Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 1, Task ID: 1

Task ID: Risk Level: 10

Date Processed: 2016-03-28 07:35:09 (UTC)

Processing Time: 63.49 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\spyeye_injector.exe"

Sample ID: Type: basic Owner: admin

Label: spyeye_injector.exe 2016-03-28 07:35:09 (UTC) Date Added:

File Type: PE32:win32:gui File Size: 103936 bytes

b98bb6d7428c3dbffcfcab2414c6daa2 MD5:

SHA256: fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029

Description: None

Pattern Matching Results

Writes to memory of system processes

Modifies registry autorun entries 10 Suspicious writeprocess: Spyeye [Banking]

5 Abnormal sleep detected

Connects to local host

2 PE: Nonstandard section

4 Reads process memory

5 PE: Contains compressed section

6 Renames file on boot

5 Packer: UPX

Adds autostart object

10 Creates malicious mutex: Spyeye [Banking]

Static Events

Reads from process:

Anomaly: PE: Contains a virtual section

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

Packer:

Process/Thread Events

Creates process: C:\windows\temp\spyeye_injector.exe

["C:\windows\temp\spyeye_injector.exe"]

Creates process: C:\WinOldFileq\83A49421850.exe ["C:\WinOldFileq\83A49421850.exe"]

Creates process: C:\Users\Admin\AppData\Local\Temp\3MU581D.exe

["C:\Users\Admin\AppData\Local\Temp\3MU581D.exe"] PID:1100 C:\Windows\explorer.exe Reads from process:

PID:408 C:\Windows\System32\wininit.exe PID:480 C:\Windows\System32\lsass.exe Reads from process: Reads from process: PID:488 C:\Windows\System32\winlogon.exe Reads from process: PID:592 C:\Windows\System32\svchost.exe PID:624 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:708 C:\Windows\System32\svchost.exe Reads from process: PID:716 C:\Windows\System32\dwm.exe PID:788 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:852 C:\Windows\System32\svchost.exe Reads from process: PID:888 C:\Windows\System32\svchost.exe PID:312 C:\Windows\System32\spoolsv.exe Reads from process: Reads from process: PID:552 C:\Windows\System32\svchost.exe Reads from process: PID:664 C:\Windows\System32\svchost.exe PID:1424 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:2020 C:\Windows\System32\taskhostex.exe Reads from process: PID:1220 C:\Windows\System32\dllhost.exe Reads from process: PID:2060 C:\Windows\System32\svchost.exe Reads from process: PID:1928 C:\Windows\System32\wbem\unsecapp.exe Reads from process: PID:1840 C:\Windows\System32\wbem\WmiPrvSE.exe Reads from process: PID:2896 C:\Windows\System32\conhost.exe

Writes to process: PID:2416 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe

Writes to process: PID:2936 C:\Users\Admin\AppData\Local\Temp\3MU581D.exe

PID:2912 C:\Windows\Temp\spyeye_injector.exe Writes to process:

Writes to process: PID:2896 C:\Windows\System32\conhost.exe

Terminates process: C:\WinOldFileq\83A49421850.exe Terminates process: C:\Windows\Temp\spyeye_injector.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\RPCController
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW 00000000

\BaseNamedObjects\O55a1WUoIYACUYKgMCIWOEMUQISIQ Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex Creates mutex: $\verb|\Sessions|1\BaseNamedObjects|\ZonesLockedCacheCounterMutex|$ Creates mutex:

Creates semaphore: \Sessions\1\BaseNamedObjects\4FBEA4B1

File System Events

Creates C:\WinOldFileq Creates: C:\WinOldFileg\

C:\WinOldFileq\83A49421850.exe Creates: C:\WinOldFileq\6C3E79A93CD5139 Creates: C:\Users\Admin\AppData\Local\Temp\ Creates:

 $C: \verb|Vsers| Admin| AppData| Local| Temp| 3MU581D.tmp|$ Creates: C:\Users\Admin\AppData\Local\Temp\3MU581D.exe Creates:

C:\Users\Admin Creates:

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

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

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

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History Creates: Opens: C:\Windows\Prefetch\SPYEYE_INJECTOR.EXE-619282B0.pf

C:\Windows Opens:

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

C:\Windows\SysWOW64 Opens:

Opens: C:\Windows\SysWOW64\apphelp.dll Opens: C:\Windows\Temp\spyeye_injector.exe C:\Windows\SysWOW64\ntdll.dll Opens: Opens: C:\Windows\SysWOW64\kernel32.dll C:\Windows\SysWOW64\KernelBase.dll Opens: C:\Windows\apppatch\sysmain.sdb Opens: Opens: C:\Windows\SysWOW64\sechost.dll C:\Windows\SysWOW64\msvcrt.dll Opens: Opens: C:\Windows\SysWOW64\bcryptprimitives.dll

