Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 15, Task ID: 39

Task ID: Risk Level: 10

Date Processed: 2016-03-29 05:50:03 (UTC)

Processing Time: 60.0 seconds Virtual Environment: IntelliVM

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

Sample ID: 15 Type: basic Owner: admin

spyeye%inj%ector%.exe Label: 2016-03-29 05:50:03 (UTC) Date Added:

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

b98bb6d7428c3dbffcfcab2414c6daa2 MD5:

fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029 SHA256:

Description: None

Pattern Matching Results

Modifies registry autorun entries

- Writes to memory of system processes
- 10 Suspicious writeprocess: Spyeye [Banking]
- 5 Abnormal sleep detected
- 2 PE: Nonstandard section
- 4 Reads process memory
- 5 PE: Contains compressed section
- 6 Renames file on boot
- 5 Packer: UPX
- 5 Adds autostart object
- 10 Creates malicious mutex: Spyeye [Banking]

Static Events

Anomaly: PE: Contains a virtual section Anomaly: PE: Contains one or more non-standard sections Packer:

Process/Thread Events

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

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

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

Creates process: C:\Users\Admin\AppData\Local\Temp\o971A35.exe

["C:\Users\Admin\AppData\Local\Temp\o971A35.exe"] Reads from process: PID:1148 C:\Windows\explorer.exe

Reads from process: PID:412 C:\Windows\System32\wininit.exe Reads from process: PID:448 C:\Windows\System32\winlogon.exe PID:504 C:\Windows\System32\lsass.exe Reads from process: Reads from process: PID:596 C:\Windows\System32\svchost.exe PID:632 C:\Windows\System32\svchost.exe Reads from process: PID:712 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:732 C:\Windows\System32\dwm.exe Reads from process: PID:800 C:\Windows\System32\svchost.exe PID:856 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:900 C:\Windows\System32\svchost.exe Reads from process: PID:360 C:\Windows\System32\spoolsv.exe PID:556 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:344 C:\Windows\System32\svchost.exe Reads from process: PID:1436 C:\Windows\System32\svchost.exe Reads from process: PID:1996 C:\Windows\System32\taskhostex.exe Reads from process: PID:1340 C:\Windows\System32\svchost.exe Reads from process: PID:2068 C:\Windows\System32\dllhost.exe Reads from process: PID:2080 C:\Windows\System32\wbem\unsecapp.exe Reads from process: PID:3056 C:\Windows\System32\wbem\WmiPrvSE.exe Reads from process: PID:764 C:\Windows\System32\conhost.exe Writes to process:

PID:2436 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe

Writes to process: PID:652 C:\Users\Admin\AppData\Local\Temp\o971A35.exe

Writes to process: PID:292 C:\Windows\Temp\spyeye_inj_ector_.exe PID:764 C:\Windows\System32\conhost.exe Writes to process:

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

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex	
Creates mutex:	\BaseNamedObjects\RPCController	
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW 00000000	
Creates mutex:	\BaseNamedObjects\5U7M5C7E9C9Y1U3A9A7A1S3U7I7Y97K	

Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex \Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex

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

File System Events

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

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

Creates: C:\Users\Admin\AppData\Local\Temp\0971A35.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\0971A35.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
Opens: C:\Windows\Prefetch\SPYEYE_INJ_ECTOR_.EXE-76AA8D3E.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\SysWOW64\bcryptprimitives.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\spicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\advapi32.dll

Opens: C:

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

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

Opens: C:\WinOldFileq\83A49421850.exe

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 Opens: C:\Windows\SysWOW64\gdi32.dll C:\Windows\SysWOW64\user32.dll Opens: C:\Windows\SysWOW64\shlwapi.dll Opens: Opens: C:\Windows\SysWOW64\imm32.dll C:\Windows\SysWOW64\msctf.dll Opens: Opens: C:\Windows\SysWOW64\msimg32.dll Opens: C:\Windows\SysWOW64\combase.dll C:\Windows\SysWOW64\ole32.dll Opens: Opens: C:\Windows\SysWOW64\urlmon.dll

