Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 5011, Task ID: 40059

Task ID: 40059 Risk Level: 10

Date Processed: 2016-05-03 05:04:46 (UTC)

Processing Time: 61.84 seconds
Virtual Environment: IntelliVM

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

Sample ID: 5011 Type: basic Owner: admin

Label: spyeye_injector.exe
Date Added: 2016-05-03 05:04:45 (UTC)

File Type: PE32:win32:gui File Size: PE32:win32:gui

MD5: b98bb6d7428c3dbffcfcab2414c6daa2

SHA256: fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029

Description: None

Pattern Matching Results

10 Creates malicious mutex: Spyeye [Banking]

- 10 Suspicious writeprocess: Spyeye [Banking]
- 6 Modifies registry autorun entries
- 6 Renames file on boot
- 2 PE: Nonstandard section
- 5 PE: Contains compressed section
- Writes to memory of system processes
- 5 Packer: UPX
- 1 HTTP connection response code 404 (file not found)
- 5 Adds autostart object
- 4 Reads process memory
- 5 Abnormal sleep detected

Static Events

Reads from process:

Anomaly: PE: Contains a virtual section

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

Packer: UPX

Process/Thread Events

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

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

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

PID:412 C:\Windows\System32\wininit.exe

Creates process: C:\Users\Admin\AppData\Local\Temp\g0TFB14.exe

["C:\Users\Admin\AppData\Local\Temp\g0TFB14.exe"]
Reads from process: PID:1288 C:\Windows\explorer.exe

Reads from process: PID:448 C:\Windows\System32\winlogon.exe Reads from process: PID:496 C:\Windows\System32\lsass.exe PID:592 C:\Windows\System32\svchost.exe Reads from process: PID:636 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:708 C:\Windows\System32\svchost.exe Reads from process: PID:720 C:\Windows\System32\dwm.exe PID:768 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:844 C:\Windows\System32\svchost.exe Reads from process: PID:888 C:\Windows\System32\svchost.exe PID:312 C:\Windows\System32\spoolsv.exe Reads from process: Reads from process: PID:484 C:\Windows\System32\svchost.exe Reads from process: PID:652 C:\Windows\System32\svchost.exe Reads from process: PID:1508 C:\Windows\System32\svchost.exe Reads from process: PID:2036 C:\Windows\System32\taskhostex.exe Reads from process: PID:408 C:\Windows\System32\svchost.exe Reads from process: PID:2064 C:\Windows\System32\dllhost.exe Reads from process: PID:2800 C:\Windows\System32\wbem\unsecapp.exe Reads from process: PID:2932 C:\Windows\System32\wbem\WmiPrvSE.exe PID:3012 C:\Windows\System32\conhost.exe Reads from process:

Writes to process: PID:2492 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe

Writes to process: PID:3012 C:\Windows\System32\conhost.exe

Writes to process: PID:316 C:\Users\Admin\AppData\Local\Temp\g0TFB14.exe

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

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\RPCController
Creates mutex: \Sessions\1\BaseNamedObjects\zXeRY3a_PtW|00000000
Creates mutex: \BaseNamedObjects\7015cQ07MSCU9AWCQ7fPX6bRH6hFFXT

