# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 5011, Task ID: 40061

Task ID: 40061 Risk Level: 10

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

Processing Time: 62.33 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: 103936 bytes

MD5: b98bb6d7428c3dbffcfcab2414c6daa2

SHA256: fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029

Description: None

### Pattern Matching Results

7 Injects thread into Windows process

- Creates malicious mutex: Spyeye [Banking]
- 5 Installs service
- 5 PE: Contains compressed section
- 4 Terminates process under Windows subfolder
- 10 Suspicious writeprocess: Spyeye [Banking]
- 1 HTTP connection response code 404 (file not found)
- 7 Writes to memory of system processes
- 6 Writes to system32 folder
- 5 Packer: UPX
- 6 Notifies system about Internet connection change
- 5 Adds autostart object
- 6 Modifies registry autorun entries
- 4 Reads process memory
- 3 HTTP connection response code 200 (success)
- 2 PE: Nonstandard section
- 3 Long sleep detected
- 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\83A494219A6.exe ["C:\WinOldFileq\83A494219A6.exe"]
Creates process: C:\Windows\system32\rundll32.exe ["C:\Windows\system32\rundll32.exe"]

PID:2820 C:\Windows\System32\rundll32.exe

"C:\Windows\system32\WININET.dll",DispatchAPICall 1 ]

Reads from process: PID:2828 C:\Windows\System32\rundll32.exe Reads from process: PID:3064 C:\Windows\System32\calc.exe PID:3116 C:\Windows\System32\rundll32.exe Reads from process: Reads from process: PID:3168 C:\Windows\System32\rundl132.exe PID:3220 C:\Windows\System32\rundll32.exe Reads from process: PID:3264 C:\Windows\System32\rundl132.exe Reads from process: Reads from process: PID:3324 C:\Windows\System32\rundll32.exe Reads from process: PID:3352 C:\Windows\System32\rundll32.exe PID:3392 C:\Windows\System32\rundll32.exe Reads from process: Reads from process: PID:3440 C:\Windows\System32\rundl132.exe Reads from process: PID:3532 C:\Windows\System32\rundll32.exe Reads from process: PID:3588 C:\Windows\System32\rundll32.exe Reads from process: PID:3640 C:\Windows\System32\rundll32.exe Reads from process: PID:3696 C:\Windows\System32\rundll32.exe Reads from process: PID:3764 C:\Windows\System32\rundll32.exe Reads from process: PID:3840 C:\Windows\System32\rundll32.exe Reads from process: PID:3884 C:\Windows\System32\rundll32.exe Reads from process: PID:3928 C:\Windows\System32\rundll32.exe Reads from process: PID:3976 C:\Windows\System32\rundll32.exe Reads from process: PID:2148 C:\Windows\System32\rundll32.exe Reads from process: PID:2248 C:\Windows\System32\rundll32.exe Reads from process: PID:1968 C:\Windows\System32\rundll32.exe Reads from process: PID:2088 C:\Windows\System32\rundll32.exe Reads from process: PID:2124 C:\Windows\System32\rundll32.exe Reads from process: PID:2608 C:\Windows\System32\rundll32.exe Reads from process: PID:2668 C:\Windows\System32\rundll32.exe

```
PID:2908 C:\Windows\System32\rundll32.exe
Reads from process:
                         PID:1092 C:\Windows\explorer.exe
Writes to process:
Writes to process:
                         PID:360 C:\Windows\System32\wininit.exe
Writes to process:
                         PID:396 C:\Windows\System32\winlogon.exe
                         PID:464 C:\Windows\System32\lsass.exe
Writes to process:
Writes to process:
                         PID:472 C:\Windows\System32\lsm.exe
Writes to process:
                         PID:572 C:\Windows\System32\svchost.exe
                         PID:640 C:\Windows\System32\svchost.exe
Writes to process:
Writes to process:
                         PID:688 C:\Windows\System32\svchost.exe
Writes to process:
                         PID:816 C:\Windows\System32\svchost.exe
                         PID:860 C:\Windows\System32\svchost.exe
Writes to process:
Writes to process:
                         PID:968 C:\Windows\System32\svchost.exe
Writes to process:
                         PID:1144 C:\Windows\System32\dwm.exe
                         PID:1276 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:
Writes to process:
                         PID:1348 C:\Windows\System32\spoolsv.exe
Writes to process:
                         PID:1388 C:\Windows\System32\taskhost.exe
                         PID:1396 C:\Windows\System32\svchost.exe
Writes to process:
Writes to process:
                         PID:1468 C:\Windows\System32\svchost.exe
Writes to process:
                         PID:1556 C:\Windows\System32\svchost.exe
                         PID:1932 C:\Windows\System32\UIODetect.exe
Writes to process:
Writes to process:
                         PID:280 C:\Windows\System32\svchost.exe
Writes to process:
                         PID:1508 C:\Windows\System32\mobsync.exe
                         PID:1064 C:\Windows\System32\taskhost.exe
Writes to process:
Writes to process:
                         PID:2308 C:\Windows\System32\wbem\unsecapp.exe
Writes to process:
                         PID:2420 C:\Windows\System32\wbem\WmiPrvSE.exe
                         PID:2476 C:\Windows\System32\conhost.exe
Writes to process:
                         PID:2488 C:\Windows\Temp\spyeye_injector.exe
Writes to process:
                         PID:2828 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:3116 C:\Windows\System32\rundll32.exe
Writes to process:
Writes to process:
                         PID:3168 C:\Windows\System32\rundll32.exe
                         PID:3220 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:3264 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:3324 C:\Windows\System32\rundll32.exe
Writes to process:
Writes to process:
                         PID:3352 C:\Windows\System32\rundll32.exe
                         PID:3392 C:\Windows\System32\rundl132.exe
Writes to process:
                         PID:3440 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:3532 C:\Windows\System32\rundll32.exe
Writes to process:
Writes to process:
                         PID:3588 C:\Windows\System32\rundl132.exe
                         PID:3640 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:3696 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:3764 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:3840 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:3884 C:\Windows\System32\rundll32.exe
Writes to process:
Writes to process:
                         PID:3928 C:\Windows\System32\rundl132.exe
                         PID:3976 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:2148 C:\Windows\System32\rundll32.exe
Writes to process:
Writes to process:
                         PID:2248 C:\Windows\System32\rundll32.exe
Writes to process:
                         PID:1968 C:\Windows\System32\rundll32.exe
                         PID:2088 C:\Windows\System32\rundll32.exe
Writes to process:
Writes to process:
                         PID:2124 C:\Windows\System32\rundl132.exe
                         PID:2608 C:\Windows\System32\rundll32.exe
Writes to process:
Writes to process:
                         PID:2668 C:\Windows\System32\rundl132.exe
Writes to process:
                         PID:2820 C:\Windows\System32\rundll32.exe
                         PID:2908 C:\Windows\System32\rundll32.exe
Writes to process:
                         C:\WinOldFileq\83A494219A6.exe
Terminates process:
Terminates process:
                         C:\Windows\Temp\spyeye_injector.exe
                         C:\Windows\System32\rundll32.exe
Terminates process:
                         C:\Windows\System32\mobsync.exe
Terminates process:
Creates remote thread:
                         C:\Windows\System32\rundl132.exe
Creates remote thread:
                         C:\Windows\System32\wininit.exe
Creates remote thread:
                         C:\Windows\System32\spoolsv.exe
Creates remote thread:
                         C:\Windows\System32\lsm.exe
                         C:\Windows\System32\svchost.exe
Creates remote thread:
Creates remote thread:
                         C:\Windows\System32\wbem\WmiPrvSE.exe
Creates remote thread:
                         C:\Windows\System32\taskhost.exe
                         C:\Windows\System32\lsass.exe
Creates remote thread:
Creates remote thread:
                         C:\Windows\System32\ivm\ivm-service.exe
Creates remote thread:
                         C:\Windows\System32\tlntsrv.exe
Creates remote thread:
                         C:\Windows\explorer.exe
                         C:\Windows\System32\UI0Detect.exe
Creates remote thread:
                         C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Creates remote thread:
Creates remote thread:
                         C:\Windows\System32\dwm.exe
```

# Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\RPCController
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW 00000046
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW 00000000
Creates mutex:	\BaseNamedObjects\QCK1I5M9QoJxnXIFArGIvQFBLQ3VUs8
Creates mutex:	\BaseNamedObjects\zXeRY3a_PtW 0000000
Creates mutex:	\Sessions\1\BaseNamedObjects\_!MSFTHISTORY!_

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet

files!content.ie5!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!

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

\Sessions\1\BaseNamedObjects\RasPbFile Creates mutex:

\Sessions\1\BaseNamedObjects\\_!MSFTHISTORY!\_LOW!\_ Creates mutex:

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet

files!low!content.ie5!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!low!

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!low!history.ie5!

Creates mutex: \Sessions\1\BaseNamedObjects\IESQMMUTEX\_0\_208 Creates event: \BaseNamedObjects\SvcctrlStartEvent A3752DX Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED

Creates event: \BaseNamedObjects\BFE\_Notify\_Event\_{109e966d-3152-488e-bba0-

f5d178e39820}

\BaseNamedObjects\BFE\_Notify\_Event\_{70064256-b57a-4a42-920e-Creates event:

9e57be0b48ab}

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

### File System Events

Creates:	C:/winoidFiled
Creates:	C:\WinOldFileq\

Creates: C:\WinOldFileq\83A494219A6.exe C:\WinOldFileq\9C413B7B23C1D6D Creates:

C:\Users\Admin Creates:

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

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

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

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History Creates:

Creates: C:\Users\Admin\Favorites

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE Creates:  $C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache|\\$ Creates: Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache

C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf Creates: C:\Windows\Prefetch\MOBSYNC.EXE-C5E2284F.pf Creates: Creates: C:\Windows\Prefetch\TASKHOST.EXE-7238F31D.pf Creates: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf

Creates: C:\Windows\system32\wdi

Creates: C:\Windows\system32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}

C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-Creates:

172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}

C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-

172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}\snapshot.etl

C:\Windows\system32\wdi\{86432a0b-3c7d-4ddf-a89c-Creates:

172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}

Creates: C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics\_SystemData.bin Creates: C:\Windows\System32\wdi\BootPerformanceDiagnostics\_SystemData.bin

Opens: C:\Windows\Prefetch\SPYEYE\_INJECTOR.EXE-619282B0.pf

Opens: C:\Windows\System32

C:\Windows\System32\sechost.dll Opens: Opens: C:\Windows\System32\kernel32.dll

Opens: C:\

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

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

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

Opens: C:\Windows\Temp\spyeye\_injector.exe Opens: C:\WinOldFileq\83A494219A6.exe Opens: C:\Windows\AppPatch\sysmain.sdb Opens: C:\WinOldFileq\ui\SwDRM.dll

Opens: C:\Windows\Prefetch\83A494219A6.EXE-0D3DE1A1.pf

Opens: C:\Windows\System32\imm32.dll Opens: C:\WinOldFileq\MSIMG32.dll Opens: C:\Windows\System32\msimg32.dll Opens: C:\WinOldFileq\9C413B7B23C1D6D

C:\Windows\MSIMG32.dll Opens:

C:\Windows\System32\user32.dll Opens: Opens: C:\Windows\System32\wininet.dll C:\Windows\System32\ws2\_32.dll Opens: Opens: C:\Windows\System32\advapi32.dll Opens: C:\Windows\System32\crypt32.dll Opens: C:\Windows\System32\tzres.dll C:\Windows\System32\en-US\tzres.dll.mui Opens:

```
Opens:
                         C:\Windows\System32\mswsock.dll
                         C:\Windows\System32\WSHTCPIP.DLL
 Opens:
 Opens:
                         C:\Windows\Explorer.EXE.Local\
                         C:\Windows\winsxs\x86_microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
 Opens:
                         C:\Users\Admin
 Opens:
                         C:\Users\Admin\AppData\Local
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
```

Files\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5

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

Files\Content.IE5\desktop.ini

Opens: C:\Users\Admin\AppData\Roaming

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5

Opens:

C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini

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

Files\Content.IE5\index.dat

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

Opens:

C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

Opens: C:\Windows\dnsapi.DLL

Opens: C:\Windows\System32\dnsapi.dll
Opens: C:\windows\temp\MSIMG32.dll
Opens:

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

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

Opens: C:\Windows\system32\wbem\MSIMG32.dll
Opens: C:\Windows\System32\aeevts.dll
Opens: C:\Windows\System32\en-US\aeevts.dll.mui

