HKCU \setminus software \setminus classes \setminus clsid \setminus \{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}\treatas
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\progid
 Opens key:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid
                          HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
 Opens key:
00aa004b2e24}\inprocserver32
```

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler32

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler

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

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\treatas

00c04fb68820}\progid

 $\label{lem:continuous} Opens~key: $$ HKCR\clsid_{8bc3f05e-d86b-11d0-a075-00c04fb68820}\right.$$ Opens~key: $$ HKCU_software\classes\clsid_{8bc3f05e-d86b-11d0-a075-}$$$

00c04fb68820}\inprocserver32

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler32

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler

 $Opens\ key: \\ HKLM\software\microsoft\cryptography\defaults\provider\microsoft\ strong$

cryptographic provider

Opens key: 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\software\microsoft\cryptography\offload

Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-00000000046}

Opens key: HKCR\interface\{00000134-0000-0000-000000000046} Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-

00000000046}\proxystubclsid32

Opens key: HKCR\interface\{00000134-0000-0000-000000000046}\proxystubclsid32

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

HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\

Opens key:

HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs

Opens key: HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}

Opens key: $\begin{tabular}{ll} HKCR\interface \{f309ad18-d86a-11d0-a075-00c04fb68820\} \\ Opens key: \\ HKCU\software \classes \interface \{f309ad18-d86a-11d0-a075-00c04fb68820\} \\ \end{tabular}$

00c04fb68820}\proxystubclsid32

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

00aa004b2e24}\treatas

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

00aa004b2e24}\progid

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

00aa004b2e24}\inprocserver32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprochandler32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprochandler

 $\label{thm:continuous} Opens \ key: \ HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\ inprochandler \\ Opens \ key: \ HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\$

Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
Opens key: HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-

930efe48a887}\proxystubclsid32

Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32

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

Opens key: HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}

 $\label{lem:opensky:opensky: HKCR\interface §9556dc99-828c-11cf-a37e-00aa003240c7} \\ Opensky: HKCU\software \classes \interface §9556dc99-828c-11cf-a37e-00aa003240c7 \\ \\ Opensky: HKCU \software \classes \interface §9556dc99-828c-11cf-a37e-00aa003240c7 \\ \\ Opensky: HKCU \software \classes \$

00aa003240c7}\proxystubclsid32

 $\label{lem:continuous} Opens \ key: \ HKCR \ interface \ \{9556dc99-828c-11cf-a37e-00aa003240c7\} \ proxystubclsid32 \ Opens \ key: \ HKCU \ software \ classes \ clsid \ \{d68af00a-29cb-43fa-8504-ce99a996d9ea\} \$

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR\clsid\d68af00a-29cb-43fa-8504-ce99a996d9ea\} \\ Opens key: \\ HKCU\software\classes\clsid\d68af00a-29cb-43fa-8504-\\ \end{tabular}$

ce99a996d9ea}\treatas

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

ce99a996d9ea}\progid

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

ce99a996d9ea}\inprocserver32

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandler32

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandler

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler

Opens key: HKLM\software\microsoft\wbem\cimom

Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-000000000001}

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\
Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-

000000000001}\proxystubclsid32

Opens key: $\begin{tabular}{ll} HKCR\interface\{0.27947e1-d731-11ce-a357-00000000001\}\proxystubclsid32\\ Opens key: \\ HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd} \end{tabular}$

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\treatas

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\progid

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler
Opens key: HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}

 Opens key:
 HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}

 Opens key:
 HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}

00104b703efd}\proxystubclsid32

Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-00104b703efd}

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32

Opens key: HKLM\software\microsoft\windows defender

Opens key: HKLM\system\currentcontrolset\services\netbt\linkage Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value: HKLM\system\currentcontrol\set\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrol\set\control\terminal server[tsuserenabled]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

Queries value: HKCU\control panel\desktop[preferreduilanguages]

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

Queries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrol\set\control\nls\sorting\versions[]

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

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

nt\currentversion\compatibility32[857bd61a8241ac81385ee957d8137887]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

Queries value: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]

Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]

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

settings[disableimprovedzonecheck]

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

settings[security_hklm_only]

Queries value: HKLM\system\currentcontrol\s\customlocale[en-us]
Queries value: HKLM\system\currentcontrol\s\extendedlocale[en-us]

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

Queries value:

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

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

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

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494eb29c-65b732d3d21a}[category] Queries value: b29c-65b732d3d21a}[name] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494eb29c-65b732d3d21a}[parentfolder] Queries value: b29c-65b732d3d21a}[description] Queries value: b29c-65b732d3d21a}[relativepath] Queries value: b29c-65b732d3d21a}[parsingname] Queries value: b29c-65b732d3d21a}[infotip] b29c-65b732d3d21a}[localizedname] b29c-65b732d3d21a}[icon] Queries value: b29c-65b732d3d21a}[security] $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-d14bf$ b29c-65b732d3d21a}[streamresource] b29c-65b732d3d21a}[streamresourcetype] $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-c1bf-494e-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-c1bf-494e-microsoft \setminus explorer \setminus explore$ b29c-65b732d3d21a}[localredirectonly] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494eb29c-65b732d3d21a}[roamable] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494eb29c-65b732d3d21a}[precreate] Oueries value: b29c-65b732d3d21a}[stream] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494eb29c-65b732d3d21a}[publishexpandedpath] Oueries value: b29c-65b732d3d21a}[attributes] Queries value: $HKLM \ software \ microsoft \ windows \ current version \ (software) \ folder descriptions \ (software) \ descriptions \ de$ b29c-65b732d3d21a}[foldertypeid] Oueries value: b29c-65b732d3d21a}[initfolderhandler] Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num] Queries value: Queries value:

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 000000000001 \ [packed catalog item]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem] Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem] Queries value:

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \noon 00000000017 \[packed catalog item] \queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000001 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000003 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ name space_catalog5 \ catalog_entries \ 000000000004 \ [library path]$

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\00000000004[providerid] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000004 \ [address family]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000004 [supported name space]]$ Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ no mespace_catalog \ set alog_entries \ (0000000000004 \ [version]) \ details \$ Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 10000000000004 \ [storesservice class in fo]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerinfo] Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries \ 0000000000005 \ [displaystring]$ Queries value:

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

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space _ catalog 5 \ (catalog_entries \ 0000000000005 [supported name space]$ Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ set alog_entries \ (0000000000005[provider info]) \ (provider \ name space_catalog \ name space_cata$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ (catalog_entries \ 000000000006[library path])$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006[providerid] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 \ [address family]$ Oueries value:

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

Oueries value:

Oueries value:

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

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

Oueries value:

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

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

Oueries value:

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

HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping] Oueries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\psched[winsock 2.0 provider id]

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

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

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

Queries value:

HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]

Queries value:

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

Oueries value:

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

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

migration\providers\tcpip6[winsock 2.0 provider id]

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname] HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns secure name query fall back]$ HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Queries value: $\label{lem:hklm} \verb+Kklm/system/currentcontrolset/services/dnscache/parameters[direct access query order]+ \\$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [queryipm atching]$ Queries 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] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [updates ecurity level]$ Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Queries value:
Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Oueries 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]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Oueries value:
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]
 Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
 Queries value:
                         \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options[disablelocaloverride]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
                         HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
 Oueries value:
a3fe-553973d0b723]
 Queries value:
                         HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce41
 Queries value:
                         \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[fromcachetimeout]
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[certificaterevocation]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablekeepalive]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[idnenabled]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[cachemode]
 Queries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
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\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
 Queries value:
                         \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
```

```
settings[proxyhttp1.1]
              HKCU\software\policies\microsoft\windows\currentversion\internet
Oueries value:
settings[proxyhttp1.1]
Queries value:
              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value:
              HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
              HKCU\software\microsoft\windows\currentversion\internet
Oueries value:
settings[disablebasicoverclearchannel]
              HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
              HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
              \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
Oueries value:
settings[clientauthbuiltinui]
              HKCU\software\microsoft\windows\currentversion\internet
Queries value:
settings[syncmode5]
              HKLM\software\microsoft\windows\currentversion\internet
 Queries 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\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
ba85-6007caedcf9d}[category]
 Oueries value:
ba85-6007caedcf9d}[name]
 Queries value:
ba85-6007caedcf9d}[parentfolder]
 Oueries value:
ba85-6007caedcf9d}[description]
 Oueries value:
ba85-6007caedcf9d}[relativepath]
 Queries value:
ba85-6007caedcf9d}[parsingname]
 Queries value:
ba85-6007caedcf9d}[infotip]
 Queries value:
ba85-6007caedcf9d}[localizedname]
 Queries value:
ba85-6007caedcf9d}[icon]
 Queries value:
ba85-6007caedcf9d}[security]
 Queries value:
ba85-6007caedcf9d}[streamresource]
 Oueries value:
ba85-6007caedcf9d}[streamresourcetype]
 Oueries value:
ba85-6007caedcf9d}[localredirectonlv]
 Oueries value:
ba85-6007caedcf9d}[roamable]
 Queries value:
ba85-6007caedcf9d}[precreate]
 Queries value:
ba85-6007caedcf9d}[stream]
 Queries value:
ba85-6007caedcf9d}[publishexpandedpath]
```