C:\Windows\SysWOW64\oleaut32.dll

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

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

Opens: C:\Windows\Prefetch\0971A35.EXE-1EB0C7C3.pf

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

 ${\tt Files \ } counters. dat$

Opens:

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

controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985

 $Opens: C: \windows \winSxS \x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985 \comctl32.dl1$

Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\SysWOW64\winhttp.dll
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens:

 ${\tt C: \V Sers \Admin \App Data \Roaming \Microsoft \System Certificates \My \App Container \User \Cert \Read}$

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

C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs Opens: Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs

Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL C:\Windows\SysWOW64\winnsi.dll Opens: Opens: C:\windows\temp\spyeye_inj_ector_.exe C:\Windows\SysWOW64\clbcatq.dll Opens: C:\Windows\SysWOW64\cryptsp.dll Opens: Opens: C:\Windows\SysWOW64\rsaenh.dll Opens: C:\Windows\SysWOW64\dnsapi.dll Opens: C:\Windows\SysWOW64\NapiNSP.dll C:\Windows\SysWOW64\pnrpnsp.dll Opens: Opens: C:\Windows\SysWOW64\nlaapi.dll C:\Windows\SysWOW64\winrnr.dll Opens: Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll Opens: C:\Windows\SysWOW64\dhcpcsvc.dll Opens: C:\Windows\System32\Drivers\etc\hosts Opens: C:\Windows\SysWOW64\rasadhlp.dll Writes to: C:\WinOldFileq\83A49421850.exe Writes to: C:\WinOldFileq\6C3E79A93CD5139

C:\Users\Admin\AppData\Local\Temp\o971A35.exe Writes to:

Reads from: C:\Windows\SysWOW64\ntdll.dll

Reads from: C:\Windows\Temp\spyeye_inj_ector_.exe C:\WinOldFileq\83A49421850.exe Reads from:

Reads from: C:\WinOldFileq\6C3E79A93CD5139

Reads from: C:\Users\Admin\AppData\Local\Temp\o971A35.exe

C:\Windows\SysWOW64\user32.dll Reads from: Reads from: C:\Windows\SysWOW64\wininet.dll Reads from: C:\Windows\SysWOW64\ws2_32.dll Reads from: C:\Windows\SysWOW64\advapi32.dll Reads from: C:\Windows\SysWOW64\crypt32.dll Reads from: C:\Windows\System32\Drivers\etc\hosts Deletes: C:\Windows\Temp\spyeye_inj_ector_.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 \Rightarrow 23.221.10.57 e10088.dspb.akamaiedge.net ⇒ 184.86.231.62 DNS response: DNS response: e10088.dspb.akamaiedge.net ⇒ 104.118.236.194

Connects to: 88.198.13.147:443 Connects to: 8.8.8.8:53 Connects to: 4.2.2.1:53 Connects to: 104.239.213.7:80 Sends data to: 8.8.8.8:53 88.198.13.147:443 Sends data to: Sends data to: 4.2.2.1:53 Receives data from: 8.8.8.8:53 Receives data from: 88.198.13.147:443 Receives data from: 4.2.2.1:53

Windows Registry Events

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:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\1		
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:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\4		
Creates key:	HKCU\software\microsoft\windows\currentversion\internet		
settings\lockdown_zones\1			
Creates key:	HKCII\software\microsoft\windows\currentyersion\internet		

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

settings\lockdown_zones\2

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

settings\lockdown_zones\3

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

settings\lockdown_zones\4

Creates key: HKCU\software\microsoft\internet explorer\phishingfilter HKCU\software\microsoft\internet explorer\recovery Creates key: Creates key: HKCU\software\microsoft\systemcertificates\my

Creates key: HKCU\software\microsoft windows

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

settings\connections

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

settings\zonemap\

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]

 $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$ Deletes value:

settings[autodetect]

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

settings\zonemap[proxybypass]

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet$ Deletes value:

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet$ Deletes value:

settings\zonemap[intranetname]

Opens key: HKLM\software\microsoft\wow64

Opens key: HKI M\system\currentcontrolset\control\terminal server Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

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

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

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

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

Opens key:

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

 $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\windows}\ nt\current\version\app\compatflags}$ Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation

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

execution options

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

options

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

options\dllnxoptions

HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy Opens key:

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

Opens key:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration Opens key: HKLM\system\currentcontrolset\control\computername

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

Opens key: HKLM\system\setup

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids

 $\label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hichare}$\mbox{$\mbox{microsoft}\mbox{$\mbox{windows}$ nt}$\currentversion} \mbox{$\mbox{image}$ file execution} \mbox{$$\mbox{\mbox Opens key:

options\83a49421850.exe

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

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

Opens key: HKLM\software\policies\microsoft\windows\appcompat $\label{lem:hkcu} \verb+KKCU\+ software \verb+\microsoft\+ windows \verb+\currentversion\+ explorer \verb+\shell folders+ \\$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers

HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

HKLM\software\microsoft\windows Opens key: nt\currentversion\appcompatflags\custom\83a49421850.exe

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

Opens key:

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:

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

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

Opens key: HKLM\software\microsoft\ole

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

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

options\o971a35.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\o971a35.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\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol

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

explorer\main\featurecontrol

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

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

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

explorer\main\featurecontrol\feature_browser_emulation

Opens key: $\mbox{HKCU\software\mbox{\swindows\currentversion\internet}}$

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

nt\currentversion\appcompatflags

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

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

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: $\label{lem:hklmlsoftware\wow6432node\microsoft\windows\tablet\ pc\mbox{\colored}$

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

settings\5.0\user agent\post platform

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

 ${\tt settings \ 1.0 \ laser \ agent \ post \ platform}$

Opens key: ${\tt HKLM\system\currentcontrolset\control\cmf\config}$

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

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

Opens key: HKLM\software\microsoft\rpc

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

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

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

settings\5.0\cache

Opens key:

 $\label{lem:hklm} \verb+KLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions$

Opens key:

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

Opens key:

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

33be-4251-ba85-6007caedcf9d}\propertybag

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

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

Opens key:

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

Opens key: HKU\

Opens key: HKU\.default

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

shell folders

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

 $\verb|nt\current| version \verb|\profile| list$

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

folders Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

Opens key: HKCU\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature_http_username_password_disable| \\$

```
HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature http username password disable
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_handling
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_handling
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature bufferbreaking 818408
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
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
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature disallow null in response headers
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature digest no extras in uri
                         HKLM \verb|\software\\| wow 6432 node \verb|\microsoft\\| internet
 Opens kev:
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
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 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
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature preserve spaces in filenames kb952730
                         \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \ \ \mbox{\tt settings}
 Opens key:
                         HKLM\software\wow6432node\policies\microsoft\internet explorer
 Opens kev:
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer
 Opens key:
                         HKLM\software\wow6432node\policies\microsoft\internet explorer\main
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\main
 Opens key:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
```

settings

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

settings\5.0\cache

Opens key:

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

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

settings\5.0\cache

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

settings\5.0\cache

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266 HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543

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

explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature sch send aux record kb 2618444

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

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

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\15b8b2fb

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens kev:

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

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001

Opens key:

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

Opens kev:

Opens kev:

Opens kev:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key:

Opens kev:

Opens kev:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014 Opens kev:

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

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005 Opens key:

Opens key:

HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0 Opens kev: Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

0\certdllopenstoreprov

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

0\certdllopenstoreprov\#16

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

0\certdllopenstoreprov\ldap

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1 Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

1\certdllopenstoreprov

HKCU\software\microsoft\systemcertificates\my\physicalstores Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock\parameters Opens kev: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

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

migration\providers\tcpip

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

nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001

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\

 $Opens\;key: \\ \qquad \qquad \mathsf{HKCU} \\ software \\ \mathsf{microsoft} \\ systemcertificates \\ \mathsf{my} \\ \mathsf{certificates} \\$

Opens key: HKCU\software\microsoft\systemcertificates\my\crls
Opens key: HKCU\software\microsoft\systemcertificates\my\ctls
Opens key: HKCU\software\microsoft\systemcertificates\my\keys
Opens key: HKLM\software\policies\microsoft\peerdist\service

Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\service Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock

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

migration\providers\tcpip6

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

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:

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

Opens key:

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

Opens key:

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

Opens key:

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

Opens key:

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

settings\5.0\cache\cookies

Opens key:

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

Opens key

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

Opens key

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

Opens key:

 $\label{lem:hklmsoftware} HKLM software \wow 6432 node \windows \current version \explorer \folder descriptions \calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \property bag$

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

 $\verb|settings\5.0| cache \verb|history| \\$

Opens key:

 $\label{lem:hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \eqref{d9dc8a3b-b784-432e-a781-5a1130a75963}$

Opens key:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\property bag$

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

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

Opens key: HKCU\software\classes\
Opens key: HKLM\software\microsoft\com3

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

Opens key: HKLM\software\microsoft\windowsruntime\clsid\{00000323-0000-0000-c000-

000000000046}

Opens key: HKCR\activatableclasses\clsid

Opens key: HKCR\activatableclasses\clsid\{00000323-0000-0000-c000-000000000046}

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

Opens key: HKCU\software\classes\wow6432node\clsid\{00000323-0000-0000-c000-

00000000046}

Opens key: HKCR\wow6432node\clsid\{00000323-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\clsid\{00000323-0000-0000-c000-00000000046}

Opens key: HKCR\clsid\{00000323-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\activatableclasses\clsid

Opens key: HKCU\software\classes\activatableclasses\clsid\{00000323-0000-0000-c000-

000000000046}

Opens key: HKCU\software\classes\appid\o971a35.exe

Opens key: HKCR\appid\o971a35.exe

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

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

Opens key:

 $\label{lem:hklmlsoftware} HKLM \ software \ \ cryptography \ \ defaults \ \ provider \ \ \ cryptographic provider$