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

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

File System Events C:\WinOldFileq Creates: Creates: C:\WinOldFileq\ C:\WinOldFileg\83A49421850.exe Creates: C:\WinOldFileq\6C3E79A93CD5139 Creates: C:\Users\Admin\AppData\Local\Temp\ Creates: C:\Users\Admin\AppData\Local\Temp\g0TFB14.tmp Creates: Creates: C:\Users\Admin\AppData\Local\Temp\gOTFB14.exe Creates: C:\Users\Admin 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: Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History C:\Windows\Prefetch\SPYEYE_INJECTOR.EXE-619282B0.pf Opens: Opens: C:\Windows Opens: C:\Windows\System32\wow64.dll C:\Windows\SysWOW64 Opens: Opens: C:\Windows\SysWOW64\apphelp.dll Opens: C:\Windows\Temp\spyeye_injector.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 C:\Windows\SysWOW64\bcryptprimitives.dll Opens: Opens: C:\Windows\SysWOW64\cryptbase.dll Opens: C:\Windows\SysWOW64\sspicli.dll Opens: C:\Windows\SysWOW64\rpcrt4.dll C:\Windows\SysWOW64\advapi32.dll Opens: Opens: C:\ Opens: C:\Windows\Globalization\Sorting\SortDefault.nls C:\WinOldFileq Opens: Opens: C:\WinOldFileg\ Opens: C:\WinOldFileq\83A49421850.exe C:\Windows\Prefetch\83A49421850.EXE-56DEA472.pf Opens: 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: Opens: C:\Windows\SysWOW64\shlwapi.dll 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: C:\Windows\SysWOW64\urlmon.dll Opens: Opens: C:\Windows\SysWOW64\oleaut32.dll Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\WinOldFileq\6C3E79A93CD5139 Opens: C:\Users\Admin\AppData\Local\Temp\gOTFB14.exe Opens: C:\Users\Admin\AppData\Local\Temp C:\Users Opens: Opens: C:\Users\Admin Opens: C:\Users\Admin\AppData Opens: C:\Users\Admin\AppData\Local Opens: C:\Windows\Prefetch\GOTFB14.EXE-5CF16FB1.pf Opens: C:\Windows\SysWOW64\SHCore.dll Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\Windows\SysWOW64\secur32.dll Opens: C:\Windows\SysWOW64\profapi.dll C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Opens: Files\counters.dat C:\Windows\WinSxS\x86_microsoft.windows.common-Opens: controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985 C:\Windows\WinSxS\x86_microsoft.windows.commoncontrols_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll C:\Windows\WindowsShell.Manifest Opens: Opens:

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

Opens:

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

```
Opens:
                        C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs
Opens:
                        C:\Windows\SysWOW64\tzres.dll
                        C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens:
Opens:
                        C:\Windows\SysWOW64\winhttp.dll
Opens:
                        C:\Windows\SysWOW64\mswsock.dll
                        C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:
Opens:
                        C:\Windows\SysWOW64\winnsi.dll
Opens:
                        C:\Windows\SysWOW64\clbcatq.dll
                        C:\Windows\SysWOW64\cryptsp.dll
Opens:
Opens:
                        C:\Windows\SysWOW64\rsaenh.dll
Opens:
                        C:\Windows\SysWOW64\dnsapi.dll
                        C:\Windows\SysWOW64\NapiNSP.dll
Opens:
Opens:
                        C:\Windows\SysWOW64\pnrpnsp.dll
                        C:\Windows\SysWOW64\nlaapi.dll
Opens:
                        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
                        C:\WinOldFileq\83A49421850.exe
Writes to:
Writes to:
                        C:\WinOldFileq\6C3E79A93CD5139
Writes to:
                        C:\Users\Admin\AppData\Local\Temp\g0TFB14.exe
                        C:\Windows\SysWOW64\ntdll.dll
Reads from:
Reads from:
                        C:\Windows\Temp\spyeye_injector.exe
Reads from:
                        C:\WinOldFileq\83A49421850.exe
Reads from:
                        C:\WinOldFileq\6C3E79A93CD5139
Reads from:
                        C:\Users\Admin\AppData\Local\Temp\gOTFB14.exe
Reads from:
                        C:\Windows\SysWOW64\user32.dll
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
```

Network Events

Deletes:

DNS guery:	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 ⇒ 96.6.72.154
DNS response:	e10088.dspb.akamaiedge.net ⇒ 104.109.84.116
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
Connects to:	198.105.244.11:80
Sends data to:	8.8.8.8:53
Sends data to:	4.2.2.1:53
Sends data to:	88.198.13.147:443
Sends data to:	alexevartemov.com:80 (104.239.213.7)
Sends data to:	alexevartemov.com:80 (198.105.244.11)
Receives data from:	8.8.8.8:53
Receives data from:	4.2.2.1:53
Receives data from:	88.198.13.147:443
Receives data from:	alexeyartemov.com:80 (104.239.213.7)
Receives data from:	alexeyartemov.com:80 (198.105.244.11)