Opens: C:\windows\System32\en-us\aeevts.dll.mu:
Opens: C:\windows\temp\spyeye\_injector.exe
Opens: C:\windows\RASAPI32.dll
Opens: C:\windows\System32\rasapi32.dll
Opens: C:\windows\rasman.dll

Opens: C:\Windows\System32\rasman.dll
Opens: C:\Windows\rtutils.dll

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

Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\

Opens: C:\Windows\System32\ras

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk

Opens: C:\Windows\sensapi.dll

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

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

Files\Low

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

Opens: C:\Users\Admin\AppData

Opens: C:\Users

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

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

Opens: C:\Users\Admin\AppData\Roaming\Microsoft

Opens: C:\Windows\System32\Sens.dl1
Opens: C:\Users\Admin\Favorites
Opens: C:\Windows\System32\stdole2.tlb

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

Files\Virtualized

 Opens:
 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE

 Opens:
 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache

 Opens:
 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low

 Opens:
 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache

 Opens:
 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache

 Opens:
 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low

Opens: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf

Opens: C:

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Low\Content.IE5

Opens: C:\Windows

Opens: C:\Windows\AppPatch
Opens: C:\Windows\Globalization
Opens: C:\Windows\Globalization\Sorting
Opens: C:\Windows\System32\en-US

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

```
C:\Windows\System32\KernelBase.dll
 Opens:
                         C:\Windows\Svstem32\locale.nls
 Opens:
                         C:\Windows\System32\gdi32.dll
                         C:\Windows\System32\lpk.dll
 Opens:
 Opens:
                         C:\Windows\System32\usp10.dll
 Opens:
                         C:\Windows\System32\msvcrt.dll
 Opens:
                         C:\Windows\System32\imagehlp.dll
 Opens:
                         C:\Windows\System32\apphelp.dll
 Opens:
                         C:\Windows\AppPatch\AcLayers.dll
 Opens:
                         C:\Windows\System32\sspicli.dll
 Opens:
                         C:\Windows\System32\rpcrt4.dll
 Opens:
                         C:\Windows\System32\shell32.dll
 Opens:
                         C:\Windows\System32\shlwapi.dll
 Opens:
                         C:\Windows\System32\ole32.dll
 Opens:
                         C:\Windows\System32\oleaut32.dll
 Opens:
                         C:\Windows\System32\userenv.dll
 Opens:
                         C:\Windows\System32\profapi.dll
 Opens:
                         C:\Windows\System32\winspool.drv
 Opens:
                         C:\Windows\System32\mpr.dll
 Opens:
                         C:\Windows\System32\msctf.dll
 Opens:
                         C:\Windows\System32\en-US\rundll32.exe.mui
 Opens:
                         C:\Windows\System32\urlmon.dll
 Opens:
                         C:\Windows\System32\msasn1.dll
 Opens:
                         C:\Windows\System32\iertutil.dll
 Opens:
                         C:\Windows\System32\uxtheme.dll
 Opens:
                         C:\Windows\System32\dwmapi.dll
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
                         C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\index.dat
                        C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
 Opens:
 Opens:
Opens:
                         C:\Windows\System32\nsi.dll
 Opens:
                         C:\Windows\System32\IPHLPAPI.DLL
 Opens:
                         C:\Windows\System32\winnsi.dll
 Opens:
                         C:\Windows\System32\nlaapi.dll
 Opens:
                         C:\Windows\System32\cryptbase.dll
 Opens:
                         C:\Windows\System32\rasadhlp.dll
 Opens:
                         C:\Windows\System32\en-US\wininet.dll.mui
 Opens:
                         C:\Windows\System32\rpcss.dll
 Opens:
                         C:\Windows\System32\NapiNSP.dll
 Opens:
                         C:\Windows\System32\pnrpnsp.dll
 Opens:
                         C:\Windows\System32\winrnr.dll
 Opens:
                         C:\Windows\System32\wship6.dll
 Opens:
                         C:\Windows\rasadhlp.dll
 Opens:
                         C:\Windows\system32\WININET.dll.manifest
                         C:\Windows\system32\rundll32.exe.Local\
 Opens:
                         C:\Program Files\Adobe\Reader 9.0\Reader\MSIMG32.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Low\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\desktop.ini
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\desktop.ini
 Opens:
 Opens:
                         C:\Windows\System32\drivers\etc\hosts
                         C:\Windows\System32\FWPUCLNT.DLL
 Opens:
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\desktop.ini
 Opens:
                         C:\Windows\System32\dot3api.dll
 Opens:
                         C:\Windows\System32\eappcfg.dll
 Opens:
                         C:\Windows\System32\wlanhlp.dll
 Opens:
                         C:\Windows\System32\wlanapi.dll
 Opens:
                         C:\Windows\System32\wlanutil.dll
 Opens:
                         C:\Windows\System32\onex.dll
 Opens:
                         C:\Windows\System32\eappprxy.dll
 Opens:
                         C:\Windows\Prefetch\MOBSYNC.EXE-C5E2284F.pf
 Opens:
                         C:\Windows\Prefetch\TASKHOST.EXE-7238F31D.pf
 Opens:
                         C:\Windows\Prefetch\UNSECAPP.EXE-A02905A6.pf
                         C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf
 Opens:
 Opens:
                         C:\Windows\System32\calc.exe
                         C:\Windows\Prefetch\PARANORMAL.EXE-7FD43081.pf
 Opens:
 Opens:
                         C:\Windows\Prefetch
                         C:\Windows\Prefetch\CALC.EXE-77FDF17F.pf
 Opens:
 Opens:
                         C:\$Extend
 Opens:
                         C:\dump.pcap
                         C:\Windows\system32\wdi\{86432a0b-3c7d-4ddf-a89c-
 Opens:
172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}\snapshot.etl
 Opens:
                         C:\Windows\System32\WDI\LogFiles\WdiContextLog.etl.001
 Opens:
                         C:\Windows\System32\wdi\LogFiles\WdiContextLog.etl.001
 Opens:
                         C:\Windows\System32\wdi\LogFiles\ShutdownCKCL.etl
                         C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-
 Opens:
172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}\snapshot.etl
```

Opens:

C:\Windows\System32\wdi\LogFiles\WdiContextLog.et1.002 Opens: Opens: C:\Windows\System32\wdi\LogFiles\BootCKCL.etl Opens:

C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics\_SystemData.bin

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

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Opens:

Performance%40perational.evtx

C:\Windows\System32\wdi\BootPerformanceDiagnostics\_SystemData.bin Opens:

Writes to: C:\WinOldFileg\83A494219A6.exe Writes to: C:\WinOldFileq\9C413B7B23C1D6D Writes to:

C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf Writes to: C:\Windows\Prefetch\MOBSYNC.EXE-C5E2284F.pf Writes to: C:\Windows\Prefetch\TASKHOST.EXE-7238F31D.pf Writes to: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf Writes to: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-

172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}\snapshot.etl

Writes to: C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics\_SystemData.bin

Writes to: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-

Performance%40perational.evtx

Writes to: C:\Windows\System32\wdi\BootPerformanceDiagnostics\_SystemData.bin

Reads from: C:\Windows\System32\ntdll.dll Reads from: C:\Windows\Temp\spyeye\_injector.exe Reads from: C:\WinOldFileq\83A494219A6.exe C:\WinOldFileq\9C413B7B23C1D6D Reads from: Reads from: C:\Windows\System32\user32.dll Reads from: C:\Windows\System32\wininet.dll Reads from: C:\Windows\System32\ws2\_32.dll Reads from: C:\Windows\System32\advapi32.dll Reads from: C:\Windows\System32\crypt32.dll Reads from: C:\Windows\System32\Sens.dll Reads from: C:\Windows\System32\stdole2.tlb

Reads from: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf

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

Reads from: C:\Windows\System32\wdi\LogFiles\WdiContextLog.etl.001 Reads from: C:\Windows\System32\wdi\LogFiles\ShutdownCKCL.etl Reads from: C:\Windows\System32\wdi\LogFiles\WdiContextLog.et1.002 Reads from: C:\Windows\System32\wdi\LogFiles\BootCKCL.etl Reads from: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-

172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}\snapshot.etl

C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics\_SystemData.bin Reads from:

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Reads from:

Performance%40perational.evtx

C:\Windows\System32\wdi\BootPerformanceDiagnostics\_SystemData.bin Reads from:

Deletes: C:\Windows\Temp\spveve injector.exe

#### Network Events

DNS query: alexeyartemov.com DNS query: wpad

DNS query: www.msftncsi.com

DNS query: teredo.ipv6.microsoft.com

alexeyartemov.com  $\Rightarrow$  198.105.244.11 DNS response: DNS response: alexeyartemov.com ⇒ 104.239.213.7 DNS response: a1961.g2.akamai.net ⇒ 58.27.86.16 a1961.g2.akamai.net  $\Rightarrow$  58.27.86.67 DNS response:

Connects to: 88.198.13.147:443 Connects to: 8.8.8.8:53 Connects to: 4.2.2.1:53 Connects to: 224.0.0.252:5355 Connects to: 198.105.244.11:80 Connects to: 58.27.86.16:80 104.239.213.7:80 Connects to: 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: 224.0.0.252:5355

alexeyartemov.com:80 (198.105.244.11) Sends data to: Sends data to: a1961.g2.akamai.net:80 (58.27.86.16) Sends data to: alexeyartemov.com:80 (104.239.213.7)

Receives data from: 8.8.8.8:53 Receives data from: 4.2.2.1:53 Receives data from: 88.198.13.147:443

alexeyartemov.com:80 (198.105.244.11) Receives data from: a1961.g2.akamai.net:80 (58.27.86.16) Receives data from: alexeyartemov.com:80 (104.239.213.7) Receives data from:

# Windows Registry Events

Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\run</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\0</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\1</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\2</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\3</pre>
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\4

Creates key: HKLM\software\microsoft\windows nt\currentversion\networklist\nla\cache

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

settings\lockdown\_zones\1

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

settings\lockdown\_zones\2

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

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: HKLM\software\microsoft\windows

nt\currentversion\networklist\nla\cache\intranet

Creates key: HKLM\software\microsoft\windows

nt\currentversion\networklist\nla\cache\intranet\

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

Creates key: HKCU\software\microsoft windows
Creates key: HKLM\software\microsoft\tracing

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

settings\connections

Creates key: HKLM\software\classes
Creates key: HKCU\software\appdatalow

Creates key: HKCU\software\microsoft\internet explorer\internetregistry
Creates key: HKCU\software\microsoft\internet explorer\lowregistry

Creates key: HKCU\software\microsoft\internet

explorer\lowregistry\dontshowmethisdialogagain

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

settings\5.0\lowcache

Creates key: HKCU\software\microsoft\internet explorer\intelliforms
Creates key: HKCU\software\microsoft\internet explorer\toolbar

Creates key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser

Creates key:

HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites

Creates key: HKCU\software\microsoft\internet explorer\pagesetup

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

settings\passport\lowdamap

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
Creates key: HKCU\software\microsoft\internet explorer\zoom

Creates key: HKCU\software\microsoft\internet explorer\browseremulation\lowmic

Creates key: HKCU\software\microsoft\internet explorer\ietld\lowmic Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location

awareness

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

Creates key: HKLM\software

Creates key: HKLM\software\microsoft

Creates key: HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-

08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection

Creates key: HKU\s-1-5-21-2160590473-689474908-1361669368-1002\software\microsoft\ras

autodial

 $\label{lem:creates} Creates \ key: \\ HKU\s-1-5-21-2160590473-689474908-1361669368-1002\\software\mbox{\em microsoft} \ rass \\ REAL \ rass \\ R$ 

autodial\default

Creates key: HKLM\software\microsoft\ras autodial 
Creates key: HKLM\software\microsoft\ras autodial\default

Creates key:

HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
Creates key: HKCU\software\microsoft\windows\currentversion\internet

settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}

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

settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}\ae-54-c5-b6-a2-81

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

settings\wpad\ae-54-c5-b6-a2-81

Creates kev:

 $HKLM \verb|\software\microsoft\windows\currentversion\diagnostics\performance\boot$ 

Creates key:

 $\label{thm:hklm} $$HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot\creates\key:$ 

Creates key:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown
Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

Deletes value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver]

Deletes value:

c19ce8a73253}[dhcpnameserver]

