Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3314, Task ID: 763

Task ID: 763 Risk Level: 10

Date Processed: 2016-05-18 10:35:31 (UTC)

Processing Time: 62.3 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

3 HTTP connection - response code 200 (success)

10 Creates malicious events: Cycbot [Backdoor]

4 Checks whether debugger is present

Process/Thread Events

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

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

 $\label{lem:creates} C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe $$[C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe startC:\Program Files$

 $(x86)\LP\36D6\027.exe\%C:\Program Files (x86)\LP\36D6]$

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

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

 $startC: \Users\Admin\AppData\Roaming\6A47B\FAC36.exe\%C: \Users\Admin\AppData\Roaming\6A47B\Barrer Barrer Barrer$

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

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects\{5D92BB9F-9A66-458f-ACA4-66172A7016D4}
Creates mutex:	\Sessions\1\BaseNamedObjects\{4D92BB9F-9A66-458f-ACA4-66172A7016D4}
Creates mutex:	\Sessions\1\BaseNamedObjects\{61B98B86-5F44-42b3-BCA1-33904B067B81}
Creates mutex:	\Sessions\1\BaseNamedObjects\{B16C7E24-B3B8-4962-BF5E-4B33FD2DFE78}
Creates mutex:	\Sessions\1\BaseNamedObjects\{B37C48AF-B05C-4520-8B38-2FE181D5DC78}
Creates mutex:	\Sessions\1\BaseNamedObjects\{OECE180F-6E9E-4FA6-A154-6876D9DB8906}
Creates mutex:	\Sessions\1\BaseNamedObjects\4A3282FEF482C0F79E1
Creates event:	\Sessions\1\BaseNamedObjects\{6B985724-623F-492e-B0D6-C9715ADE853B}

File System Events

Creates: C:\Program Files (x86)
Creates: C:\Program Files (x86)\7B0FE
Creates: C:\Users\Admin\AppData\Roaming
Creates: C:\Users\Admin\AppData\Roaming\6A47B
Creates: C:\Users\Admin\AppData\Roaming\6A47B\B0FE.A47

Creates: C:\Program Files (x86)\LP
Creates: C:\Program Files (x86)\LP\36D6

Opens: C:\Windows\Prefetch\857BD61A8241AC81385EE957D8137-5577336B.pf

Opens: C:\Window

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe

C:\Windows\SysWOW64\ntdll.dll Opens: Opens: C:\Windows\SysWOW64\kernel32.dll C:\Windows\SysWOW64\KernelBase.dll Opens: Opens: C:\Windows\apppatch\sysmain.sdb C:\Windows\SysWOW64\oleacc.dll Opens: Opens: C:\Windows\SysWOW64\msimg32.dll Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\msvcrt.dll

Opens: C:\Windows\SyswOW64\bcryptprimitives.dll
Opens: C:\Windows\SyswOW64\cryptpase.dll
Opens: C:\Windows\SyswOW64\cryptbase.dll
Opens: C:\Windows\SyswOW64\rpcrt4.dll
Opens: C:\Windows\SyswOW64\rpcrt4.dll
Opens: C:\Windows\SyswOW64\gdi32.dll

Opens: C:\Windows\SysWOW64\user32.dll

C:\Windows\SysWOW64\imm32.dll Opens: Opens: C:\Windows\SysWOW64\msctf.dll C:\Windows\SysWOW64\oleaccrc.dll Opens: Opens: C:\Windows\SysWOW64\combase.dll Opens: C:\Windows\SysWOW64\oleaut32.dll Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\Globalization\Sorting\SortDefault.nls C:\Windows\SysWOW64\advapi32.dll Opens: C:\Windows\SysWOW64\rasapi32.dll Opens: Opens: C:\Windows\SysWOW64\rasman.dll C:\Windows\SysWOW64\nsi.dll Opens: Opens: C:\Windows\SysWOW64\ws2_32.dll Opens: C:\Windows\SysWOW64\shlwapi.dll C:\Windows\SysWOW64\shell32.dll Opens: Opens: C:\Windows\SysWOW64\winhttp.dll C:\Windows\SysWOW64\iertutil.dll Opens: Opens: C:\Windows\SysWOW64\wininet.dll Opens: C:\ Opens: C:\Windows\SysWOW64\SHCore.dll Opens: C:\Users\Admin\AppData\Roaming\6A47B\B0FE.A47 Opens: C:\Windows\SysWOW64\mswsock.dll Opens: C:\Windows\SysWOW64\dnsapi.dll Opens: C:\Windows\SysWOW64\rasadhlp.dll Opens: C:\Windows\Temp Opens: C:\Windows\SysWOW64\secur32.dll C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: Opens: C:\Windows\SysWOW64\winnsi.dll

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

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\counters.dat

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

C:\Users\Admin\AppData\Roaming\Cloud AV 2012\ahst.lni Opens:

Opens: C:\Windows\SysWOW64\clbcatq.dll Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll C:\Windows\SysWOW64\dhcpcsvc.dll Opens:

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

controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985

C:\Windows\WinSxS\x86_microsoft.windows.common-Opens: controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll

Opens: C:\Windows\WindowsShell.Manifest C:\Windows\SysWOW64\FirewallAPI.dll Opens: Opens: C:\Windows\System32\Drivers\etc\hosts Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL C:\Windows\SysWOW64\wbem\wbemprox.dll Opens: Opens: C:\Windows\SysWOW64\wbemcomn.dll Opens: C:\Windows\SysWOW64\cryptsp.dll C:\Windows\SysWOW64\rsaenh.dll Opens: Opens: C:\Windows\SysWOW64\wbem\wbemsvc.dll C:\Windows\SysWOW64\rtutils.dll Opens:

C:\Windows\SysWOW64\wbem\fastprox.dll Opens: Opens: C:\Users\Admin\AppData\Roaming\Mozilla\ C:\Users\Admin\AppData\Roaming\Opera\ Opens: Opens: C:\Windows\SysWOW64\NapiNSP.dll Opens: C:\Windows\SysWOW64\pnrpnsp.dll Opens: C:\Windows\SysWOW64\nlaapi.dll Opens: C:\Windows\SysWOW64\winrnr.dll

C:\Users\Admin\AppData\Roaming\6A47B\B0FE.A47 Writes to: Reads from: C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe

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

Network Events

DNS query:

DNS auerv:

DNS query: binghamtonschools.org DNS query: fzs.enotusfed.com DNS query: uupi1pm.enotusfed.com DNS query: www.google.com DNS query: zxnz.opalimanos.com DNS query: ctldl.windowsupdate.com DNS query: vla248.opalimanos.com DNS query: 57i.kupinosis.com DNS query: ocsp.verisign.com DNS guery: Okkjkdy8rq.kupinosis.com DNS query: 15jb148p7z.dudlik-munik.com DNS query: 35211w.enotusfed.com DNS query: crl.verisign.com DNS query: vrmy94bxc.opalimanos.com DNS query: xprstats.com DNS query: patentgenius.com DNS query: h4f71.dudlik-munik.com DNS query: v7fd.dudlik-munik.com 1uu0l3f1s2.enotusfed.com DNS query:

dp3dd.dudlik-munik.com csc3-2009-2-crl.verisign.com

```
-8nc2.enotusfed.com
  DNS query:
                           binghamtonschools.org ⇒ 174.129.25.170
  DNS response:
                           www.google.com \Rightarrow 58.27.108.172
  DNS response:
                           www.google.com ⇒ 58.27.108.173
  DNS response:
  DNS response:
                           www.google.com ⇒ 58.27.108.152
  DNS response:
                           www.google.com \Rightarrow 58.27.108.162
                           www.google.com ⇒ 58.27.108.187
  DNS response:
                           www.google.com \Rightarrow 58.27.108.167
  DNS response:
  DNS response:
                           www.google.com ⇒ 58.27.108.178
                           www.google.com ⇒ 58.27.108.157
  DNS response:
                           www.google.com ⇒ 58.27.108.183
  DNS response:
  DNS response:
                           www.google.com \Rightarrow 58.27.108.177
  DNS response:
                           www.google.com \Rightarrow 58.27.108.182
                           www.google.com \Rightarrow 58.27.108.168
  DNS response:
  DNS response:
                           www.google.com \Rightarrow 58.27.108.148
                           www.google.com ⇒ 58.27.108.163
  DNS response:
                           www.google.com \Rightarrow 58.27.108.158
  DNS response:
  DNS response:
                           www.google.com ⇒ 58.27.108.153
  DNS response:
                           a1621.g.akamai.net ⇒ 58.27.86.73
                           a1621.g.akamai.net ⇒ 58.27.86.56
  DNS response:
  DNS response:
                           e8218.dscb1.akamaiedge.net \Rightarrow 23.15.155.27
  DNS response:
                           15jb148p7z.dudlik-munik.com ⇒ 173.230.133.99
                           e6845.dscb1.akamaiedge.net \Rightarrow 23.15.149.163
  DNS response:
  DNS response:
                           patentgenius.com ⇒ 76.76.19.57
  DNS response:
                           h4f71.dudlik-munik.com \Rightarrow 173.230.133.99
                           v7fd.dudlik-munik.com \Rightarrow 173.230.133.99
  DNS response:
  DNS response:
                           dp3dd.dudlik-munik.com \Rightarrow 173.230.133.99
  Connects to:
                           174.129.25.170:80
                           58.27.108.172:80
  Connects to:
  Connects to:
                           58.27.86.73:80
  Sends data to:
                           0.0.0.0:53
                           binghamtonschools.org:80 (174.129.25.170)
  Sends data to:
  Sends data to:
                           www.google.com:80 (58.27.108.172)
  Sends data to:
                           a1621.g.akamai.net:80 (58.27.86.73)
                           127.0.0.1:49162
  Sends data to:
  Receives data from:
                           0.0.0.0:53
  Receives data from:
                           binghamtonschools.org:80 (174.129.25.170)
  Receives data from:
                           127.0.0.1:49162
  Receives data from:
                           www.google.com:80 (58.27.108.172)
  Receives data from:
                           a1621.g.akamai.net:80 (58.27.86.73)
  Receives data from:
                           127.0.0.1:49165
  Receives data from:
                           127.0.0.1:49166
  Receives data from:
                           127.0.0.1:49167
  Receives data from:
                           127.0.0.1:49168
  Receives data from:
                           127.0.0.1:49169
  Receives data from:
                           127.0.0.1:49170
  Receives data from:
                           127.0.0.1:49171
  Receives data from:
                           127.0.0.1:49172
  Receives data from:
                           127.0.0.1:49173
  Receives data from:
                           127.0.0.1:49174
  Receives data from:
                           127.0.0.1:49175
  Receives data from:
                           127.0.0.1:49176
  Receives data from:
                           127.0.0.1:49177
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\wow6432node\microsoft\wbem\cimom
  Creates key:
                           HKLM\software\wow6432node\microsoft\tracing
  Creates kev:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32
  Deletes value:
                           HKCU\software\microsoft\windows\currentversion\internet
                           HKCU\software\microsoft\windows\currentversion\internet
  Deletes value:
settings[autoconfigurl]
  Deletes value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[autodetect]
```

settings[proxyoverride]

Opens key: HKLM\software\microsoft\wow64

 ${\tt HKLM} \verb| system \verb| current control \verb| server| \\$ Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll Opens key:

 $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\system\currentcontrolset\control\nls\customlocale