C:\Windows\Temp\spyeye_injector.exe

Windows Registry Events

Creates key:	HKLM\system\currentcontrolset\control\session manager
Creates key:	HKCU\software\microsoft\windows\currentversion\run
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\0</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\1</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\2</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\3</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\4</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>
<pre>settings\lockdown_zones\</pre>	1
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>
settings\lockdown_zones\	2
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>
settings\lockdown_zones\	3
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\	4
Creates key:	HKCU\software\microsoft\internet explorer\phishingfilter
Creates key:	HKCU\software\microsoft\internet explorer\recovery
Creates key:	HKCU\software\microsoft\systemcertificates\my
Creates key:	HKCU\software\microsoft windows
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\connections	
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters

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

settings\zonemap\

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

settings[proxyserver]

Deletes value:

HKCU\software\microsoft\windows\currentversion\internet

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings[autodetect]

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

settings\zonemap[proxybypass]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

HKI M\software\wow6432node\microsoft\windows\currentyersion\internet Deletes value:

settings\zonemap[intranetname]

Opens key: HKLM\software\microsoft\wow64

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

Opens kev:

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

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

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: 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: HKCU\

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

Opens key: HKCU\software\policies\microsoft\control panel\desktop ${\it HKCU} \ control\ panel\ desktop\ language configuration$ Opens key:

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 HKCU\software\microsoft\windows nt\currentversion\appcompatflags 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 kev: HKLM\software\microsoft\windows nt\currentversion\image file execution

options Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions

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

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

Opens kev:

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

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

HKLM\system\setup Opens key:

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

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

options\83a49421850.exe

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

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

HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens key: Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} is software \end{tabular} is s$ Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

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

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

Opens key: HKLM\

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

nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

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

compatibility

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

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

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

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

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

options\gotfb14.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\gotfb14.exe

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

Opens key:

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

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\featurecontrol

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

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

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

explorer\main\featurecontrol\feature_browser_emulation

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

settings\5.0\user agent

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

settings\5.0\user agent

Opens key: HKLM\software\wow6432node\policies

HKCU\software\policies Opens key:

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

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

settings\user agent

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

settings

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

settings\user agent

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

settings\5.0\user agent\pre platform

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

settings\5.0\user agent\pre platform

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

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

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

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

settings\5.0\user agent\post platform

Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$

settings\5.0\user agent\post platform

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

Opens key: HKLM\software\microsoft\rpc

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

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

Opens key:

settings\5.0\cache

Opens kev:

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

Opens kev:

33be-4251-ba85-6007caedcf9d}

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

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

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

Opens key:

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

Opens key: HKU\

HKU\.default Opens key:

Opens key: $\label{thm:local_hammon} \begin{tabular}{ll} HKU\label{thm:local_hammon} HKU\label{thm:local_hammon} \end{tabular} and the local_hammon \begin{tabular}{ll} hKU\label{thm:local_hammon} HKU\label{thm:local_hammon} \end{tabular} and the local_hammon \begin{tabular}{ll} hKU\label{tabular} \end{tabular} a$

shell folders

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

nt\currentversion\profilelist

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

folders Opens kev:

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

HKCU\software\microsoft\internet Opens kev:

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

 $\verb|explorer| \verb|main| feature control| retry_header on lypost_on connection reset| \\$

```
HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKCU\software\microsoft\internet
 Opens kev:
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 key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                         HKCU\software\microsoft\internet
 Opens kev:
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 key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature digest no extras in uri
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature exclude invalid client cert kb929477
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 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
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet settings
 Opens key:
                         HKLM\software\wow6432node\policies\microsoft\internet explorer
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer
                         HKLM\software\wow6432node\policies\microsoft\internet explorer\main
 Opens kev:
 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 kev:
HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ 15.0 \ (cache
```

HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\5.0\cache Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266 HKLM\software\wow6432node\microsoft\internet Opens key: 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 HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444 HKLM\system\currentcontrolset\services\winsock2\parameters Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1783a121 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev: Opens kev: Opens kev: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004 Opens key: Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ oid \ lencoding type$ 0\certdllopenstoreprov $\label{lem:hklm} \verb+KLM\software\wow6432 node\microsoft\cryptography\oid\encoding type \\$ Opens key: 0\certdllopenstoreprov\#16 Opens key: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| cryptography\\| oid\\| encoding type$ 0\certdllopenstoreprov\ldap Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ oid \ lencoding type \ 1$ Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

1\certdllopenstoreprov

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

 $Opens~key: \\ HKLM\software\wow6432node\microsoft\windows \\ nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001 \\$