Deletes value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain]

Deletes value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpdomain]

Deletes value:

HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip\_{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpnameserverlist]

Deletes value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpsubnetmaskopt]

Deletes value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \ [dhcpdefaultgateway]$ 

Deletes value: HKLM\system\currentcontrolset\services\netbt\parameters[dhcpscopeid]

Deletes value:

 $HKLM \ system \ current control set \ services \ terms \ interfaces \ tcpip_{128919e8-8a5e-41d1-ac17-c19ce8a73253} \ [dhcpnetbiosoptions]$ 

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

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

Opens key: HKCU\

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

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrol\set\control\nls\sorting\versions

Opens key: HKLM\

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

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

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

Opens key: HKLM\system\setup

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

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

options\83a494219a6.exe

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

 $Opens \ key: \\ HKLM \ software \ microsoft \ windows \\ nt \ current version \ app compatflags \ custom \ 83a494219a6.exe$ 

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

Opens key: HKLM\hardware\devicemap\video

 $Opens~key: \\ HKLM \ system \ current control \ video \ \{c54b6caf-be91-4a10-ab56$ 

fd27e3774e32}\0000

Opens key:

 $\label{local-bound} \begin{tabular}{ll} HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev\_beef&subsys\_00000000&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-beef}. HKLM\system\currentcontrol\enum\pci\ven_80ee\&dev\_beef\&subsys\_00000000&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrolset\control\enum\pci\ven_80ee\&dev\_beef\&subsys\_00000000&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrolset\control\enum\pci\ven_80ee\&dev\_beef\&subsys\_00000000&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrol\enum\pci\ven_80ee\&dev\_beef\&subsys\_00000000&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrol\enum\pci\ven_80ee\&dev\_beef\&subsys\_00000000&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrol\enum\pci\ven_80ee\&dev\_beef\&subsys\_00000000&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrol\enum\pci\ven_80ee\&dev\_beef\&subsys\_00000000&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrol\enum\pci\currentcontrol\enum$ 

9dd4432fa2e9}\0000

0d8e74595f78}\0000

Opens key: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-

8ed0c8eb59a8}\0000

Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows

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

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

settings

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

Opens key:  ${\tt HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows}$ 

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock

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

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

 $\verb|migration\providers\psched|\\$ 

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

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

migration\providers\tcpip

Opens key:

 $HKLM \ system \ current control set \ services \ tcpip6 \ parameters \ interfaces \ \{f3229805-869e-479e-ba76-dd643f1d1b80\}$ 

Opens key: HKLM\software\microsoft\internet explorer

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user agent Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent Opens kev: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\user agent

settings\5.0\user agent

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

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

settings\user agent

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

settings\user agent

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user

agent\ua tokens

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

agent\pre platform

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

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\microsoft\windows\currentversion\internet settings\user

agent\post platform

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

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: Opens key:  $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc main\feature} control} \\$ 

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_browser\_emulation Opens key:

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

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

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

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

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

settings

 $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ internet\ explorer\+ main\+ feature control$ Opens key: Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol

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

settings\5.0\cache

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

settings\5.0\cache Opens key:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content

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

settings\5.0\cache\content

Opens key:  $HKCU \ software \ `microsoft\ `windows \ `current version \ `explorer \ 's ession in follows \ 'current version' \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer' \ 'explorer' \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer'' \ 'expl$ 

Opens key:

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

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

folders

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

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

settings\5.0\cache\history

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

settings\5.0\cache\history

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

settings\5.0\cache\extensible cache

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat

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

settings\5.0\cache\extensible cache\iecompat  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ 

Opens key: settings\5.0\cache\extensible cache\ietld

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

settings\5.0\cache\extensible cache\privacie:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset Opens key: HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_bufferbreaking_818408
                        HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_bufferbreaking_818408
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                        HKLM\software\microsoft\internet
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\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                        HKLM\software\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\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                        HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                        HKCU\software\microsoft\windows\currentversion\internet settings\wpad
 Opens kev:
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
 Opens key:
                        HKLM\system\currentcontrolset\control\cryptography\providers
 Opens kev:
                        HKLM\system\currentcontrolset\control\cryptography\configuration
 Opens key:
                        HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens kev:
dd643f1d1b80}
 Opens key:
44e829c34f68}
```

```
Opens key:
c19ce8a73253}
44e829c34f68}
   Opens kev:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{0aab3bce-41ed-11e5-bf5b-
080027dfc114}
   Opens key:
c19ce8a73253}
   Opens key:
080027dfc114}
   Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus topip6 \setminus parameters \setminus interfaces \setminus \{69d2510e-6c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b3bc-4c18-11e3-b5bc-4c18-11e3-b5bc-4c18-11e3-b5bc-4c18-5c18-11e3-b5bc-4c18-5c18-11e3-b5bc-4c18-11e3-b5bc-4c18-
a199dcc7ccd3}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{69d2510e-6c18-11e3-b3bc-
a199dcc7ccd3}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{7c5653f0-144a-4534-9e34-
28ac99cba85e}
   Opens key:
                                               HKCU\appevents\schemes\
   Opens key:
                                               HKCU\appevents\schemes\apps\.default\open\.current
   Opens key:
                                               HKCU\appevents\schemes\apps\.default\open\.current\active
   Opens key:
806e6f6e6963}
   Opens key:
28ac99cba85e}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{69d2510f-6c18-11e3-b3bc-
a199dcc7ccd3}
   Opens key:
                                               HKLM\software\microsoft\cryptography\oid
                                               HKLM\software\microsoft\cryptography\oid\encodingtype 0
   Opens key:
   Opens key:
                                               HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov
                                               HKLM\software\microsoft\cryptography\oid\encodingtype
   Opens key:
0\certdllopenstoreprov\#16
   Opens key:
                                               HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\ldap
   Opens key:
                                               HKLM\software\microsoft\cryptography\oid\encodingtype 1
   Opens key:
                                               HKLM\software\microsoft\cryptography\oid\encodingtype
1\certdllopenstoreprov
   Opens key:
                                               HKCU\software\microsoft\systemcertificates\my\physicalstores
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002
                                               HKCU\software\microsoft\systemcertificates\my
   Opens key:
                                               HKCU\software\microsoft\systemcertificates\my\
   Opens key:
                                               HKCU\software\microsoft\systemcertificates\my\certificates
   Opens key:
   Opens key:
                                               HKCU\software\microsoft\systemcertificates\my\crls
   Opens kev:
                                               HKCU\software\microsoft\systemcertificates\my\ctls
   Opens key:
                                               HKCU\software\microsoft\systemcertificates\my\keys
   Opens kev:
806e6f6e6963}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{69d2510f-6c18-11e3-b3bc-
a199dcc7ccd3}
   Opens key:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{8ff7f47b-d658-4061-baea-defaces, and backets \ defaces, and backets \ defaces, and backets \ defaces, and backets \ defaces \ defa
1709a0196aed}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
   Opens key:
                                               HKCU\appevents\schemes\apps\.default\close\.current
                                               HKCU\appevents\schemes\apps\.default\close\.current\active
   Opens kev:
                                               HKLM\software\microsoft\windows
   Opens key:
nt\currentversion\appcompatflags\compatibility assistant
   Opens kev:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6fe-7037-11de-816d-
001c23e25b76}
   Opens kev:
001c23e25b76}
   Opens kev:
```

 $HKLM \ system \ current control set \ services \ typip \ parameters \ interfaces \ \{e29ac701-7037-11de-816d-104814, and \ extractions and \ extractions are the system \ for the system \ for \ extractions and \ extractions are the system \ for \ extractions and \ extractions are the system \ for \ extractions and \ extractions are the system \ for \ extractions \$ 

001c23e25b76} Opens kev:

```
001c23e25b76}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac700-7037-11de-816d-
001c23e25b76}
     Opens kev:
001c23e25b76}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{db2b4279-b5cf-4626-9dba-
32d0ece44c87}
     Opens kev:
32d0ece44c87}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e2f8a220-af88-446c-9a55-
453e58dd3a33}
     Opens kev:
                                                                             HKLM\system\currentcontrolset\services\tcpip\linkage
     Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e28d896f-9ea8-433a-9c10-
66c97c19a921}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e28d896f-9ea8-433a-9c10-
66c97c19a921}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{dcb14c61-690d-46f7-8a89-
150432fa5c44}
e4c1f1f568cb}
     Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{483c9ff8-503d-414b-b402-
e4c1f1f568cb}
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{c0de3e38-8ba7-479f-8b75-
833f294c5aa8}
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{c0de3e38-8ba7-479f-8b75-
833f294c5aa8}
                                                                             HKLM\system\currentcontrolset\services\eventlog\system
     Opens key:
     Opens key:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{eef54e71-0661-422d-9a98-424e14, and because the substitution of the substitution of
 82fd4940b820}\channelreferences
     Opens kev:
82fd4940b820}\channelreferences\0
     Opens key:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{eef54e71-0661-422d-9a98-424e14, and because the substitution of the substitution of
 82fd4940b820}\channelreferences\1
     Opens kev:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\2
     Opens kev:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{eef54e71-0661-422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-142
82fd4940b820}\channelreferences\3
     Opens kev:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\4
     Opens kev:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\5
     Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\6
     Opens kev:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
```

82fd4940b820}\channelreferences\7

HKLM\software\microsoft\tracing\explorer\_rasapi32 Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: HKLM\software\microsoft\tracing\explorer\_rasmancs HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e} Opens kev:  $HKCR \ clsid \ \{d5978620 - 5b9f - 11d1 - 8dd2 - 00aa004abd5e\} \ treatas$ Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\progid Opens key: Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32  $HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\$ Opens key: Opens key:  $HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\ \ \ in prochandler$ Opens key: HKCU\software\classes\ HKLM\software\classes Opens key: Opens key: HKCU\software\classes\autoproxytypes Opens key: HKCR\autoproxytypes

Opens key: HKCU\software\classes\autoproxytypes\application/x-internet-signup

Opens key: HKCR\autoproxytypes\application/x-internet-signup

Opens key:  $\label{lem:hkcu} \verb+KKCU\+ software \verb+\classes+ autoproxy types+ application/x-ns-proxy-autoconfiger and the property of the$ 

Opens key: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig

```
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
     Opens key:
HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib
     Opens key:
                                                                            HKCR\tvpelib
     Opens key:
                                                                            HKCR \typelib \d597deed-5b9f-11d1-8dd2-00aa004abd5e\}
     Opens key:
                                                                            HKCR \typelib \d597deed-5b9f-11d1-8dd2-00aa004abd5e \center{lib} \center{lib} \d597deed-5b9f-11d1-8dd2-00aa004abd5e \center{lib} \d597deed-5b9f-11d1-8dd2-00a
                                                                            HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0
     Opens key:
                                                                            Opens key:
                                                                            HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}
     Opens key:
     Opens key:
                                                                            HKCR\typelib\{00020430-0000-0000-c000-00000000046}
     Opens key:
                                                                            HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0
     Opens key:
                                                                            HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
                                                                            HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
     Opens key:
     Opens key:
                                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\rundll32.exe
                                                                            HKI M\software\microsoft\windows
     Opens key:
 nt\currentversion\appcompatflags\custom\rundll32.exe
     Opens key:
                                                                            HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
     Opens key:
                                                                            HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                                                            HKCU\software\microsoft\internet
     Opens kev:
 explorer\main\featurecontrol\feature_mime_handling
     Opens key:
                                                                           HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_mime_handling
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows\ipsec\gptipsecpolicy
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows\ipsec\policy\local
     Opens key:
                                                                            HKCU\software\microsoft\windows nt\currentversion\appcompatflags
     Opens key:
                                                                            HKLM\system\currentcontrolset\control\cmf\config
     Opens key:
                                                                            HKLM\system\currentcontrolset\control\networkprovider\hworder
     Opens key:
                                                                            HKLM \ sam \ domains \ account \ groups \ \ 000003ea
     Opens key:
                                                                            HKLM\sam\sam\domains\account\aliases\000003ea
     Opens key:
                                                                            HKLM\sam\sam\domains\account\users\000003ea
                                                                            HKLM\system\currentcontrolset\services\winsock2\parameters
     Opens key:
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\dnscache\parameters
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows nt\dnsclient
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\dns
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
     Opens key:
Opens key:
                                                                            HKLM\software\microsoft\rpc
                                                                            HKLM\software\policies\microsoft\system\dnsclient
     Opens kev:
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows nt\rpc
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
                                                                            HKCU\software\microsoft\windows\currentversion\internet
     Opens key:
 settings\5.0\lowcache
     Opens kev:
                                                                            HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\lowcache\content
     Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
ba85-6007caedcf9d}
     Opens key:
                                                                            HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
     Opens kev:
ba85-6007caedcf9d}\propertybag
     Opens key:
                                                                            HKCU\software\microsoft\windows\currentversion\explorer
     Opens key:
                                                                            HKLM\software\policies\microsoft\windows\explorer
     Opens key:
                                                                            HKCU\software\policies\microsoft\windows\explorer
     Opens key:
9d55-7b8e7f157091}
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ 'f1b32785-6fba-4fcf-explorer' \ 'folder \ 'f1b32785-6fba-4fcf-explorer' \ 'f1b32785-6fba-4fc
9d55-7b8e7f157091}\propertybag
     Opens key:
HKLM \setminus software \setminus irrosoft \setminus ir
9afe-ea3317b67173}
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
     Opens key:
                                                                            HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\lowcache\cookies
     Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}
     Opens kev:
HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `ex
```

908e-08a611b84ff6}\propertybag Opens kev: a03a-e3ef65729f3d} Opens kev: a03a-e3ef65729f3d}\propertybag HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\lowcache\history Opens key:  $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ 'folder descriptions \ '\{d9dc8a3b-b784-432e-d742e-d$ a781-5a1130a75963} Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}\propertybag HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\lowcache\extensible cache Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\lowcache\extensible cache\iecompat HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\lowcache\extensible cache\ietld HKLM\software\microsoft\windows Opens key: nt\currentversion\networklist\profiles\{af1709b3-b8ae-42fd-82e7-ca712dddaac3} HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3} HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\307bda19-07de87e0 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\307bda19 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries Opens key:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col\_catalog \\ \setminus catalog \\ \setminus$ Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000000 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000003 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000010 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000011 Opens key: Opens key: HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000013 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000014 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000016 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000017 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000018 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\0000000c

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 00000000000001)$ 

Opens key:

Opens kev:

Opens key:

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
```