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

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

```
Opens key:
                                              HKLM\software\wow6432node\policies\microsoft\mui\settings
   Opens key:
                                              HKLM\software\policies\microsoft\mui\settings
   Opens key:
                                              HKCU\
                                              HKCU\control panel\desktop\muicached\machinelanguageconfiguration
   Opens key:
   Opens key:
                                              HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
   Opens key:
                                              HKCU\software\policies\microsoft\control panel\desktop
                                              HKCU\control panel\desktop\languageconfiguration
   Opens key:
                                              HKCU\control panel\desktop
   Opens key:
                                              HKCU\control panel\desktop\muicached
   Opens key:
                                              HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
   Opens key:
                                              HKLM\system\currentcontrolset\control\nls\sorting\versions
   Opens key:
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
   Opens key:
                                              HKCU\software\microsoft\windows nt\currentversion\appcompatflags
                                             HKLM\software\microsoft\windows
   Opens key:
nt\currentversion\appcompatflags\disable8and16bitmitigation
   Opens key:
                                              HKLM\system\currentcontrolset\control\session manager
                                              HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
   Opens kev:
execution options
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
   Opens key:
                                              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
   Opens key:
                                              HKLM\system\currentcontrolset\control\lsa
   Opens kev:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
   Opens key:
                                             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
                                              HKLM\software\wow6432node\microsoft\windows
   Opens key:
nt\currentversion\compatibility32
                                             HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
   Opens key:
compatibility
   Opens key:
                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows & nt\currentversion\windows & nt\current\currentversion\windows & nt\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current
   Opens key:
   Opens key:
                                             HKLM\software\wow6432node\microsoft\ole
   Opens key:
                                             HKLM\software\wow6432node\microsoft\ole\tracing
                                             HKLM\software\microsoft\ole\tracing
   Opens key:
                                              HKLM\software\wow6432node\microsoft\oleaut
   Opens key:
   Opens key:
                                             HKCU\software\classes\
                                             HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-
   Opens key:
00aa00389b71}\proxystubclsid32
                                             HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
   Opens key:
00aa00389b71}\proxystubclsid32
                                              Opens key:
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale
   Opens kev:
                                             \label{thm:linear} \mbox{HKCU\software\mbox{\sc microsoft\windows}} \ \ \mbox{nt\currentversion\windows}
   Opens key:
   Opens key:
                                              HKLM\software\wow6432node\microsoft\rpc
                                              HKLM\system\currentcontrolset\control\computername\activecomputername
   Opens key:
   Opens key:
                                             HKLM\system\setup
   Opens key:
                                              HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \ nt \setminus rpc
   Opens kev:
                                              HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                             HKLM\software\policies\microsoft\sqmclient\windows
                                              HKLM\software\microsoft\sqmclient\windows
   Opens key:
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
   Opens key:
c1bf-494e-b29c-65b732d3d21a}
c1bf-494e-b29c-65b732d3d21a}\propertybag
   Opens key:
                                             HKLM\software\wow6432node\microsoft\windows\currentversion
   Opens key:
a0fb-4bfc-874a-c0f2e0b9fa8e}
   Opens kev:
HKLM \label{lem:hklm} White the latest and the la
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
   Opens key:
Opens key:
                                              HKLM\system\currentcontrolset\services\winsock2\parameters
   Opens kev:
                                              HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1b6cd5d7
   Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
   Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
   Opens key:
Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ parameters \ protocol\_catalog\_entries \ protocol\_catalog \ parameters \ parameters
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
  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 key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006
  Opens key:
                                 HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:
                                 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:
                                 HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:
                                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                                 HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:
  Opens key:
                                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
  Opens key:
                                 HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters
                                 HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
  Opens kev:
  Opens key:
                                 HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:
                                 HKLM\software\wow6432node\policies\microsoft\system\dnsclient
  Opens key:
                                 HKLM\software\policies\microsoft\system\dnsclient
  Opens key:
                                 \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\857bd61a8241ac81385ee957d8137887.exe
                                 HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens kev:
  Opens key:
                                 HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:
                                 HKLM\software\wow6432node\policies\microsoft\windows\appcompat
  Opens key:
                                 HKLM\software\policies\microsoft\windows\appcompat
  Opens key:
                                 HKCU\software\microsoft\windows nt\currentversion
                                 \label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current version\app compatflags\layers} \\
  Opens key:
  Opens key:
                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
                                 HKLM\software\wow6432node\microsoft\windows
  Opens key:
nt\currentversion\appcompatflags\custom\857bd61a8241ac81385ee957d8137887.exe
                                 HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:
  Opens key:
                                 HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:
                                 HKLM\software\microsoft\windows
HKLM\system\currentcontrolset\services\dns
  Opens key:
                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache
  Opens kev:
33be-4251-ba85-6007caedcf9d}
  Opens key:
33be-4251-ba85-6007caedcf9d}\propertybag
                                 HKLM\system\currentcontrolset\control\sqmservicelist
  Opens kev:
  Opens key:
                                 HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
  Opens key:
                                 HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens kev:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
                                 HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:
```

Opens key:

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

Opens key:

HKU\
Opens key:

HKU\.default

Opens kev:

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

Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders

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

nt\currentversion\profilelist

Opens kev: HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

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

Opens key: HKLM\software\microsoft\com3

HKLM\software\microsoft\windowsruntime\clsid Opens key:

Opens kev:

b913c40c9cd4}

Opens key: HKCR\activatableclasses\clsid

HKCR\activatableclasses\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943ab913c40c9cd4}

Opens key:

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

b913c40c9cd4}\treatas

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

Opens key:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e93

Opens key:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}

Opens key:

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

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}

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

b913c40c9cd4}\inprocserver32 HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\inprocserver32