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\

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

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\system\currentcontrolset\control\cmf\config
 Opens key:
                 HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens key:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000000066
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\17506cf5
                 HKLM\software\policies\microsoft\peerdist\service
 Opens key:
 Opens key:
                 HKLM\software\microsoft\windows nt\currentversion\peerdist\service
                 HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key:
 Opens key:
                 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
 Opens key:
                 HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key:
                 HKLM\system\currentcontrolset\services\winsock\setup migration\providers
 Opens key:
                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
                 HKLM\system\currentcontrolset\services\winsock\setup
 Opens key:
migration\providers\tcpip
                 HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\content
 Opens key:
                 HKLM\software\wow6432node\policies\microsoft\windows\explorer
 Opens key:
                 HKLM\software\policies\microsoft\windows\explorer
 Opens key:
                 HKCU\software\policies\microsoft\windows\explorer
 Opens kev:
6fba-4fcf-9d55-7b8e7f157091}
 Opens key:
6fba-4fcf-9d55-7b8e7f157091}\propertybag
 Opens kev:
0e22-4760-9afe-ea3317b67173}
 Opens key:
0e22-4760-9afe-ea3317b67173}\propertybag
 Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
 Opens key:
                 HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
 Opens key:
c0e9-4171-908e-08a611b84ff6}
{\tt c0e9-4171-908e-08a611b84ff6} \setminus {\tt propertybag}
65f9-4cf6-a03a-e3ef65729f3d}
```

Opens key:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\property bag$

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

settings\5.0\cache\history

Opens key:

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

Opens key:

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

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

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

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

Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash windows runtime \backslash clsid}$

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-

000000000046}

 Opens key:
 HKCR\wow6432node\clsid\{00000323-0000-0000-c000-000000000046}\

 Opens key:
 HKCU\software\classes\clsid\{00000323-0000-0000-c000-000000000046}\

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\gotfb14.exe

Opens key: HKCR\appid\gotfb14.exe

Opens key: $\label{thm:microsoft} \mbox{ HKLM} \mbox{ hkcm} \mbox{ HKLM} \mbox{ hkcm} \mbox{ hk$

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

Opens key:

 $\label{lem:hklmlsoftwarelwow6432} HKLM \ software \ \ cryptography \ \ defaults \ \ provider \ \ \ cryptographic provider$

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 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{a168 \\ add \\ c-1674-49 \\ da-ad4f-1674-49 \\ da-ad4f-1674-49$ 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{local-observation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sl}} \mbox{\tt zones\sl} \mbox{\tt 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:
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 \ policies \ vones \ 4432 node \ vones \ 4432 node \ policies \ 4432 node \ 
                                      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:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
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: $HKLM \ system \ current controls et \ services \ tcpip \ (parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-4054401-87b7-405401-87b7-87b7-405401-87b7-$ 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: $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{a04231f6-42eb-4732-b850-472-b850-472$ 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\enus[alternatecodepage] HKCU\control panel\desktop[preferreduilanguages] Oueries value: $\label{local-control} \mbox{ HKCU\control panel\desktop\muicached[machinepreferreduilanguages]} \label{local-control}$ 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_injector.exe] Queries value: $HKLM \verb|\system| current control \verb|\sa| fips algorithm policy[enabled]$ 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\currentcontrolset\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]

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

Oueries value:

folders[cache]

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

options\dllnxoptions[83a49421850.exe]

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

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

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

nt\currentversion\compatibility32[83a49421850]

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

nt\currentversion\windows[loadappinit_dlls]

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

 $\label{lem:lem:queries} Queries \ value: & HKLM\software\microsoft\ole[aggressivemtatesting] \\ Queries \ value: & HKLM\system\currentcontrolset\control\session \\ \end{cases}$

manager[pendingfilerenameoperations2]

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

manager[pendingfilerenameoperations]

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

options\dllnxoptions[gotfb14.exe]

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

nt\currentversion\compatibility32[gotfb14]

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

settings[security_hklm_only]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[gotfb14.exe] Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_browser_emulation[*]

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

settings\5.0\user agent[]

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

settings\5.0\user agent[]

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

settings\5.0\user agent[compatible]

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

settings\5.0\user agent[compatible]

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

settings\5.0\user agent[version]

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

 ${\tt settings \ 1.0 \ user \ agent[version]}$

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

settings\5.0\user agent[platform]

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

settings\5.0\user agent[platform]

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

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

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

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

settings[syncmode5]

 $\label{thm:local_queries} Queries \ value: \\ HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet \\$

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

Queries value:

 $\label{limits} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fold$

Queries value:

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

Queries value:

 $\label{thm:hk.mass} HKL^{M} software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \earlies -33be-4251-ba85-6007 caed cf9d \cite{thm:hk.mass} [parent folder]$

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007 caedcf9d}\[localized name]$

Queries value:

```
33be-4251-ba85-6007caedcf9d}[icon]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[security]
   Queries value:
33be-4251-ba85-6007caedcf9d}[streamresource]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
   Queries value:
33be-4251-ba85-6007caedcf9d}[localredirectonly]
   Queries value:
33be-4251-ba85-6007caedcf9d}[roamable]
   Queries value:
33be-4251-ba85-6007caedcf9d}[precreate]
33be-4251-ba85-6007caedcf9d}[stream]
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
33be-4251-ba85-6007caedcf9d}[attributes]
33be-4251-ba85-6007caedcf9d}[foldertypeid]
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
                                            HKU\.default\software\microsoft\windows\currentversion\explorer\user
   Queries value:
shell folders[cache]
   Queries value:
                                            HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Queries value:
folders[cache]
   Queries value:
                                            \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \cite{thm:hkcu}. The third \cite{thm:hkcu} is the third \cite{t
settings[mbcsapiforcrack]
                                            HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_http_username_password_disable[gotfb14.exe]
                                            HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature http username password disable[*]
   Queries value:
                                            HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                            HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
   Oueries value:
                                            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[gotfb14.exe]
   Queries value:
                                            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
                                            HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[gotfb14.exe]
   Oueries value:
                                            HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[*1
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                                             HKLM\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[secureprotocols]
                                             \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
   Queries value:
settings[secureprotocols]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[certificaterevocation]
   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[disablekeepalive]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[preconnectlimit]
   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[preresolvelimit]
   Queries value:
                                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[sqmhttpstreamrandomuploadpoolsize]
                                             \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows \verb+current version \verb+\internet+ in the lemma + the lemma 
  Oueries value:
settings[cachemode]
```

settings[enablehttp1_1]

Queries value:

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

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

```
settings[enablehttp1_1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttp1_1]
 Queries value:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Queries value:
                           \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings[proxyhttp1.1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
 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[disablebasicoverclearchannel]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[clientauthbuiltinui]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[mbcsservername]
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[utf8servernameres]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxhttpredirects]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
 Queries value:
settings[sendtimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[certcachenovalidate]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[ftpdefaultexpirytimesecs]
```