Opens key: HKLM\software\policies\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-00000000046} $\label{local-eq:hkcr-wow6432} \begin{tabular}{ll} HKCR\wow6432 node\interface \ \{00000134-0000-0000-c000-0000000000046\} \end{tabular}$ Opens key: $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{00000134-0000-0000-c000-c000-c000-c0000-c00-c000-c000-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c000-c00-$ Opens key: 000000000046}\proxystubclsid32 HKCR\wow6432node\interface\{00000134-0000-0000-c000-Opens key: 00000000046}\proxystubclsid32 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{a168 \\ aadc-1674-49 \\ da-ad4f-1674-49 \\ d$ Opens kev: 4f27df8760d0} Opens key: $HKCR \setminus wow 6432 \\ node \setminus interface \setminus \{a168 \\ aadc-1674-49 \\ da-ad4f-4f27 \\ df8760 \\ d0\}$ $\label{local-condition} HKCU \software \classes \wow 6432 node \interface \ \{a168 aadc-1674-49 da-ad4f-168 aadc-1674-49 da-ad4f-168 aadc-168 aacc-168 aacc$ Opens key: 4f27df8760d0}\proxystubclsid32 HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-Opens key: 4f27df8760d0}\proxystubclsid32 Opens key: 60ce2149e33c} Opens key: HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32 HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens kev: 60ce2149e33c}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens kev: 60ce2149e33c}\inprochandler32 HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens key: 60ce2149e33c}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens key: 60ce2149e33c}\inprochandler HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-Opens kev: 60ce2149e33c}\inprochandler HKLM\system\currentcontrolset\control\sqmservicelist Opens key: Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient Opens key: Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: HKLM\system\currentcontrolset\services\dns $HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\|$ Opens key: nt\dnsclient\dnspolicyconfig HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig Opens key: Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens kev: 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 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet$ settings\zonemap\domains\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ Opens key: settings\zonemap\domains\ HKLM\zonemap\ranges\ Opens key: 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 $explorer \verb|\main| featurecontrol| feature_zones_check_zonemap_policy_kb941001$ Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap Opens key: $\label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\currenters$

```
settings\zonemap\ranges\
                                                          HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\protocoldefaults\
    Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
    Opens key:
                                                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                                         HKLM\software\policies\microsoft\internet explorer\security
    Opens key:
    Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\
    Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
                                                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
    Opens key:
    Opens key:
                                                          \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sl} \\ 2
    Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
    Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
    Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
    Opens kev:
                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
   Opens key:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
    Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
settings\zones\0
   Opens key:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
    Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet settings \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet settings \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus internet settings \setminus software \setminus wow 6432 \\ node \setminus policies \setminus microsoft \setminus windows \setminus current \\ version \setminus microsoft \setminus microsoft \setminus windows \setminus current \\ version \setminus microsoft \setminus micro
    Opens key:
                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\1
                                                          HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\zonemap\
    Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\2
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens key:
settings\zones\2
    Opens key:
HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\3
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens key:
settings\zones\3
    Opens key:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ vones \ 4432 node \ 4432 node \ vones \ 4432 node \ 4432 n
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
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
   Opens key:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
    Opens key:
settings\lockdown_zones\
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens key:
settings\lockdown_zones
   Opens key:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                          HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\
                                                          HKCU\software\microsoft\windows\currentversion\internet
    Opens kev:
settings\lockdown_zones\0
    Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\0
    Opens key:
                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                                         HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\0
   Opens key:
                                                         \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\lockdown_zones\1
    Opens key:
settings\lockdown_zones\1
   Opens key:
                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
   Opens key:
                                                         \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\1
```

```
Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
   Opens key:
HKLM \verb|\software\\| wow 6432 node \verb|\policies\\| microsoft\\| windows\\| current version\\| internet
settings\lockdown_zones\2
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\lockdown_zones\2
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                                  \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Opens kev:
settings\lockdown_zones\3
   Opens key:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
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\software\wow6432node\policies\microsoft\system\dnsclient
   Opens key:
   Opens key:
                                                  HKLM\software\policies\microsoft\system\dnsclient
   Opens key:
HKLM \ system \ current controls et \ services \ tcpip \ (parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-4054401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-4054001-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7-405401-87b7
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:
806e6f6e6963}
   Opens key:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{a04231f6-42eb-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-4732-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472-b850-472
25b8d56dd1d8}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
   Opens key:
                                                  HKLM\system\currentcontrolset\services\tcpip\linkage
   Queries value:
                                                  HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
                                                  HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Oueries value:
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                                 HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
   Queries value:
                                                  HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
   Oueries value:
                                                  HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
                                                  HKCU\control panel\desktop[preferreduilanguages]
   Oueries value:
                                                  \label{lem:hkcu} \verb|HKCU| control panel| desktop| \verb|muicached[machinepreferreduil] anguages]| \\
   Oueries value:
   Oueries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side [prefer external manifest]
                                                  Oueries value:
   Queries value:
                                                  HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
   Oueries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[spyeye_inj_ector_.exe]
   Queries value:
                                                  HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
   Oueries value:
                                                  HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                                  HKLM\svstem\setup[oobeinprogress]
   Oueries value:
   Oueries value:
                                                  HKLM\system\setup[systemsetupinprogress]
```

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

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

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

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

Oueries value:

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

folders[cache]

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

options\dllnxoptions[83a49421850.exe]

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

HKLM\software\microsoft\windows Oueries value: 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]

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

Queries value: HKLM\software\microsoft\ole[aggressivemtatesting] ${\tt HKLM \ } system \verb| current control set \verb| control \ \\ session$ Queries value:

manager[pendingfilerenameoperations2]

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

manager[pendingfilerenameoperations]

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

options\dllnxoptions[o971a35.exe]

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

nt\currentversion\compatibility32[o971a35]

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

settings[security_hklm_only]

HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_browser_emulation[o971a35.exe] HKLM\software\wow6432node\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_browser_emulation[*]

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

settings\5.0\user agent[]

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

settings\5.0\user agent[]

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

settings\5.0\user agent[compatible]

Queries value:

settings\5.0\user agent[compatible]

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

nt\currentversion\compatibility32[spyeye_inj_ector_]

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

settings\5.0\user agent[version]

Queries value:

settings\5.0\user agent[version]

HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\user agent[platform]

Oueries value:

settings\5.0\user agent[platform]

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

Queries value: HKLM\software\wow6432node\microsoft\windows\tablet pc[istabletpc] Oueries value: HKLM\system\currentcontrolset\control\cmf\config[system] Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

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

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

settings[syncmode5]

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

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} White the software \label{lklm} White the$