Opens: C:\Windows\SysWOW64\cryptbase.dll C:\Windows\SysWOW64\sspicli.dll Opens: C:\Windows\SysWOW64\rpcrt4.dll Opens: Opens: C:\Windows\SysWOW64\advapi32.dll

Opens:

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\WinOldFileg Opens: C:\WinOldFileq\

C:\WinOldFileq\83A49421850.exe Opens:

Opens: C:\Windows\Prefetch\83A49421850.EXE-56DEA472.pf

Opens: C:\Windows\SysWOW64\msasn1.dll C:\Windows\SysWOW64\crypt32.dll Opens: Opens: C:\Windows\SysWOW64\nsi.dll Opens: C:\Windows\SysWOW64\ws2_32.dll Opens: C:\Windows\SysWOW64\iertutil.dll Opens: C:\Windows\SysWOW64\wininet.dll C:\Windows\SysWOW64\gdi32.dll Opens: Opens: C:\Windows\SysWOW64\user32.dll Opens: C:\Windows\SysWOW64\shlwapi.dll C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\SysWOW64\msctf.dll Opens: Opens: C:\Windows\SysWOW64\msimg32.dll C:\Windows\SysWOW64\combase.dll Opens: Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\SysWOW64\urlmon.dll Opens: C:\Windows\SysWOW64\oleaut32.dll

Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\WinOldFileq\6C3E79A93CD5139 Opens: C:\Users\Admin\AppData\Local\Temp\3MU581D.exe

C:\Users\Admin\AppData\Local\Temp Opens: C:\Users Opens: C:\Users\Admin

Opens: C:\Users\Admin\AppData Opens: C:\Users\Admin\AppData\Local

Opens: C:\Windows\Prefetch\3MU581D.EXE-B9DB56B9.pf

Opens: C:\Windows\SysWOW64\SHCore.dll Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\Windows\SysWOW64\profapi.dll C:\Windows\SysWOW64\secur32.dll Opens: Opens:

 $C: \verb|VISers| Admin\\| AppData\\| Roaming\\| Microsoft\\| SystemCertificates\\| My\\| AppContainer\\| UserCertRead$ Opens:

C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates

C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs Opens: Opens: Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\counters.dat

Opens:

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

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
                         C:\Windows\WindowsShell.Manifest
 Opens:
                         C:\Windows\SysWOW64\tzres.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens:
                         C:\Windows\SysWOW64\winhttp.dll
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                         C:\Windows\SysWOW64\winnsi.dll
                         C:\Windows\SysWOW64\clbcatq.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\netapi32.dll
                         C:\Windows\SysWOW64\netutils.dll
 Opens:
                         C:\Windows\SysWOW64\srvcli.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\wkscli.dll
 Opens:
                         C:\Windows\SysWOW64\nlaapi.dll
                         C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\FWPUCLNT.DLL
                         C:\Windows\SysWOW64\NapiNSP.dll
 Opens:
                         C:\Windows\SysWOW64\pnrpnsp.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\winrnr.dll
 Opens:
                         C:\Windows\SysWOW64\dhcpcsvc6.dll
                         C:\Windows\SysWOW64\dhcpcsvc.dll
 Opens:
 Opens:
                         C:\Windows\System32\Drivers\etc\hosts
                         C:\WinOldFileq\83A49421850.exe
 Writes to:
 Writes to:
                         C:\WinOldFileq\6C3E79A93CD5139
 Writes to:
                         C:\Users\Admin\AppData\Local\Temp\3MU581D.exe
 Reads from:
                         C:\Windows\SysWOW64\ntdll.dll
 Reads from:
                         C:\Windows\Temp\spyeye_injector.exe
 Reads from:
                         C:\WinOldFileq\83A49421850.exe
 Reads from:
                         C:\WinOldFileq\6C3E79A93CD5139
 Reads from:
                         C:\Users\Admin\AppData\Local\Temp\3MU581D.exe
 Reads from:
                         C:\Windows\SysWOW64\user32.dll
                         C:\Windows\SysWOW64\wininet.dll
 Reads from:
 Reads from:
                         C:\Windows\SysWOW64\ws2_32.dll
 Reads from:
                         C:\Windows\SysWOW64\advapi32.dll
                         C:\Windows\SysWOW64\crypt32.dll
 Reads from:
 Reads from:
                         C:\Windows\System32\Drivers\etc\hosts
 Deletes:
                         C:\Windows\Temp\spyeye_injector.exe
```

Network Events

DNS query:	alexeyartemov.com
DNS query:	www.microsoft.com
DNS response:	alexeyartemov.com ⇒ 198.105.244.11
DNS response:	alexeyartemov.com ⇒ 104.239.213.7
DNS response:	e10088.dspb.akamaiedge.net ⇒ 23.7.35.22
DNS response:	e10088.dspb.akamaiedge.net ⇒ 184.86.231.62
DNS response:	e10088.dspb.akamaiedge.net \Rightarrow 23.72.44.137
DNS response:	e10088.dspb.akamaiedge.net ⇒ 23.221.32.209
DNS response:	e10088.dspb.akamaiedge.net \Rightarrow 23.46.28.174
Connects to:	88.198.13.147:443
Connects to:	198.105.244.11:80
Connects to:	0.0.0.80
Connects to:	127.0.0.1:80
Connects to:	104.239.213.7:80
Sends data to:	8.8.8.8:53
Sends data to:	4.2.2.1:53
Sends data to:	88.198.13.147:443
Sends data to:	alexeyartemov.com:80 (198.105.244.11)
Sends data to:	0.0.0.0:53
Receives data from:	8.8.8.8:53
Receives data from:	4.2.2.1:53
Receives data from:	alexeyartemov.com:80 (198.105.244.11)
Receives data from:	0.0.0:53

Windows Registry Events

111114111111111111111111111111111111111		
Creates key:	HKLM\system\currentcontrolset\control\session manager	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\run</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\0</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\1</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\2</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\3</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\4</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\lockdown_zones\1		
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\lockdown_zones\2		
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\lockdown_zones\3		
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	