```
Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
 Queries value:
                       HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[wpadsearchalldomains]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasshttpnocachecheck]
                        Queries value:
settings[bypasshttpnocachecheck]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
                       HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings[bypasssslnocachecheck]
                        Queries value:
settings[enablehttptrace]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
                        Queries value:
settings[nocheckautodialoverride]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
 Oueries value:
                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                       HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[sharecredswithwinhttp]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheenabled]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheentries]
                        \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[dnscachetimeout]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonpost]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonbadcertrecving]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                       HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonhttpstohttpredirect]
 Queries value:
                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Queries value:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9[serial access num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Queries 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\000000000003[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
```

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 00000000000007 \ [packed catalog item] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]

Oueries value:

Queries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]    Oueries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 000000000001 \ [enabled] \ Oueries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version] Oueries value:

 $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus catalog \le ca$

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

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo]
Oueries value:

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[enabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1923240461-1905901954-2556564120-1001[profileimagepath]

Queries value:

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

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

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

Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000005 \ [displaystring]$ Oueries value:

Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000005 [supported name space]]$ Oueries value:

Queries value:

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

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

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

reporting\wmr[disable]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[librarypath]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000006[displaystring]$ Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog S \setminus catalog_entries \setminus 0000000000006[providerid]$ Queries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 [supported name space]]$ Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus catalog \le catalog \le catalog \le catalog = not in the control set \setminus services \setminus catalog \le catalo$

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog_entries \ (00000000006[storesserviceclass info]) \ (catalog_entries) \$ Queries value:

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

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

settings[proxysettingsperuser]

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

settings[badproxyexpirestime]

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] $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$

Queries value:

settings[disablebranchcache]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[usefirstavailable]

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

settings[combinefalsestartdata] HKCU\software\microsoft\windows\currentversion\internet

Queries value: settings[disablefalsestartblacklist]

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

settings[enforcep3pvalidity]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\peerdist\service[enable]

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping] HKLM\system\currentcontrolset\services\winsock\setup Oueries value:

migration\providers\tcpip6[winsock 2.0 provider id]

Oueries value:

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

Queries value:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock [used elayed acceptance]$

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

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

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

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[proxyenable] $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+$ Queries value: settings[proxyserver] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[autoconfigurl] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autodetect] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\connections[savedlegacysettings] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[defaultconnectionsettings] Queries value: 6fba-4fcf-9d55-7b8e7f157091}[category] Queries value: 6fba-4fcf-9d55-7b8e7f157091}[name] Queries value: $HKLM \label{lem:hklm} White the latest and the la$ 6fba-4fcf-9d55-7b8e7f157091}[parentfolder] Queries value: 6fba-4fcf-9d55-7b8e7f157091}[description] Oueries value: 6fba-4fcf-9d55-7b8e7f157091}[relativepath] Queries value: 6fba-4fcf-9d55-7b8e7f157091}[parsingname] Oueries value: 6fba-4fcf-9d55-7b8e7f157091}[infotip] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}[localizedname] Oueries value:

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

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \ ff 1b 32785-1b 32785-1b$ 6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]

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

folders[local appdata]

Queries value:

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

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

Oueries value

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[infotip]} Infotip in the property of the property of$

Oueries value:

 $\label{thm:localized} $HKLM\software\wow6432\node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localized name]}$

Queries value:

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

Queries value:

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

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:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \mbox{$5e6c858f-0e22-4760-9afe-ea3317b67173} [attributes]$

Queries value:

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

Queries 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:

Queries value:

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

Queries value:

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{Coe9-4171-908e-08a611b84ff6} \cite{Coe9-4171-908e-08a611b84ff$

Queries value:

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

Queries value:

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

Queries value

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

Queries value:

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

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-16444, 2b0f765d-16444, 2b0f766d-16444, 2b0f76d-16444, 2b0f76d-16444, 2b0f76d-16444, 2b0f76d-16444, 2b0f76d-16444, 2b0f76d-164444, 2b0$ c0e9-4171-908e-08a611b84ff6}[security]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-16444, 2b0f765d-16444, 2b0f766d-16444, 2b0f76d-16444, 2b0f76d-164444, 2b0f76d-1644$ c0e9-4171-908e-08a611b84ff6}[streamresource]

Oueries value:

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

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[localredirectonly]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}[roamable]

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

folders[cookies]

Queries value:

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

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

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

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

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

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$ 65f9-4cf6-a03a-e3ef65729f3d}[infotip]

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

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

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

Queries value:

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

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

Queries value:

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

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{3eb685db-10explorer\} \ folder \ before \ folder \ before \ folder \ folder \ before \ folder \ fol$ 65f9-4cf6-a03a-e3ef65729f3d}[precreate]

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

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

folders[appdata]
Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[cachelimit]

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries 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:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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

folders[history]

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

settings\5.0\cache\history[cachelimit]

Oueries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll] HKLM\software\microsoft\com3[com+enabled] Oueries value: Oueries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel] Queries value: HKLM\software\microsoft\ole[defaultaccesspermission] Oueries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous] Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type] Oueries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path] HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems] Queries value: Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds] HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds] Queries value: Oueries value: HKLM\software\microsoft\cryptography[machineguid] HKCR\wow6432node\interface\{00000134-0000-0000-c000-Oueries value: 00000000046}\proxystubclsid32[] Queries value: HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32[] HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[] Queries value: Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\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] Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user Oueries value: shell folders[local appdata] HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Oueries value: Queries value: $HKLM \verb|\system| current controlset \verb|\services| dns cache \verb|\parameters[queryadaptername]|$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [domain named evolution level]$ HKLM\svstem\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Queries value: $HKLM \ system \ current control set \ services \ dns cache \ parameters [allow unqualified query]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [allow unqualified query]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\svstem\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns] Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [query net bt fqdn]$

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value: Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register reverse lookup]$ Queries 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] HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Oueries value: $\label{lem:hklm} \verb+Kklm \ system \ current control set \ \verb+services \ \verb+dns \ cache \ \verb+parameters \ [registration overwrite]$ HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Oueries 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: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use compartments]$ Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]

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] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[autoproxydetecttype] Oueries value: settings\winhttp[disablebranchcache] Queries value: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[winhttplowercasehost] HKLM\software\policies\microsoft\internet Queries value: explorer\security[disablesecuritysettingscheck] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[flags] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\1[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\2[flags] $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+$ Queries value: settings\zones\3[flags] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\4[flags] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[gotfb14.exe] HKCU\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet$ Oueries value: explorer\main\featurecontrol\feature_localmachine_lockdown[gotfb14.exe] HKLM\software\wow6432node\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_localmachine_lockdown[*] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[createuricachesize] Oueries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[createuricachesize] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[createuricachesize] Queries value: settings[createuricachesize] Queries value: $HKLM \verb|\software\policies\microsoft\windows\currentversion\ | internet$ settings[enablepunycode] Oueries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablepunycode] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enablepunycode] $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings\zonemap[autodetect] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[1a10] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[searchlist1 Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enabledhcp] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationenabled] Oueries value: 55779daa70e9}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[domain] Queries value: 55779daa70e9}[dhcpdomain] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpv6domain] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver] Queries value:

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

Oueries value:

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

Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationenabled]
  Queries value:
806e6f6e6963}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[domain]
  Oueries value:
806e6f6e6963}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpnameserver]
                                   HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{b5105d63-74c6-4dc1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-87b7-40c1-8
55779daa70e9}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[disableadapterdomainname]
  Queries value:
55779daa70e9}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[enablemulticast]
  Queries value:
806e6f6e6963}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disableadapterdomainname]
  Queries value:
806e6f6e6963}[disabledynamicupdate]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enableadapterdomainnameregistration]
  Queries value:
806e6f6e6963}[registrationmaxaddresscount]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[maxnumberofaddressestoregister]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enablemulticast]
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Sets/Creates value:
                                   HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
  Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fuvux1d7fenotdr]
  Sets/Creates value:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
  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:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1406]
  Sets/Creates value:
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown zones\1[1406]
  Sets/Creates value:
                                   \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\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]
```

HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]

HKCU\software\microsoft\windows\currentversion\internet

HKCU\software\microsoft\internet

HKCU\software\microsoft\internet

Sets/Creates value:

Sets/Creates value:

Sets/Creates value:

Sets/Creates value:

settings[globaluseroffline]

explorer\phishingfilter[shownservicedownballoon]

explorer\recovery[clearbrowsinghistoryonexit]

Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings[enablehttp1_1]		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
<pre>settings[proxyhttp1.1]</pre>		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings[warnonpost]		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings[warnonpostredin	rect]	
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\zones\1[1409]		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\zones\1[1609]		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\zones\1[1406]		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\zones\2[1409]		
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>	
settings\zones\2[1609]		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\zones\2[1406]		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\zones\3[1409]	and the second s	
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\zones\3[1609]	HIGH - Channel and the control of th	
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\zones\3[1406]		
Value changes: settings\zones\4[1409]	HKCU\software\microsoft\windows\currentversion\internet	
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\zones\4[1609]	nkco/sortware/mitcrosort/windows/current/erston/internet	
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\zones\4[1406]	TINCO (301 twal e (IIIICI 0301 t (WIIIdows (Cdi i elit vei 31011/11)tei ilet	
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings[proxyenable]	Tinco (30) twal e (iii) cl 030) t (williauws (cull eliteris io) (tintel liet	
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\connections[sa\		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\5.0\cache\conte		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\5.0\cache\cooki		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\5.0\cache\histo		
Value changes:	HKCU\software\microsoft\windows\currentversion\internet	
settings\zonemap[uncasir		
Value changes: HKCU\software\microsoft\windows\currentversion\internet		
settings\zonemap[autodet		
Value changes: HKCU\software\microsoft\windows\currentversion\internet		
settings[globaluseroffline]		