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

```
33be-4251-ba85-6007caedcf9d}[infotip]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[localizedname]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[icon]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[security]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[streamresource]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[localredirectonly]
   Queries value:
33be-4251-ba85-6007caedcf9d}[roamable]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[precreate]
   Queries value:
33be-4251-ba85-6007caedcf9d}[stream]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
   Queries value:
33be-4251-ba85-6007caedcf9d}[attributes]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[foldertypeid]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
   Queries value:
                                          HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| user | leads to be a considered for the constraints of the constraints
shell folders[cache]
                                          HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
   Oueries value:
   Queries value:
                                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                                          HKCU\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[mbcsapiforcrack]
   Queries value:
                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature http username password disable[0971a35.exe]
   Queries value:
                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
                                         HKCU\software\microsoft\internet
   Oueries value:
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[o971a35.exe]
                                         HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_mime_handling[*]
                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[o971a35.exe]
   Queries value:
                                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                                          HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[fromcachetimeout]
                                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
   Oueries value:
settings[secureprotocols]
                                          \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu} \mbox{\tt hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu
   Queries value:
settings[secureprotocols]
                                          HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[secureprotocols]
                                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Oueries value:
settings[certificaterevocation]
   Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
                                          HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[idnenabled]
   Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings[preconnectlimit]
                                          HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
```

HKCU\software\microsoft\windows\currentversion\internet

settings[preresolvelimit]

settings[sqmhttpstreamrandomuploadpoolsize]

Oueries value:

```
Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
 Queries value:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Queries value:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablenegotiate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablebasicoverclearchannel]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[clientauthbuiltinui]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enableautoproxyresultcache]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[displayscriptdownloadfailureui]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsservername]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[utf8servernameres]
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[disableworkerthreadhibernation]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketsendbufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxhttpredirects]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                           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
 Queries value:
settings[connectretries]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[certcachenovalidate]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
```

```
settings\5.0\cache[scavengecachefilelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[httpdefaultexpirytimesecs]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[disablecachingofsslpages]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Oueries value:
settings[leashlegacycookies]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:
                           HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings[dialupuselansettings]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           Queries value:
settings[bypasshttpnocachecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[enablehttptrace]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dontusednsloadbalancing]
  Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Queries value:
settings[sharecredswithwinhttp]
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
  Oueries value:
settings[mimeexclusionlistforcache]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[headerexclusionlistforcache]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscacheenabled]
                           \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}.
  Queries value:
settings[dnscacheentries]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dnscachetimeout]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonzonecrossing]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[warnonbadcertrecving]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[alwaysdrainonredirect]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonhttpstohttpredirect]
  Oueries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
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]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
  Oueries value:
Oueries value:
```

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000003 \ [storesserviceclassinfo] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \names \pace_catalog 5 \catalog_entries \names \names \pace_catalog 5 \catalog_entries \names \$