```
settings\lockdown_zones\4
 Creates key:
                          HKCU\software\microsoft\internet explorer\phishingfilter
 Creates key:
                          HKCU\software\microsoft\internet explorer\recovery
 Creates key:
                          HKCU\software\microsoft\systemcertificates\my
 Creates kev:
                          HKCU\software\microsoft windows
                          \label{local-observation} \begin{tabular}{l} HKCU \software \verb|\microsoft| windows \current version \end{tabular} internet \end{tabular}
 Creates key:
settings\connections
 Creates key:
                          HKLM\system\currentcontrolset\services\tcpip\parameters
 Creates key:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
 Creates key:
                          HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
 Creates key:
                          HKCU\software
                          HKCU\software\microsoft
 Creates key:
                          HKCU\software\microsoft\windows nt
 Creates key:
                          HKCU\software\microsoft\windows nt\currentversion
 Creates key:
 Creates key:
                          HKCU\software\microsoft\windows nt\currentversion\network
 Deletes value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
 Deletes value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
 Deletes value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
 Deletes value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[autodetect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Deletes value:
settings\zonemap[proxybypass]
 Deletes value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
 Deletes value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
 Deletes value:
                          HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet
settings\zonemap[intranetname]
 Opens key:
                          HKLM\software\microsoft\wow64
 Opens key:
                          HKLM\system\currentcontrolset\control\terminal server
 Opens key:
                          HKLM\system\currentcontrolset\control\safeboot\option
 Opens key:
                          HKLM\system\currentcontrolset\control\srp\gp\dll
 Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ safer \ 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 key:
                          HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
                          HKLM\software\wow6432node\policies\microsoft\mui\settings
 Opens key:
 Opens key:
                          HKLM\software\policies\microsoft\mui\settings
 Opens key:
                          HKCU\
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU\control\ panel\desktop\muicached\machinelanguageconfiguration \end{tabular}
 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:
 Opens key:
                          HKCU\control panel\desktop
 Opens kev:
                          HKCU\control panel\desktop\muicached
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side
 Opens key:
 Opens key:
                          HKLM\system\currentcontrolset\control\nls\sorting\versions
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
                          HKCU\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key:
 Opens key:
                          HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
 Opens key:
                          HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
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 key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                          HKLM\system\currentcontrolset\control\computername
 Opens kev:
 Opens key:
                          Opens key:
                          HKLM\system\setup
 Opens key:
                          HKLM\system\currentcontrolset\control\nls\extendedlocale
 Opens key:
                          HKLM\system\currentcontrolset\control\nls\sorting\ids
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\83a49421850.exe
```

Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

Opens key: Opens key:

Opens key:

HKLM\system\currentcontrolset\control\session manager\appcertdlls

HKLM\software\wow6432node\policies\microsoft\windows\appcompat

HKLM\system\currentcontrolset\control\session manager\appcompatibility

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\83a49421850.exe

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

Opens key: HKLM\

Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

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

compatibility

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

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

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

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

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

options\3mu581d.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\3mu581d.exe

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

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

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

explorer\main\featurecontrol

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

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

explorer\main\featurecontrol\feature_browser_emulation

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

settings\5.0\user agent

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

settings\5.0\user agent

Opens key: HKLM\software\wow6432node\policies

Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

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

settings\user agent

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

Settings

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

settings\user agent

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

settings\5.0\user agent\pre platform

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

settings\5.0\user agent\pre platform

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

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

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

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

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

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

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

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

 $\label{lem:continuous} Opens~key: $$ HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0 $$ Opens~key: $$ HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype $$ Opens~key: $$ Opens~key: $$ HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype $$ Opens~key: $$ Opens~$

0\certdllopenstoreprov

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

1\certdllopenstoreprov

Opens key: HKU

Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores

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

 $nt \verb|\currentversion| profile list \verb|\s-1-5-21-1923240461-1905901954-2556564120-1001| list \verb|\currentversion| profile list \verb|\s-1-5-21-1923240461-1905901954-2556564120-1001| list \verb|\s-1-5-21-1923240461-1905901954-255656564120-1001| list \verb|\s-1-5-21-19232404-25566564120-1001| list \verb|\s-1-5-21-19232404-2556664120-1001| list \verb|\s-1-5-21-19232404-2556664120-1001| list \verb|\s-1-5-21-19232404-25566564$

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

1923240461-1905901954-2556564120-1001

Opens key: HKCU\software\microsoft\systemcertificates\my
Opens key: HKCU\software\microsoft\systemcertificates\my\

Opens key: HKCU\software\microsoft\systemcertificates\my\certificates

HKCU\software\microsoft\systemcertificates\my\crls Opens key: HKCU\software\microsoft\systemcertificates\my\ctls Opens key: HKCU\software\microsoft\systemcertificates\my\keys Opens kev: HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions Opens key: 33be-4251-ba85-6007caedcf9d} Opens kev: 33be-4251-ba85-6007caedcf9d}\propertybag Opens key: HKCU\software\microsoft\windows\currentversion\explorer Opens key: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following \ description \ for the context of the context of$ Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current \vee explorer \setminus session in follows \cap the following of the fol$ Opens key: HKU\.default Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist HKCU\software\microsoft\windows\currentversion\explorer\user shell Opens kev: folders Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side \ assembly storage roots$ HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_http_username_password_disable Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset HKCU\software\microsoft\internet Opens key: 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: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet$ explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611 HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature bufferbreaking 818408 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954 Opens key: HKLM\software\wow6432node\microsoft\internet 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 HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274

Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb91027
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                       HKLM\software\wow6432node\microsoft\internet
 Opens 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
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                       HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                       HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
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
 Opens key:
                       HKCU\software\microsoft\windows\currentversion\internet settings
 Opens kev:
                       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 \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings
                       HKLM\system\currentcontrolset\control\cmf\config
 Opens key:
 Opens key:
                       HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens key:
                       HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ 5.0 \ cache
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
 Opens key:
                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens kev:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                       HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
 Opens kev:
                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
 Opens kev:
                       HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
                       HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2e7a8a54
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 Opens key:
Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010

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

Opens kev:

Opens key:

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: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 00000000000001) \ (catalog_entries \ name space_catalog 5) \ (catalog_entries$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006 Opens key: HKLM\system\currentcontrolset\services\winsock\parameters HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip Opens key: HKLM\software\policies\microsoft\peerdist\service Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\service HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\content Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer Opens key: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer Opens key: 6fba-4fcf-9d55-7b8e7f157091} Opens key: 6fba-4fcf-9d55-7b8e7f157091}\propertybag Opens kev: 0e22-4760-9afe-ea3317b67173} Opens key: 0e22-4760-9afe-ea3317b67173}\propertybag Opens kev: HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\cookies Opens key: c0e9-4171-908e-08a611b84ff6} Opens key: c0e9-4171-908e-08a611b84ff6}\propertybag Opens key: $HKLM \label{lem:hklm} Which was the statement of the st$ 65f9-4cf6-a03a-e3ef65729f3d} Opens key: 65f9-4cf6-a03a-e3ef65729f3d}\propertybag HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache\history Opens key: b784-432e-a781-5a1130a75963} Opens kev: b784-432e-a781-5a1130a75963}\propertybag Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions HKLM\software\microsoft\rpc\extensions Opens key: Opens key: HKCU\software\classes\ Opens key: HKLM\software\microsoft\com3 HKLM\software\microsoft\windowsruntime\clsid Opens key: Opens key: $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{00000323-0000-0000-c000-c000-c000-c000-c000-c000-c0000-c00-c000-c000-c000-c000-c00-c000-c000-c000-c0$ 000000000046} Opens key: HKCR\activatableclasses\clsid

Opens key: HKCR\activatableclasses\clsid\{00000323-0000-0000-c000-00000000046} HKLM\software\wow6432node\microsoft\oleaut Opens kev: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00000323-0000-0000-c000-c000-c00-c000-c000-c00-c00-c000-c000-c000-c00-$ Opens key: 000000000046} Opens key: HKCR\wow6432node\clsid\{00000323-0000-0000-c000-00000000046} $\label{local-observation} HKCU \setminus software \setminus classes \setminus clsid \setminus \{00000323-0000-0000-c000-000000000046\}$ Opens key: Opens key: HKCR\clsid\{00000323-0000-0000-c000-00000000046} HKCU\software\classes\activatableclasses\clsid Opens kev:

Opens key:

```
000000000046}
                          HKCU\software\classes\appid\3mu581d.exe
 Opens key:
                          HKCR\appid\3mu581d.exe
 Opens key:
                          HKLM\software\wow6432node\microsoft\ole\appcompat
 Opens key:
 Opens kev:
                          HKLM\software\microsoft\ole\appcompat
 Opens key:
provider
```

 $HKLM \label{lem:hklm} White the latest and the la$

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

Opens key: HKLM\software\microsoft\cryptography

Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload

Opens key:

000000000046}

HKCR\wow6432node\interface\{00000134-0000-0000-c000-00000000046} Opens key: Opens key:

00000000046}\proxystubclsid32

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

000000000046}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-

4f27df8760d0}

Opens key: $HKCR \setminus \{a168aadc-1674-49da-ad4f-4f27df8760d0\}$ Opens key: HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-

4f27df8760d0}\proxystubclsid32

HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-Opens key:

4f27df8760d0}\proxystubclsid32

HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-Opens key:

60ce2149e33c}

Opens key: HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens kev:

60ce2149e33c}

Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-

60ce2149e33c}\treatas

Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens key:

60ce2149e33c}\inprocserver32

HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens kev:

60ce2149e33c}\inprocserver32

Opens key:

60ce2149e33c}\inprochandler32

HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens key:

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: $HKLM \setminus system \setminus current control \setminus sqmservice list$ Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient Opens kev:

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

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

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

nt\dnsclient\dnspolicyconfig

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

Opens key:

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

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

settings\winhttp

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

Opens key:

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

. HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

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

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

Opens key:

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

settings\zonemap\domains\

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

Opens key:

HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\domains\

Opens key: HKLM\zonemap\ranges\ Opens key: HKCU\zonemap\ranges\

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

Opens kev:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$

settings\zonemap

Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$

settings\zonemap Opens kev: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\protocoldefaults\ Opens key: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\zonemap\domains\ HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key: settings\zonemap\domains\ Opens key: HKLM\software\policies\microsoft\internet explorer\security Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 Opens kev: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\ Opens kev: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0 $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\zones\0 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1 HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\1 HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\1 HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ Opens kev: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2 HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\2 $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\zones\2 Opens kev: HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\3 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\3 Opens kev: HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\4 HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\4 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature_localmachine_lockdown Opens key: $HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet$ settings\lockdown_zones\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\ HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\0 Opens kev: $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| current version\\| internet$ settings\lockdown_zones\0 HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev:

settings\lockdown_zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet

```
settings\lockdown_zones\1
   Opens kev:
settings\lockdown_zones\1
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\1
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown zones\1
                                                \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Opens key:
settings\lockdown_zones\2
   Opens kev:
settings\lockdown_zones\2
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
   Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\2
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
   Opens key:
settings\lockdown_zones\3
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\3
  Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                                HKCU\software\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
   Opens kev:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\4
                                               HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\4
   Opens key:
                                               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                                HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                               HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                               HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
                                               HKLM\software\wow6432node\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_zone_elevation
                                                HKLM\software\wow6432node\policies\microsoft\system\dnsclient
   Opens kev:
                                                HKLM\software\policies\microsoft\system\dnsclient
   Opens key:
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
   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 \ 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}
   Opens kev:
25b8d56dd1d83
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
   Opens key:
HKLM \ system \ current controls et \ services \ typip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4c6-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-
55779daa70e9}
                                                HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens kev:
   Queries value:
                                                HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Queries value:
                                                HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Queries value:
                                                HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
   Queries value:
                                               HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
   Queries value:
                                                HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
   Queries value:
                                                HKCU\control panel\desktop[preferreduilanguages]
                                                HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Oueries value:
   Oueries value:
Queries value:
                                                HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                                                HKCU\software\microsoft\windows
   Oueries value:
```

nt\currentversion\appcompatflags[showdebuginfo]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[usefilter]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[spyeye_injector.exe]

Oueries value: HKLM\svstem\currentcontrolset\control\lsa\fipsalgorithmpolicv[enabled]

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

Oueries value:

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

Queries value: HKLM\system\setup[oobeinprogress]

Queries value: HKLM\system\setup[systemsetupinprogress]

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

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

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

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[83a49421850.exe]

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

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

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

nt\currentversion\compatibility32[83a49421850]

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

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKLM\system\currentcontrolset\control\session

manager[pendingfilerenameoperations2]

Queries value: HKLM\system\currentcontrolset\control\session

manager[pendingfilerenameoperations]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[3mu581d.exe]

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

nt\currentversion\compatibility32[3mu581d]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer[version] Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[security_hklm_only]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[3mu581d.exe] Queries value: HKLM\software\wow6432node\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature_browser_emulation[*]|$

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

settings\5.0\user agent[]
 Queries value:

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\user agent[]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]

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

settings\5.0\user agent[compatible]

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

nt\currentversion\compatibility32[spyeye_injector]

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

settings\5.0\user agent[version]

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

settings\5.0\user agent[version]
Oueries value: HKCII\so

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

settings\5.0\user agent[platform]

settings\5.0\user agent[platform]

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

Queries value: HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc]

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

Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1923240461-1905901954-2556564120-1001[profileimagepath]

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

settings[syncmode5]

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

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

Queries value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{352481e8-microsoft \setminus windows \setminus explorer \setminus folder \}$

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-

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

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

Oueries value

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [parsing name]$

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [stream resource type]$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [publish \ expanded \ path]$

Queries value:

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

Queries value: |KLM\software

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

Queries value:

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

Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders[cache]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cache]

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

settings[mbcsapiforcrack]

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

 $explorer \verb|\main| featurecontrol| feature_http_username_password_disable[3mu581d.exe]|$

Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]

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

explorer\main\featurecontrol[feature_clientauthcertfilter]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[3mu581d.exe] Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling[*]

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

explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[3mu581d.exe]

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

explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[fromcachetimeout]

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

settings[secureprotocols]

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

settings[secureprotocols]