Opens kev:

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

settings Opens key:

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

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

settings

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

explorer\main\featurecontrol

HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens kev:

Opens key:

25b8d56dd1d8}

Opens kev:

8a6dc56e0da9}

Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}

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

b913c40c9cd4}\inprochandler32 HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-Opens key:

b913c40c9cd4}\inprochandler32

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

b913c40c9cd4}\inprochandler

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

b913c40c9cd4}\inprochandler

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

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

explorer\main\featurecontrol

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable

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

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling

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

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

explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611

Opens key: HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
 Opens key:
                         HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKLM\software\wow6432node\microsoft\rpc\securityservice
 Opens key:
                         HKLM\software\microsoft\rpc\securityservice
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                         HKLM\system\currentcontrolset\services\tcpip\linkage
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature exclude invalid client cert kb929477
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature return failed connect content kb942615
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature preserve spaces in filenames kb952730
                         HKCU\software\microsoft\windows\currentversion\internet settings
 Opens key:
 Opens key:
                         HKLM\software\wow6432node\policies
 Opens key:
                         HKCU\software\policies
                         HKCU\software
 Opens key:
 Opens key:
                         HKLM\software\wow6432node
 Opens key:
                         HKLM\software\wow6432node\policies\microsoft\internet explorer
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer
 Opens key:
                         HKLM\software\wow6432node\policies\microsoft\internet explorer\main
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\main
 Opens key:
                         HKLM\software\wow6432node\microsoft\rpc\extensions
 Opens key:
                         HKLM\software\microsoft\rpc\extensions
 Opens kev:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
 Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ 1.0 \ cache
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
```

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266 HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543 HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444 Opens key: HKCU\software\classes\appid\857bd61a8241ac81385ee957d8137887.exe Opens key: HKCR\appid\857bd61a8241ac81385ee957d8137887.exe Opens kev: 00aa004b2e24} Opens key: $HKCR \land activatable classes \land clsid \land \{4590f811-1d3a-11d0-891f-00aa004b2e24\}$ Opens key: 00aa004b2e24} HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-Opens kev: 00aa004b2e24}\treatas Opens key: $HKCR \setminus wow 6432 \\ node \\ clsid \\ \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \\ \setminus treat \\ as \\ (4590f811-1d3a-11d0-891f-00aa004b2e24) \\ \setminus treat \\ (4590f811-1d3a-11d0-891f-00aa004b2e24) \\ \cdot treat \\ (4590f811-1d0-891f-00aa004b2e24) \\ \cdot treat \\ \cdot treat \\ (4590f811-1d0-891f-00aa004b2e24) \\ \cdot treat \\ \cdot treat$ Opens key: 00aa004b2e24}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32 HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-Opens key: 00aa004b2e24}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-Opens key: 00aa004b2e24}\inprochandler HKLM\software\microsoft\windowsruntime\clsid\{c39ee728-d419-4bd4-a3ef-Opens key: eda059dbd935} Opens key: HKCR\activatableclasses\clsid\{c39ee728-d419-4bd4-a3ef-eda059dbd935} HKCU\software\classes\activatableclasses\clsid Opens key: Opens key: HKCU\software\classes\activatableclasses\clsid\{c39ee728-d419-4bd4-a3efeda059dbd935} HKCU\software\classes\clsid\{c39ee728-d419-4bd4-a3ef-eda059dbd935} Opens key:

Opens key: HKCR\clsid\{c39ee728-d419-4bd4-a3ef-eda059dbd935}

Opens key:

provider

HKLM\software\policies\microsoft\cryptography Opens kev:

Opens key: HKLM\software\microsoft\cryptography

Opens key: $HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| cryptography \verb|\softload|| and the software \verb|\software\\| wow 6432 node \verb|\microsoft\\| cryptography \verb|\softload|| and the software \verb|\software\\| wow 6432 node \verb|\microsoft\\| cryptography \verb|\softload|| and the software \verb|\software\\| cryptography \verb|\software\\| cryptogr$

Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-

000000000046}

 $\label{local-eq:hkcr-wow6432} HKCR \setminus wow6432 \\ node \setminus interface \setminus \{00000134-0000-0000-c000-0000000000046\}$ Opens key: Opens kev: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-

 $000000000046 \} \verb|\proxystubclsid32|$

HKCR\wow6432node\interface\{00000134-0000-0000-c000-Opens key:

00000000046}\proxystubclsid32

 $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ tcpip \+ parameters$ Opens key:

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{8bc3f05e-d86b-11d0-a075-d86b-11d0-a07$

00c04fb68820}

Opens key: HKCR\activatableclasses\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}

HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\treatas

 $HKCR \setminus wow6432 node \\ clsid \\ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} \\ \\ \\ treatas$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{8bc3f05e-d86b-11d0-a075-$

00c04fb68820}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-Opens kev:

00c04fb68820}\inprochandler32

Opens key:

00c04fb68820}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler

HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-Opens kev:

00c04fb68820}\inprochandler

Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{0000032a-0000-0000-c000-c000-c000-c000-c00-c00-c000-c000-c00-c000-c000-c000-c000-c00-c00-c000-c00$

00000000046}

Opens key:

Opens key: 000000000046} Opens key: HKCR\wow6432node\clsid\{0000032a-0000-0000-c000-00000000046} HKCU\software\classes\clsid\{0000032a-0000-0000-c000-00000000046} Opens key: Opens key: HKCR\clsid\{0000032a-0000-0000-c000-00000000046} Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{0000032a-0000-0000-c000-c000-c00-c00-c000-c000-c000-c00-c000-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c000-c00-$ 000000000046} HKLM\software\microsoft\windowsruntime\clsid\{00000339-0000-0000-c000-Opens key: 00000000046} HKCR\activatableclasses\clsid\{00000339-0000-0000-c000-00000000046} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00000339-0000-0000-c000-000000000046} Opens key: HKCR\wow6432node\clsid\{00000339-0000-0000-c000-000000000046} HKCU\software\classes\clsid\{00000339-0000-0000-c000-00000000046} Opens key: Opens key: HKCR\clsid\{00000339-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\activatableclasses\clsid\{00000339-0000-0000-c000-000000000046} Opens key: HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820} HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820} Opens key: Opens key: HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32 HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-Opens kev: 00c04fb68820}\proxystubclsid32 Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{7c857801-7381-11cf-884d-11c$ 00aa004b2e24} Opens key: $HKCR \land ctivatable classes \land clsid \land \{7c857801-7381-11cf-884d-00aa004b2e24\}$ Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7c857801-7381-11cf-884d-11cf-8$ 00aa004b2e24} Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7c857801-7381-11cf-884d-1464\} \\ + 11cf-884d-1464 \\ +$ 00aa004b2e24}\treatas $HKCR \setminus wow6432 node \\ clsid \\ \{7c857801-7381-11cf-884d-00aa004b2e24\} \\ \setminus treatas$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{7c857801-7381-11cf-884d-11cf-8$ 00aa004b2e24}\inprocserver32 HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprocserver32 $HKCU \setminus software \setminus classes \setminus wow 6432 node \setminus clsid \setminus \{7c857801-7381-11cf-884d-11cf-88$ Opens key: 00aa004b2e24}\inprochandler32 HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprochandler HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprochandler Opens key: HKCU\software\classes\wow6432node\interface\{b06b0ce5-689b-4afd-b326-0a08a1a647af} Opens key: $HKCR\wow6432 node\interface \ \{b06b0ce5-689b-4afd-b326-0a08a1a647af\}$ HKCU\software\classes\wow6432node\interface\{b06b0ce5-689b-4afd-b326-Opens kev: 0a08a1a647af}\proxystubclsid32 HKCR\wow6432node\interface\{b06b0ce5-689b-4afd-b326-Opens key: 0a08a1a647af}\proxystubclsid32 Opens key: HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} Opens key: 60ce2149e33c}\treatas HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserv er32 HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens kev: 60ce2149e33c}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens kev: 60ce2149e33c}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens kev: 60ce2149e33c}\inprochandler HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens key: 60ce2149e33c}\inprochandler Opens key: HKCU\software\classes\wow6432node\clsid\{c39ee728-d419-4bd4-a3efeda059dbd935} Opens kev: HKCR\wow6432node\clsid\{c39ee728-d419-4bd4-a3ef-eda059dbd935} Opens key: HKCU\software\classes\wow6432node\clsid\{c39ee728-d419-4bd4-a3efeda059dbd935}\treatas Opens key: HKCR\wow6432node\clsid\{c39ee728-d419-4bd4-a3ef-eda059dbd935}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{c39ee728-d419-4bd4-a3efeda059dbd935}\inprocserver32

Opens key: $\label{local-cond} \begin{tabular}{l} HKCR\wow6432 node\clsid\{c39ee728-d419-4bd4-a3ef-eda059dbd935}\nprocserver32 \end{tabular}$

Opens key: HKCU\software\classes\wow6432node\clsid\{c39ee728-d419-4bd4-a3efeda059dbd935}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{c39ee728-d419-4bd4-a3efeda059dbd935}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{c39ee728-d419-4bd4-a3ef-Opens kev: eda059dbd935}\inprochandler HKCR\wow6432node\clsid\{c39ee728-d419-4bd4-a3ef-Opens key: eda059dbd935}\inprochandler Opens key: $HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus interface \setminus \{d4781cd6 - e5d3 - 44df - ad94 - e5d3 - e$ 930efe48a887} Opens key: HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} Opens key: 930efe48a887}\proxystubclsid32 HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-Opens key: 930efe48a887}\proxystubclsid32 Opens key: HKLM\software\microsoft\windowsruntime\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCR\activatableclasses\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff} Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas Opens key: $HKCR\wow6432 node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treat as$ $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{674b6698 - ee92 - 11d0 - ad71 - eq82 - eq82$ Opens key: 00c04fd8fdff}\inprocserver32 HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprochandler32 HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens kev: 00c04fd8fdff}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprochandler HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-Opens key: 00c04fd8fdff}\inprochandler Opens kev: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385 ee 957d8137887_rasapi 32ac + 12bc for the software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385 ee 957d8137887_rasapi 32ac + 12bc for the software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385 ee 957d8137887_rasapi 32ac + 12bc for the software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385 ee 957d8137887_rasapi 32ac + 12bc for the software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241ac81385 ee 957d8137887_rasapi 32ac + 12bc for the software \setminus wow 6432 node \setminus wow 6432 n$ HKLM\software\wow6432node\microsoft\wbem\cimom Opens key: Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (3eb685db-microsoft) \ defined a software \ wow 6432 node \ microsoft \ windows \ current \ version \ (3eb685db-microsoft) \ defined \ a software \ wow 6432 node \ microsoft \ windows \ current \ version \ (3eb685db-microsoft) \ defined \ a software \ wow 6432 node \ microsoft \ windows \ current \ version \ (3eb685db-microsoft) \ defined \ a software \ wow 6432 node \ microsoft \ windows \ current \ version \ (3eb685db-microsoft) \ defined \ a software \ wow 6432 node \ microsoft \ windows \ current \ version \ (3eb685db-microsoft) \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ a software \ wow 6432 node \ microsoft \ windows \ defined \ defined \ wow 6432 node \ wow 6432 no$ 65f9-4cf6-a03a-e3ef65729f3d} Opens kev: 65f9-4cf6-a03a-e3ef65729f3d}\propertybag Opens key: HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} Opens key: $HKCR \setminus wow 6432 \\ node \setminus interface \setminus \{9556 \\ dc \\ 99-828 \\ c-11 \\ cf-a \\ 37e-00 \\ aa \\ 003240 \\ c7\}$ HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-Opens kev: 00aa003240c7}\proxystubclsid32 HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-Opens kev: 00aa003240c7}\proxystubclsid32 Opens key: ce99a996d9ea} HKCR\activatableclasses\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea} HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens kev: Opens key: ce99a996d9ea}\treatas $HKCR\wow6432 node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treat as$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprocserv er32 HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea}\inprochandler HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-Opens key: ce99a996d9ea}\inprochandler Opens key: HKLM\software\microsoft\windowsruntime\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} Opens key: HKCR\activatableclasses\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} Opens key: HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca} Opens kev: Opens key:

252725d697ca}\treatas