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 \ caedcf9d\} \ [folder type id]$

Queries value:

Queries value:

Oueries value:

ba85-6007caedcf9d}[attributes]

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

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

folders[cache]

Oueries value:

 $\label{thm:local-prop} $$HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}\[category\]$$$

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[name]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parent folder]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [description]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 157091 \end{figure} folder \descriptions \fill 157091 \end{fill} fold 157091$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parsing name]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 152785-6 fba-4 fcf-9 d55-7 b8e7 f157091 \fill 157091 \fill$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[localized name]$

Queries value:

Queries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ for the surrent version \ explorer \ folder descriptions \ factor \ for the surrent version \ explorer \ folder \ for the surrent version \ explorer \ folder \ for the surrent version \ explorer \ folder \ for the surrent version \ explorer \ folder \ for the surrent version \ explorer \ folder \ for the surrent version \ explorer \ folder \ for the surrent version \ explorer \ folder \ for the surrent version \ explorer \ folder \ for the surrent version \ explorer \ for the surrent \ for the surrent version \ explorer \ for the surrent \ for$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [stream resource type]$

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 152785-6 fba-4 fcf-9 d55-7 b8e7 f157091 \cite{thm:hklm} \end{substitute} full the lemma \cite{thm:hklm} \footnote{thm:hklm} \end{substitute} for the lemma \cite{thm:hklm} \footnote{thm:hklm} \footno$

Queries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [stream]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[publishexpandedpath]}$

Queries value:

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

Queries value:

 $\label{lem:hkk} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}\[foldertypeid]\]$

Oueries value:

 $HKLM \coftware \mbox{$

Queries value:

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

folders[local appdata]

Queries value:

 $\label{thm:local-continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \fol$

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[name]}$

Queries value:

 $\label{thm:local-prop} $$HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[parentfolder]$$

Oueries value:

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

Queries value:

 $\label{thm:local-prop} $HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\[relative\path]$

Queries value:

c19ce8a73253}[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[registeradaptername] Oueries value: c19ce8a73253}[domain] Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-

c19ce8a73253}[dhcpdomain]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[dhcpv6domain]

Oueries value:

9afe-ea3317b67173}[parsingname]

Oueries value:

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

Queries value:

9afe-ea3317b67173}[localizedname]

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{5e6c858f-0e22-4760-1640-16400-164$ 9afe-ea3317b67173}[security]

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{5e6c858f-0e22-4760-1640-16400-164$ 9afe-ea3317b67173}[streamresourcetype]

Oueries value:

9afe-ea3317b67173}[localredirectonly]

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{5e6c858f-0e22-4760-1640-16400-164$ 9afe-ea3317b67173}[roamable]

Oueries value:

9afe-ea3317b67173}[precreate]

Queries value:

c19ce8a73253}[nameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[nameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[dhcpnameserver]

Queries value:

9afe-ea3317b67173}[stream]

Queries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1200' \ descriptions \ 'folder \ 'fo$ 9afe-ea3317b67173}[attributes]

Oueries value:

9afe-ea3317b67173}[foldertypeid]

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1260 \ 'explorer' \ 'folder descriptions' \ 'folder de$ 9afe-ea3317b67173}[initfolderhandler]

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \end{tab$ Queries value: 2160590473-689474908-1361669368-1002[profileimagepath]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enabledhcp]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationenabled]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registeradaptername]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[domain]

Oueries value:

806e6f6e6963}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[nameserver] Oueries value: 806e6f6e6963}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[registrationmaxaddresscount] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[enablemulticast] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\content[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\content[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\cookies[peruseritem] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\cookies[peruseritem] Queries value: $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `ex$ 908e-08a611b84ff6}[category] Oueries value: 908e-08a611b84ff6}[name] Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `ex$ 908e-08a611b84ff6}[parentfolder]

Oueries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-d14746-d14864-d188644-d18864-d18864-d18864-d18864-d18864-d18864-d18864-d18864-d1886464-d18864-d18864-d188644-d188644-d1886464-d18864-d1886464-d1886464-d1886464-d1886464-d1886464-d1886464-d1886464-d1886464-d188646$ 908e-08a611b84ff6}[description]

Queries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `ex$ 908e-08a611b84ff6}[relativepath]

Oueries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-d14746-d14864-d188644-d18864-d18864-d18864-d18864-d18864-d18864-d18864-d18864-d1886464-d18864-d18864-d188644-d188644-d1886464-d18864-d1886464-d1886464-d1886464-d1886464-d1886464-d1886464-d1886464-d1886464-d188646$ 908e-08a611b84ff6}[parsingname]

Queries value:

908e-08a611b84ff6}[infotip]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[queryadaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disableadapterdomainname]

Oueries value:

806e6f6e6963}[disabledynamicupdate]

Oueries value:

806e6f6e6963}[enableadapterdomainnameregistration]

Oueries value:

806e6f6e6963}[registrationmaxaddresscount]

Oueries value:

806e6f6e6963}[maxnumberofaddressestoregister]

Queries value:

806e6f6e6963}[enablemulticast]

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

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `ex$

908e-08a611b84ff6}[security]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[stream resource]$

Queries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[stream resource type]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [local redirectonly]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[roamable]}$

Oueries value:

 $HKLM \software \microsoft \windows \current version \explorer \folder descriptions \current \current$

Oueries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[stream]}$

Queries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[attributes]$

Queries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Queries value:

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

folders[cookies]

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}\cite{2}[category]$

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ 'aeb685 db-65 f9-4 cf6-a03a-e3ef65729 f3d \ [parent folder]$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local_continuous} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} \end{continuous} $$4$ eb 685 db -65 f9 -4c f6 -4$

a03a-e3ef65729f3d}[publishexpandedpath]

Queries value:

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

Queries value:

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

Oueries value:

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

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

folders[appdata]

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

settings\5.0\cache\cookies[cacheprefix]

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

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

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

settings\5.0\cache\history[peruseritem]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [category]$

Oueries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (d9dc8a3b-b784-432e-a781-5a1130a75963) \ [parent folder]$

Oueries value:

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [relative path]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the constant of the constant of$

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [icon]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [security]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [stream resource]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \explorer $$ folder descriptions $$ a781-5a1130a75963 $$ [stream resource type] $$$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \explorer \folder descriptions \explorer \folder descriptions \folder \f$

Queries value

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [roamable]$

Queries value:

Queries value

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[publishexpandedpath]}$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \explorer $$ folder descriptions $$ a781-5a1130a75963$ [attributes] $$$

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [initfolder \ handler]$

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

folders[history]

 $\label{thm:consoftware} Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$

```
settings\5.0\cache\history[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[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\domstore[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                            \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\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]
 Queries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
 Queries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
                            HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[mbcsservername]
 Queries value:
                            HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
 Queries value:
                            HKLM\software\microsoft\com3[com+enabled]
                            \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
 Queries value:
settings[utf8servernameres]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
 Queries value:
                            HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid[]
 Oueries value:
                            HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
 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[maxconnectionsperserver]
 Queries value:
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
```

```
settings[maxconnectionsperserver]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
 Queries value:
                           HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[inprocserver32]
 Queries value:
                           HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\tinprocserver32[]
                           HKCR\clsid\{304ce942-6e39-40d8-943a-
 Oueries value:
b913c40c9cd4}\inprocserver32[threadingmodel]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperproxy]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                           HKI M\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                           HKLM\software\microsoft\ole[maxsxshashcount]
 Oueries value:
 Queries value:
                           HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[certcachenovalidate]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[ftpdefaultexpirytimesecs]
 Queries value:
                           HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol \verb|\feature_disable_unicode_handle_closing_callback[857bd61a8241ac81385ee957d8137887.exe]| \\
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablecachingofsslpages]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[wpadsearchalldomains]
 Queries 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[bypasshttpnocachecheck]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
 Queries value:
                           \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[bypasssslnocachecheck]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
 Queries value:
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[nocheckautodialoverride]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

```
settings[dontusednsloadbalancing]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
  Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  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[mimeexclusionlistforcache]
                            \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}.
  Oueries value:
settings[headerexclusionlistforcache]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[dnscacheentries]
                            \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}.
  Oueries value:
settings[dnscachetimeout]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonzonecrossing]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonbadcertrecving]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonpostredirect]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[alwaysdrainonredirect]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonhttpstohttpredirect]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:
                             HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
  Queries value:
  Queries value:
                             HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
  Oueries value:
                             HKLM\software\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]
  Oueries value:
                             HKLM\software\microsoft\rpc\extensions[ndroleextdll]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nonetautodial]
                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
  Queries value:
settings[globaluseroffline]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[badproxyexpirestime]
                            HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablebranchcache]
  Queries value:
                            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[migrateproxy]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyoverride]
                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[autoconfigurl]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\connections[defaultconnectionsettings]
                             HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Oueries value:
                             HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
  Queries value:
                            HKCR\clsid\{4590f811-1d3a-11d0-891f-
  Oueries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                            HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
  Oueries value:
  Queries value:
                            HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
                            HKLM\software\microsoft\wbem\cimom[logging directory]
  Oueries value:
  Oueries value:
                             HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:
                             HKLM\software\microsoft\wbem\cimom[log file max size]
                             HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
  Oueries value:
  Queries value:
                            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
                            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
  Oueries value:
cryptographic provider[image path]
  Queries value:
                             manager[safeprocesssearchmode]
  Queries value:
                             HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
```