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog\_entries \ (00000000004[storesserviceclass info]) \ (catalog\_entries) \ 
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerinfo]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 00000000005[library path])
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000005[providerid]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000005 \ [address family]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 0000000000006[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (00000000000006 \ [enabled]) \ (enabled)
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[storesserviceclassinfo]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 0000000000006[provider info]
  Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ [ws2\_32numhandle buckets]
                                    \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[proxvsettingsperuser]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
                                    HKLM\system\currentcontrolset\services\crypt32[diaglevel]
  Queries value:
  Queries value:
                                    HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
  Queries value:
                                    HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Oueries value:
                                    HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
                                    HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
                                    HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Oueries value:
1923240461-1905901954-2556564120-1001[profileimagepath]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[globaluseroffline]
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablebranchcache]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[usefirstavailable]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[combinefalsestartdata]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[disablefalsestartblacklist]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[enforcep3pvalidity]
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\peerdist\service[enable]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                                    HKLM\system\currentcontrolset\services\winsock\setup
  Queries value:
migration\providers\tcpip6[winsock 2.0 provider id]
```

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \{ parameters \setminus winsock [minsock addrlength] \} \}$

Oueries value:

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

Oueries value:

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

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

settings[migrateproxy]

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

settings[proxyenable]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

 $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+$ Queries value:

settings[autodetect]

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

settings\connections[savedlegacysettings]

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

settings\connections[defaultconnectionsettings]

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

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785-b2786, \ b2786, \ b2$ 6fba-4fcf-9d55-7b8e7f157091}[name]

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

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

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

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

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{f1b32785-1000\} \\ f1b32785-1000 \\ f1b32785-$ 6fba-4fcf-9d55-7b8e7f157091}[infotip]

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

Oueries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{f1b32785-1000\} \\ f1b32785-1000 \\ f1b32785-$ 6fba-4fcf-9d55-7b8e7f157091}[icon]

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

Oueries value:

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \ f \ 1b32785-b1b3278-b1b32785$ 6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]

Oueries value:

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

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

Queries value:

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

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

Queries value:

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

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

Queries value:

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

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

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

folders[local appdata]

Queries value:

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

Oueries value:

Queries value:

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

Oueries value:

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

Oueries value

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

Queries value:

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

Queries value

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

Oueries value

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Hklm \end{ali$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} In the label \end{substitute} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} In the label \end{substitute} Hklm \end{substitute} Hklm \end{substitute} In the label \end{substitute} Hklm \end{substitute} In the label \end{substitute} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} In the label \end{substitute} Hklm \end{$

Oueries value:

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

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

settings\5.0\cache\content[cachelimit]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \ \ coe9-4171-908e-08a611b84ff6 \ [infotip]$

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ flocal redirect only \ label{eq:fig:condition}$

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell$

folders[cookies]

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \cite{Abcompart} \cite{Abcompart} \end{area} The label{lem:hklmsoftware} \end{area} The label{lem:hklmsoftware} \cite{Abcompart} \end{area} The label{lem:hklmsoftware} The label{lem:hklmsoftware} \cite{Abcompart} \cit$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} Wow6432 node \microsoft\windows\current version \explorer \folder descriptions \folder \folder descriptions \folder descriptions \folder \folder$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]

Queries value:

 $\label{local-prop} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\[infotip]$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \mbox{$aeb685db-65f9-4cf6-a03a-e3ef65729f3d} [stream resource]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ finit \ folder \ handler \ label{fig:eq:folder}$

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:

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

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\current version\explorer\folder descriptions\folder b784-432e-a781-5a1130a75963\folder\fo$

Queries value:

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

Oueries value:

 $\label{local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \eqref{d9dc8a3bb784-432e-a781-5a1130a75963} \cite{A3bb} \cite{A3bb$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{limit} $H\dot{L}M\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder 69dc8a3b-b784-432e-a781-5a1130a75963\folder folder 69dc8a3b-b784-432e-a781-5a1130a75960\folder$

Oueries value:

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

Queries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}[initfolderhandler]}$

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

folders[history]