```
Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablekeepalive]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[preconnectlimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[preresolvelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sqmhttpstreamrandomuploadpoolsize]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[cachemode]
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[enablehttp1_1]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttp1_1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttp1_1]
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablenegotiate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablebasicoverclearchannel]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[clientauthbuiltinui]
 Oueries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[displayscriptdownloadfailureui]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
 Queries value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings[utf8servernameres]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketreceivebufferlength]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
 Queries value:
                          HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[maxconnectionsper1 Oserver]
 Queries value:
                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[maxconnectionsperproxy]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
 Queries value:
                          HKLM\system\currentcontrolset\control\cmf\config[system]
                          HKLM\software\wow6432node\microsoft\windows\windows error
 Oueries value:
reporting\wmr[disable]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
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]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
```

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[receivetimeout] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[receivetimeout] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[disablentlmpreauth] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[scavengecachelowerbound] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[certcachenovalidate] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache[scavengecachefilelifetime] HKCU\software\policies\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache[scavengecachefilelimit] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache[scavengecachefilelimit] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache[scavengecachefilelimit] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[httpdefaultexpirytimesecs] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[ftpdefaultexpirytimesecs] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablecachingofsslpages] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[leashlegacycookies] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[dialupuselansettings] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[dialupuselansettings] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[sendextracrlf] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[wpadsearchalldomains] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[bypasshttpnocachecheck] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypasssslnocachecheck] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[bypasssslnocachecheck] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[enablehttptrace] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[nocheckautodialoverride] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[nocheckautodialoverride] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing] Oueries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[sharecredswithwinhttp] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[mimeexclusionlistforcache] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[headerexclusionlistforcache] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscacheenabled] HKCU\software\microsoft\windows\currentversion\internet Queries 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 Queries value: settings[warnalwaysonpost] 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[warnonzonecrossing] Queries value: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}$ settings[warnonbadcertrecving] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[warnonpostredirect] 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[alwaysdrainonredirect] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[warnonhttpstohttpredirect] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[tcpautotuning] Queries value:

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

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 - Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[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\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Queries value:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
- Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]
- Queries 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
- 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]
- 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\00000000003[displaystring] Queries value:
- $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ value:$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000003 \ [address family] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]

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\0000000000004[displaystring]
Oueries value:

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

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

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[enabled]
Queries value:

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

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

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

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

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

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

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

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

 $\label{lem:hklmsystem} HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog \ \ catalog_entries \ 00000000000006 \ [enabled] \ Queries \ value:$

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[storesserviceclassinfo]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006[providerinfo]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32numhandlebuckets]

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

Queries value: settings[enableautodial]

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

settings[nonetautodial]

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

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

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

Queries value:

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

Queries value:

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

settings[globaluseroffline]

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

settings[disablebranchcache]

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

settings[usefirstavailable]

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

settings[combinefalsestartdata] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[disablefalsestartblacklist] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enforcep3pvalidity] Queries value: HKLM\software\microsoft\windows nt\currentversion\peerdist\service[enable] Oueries 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[usedelavedacceptance] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyenable] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyserver] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyoverride] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autoconfigurl] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autodetect] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\connections[savedlegacysettings] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\connections[defaultconnectionsettings] Queries value: 6fba-4fcf-9d55-7b8e7f157091}[category] Oueries value: 6fba-4fcf-9d55-7b8e7f157091}[name] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}[parentfolder] Oueries value: 6fba-4fcf-9d55-7b8e7f157091}[description] Queries value: 6fba-4fcf-9d55-7b8e7f157091}[relativepath] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785-b2786, \ b2786, \ b2$ 6fba-4fcf-9d55-7b8e7f157091}[parsingname] Oueries value: 6fba-4fcf-9d55-7b8e7f157091}[infotip] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785-b2786, \ b2786, \ b2$ 6fba-4fcf-9d55-7b8e7f157091}[localizedname] Oueries value: 6fba-4fcf-9d55-7b8e7f157091}[icon] Queries value: 6fba-4fcf-9d55-7b8e7f157091}[security] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}[streamresource] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ f 1b32785 - the constant \ f 1b32785 - the co$ 6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \ ff 1b 32785-1b 32785-1b$ 6fba-4fcf-9d55-7b8e7f157091}[localredirectonly] Oueries value: 6fba-4fcf-9d55-7b8e7f157091}[roamable] Oueries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \ ff 1b 32785-1b 32785-1b$

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ \ f1b32785-b1278$

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785-b27874, \ b27874, \$

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

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

Oueries value:

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

folders[local appdata]

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} White the latest and the la$ 0e22-4760-9afe-ea3317b67173}[publishexpandedpath]

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} White the latest and the la$ 0e22-4760-9afe-ea3317b67173}[foldertypeid]

Oueries value:

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

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

settings\5.0\cache\content[cachelimit]

Queries value:

c0e9-4171-908e-08a611b84ff6}[category]

c0e9-4171-908e-08a611b84ff6}[name]

Queries value:

c0e9-4171-908e-08a611b84ff6}[parentfolder]

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

Oueries value

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\coe9-4171-908e-08a611b84ff6\[\coe9-4171-908e-08a611b84ff6\]\[\coe9-4171-908e-08a611$

Oueries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]$

Queries value:

 $\label{local_HKLM} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \coe9-4171-90$

Queries value:

 $\label{local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\explorer\folderdescriptions\currentversion\explorer\explor$

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \cosetware \$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

folders[cookies]

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\folderdes\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdescriptions\cdots\folderdes\cdots\folderdescriptions\cdots\folderdes\cd$

Oueries value

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cite{2.0} \end{constraints} \begin{center} \begin{center} Albert Albert$

Queries value:

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

Queries value:

Queries value

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cite{2.0} \end{constraints} $$Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cite{2.0} \end{constraints} $$4565729f3d\cite{2.0} \end{constraints} $$1665729f3d\cite{2.0} \end{constraints}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cite{2.0} \end{constraints} $$Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cite{2.0} \end{constraints} $$4565729f3d\cite{2.0} \cite{2.0} \end{constraints} $$1665729f3d\cite{2.0} \cite{2.0} \$

Queries value:

Queries value:

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

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

Oueries value

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[appdata]

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

settings\5.0\cache\cookies[cachelimit]

Queries value:

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

Queries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]

Queries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}\[parsing name]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[infotip]} \\$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder a3b-b784-432e-a781-5a1130a75963\folder are source\folder as a finite source\folder and the source of the source$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[localredirectonly]}$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