252725d697ca}\inprocserver32 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens kev: 252725d697ca}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Opens kev: 252725d697ca}\inprochandler Opens key: HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\inprochandler Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{027947e1 - d731 - 11ce - a357 - d731 -$ 0000000000013 HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-00000000001} Opens key: Opens key: HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32 HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-Opens key: 000000000001}\proxystubclsid32 Opens key: 00104b703efd} Opens key: HKCR\activatableclasses\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd} Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd} Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd} Opens key: 00104b703efd}\treatas Opens key: $HKCR\wow6432 node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treat as$ Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-Opens key: 00104b703efd}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-Opens key: 00104b703efd}\inprochandler HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-Opens key: 00104b703efd}\inprochandler HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-Opens key: 00104b703efd} HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd} Opens key: HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-Opens kev: 00104b703efd}\proxystubclsid32 HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-Opens kev: 00104b703efd}\proxystubclsid32 Opens key: HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd} HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd} Opens kev: Opens key: HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32 HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-Opens key: 00104b703efd}\proxystubclsid32 HKLM\software\microsoft\windows defender Opens key: Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback] Oueries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] HKLM\system\currentcontrolset\control\mui\uilanguages\en-Queries value: us[alternatecodepage] HKCU\control panel\desktop[preferreduilanguages] Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Oueries value: Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest] \ details a side by side \ for the limit of t$ Queries value: $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\sorting| versions[]$ HKCU\software\microsoft\windows Oueries value: nt\currentversion\appcompatflags[showdebuginfo] HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter] Queries value: $\label{lem:hklmsoftware} \verb+microsoft+ windows nt+ current version+ image file execution$ options\dllnxoptions[857bd61a8241ac81385ee957d8137887.exe] Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Oueries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Oueries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows

HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32[857bd61a8241ac81385ee957d8137887]

Queries value:

Queries value:

nt\currentversion\windows[loadappinit_dlls]

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

Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-

00aa00389b71}\proxystubclsid32[]

 Queries value:
 HKLM\system\currentcontrol\nls\sorting\versions[000602xx]

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

 Queries value:
 HKLM\system\currentcontrol\set\control\nls\sorting\ids[en-us]

 Queries value:
 HKLM\system\currentcontrol\set\control\nls\sorting\ids[en-us]

 Queries value:
 HKLM\system\currentcontrol\set\control\nls\sorting\ids[en]

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

Queries value:

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

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

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

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

Queries value:

 $\label{local-bound} HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\eqned \{905e63b6-c1bf-494e-b29c-65b732d3d21a\}\cutegory\cite{Abstraction} \end{substitute}$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{local-bound} HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[infotip]}$

Queries value:

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\$

Queries value:

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

Queries value:

 $\label{thm:microsoftwindows} HKLM software \noindows \$

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:microsoftwindows} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder descriptions\folder folder descriptions\folder folder descriptions\folder folder descriptions\folder folder folder descriptions\folder folder folder$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescri$

Queries value:

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

Queries value:

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ for all 1 \ for all 1 \ for all 2 \$

Oueries value

 $\label{local-HKLM} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder-a0fb-4bfc-874a-c0f2e0b9fa8e\[Parentfolder]\]$

Oueries value:

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

Oueries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions$

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions$

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:microsoftwindows} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\[publishex panded path\]$

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]

 $\label{lem:hklmsystem} HKLM \ system \ control set \ services \ \ winsock 2 \ parameters \ protocol_catalog 9 \ [num_catalog_entries] \ Queries \ value:$

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000006[packedcatalogitem]
 Queries value:

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]

 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000002 [library path] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000003 [library path] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries 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\000000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]

 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000004 \ [provider info] \ Queries \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000005 [library path] \\ Queries \ value:$

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000005 [displaystring]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 \ [address family]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[displaystring]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000006[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[addressfamily]
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (00000000000006 \ [enabled]) \ (enabled)
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (0000000000006 \ [version]) \ details \ 
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
                                                 HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Queries value:
   Oueries value:
                                                 HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[mapping]
   Queries value:
                                                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
   Queries value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
   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:
HKLM\svstem\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
   Queries value:
                                                HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:
                                                 HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
                                                HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
   Oueries value:
   Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} icrosoft \end{tabular} windows \end{tabular} although the local conditions and the local conditions are local conditions. The local conditions are local conditions and the local conditions are local conditions and the local conditions are local conditions. The local conditions are local conditions are local conditions are local conditions and the local conditions are local conditions. The local conditions are local conditions are local conditions are local conditions are local conditions. The local conditions are local conditions are local conditions are local conditions are local conditions. The local conditions are lo
                                                HKCU\software\microsoft\windows\currentversion\explorer\shell
   Queries value:
folders[cache]
   Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[quervadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Queries value:
Queries value:
```