```
Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
  Oueries value:
                                    HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                                    HKLM\software\microsoft\com3[com+enabled]
                                    HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\ole[defaultaccesspermission]
  Oueries value:
                                    HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Oueries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ defaults \ provider \
provider[image path]
                                    {\tt HKLM \setminus software \setminus policies \setminus microsoft \setminus cryptography[privkey cachemaxitems]}
  Oueries value:
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
                                    HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
                                    HKCR\wow6432node\interface\{00000134-0000-0000-c000-
00000000046}\proxystubclsid32[]
                                    HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-
  Queries value:
4f27df8760d0}\proxystubclsid32[]
                                    HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]
  Oueries value:
                                    HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
  Queries value:
60ce2149e33c}\inprocserver32[inprocserver32]
                                   HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
  Queries value:
60ce2149e33c}\inprocserver32[]
                                    HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
  Queries value:
60ce2149e33c}\inprocserver32[threadingmodel]
                                    HKLM\software\microsoft\ole[maxsxshashcount]
                                    HKU\.default\software\microsoft\windows\currentversion\explorer\user
  Oueries value:
shell folders[local appdata]
                                    HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
  Queries value:
HKLM\svstem\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
Queries value:
HKLM \verb| system| current control set \verb| services| tcpip| parameters [usedomain named evolution]
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [prioritize record data]
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Queries value:
                                    HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution]
  Queries value:
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [query net bt fqdn]
```

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Queries value: Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicasts enderflags]$

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicasts endermax time out]$

HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value:

Oueries value:

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

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

Oueries value:

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

Oueries value:

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

HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Queries value:

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

Oueries 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]

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns query time outs]$

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoproxydetecttype] Queries value: settings\winhttp[disablebranchcache] Oueries value: Queries value: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$ settings[winhttplowercasehost] Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\0[flags] Queries value: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings\zones\1[flags] Queries value: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+$ settings\zones\2[flags] HKCU\software\microsoft\windows\currentversion\internet Oueries 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[o971a35.exe] HKCU\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_localmachine_lockdown[o971a35.exe] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] Oueries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[createuricachesize] HKCU\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[createuricachesize] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[createuricachesize] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[createuricachesize] Oueries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[enablepunycode] HKCU\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[enablepunycode] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[enablepunycode] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zonemap[autodetect] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[1a10] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[searchlist] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enabledhcp] Queries value: 55779daa70e9}[registrationenabled] Oueries value: 55779daa70e9}[registeradaptername] Queries value: 55779daa70e9}[domain] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-8$ 55779daa70e9}[dhcpdomain] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ harameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-8$ 55779daa70e9}[dhcpv6domain] Oueries value: $HKLM \ system \ current control set \ services \ trpip6 \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-405d63-87b7-405d63-87b7-405d64-87b7-405d64-87b7-405d64-87b7-405d64-87b7-405d64-87b7-405d64-87b7-405d64-87b7-405d64-87b7-405d64-87b7$ 55779daa70e9}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-

55779daa70e9}[nameserver]

55779daa70e9}[dhcpnameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[domain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpdomain] Oueries 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: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationmaxaddresscount] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[maxnumberofaddressestoregister] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[enablemulticast] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[queryadaptername] Queries value: 806e6f6e6963}[disableadapterdomainname] HKLM\svstem\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disabledynamicupdate] 806e6f6e6963}[enableadapterdomainnameregistration] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationmaxaddresscount] Oueries 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] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Sets/Creates value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations] Sets/Creates value: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \run [1h6wzb8fuvux1d7fenotdr] \end{tabular}$ $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ Sets/Creates value: settings[warnonintranet] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1409] Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1609] Sets/Creates 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\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]

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

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]

Sets/Creates value:	HKCU\software\microsoft\windows\currentversion\internet		
settings[globaluseroffline]			
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings[enablehttp1_1]			
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings[proxyhttp1.1]			
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings[warnonpost]			
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings[warnonpostredi	=		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings\zones\1[1409]	UVCU) - Character Characte		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings\zones\1[1609]	UVCID - Character (A) - index of the character (A) index of the character (
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings\zones\1[1406]	UVCU) ft\		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings\zones\2[1409]	HKCU\software\microsoft\windows\currentversion\internet		
Value changes: settings\zones\2[1609]	HILLOUSOIT (MAI e / IIII CI OSOIT / WIII HOWS / CHI I EIIT VEI SIOII / III TEI II ET		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings\zones\2[1406]	TilkCo (Soft Wai e (iii)Ci OSOft (Willidows (Cui i elit Vei Sioi)(Ii)Cei iiet		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings\zones\3[1409]	TINCO (30) twal e (IIII Ci 030) t (WITHOWS (CUI I effected 310)) (ITTENTICE		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings\zones\3[1609]	TINCO (SOT EWAT & MILET OSOT & WITHOWS (CALL CITE VET STOT) (ITTECT THE		
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]			
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>		
settings\zones\4[1406]			
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>		
settings[proxyenable]			
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>		
settings\connections[savedlegacysettings]			
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>		
settings\5.0\cache\cont	ent[cacheprefix]		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>		
settings\5.0\cache\cook	ies[cacheprefix]		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>		
settings\5.0\cache\hist	ory[cacheprefix]		
Value changes: HKCU\software\microsoft\windows\currentversion\internet			
settings\zonemap[uncasintranet]			
Value changes: HKCU\software\microsoft\windows\currentversion\internet			
settings\zonemap[autodetect]			
Value changes:	HKCU\software\microsoft\windows\currentversion\internet		
settings[globaluseroffline]			