```
Queries value:
                                                             HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
    Oueries value:
                                                             HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
    Oueries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
                                                             HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
    Oueries value:
    Queries value:
                                                             HKLM\software\microsoft\cryptography[machineguid]
    Oueries value:
                                                             HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
    Oueries value:
                                                             HKLM\software\microsoft\rpc\extensions[remoterpcdll]
    Queries value:
                                                             HKLM\software\microsoft\tracing[enableconsoletracing]
    Oueries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enablefiletracing]
    Queries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filetracingmask]
    Oueries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enableconsoletracing]
    Queries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[consoletracingmask]
    Queries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[maxfilesize]
    Queries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filedirectory]
                                                             HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\profilelist[programdata]
                                                             HKLM\software\microsoft\sqmclient\windows\disabledprocesses[fbac773d]
    Queries value:
    Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
    Oueries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[enablefiletracing]
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus tracing \setminus 857bd61a8241ac81385ee957d8137887\_rasmancs[filetracingmask]
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887 rasmancs[enableconsoletracing]
    Oueries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[consoletracingmask]
    Oueries value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[maxfilesize]
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887 rasmancs[filedirectory]
    Oueries value:
                                                             HKLM\software\microsoft\ole[maximumallowedallocationsize]
                                                             HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
    Queries value:
                                                             HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
    Oueries value:
                                                            HKCR\clsid\{7c857801-7381-11cf-884d-
    Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                                            HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
    Queries value:
    Queries value:
                                                            HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
                                                            HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
    Oueries value:
    Queries value:
                                                             HKLM\system\currentcontrolset\control\nls\customlocale[en]
                                                             HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
    Oueries value:
    Oueries value:
                                                             HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
    Queries value:
                                                             HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
    Queries value:
                                                             HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
    Queries value:
                                                            HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
                                                             HKCR\clsid\{d68af00a-29cb-43fa-8504-
    Oueries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
                                                             HKLM\software\microsoft\wbem\cimom[processid]
    Queries value:
                                                             HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
    Queries value:
    Queries value:
                                                             HKLM\software\microsoft\wbem\cimom[contextlimit]
    Oueries value:
                                                             HKLM\software\microsoft\wbem\cimom[objectlimit]
                                                             HKLM\software\microsoft\wbem\cimom[identifierlimit]
    Queries value:
                                                             HKCR\interface\{027947e1-d731-11ce-a357-0000000001}\proxystubclsid32[]
    Oueries value:
    Queries value:
                                                             HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
                                                             HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
    Oueries value:
00104b703efd}\inprocserver32[inprocserver32]
    Queries value:
                                                            HKCR \c1sid \final 102-b604-00104b703efd \c1b1cad8c-2dab-11d2-b604-00104b703efd \c1b1cad8c-2da
    Queries value:
                                                            HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
                                                             HKCR \land (1c1c45ee-4395-11d2-b60b-00104b703efd) \land (2c1c45ee-4395-11d2-b60b-00104b703efd) \land (2c1c45ee-4395-11d2-b60b-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6-00104b6
    Queries value:
                                                             HKCR \land (423ec01e-2e35-11d2-b604-00104b703efd) \land (423ec01e-2e35-11d2-b604-00104b703eff) \land (423ec01e-2e35-11d2-b604-00104b703eff) \land (423ec01e-2e35-11d2-b604-00104b704-00104b704-00104b704-00104b704-00104b704-00104b704-00104b704-00104b704-00104
    Oueries value:
    Oueries value:
                                                             HKLM\software\microsoft\windows defender[disableantispyware]
    Queries value:
                                                             HKLM\system\currentcontrolset\services\netbt\linkage[export]
    Sets/Creates 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[proxyserver]
    Sets/Creates value:
HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enablefiletracing]
    Sets/Creates value:
```

HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filetracingmask]
Sets/Creates value:

Sets/Creates value:

HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enableconsoletracing]

HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[consoletracingmask]
Sets/Creates value:

 $\label{lem:hklmsoftware} $$HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[maxfilesize] $$Sets/Creates value:$

 $\label{lem:hklmsoftware} $$HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filedirectory] $$Sets/Creates value:$

HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[enablefiletracing]
Sets/Creates value:

HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[enableconsoletracing]
Sets/Creates value:

 $HKLM \ software \ microsoft \ tracing \ 857bd61a8241ac81385ee957d8137887_rasmancs [file tracing mask] \\ Sets \ / Creates \ value:$

 $\label{lem:hklmsoftware} HKLM\software\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[maxfilesize] Sets/Creates value:$

 $HKLM \setminus software \setminus microsoft \setminus tracing \setminus 857bd61a8241ac81385ee957d8137887_rasmancs[filedirectory]$

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

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

 ${\tt settings} \verb|\connections[defaultconnectionsettings]|\\$

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]