```
b784-432e-a781-5a1130a75963}[publishexpandedpath]
  Oueries value:
b784-432e-a781-5a1130a75963}[attributes]
  Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-d12b, d12b, d24b, d
b784-432e-a781-5a1130a75963}[foldertypeid]
  Oueries value:
b784-432e-a781-5a1130a75963}[initfolderhandler]
  Queries value:
                                  HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\history[cachelimit]
                                  HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                                  HKLM\software\microsoft\com3[com+enabled]
  Oueries value:
  Queries value:
                                  HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:
                                  HKLM\software\microsoft\ole[defaultaccesspermission]
                                  HKLM \verb|\system| current control \verb|\sa[everyone includes an ony mous]|
  Oueries value:
  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 \backslash software \backslash policies \backslash microsoft \backslash cryptography [privkey cachepurge interval seconds]
                                  HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:
                                  HKLM\software\microsoft\cryptography[machineguid]
  Oueries value:
  Queries value:
                                  HKCR\wow6432node\interface\{00000134-0000-0000-c000-
00000000046}\proxystubclsid32[]
  Queries value:
                                  HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32[]
                                  HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]
  Queries value:
                                  HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
  Oueries value:
60ce2149e33c}\inprocserver32[inprocserver32]
                                  HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
  Queries value:
60ce2149e33c}\inprocserver32[]
  Queries value:
                                  HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32[threadingmodel]
                                  HKLM\software\microsoft\ole[maxsxshashcount]
  Oueries value:
  Queries value:
                                  HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
                                  HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [screen badtlds]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                                  HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Oueries value:
  Oueries value:
```

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\svstem\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn] Oueries 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] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: Queries value: $HKLM \ system \ current control set \ services \ dns cache \ parameters \ [register reverse lookup]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazv] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Queries 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] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]

 $\label{lem:hklm} \mbox{HKLM} \mbox{$\tt MKLM} \mbox{$\tt MKLM} \mbox{$\tt System} \mbox{$\tt Current} \mbox{$

Queries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
  Oueries 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]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[dnsquickquervtimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
                                     \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
  Queries value:
settings[autoproxydetecttype]
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings\winhttp[disablebranchcache]
  Queries value:
HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[winhttplowercasehost]
                                     HKLM\software\policies\microsoft\internet
  Queries value:
explorer\security[disablesecuritysettingscheck]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\0[flags]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\1[flags]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\2[flags]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\3[flags]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\4[flags]
                                     HKCU\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[3mu581d.exe]
                                     HKCU\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature localmachine lockdown[*1
  Queries value:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown[3mu581d.exe]
                                     HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[createuricachesize]
  Queries value:
                                     settings[createuricachesize]
  Queries value:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
  Oueries value:
settings[enablepunycode]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunycode]
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\zonemap[autodetect]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\3[1a10]
  Oueries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
  Queries value:
                                     HKLM\system\currentcontrolset\services\winsock2\parameters[autodiald1]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[3mu581d.exe]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature zone elevation[*]
                                     HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Oueries value:
  Queries value:
                                     HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:
HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40544401-87b7-40544401-87b7-40544401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-875
55779daa70e9}[searchlist]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
  Queries value:
55779daa70e9}[registrationenabled]
```