 $HKLM \verb| system| current control set \verb| services| tcpip| parameters [usedomain named evolution]$

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]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen default servers]
 Queries value:
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\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                     HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Queries value:
Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [query net btfqdn]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Oueries value:
Queries value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
 Queries value:
                     HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
                     HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cached sockets]
```

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns query time outs]$ HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[syncmode5] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache[sessionstarttimedefaultdeltasecs] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-1644444, \ node \ nod$ 33be-4251-ba85-6007caedcf9d}[category] Oueries value: $HKLM \label{lem:hklm} White the latest and the la$ 33be-4251-ba85-6007caedcf9d}[name] Queries value: 33be-4251-ba85-6007caedcf9d}[parentfolder] Oueries value: $HKLM \label{lem:hklm} White the latest and the la$ 33be-4251-ba85-6007caedcf9d}[description] Oueries value: 33be-4251-ba85-6007caedcf9d}[relativepath] Oueries value: 33be-4251-ba85-6007caedcf9d}[parsingname] Oueries value: 33be-4251-ba85-6007caedcf9d}[infotip] Queries value: 33be-4251-ba85-6007caedcf9d}[localizedname] Oueries value: $HKLM \label{lem:hklm} White the latest and the la$ 33be-4251-ba85-6007caedcf9d}[icon] Queries value: $HKLM \label{lem:hklm} White the software \label{lklm} White the$ 33be-4251-ba85-6007caedcf9d}[security] Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

```
33be-4251-ba85-6007caedcf9d}[precreate]
    Oueries value:
33be-4251-ba85-6007caedcf9d}[stream]
    Oueries value:
HKLM \label{lem:hklm} White the software \label{lem:hklm} White \label{lklm} White the software \label{lklm} White \labe
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
    Oueries value:
33be-4251-ba85-6007caedcf9d}[attributes]
    Oueries value:
HKLM \label{lem:hklm} White the software \label{lem:hklm} White \label{lklm} White the software \label{lklm} White \labe
33be-4251-ba85-6007caedcf9d}[foldertypeid]
    Oueries value:
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
                                                         HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
    Oueries value:
    Queries value:
                                                         HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[cache]
                                                         HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
    Queries value:
    Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                                                         HKLM\software\microsoft\com3[com+enabled]
    Oueries value:
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
                                                         HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
    Queries value:
                                                         HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
    Oueries value:
b913c40c9cd4}\inprocserver32[inprocserver32]
                                                         HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[]
    Oueries value:
                                                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[security_hklm_only]
55779daa70e9}[registrationenabled]
HKLM\svstem\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
55779daa70e9}[domain]
    Queries value:
                                                         HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[threadingmodel]
                                                         HKLM\software\microsoft\ole[maxsxshashcount]
    Queries value:
                                                         HKLM\software\wow6432node\microsoft\internet
    Oueries value:
explorer\main\featurecontrol\feature http username password disable[857bd61a8241ac81385ee957d8137887.exe]
    Queries value:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpdomain]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpv6domain]
    Queries value:
HKLM \land system \land current control set \land services \land tcpip6 \land parameters \land terfaces \land \{b5105d63-74c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-87b7-4c6-8
55779daa70e9}[nameserver]
                                                         HKCU\software\microsoft\internet
    Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
    Queries value:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[857bd61a8241ac81385ee957d8137887.exe]
    Oueries value:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationenabled]
    Queries value:
806e6f6e6963}[registeradaptername]
```

```
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[domain]
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d
806e6f6e6963}[dhcpdomain]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
   Oueries value:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{97e1de57-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d6fa-11e1-be62-d
806e6f6e6963}[dhcpnameserver]
   Queries value:
                                              HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                                              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Oueries value:
   Queries value:
                                              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[857bd61a8241ac81385ee957d8137887.exe]
                                              HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
   Oueries value:
55779daa70e9}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[disableadapterdomainname]
   Queries value:
55779daa70e9}[registrationmaxaddresscount]
   Queries value:
55779daa70e9}[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[enablemulticast]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[queryadaptername]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disableadapterdomainname]
   Queries value:
806e6f6e6963}[disabledynamicupdate]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enableadapterdomainnameregistration]
   Queries value:
806e6f6e6963}[registrationmaxaddresscount]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[maxnumberofaddressestoregister]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enablemulticast]
                                              HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist1]
   Oueries value:
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\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]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[idnenabled]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[preconnectlimit]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[preresolvelimit]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[sqmhttpstreamrandomuploadpoolsize]
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
   Oueries value:
                                              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
   Queries value:
                                              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[enablehttp1_1]
```

```
Oueries value:
                           HKLM\software\microsoft\rpc\extensions[ndroleextdll]
 Oueries value:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablenegotiate]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
 Queries value:
                           \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[clientauthbuiltinui]
 Oueries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[displayscriptdownloadfailureui]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsservername]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[utf8servernameres]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxhttpredirects]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
                          HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet
 Queries value:
settings[maxconnectionsper1 Oserver]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
 Oueries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablecachingofsslpages]
```

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[leashlegacycookies] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[dialupuselansettings] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[dialupuselansettings] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sendextracrlf] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[wpadsearchalldomains] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[bypasshttpnocachecheck] $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ Queries value: settings[bypasshttpnocachecheck] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[bypasssslnocachecheck] HKI M\software\wow6432node\microsoft\windows\currentyersion\internet Oueries value: settings[bypasssslnocachecheck] $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ Queries value: settings[enablehttptrace] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[nocheckautodialoverride] HKI M\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[nocheckautodialoverride] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[dontusednsloadbalancing] $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ Queries value: settings[dontusednsloadbalancing] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[sharecredswithwinhttp] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[mimeexclusionlistforcache] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[headerexclusionlistforcache] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscacheenabled] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[dnscacheentries] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[dnscachetimeout] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpost] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[warnalwaysonpost] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonzonecrossing] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonbadcertrecving] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[warnonpostredirect] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[alwaysdrainonredirect] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonhttpstohttpredirect] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[tcpautotuning] Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxysettingsperuser] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[badproxyexpirestime] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enableautodial] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[nonetautodial] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[globaluseroffline] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings[disablebranchcache] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[usefirstavailable] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[combinefalsestartdata] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[disablefalsestartblacklist] 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[enforcep3pvalidity] Queries value: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$ settings[migrateproxy] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[proxyenable] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]

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

Queries value:

```
settings[proxyoverride]
  Oueries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[autodetect]
  Queries value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\connections[defaultconnectionsettings]
  Queries value:
                                       HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
                                      HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
  Oueries value:
  Queries value:
                                      HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
  Oueries value:
00aa004b2e24}\inprocserver32[]
  Queries value:
                                      HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
                                      HKLM\software\wow6432node\microsoft\wbem\cimom[logging directory]
  Queries value:
  Queries value:
                                       HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
  Oueries value:
                                      HKLM\software\wow6432node\microsoft\wbem\cimom[log file max size]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[tvpe]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
                                       HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
  Queries value:
HKLM \verb|\software| policies \verb|\microsoft| cryptography[privkey cachepurge interval seconds]|
                                       HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
                                       HKLM\software\microsoft\cryptography[machineguid]
  Oueries value:
                                      HKCR\wow6432node\interface\{00000134-0000-0000-c000-
  Queries value:
00000000046}\proxystubclsid32[]
  Queries value:
                                      HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
                                      HKLM \setminus software \setminus microsoft \setminus ole[maximum allowed allocation size] \\
  Oueries value:
                                      Queries value:
00c04fb68820}\proxystubclsid32[]
                                      HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
  Oueries value:
                                       HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[]
                                      HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
  Oueries value:
00aa004b2e24}\inprocserver32[threadingmodel]
                                      HKCR\wow6432node\interface\{b06b0ce5-689b-4afd-b326-
  Oueries value:
0a08a1a647af}\proxystubclsid32[]
  Queries value:
                                      HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]
                                      HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
  Queries value:
60ce2149e33c}\inprocserver32[inprocserver32]
  Queries value:
                                      HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32[]
                                      HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
  Oueries value:
60ce2149e33c}\inprocserver32[threadingmodel]
                                      HKCR\wow6432node\clsid\{c39ee728-d419-4bd4-a3ef-eda059dbd935}[]
  Queries value:
                                      HKCR\wow6432node\clsid\{c39ee728-d419-4bd4-a3ef-
  Oueries value:
eda059dbd935}\inprocserver32[inprocserver32]
  Oueries value:
                                      HKCR\wow6432node\clsid\{c39ee728-d419-4bd4-a3ef-
eda059dbd935}\inprocserver32[]
                                      HKCR\wow6432node\clsid\{c39ee728-d419-4bd4-a3ef-
  Oueries value:
eda059dbd935}\inprocserver32[threadingmodel]
  Queries value:
                                      HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32[]
                                      HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[]
  Queries value:
                                      HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
  Oueries value:
00c04fd8fdff}\inprocserver32[inprocserver32]
                                      HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
  Oueries value:
00c04fd8fdff}\inprocserver32[]
                                      HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
  Queries value:
00c04fd8fdff}\inprocserver32[threadingmodel]
  Oueries value:
                                      HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
  Queries value:
HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus tracing \setminus 857 \\ bd61a8241ac81385ee957d8137887 \\ \_rasapi32[enablefile tracing]
  Oueries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filetracingmask]
  Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 857bd 61a8241ac81385ee 957d8137887\_rasapi 32 [enable consoletracing]
  Queries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857 bd 61a8241 ac 81385 ee 957 d8137887\_rasapi 32[consoletracing mask]
  Oueries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[maxfilesize]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887 rasapi32[filedirectorv]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\wbem\cimom[processid]
```

Oueries value: HKLM\software\wow6432node\microsoft\wbem\cimom[enableprivateobjectheap]

HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit] Oueries value: Oueries value: HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit] Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[identifierlimit]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

 $HKLM \label{lem:hklm} Which is a constant with the statement of the stat$ 65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

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

folders[appdata]

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

Queries value: HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-

00aa003240c7}\proxystubclsid32[] Queries value: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]

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

ce99a996d9ea}\inprocserver32[inprocserver32]

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

ce99a996d9ea}\inprocserver32[]

Oueries value:

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

ce99a996d9ea}\inprocserver32[threadingmodel]

HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}[] Oueries value:

 $HKCR\wow6432 node\clsid\e7d35cfa-348b-485e-b524-b6466cfa-348b-485e-b646cfa-348b-4866cfa-348$ Oueries value:

252725d697ca}\inprocserver32[inprocserver32]

HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-Queries value:

252725d697ca}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524252725d697ca}\inprocserver32[threadingmodel]

Queries value: HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-

00000000001}\proxystubclsid32[]

Queries value: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]

Queries value: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32[threadingmodel]

Queries value: HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-

00104b703efd}\proxystubclsid32[]

Queries value: HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-

00104b703efd}\proxystubclsid32[]

Queries value: HKLM\software\microsoft\windows defender[disableantispyware] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]

Sets/Creates value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857 bd 61a8241 ac 81385 ee 957 d8137887_rasapi 32 [enable file tracing]$

Sets/Creates value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857bd 61a8241 ac 81385 ee 957d 8137887_rasapi 32 [enable consolet racing]$

Sets/Creates value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 857 bd 61a8241 ac 81385 ee 957 d8137887_rasapi 32[filetracing mask]$

Sets/Creates value:

Sets/Creates value:

 $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus tracing \setminus 857bd61a8241ac81385ee957d8137887_rasapi32[maxfilesize]$

Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filedirectory]

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]