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-4dc1-87b7-$ 55779daa70e9}[registeradaptername]

55779daa70e9}[domain]

Oueries value:

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

Oueries value:

55779daa70e9}[dhcpv6domain]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]

Queries value:

55779daa70e9}[nameserver]

Queries value:

55779daa70e9}[dhcpnameserver]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

Sets/Creates value: HKLM\system\currentcontrolset\control\session

manager[pendingfilerenameoperations]

Sets/Creates value:

HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fuvux1d7fenotdr]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings[warnonintranet]

HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\zones\0[1409] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1609] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\zones\0[1406] Sets/Creates value: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+$ settings\lockdown zones\1[1406] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2[1406] HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\lockdown_zones\3[1406] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4[1406] Sets/Creates value: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8] Sets/Creates value: HKCU\software\microsoft\internet explorer\phishingfilter[shownservicedownballoon] Sets/Creates value: HKCU\software\microsoft\internet explorer\recovery[clearbrowsinghistoryonexit] $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ Sets/Creates value: settings[globaluseroffline] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings[warnonpost] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings[warnonpostredirect] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1409] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\1[1609] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1406] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\2[1409] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\2[1609] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\2[1406] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\3[1409] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\3[1609] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1406] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1409] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1609] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zones\4[1406] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings[proxyenable] Value changes: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+$ settings\connections[savedlegacysettings] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\5.0\cache\cookies[cacheprefix] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cacheprefix] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zonemap[uncasintranet] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings\zonemap[autodetect] HKCU\software\microsoft\windows\currentversion\internet Value changes: settings[globaluseroffline]