Opens key: HKLM\system\currentcontrol\sqmservicelist
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\

Opens key: HKU\

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

settings\connections

Opens key: HKLM\system\currentcontrolset\enum\bth

Opens key: HKLM\system\currentcontrolset\enum\root\ms\_agilevpnminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0001

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

 $08002be10318\} \verb|\| 0001\| ndi \verb|\| interfaces$ 

Opens key: HKLM\system\currentcontrolset\enum\root\\*isatap\0000

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0009

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0009\ndi\interfaces

Opens key: HKLM\system\currentcontrolset\enum\root\ms\_12tpminiport\0000

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0002

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0002\ndi\interfaces

Opens key: HKLM\system\currentcontrolset\enum\root\\*teredo\0000

Opens key: HKLM\system\currentcontrol\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0011

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0011\ndi\interfaces

Opens key: HKLM\system\currentcontrolset\enum\root\ms\_ndiswanbh\0000

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0006

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

 $08002be10318\} \verb|\ooo6\ndi\interfaces| \\$ 

Opens key:

HKLM\system\currentcontrolset\enum\pci\ven\_8086&dev\_100e&subsys\_001e8086&rev\_02\3&267a616a&0&18
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0007

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318\0007\ndi\interfaces

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

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0007\ndi

Opens key: HKLM\software\microsoft\network\media

Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\implemented

categories\{00000003-0000-0000-c000-000000000046}

Opens key: HKLM\system\currentcontrolset\enum\root\ms\_ndiswanip\0000

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0008

Opens key: HKLM\system\currentcontrol\class\{4d36e972-e325-11ce-bfc1-

 $08002be10318\} \verb|\| 0008 \verb|\| ndi \verb|\| interfaces |$ 

Opens key: HKLM\system\currentcontrolset\enum\root\ms\_ndiswanipv6\0000

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0005

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

 $08002be10318\} \verb|\| 0005\| interfaces |$ 

Opens key: HKLM\system\currentcontrolset\enum\root\ms\_pppoeminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0004

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0004\ndi\interfaces

Opens key: HKLM\system\currentcontrolset\enum\root\ms\_pptpminiport\0000

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0003

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0003\ndi\interfaces

Opens key: HKLM\system\currentcontrolset\enum\root\ms\_sstpminiport\0000

Opens key: HKLM\system\currentcontrol\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0000

Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0000\ndi\interfaces

Opens key: HKU\s-1-5-21-2160590473-689474908-13616693681002\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKU\s-1-5-21-2160590473-689474908-1361669368-1002
Opens key: HKU\s-1-5-21-2160590473-689474908-1361669368-1002\control

panel\international

HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-Opens key: 00805fc1270e}\inprocserver32 Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32 Opens key: aad2-00805fc1270e} HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d} Opens key: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d} Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069a2dd-08002b30309d} Opens key:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{21ec 2020 - 3aea - 1069$ a2dd-08002b30309d} Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key:  $HKLM \ software \ microsoft \ windows \ current version \ explorer \ control panel \ names pace \ \{7007acc7-3202-4007acc7-32007acc$ 11d1-aad2-00805fc1270e} Opens key:  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ control panel \ names pace \ \{7007acc7-3202-4007acc7-32007acc$ 11d1-aad2-00805fc1270e} HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d} Opens kev: Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d} Opens key:  $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus \{2227a280-microsoft \setminus explorer \setminus clsid \setminus explorer \setminus clsid$ 3aea-1069-a2de-08002b30309d}  $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in foll control panel \ name space \ name customizations$ HKLM\svstem\currentcontrolset\control\mui\stringcachesettings Opens key: Opens key: HKCU\software\classes\local settings\muicache\27\52c64b7e Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key: HKLM\system\currentcontrolset\services\netbt\linkage Opens key:  $\label{lem:hkcu} \verb+KKCU \system \current control \end{to} \verb+lem \end{to} \verb+lem$ Opens key: HKLM\software\microsoft\rpc\securityservice HKU\.default\control panel\international Opens kev: Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\connections HKLM\system\currentcontrolset\services\nlasvc\parameters\internet Opens key: HKU\s-1-5-20 Opens key: Opens key: HKU\s-1-5-20\control panel\international HKLM\system\currentcontrolset\control\wmi\security Opens kev: Opens key:  $HKLM \verb|\system| current control set \verb|\services| mpssvc \verb|\parameters| portkeywords \verb|\dhcp| and the substitution of the sub$ HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip\_{128919e8-8a5e-41d1ac17-c19ce8a73253} Opens key: HKLM\system\currentcontrolset\services\{128919e8-8a5e-41d1-ac17c19ce8a73253}\parameters\tcpip Opens key: HKLM\system\currentcontrolset\services\netbt\adapters\{128919e8-8a5e-41d1-ac17-c19ce8a73253} Opens key: HKLM\system\currentcontrolset\services\netbt\parameters HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ Opens key: HKLM\software\policies\microsoft\internet explorer\security HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\classes\applications\calc.exe Opens key: Opens key: HKCR\applications\calc.exe Opens key: HKLM\software\policies\microsoft\windows\networkconnectivitystatusindicator HKLM\software\microsoft\ctf\knownclasses Opens key: Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32 Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32 Opens key: HKLM\software\policies\microsoft\netlogon\parameters Opens key:  ${\it HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ net logon \verb|\ parameters | \\$ Opens key: HKLM\software\policies\microsoft\windows\reliability analysis\wmi HKLM\software\microsoft\reliability analysis\wmi Opens kev: Opens key: HKLM\software\policies\microsoft\windows\system Opens key: HKLM\software\microsoft\windows\currentversion\winevt Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers Opens key:  $HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} White \label{limit$ 622caee05b0a}

Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/operational

HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-

 $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ eventlog \+ microsoft - windows - system \+ current \+ cur$ Opens kev:

diagnostics-performance/diagnostic

diagnostics-performance/operational

Opens key:

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -diagnostic s - wind$ performance/diagnostic

Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-

diagnostics-performance/diagnostic/loopback

Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic/loopback

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

manager[cwdillegalindllsearch]

HKLM\system\currentcontrolset\control\terminal server[tsappcompat1] Oueries value: Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]

Oueries value:

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

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

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

Queries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest] Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

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

Queries value:

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

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

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\appcompatflags\layers[c:\winoldfileq\83a494219a6.exe]

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

Queries value: HKLM\hardware\devicemap\video[maxobjectnumber] HKLM\hardware\devicemap\video[\device\video3] Queries value:

Queries value:  $HKLM \ system \ current control \ video \ \{c54b6caf-be91-4a10-ab56-be91-4a10-ab$ 

fd27e3774e32}\0000[pruningmode]

HKLM\hardware\devicemap\video[\device\video0] Queries value:

HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-Oueries value:

9dd4432fa2e9}\0000[pruningmode]

HKLM\hardware\devicemap\video[\device\video1] Queries value:

Queries value: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-

0d8e74595f78}\0000[pruningmode]

HKLM\hardware\devicemap\video[\device\video2] Queries value:

HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-Oueries value:

8ed0c8eb59a8}\0000[pruningmode]

HKLM\software\microsoft\windows Oueries value: nt\currentversion\gre\_initialize[disablemetafiles] Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[83a494219a6]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

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

settings[disableimprovedzonecheck]

 $HKLM \verb|\software\policies\microsoft\windows\currentversion\| internet$ Oueries value:

settings[security\_hklm\_only]

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

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

Oueries value:

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

Queries value:

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

migration\providers\psched[winsock 2.0 provider id]

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

HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

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

Oueries value:

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

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

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

HKLM\software\microsoft\windows nt\currentversion\compatibility32[lsass] Oueries value:

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

settings\5.0\user agent[]

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

settings\5.0\user agent[]

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

settings\5.0\user agent[compatible]

Oueries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version] HKLM\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\user agent[version] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user agent] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform] Oueries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_browser\_emulation[explorer.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation[\*] Oueries value: a3fe-553973d0b723] Queries value: HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796b924-d51178a59ce41 HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[fromcachetimeout] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[secureprotocols] HKCU\software\policies\microsoft\windows\currentversion\internet Queries value: settings[secureprotocols] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[secureprotocols]  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Oueries value: settings[certificaterevocation] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[disablekeepalive] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[disablepassport] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[idnenabled] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[cachemode] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[enablehttp1 1] Queries value:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}$ settings[enablehttp1\_1] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[enablehttp1\_1] Oueries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1] Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet 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: HKCU\software\microsoft\windows\currentversion\internet settings[disablebasicoverclearchannel] HKCU\software\microsoft\internet Oueries value: explorer\main\featurecontrol[feature\_clientauthcertfilter] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol[feature\_clientauthcertfilter] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[syncmode5]  $\label{lem:hammon} \begin{tabular}{ll} HKLM \end{tabular} windows \current version \end{tabular} in termet$ Queries value: settings\5.0\cache[sessionstarttimedefaultdeltasecs] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\content[peruseritem] Queries value:  $\label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet$ settings\5.0\cache\content[peruseritem] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\content[cacheprefix] Queries value:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\5.0\cache\content[cachelimit] Queries value:  $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}$ settings\5.0\cache\cookies[peruseritem]  $\label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet$ Oueries value: settings\5.0\cache\cookies[peruseritem] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

HKCU\software\microsoft\windows\currentversion\internet

folders[cookies]
Queries value:

```
settings\5.0\cache\cookies[cacheprefix]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\cookies[cachelimit]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:
                                      \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings\5.0\cache\history[peruseritem]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\history[cachelimit]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[enableautoproxyresultcache]
  Oueries value:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
  Queries value:
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings[mbcsservername]
                                      \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu} \mbox{\tt hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu
  Oueries value:
settings[mbcsapiforcrack]
                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \notation{Internet}{ll} \end{tabular}
  Oueries value:
settings[utf8servernameres]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disableworkerthreadhibernation]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[socketreceivebufferlength]
```

```
Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsper1_0server]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                           HKI M\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[certcachenovalidate]
 Queries 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\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[explorer.exe]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
 Queries value:
settings[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[wpadsearchalldomains]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[bypasshttpnocachecheck]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
 Queries value:
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[bypasssslnocachecheck]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
 Queries value:
                           \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[nocheckautodialoverride]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
```

```
settings[dontusednsloadbalancing]
                         HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
 Queries value:
                         \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[mimeexclusionlistforcache]
                         \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Oueries value:
settings[headerexclusionlistforcache]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
 Queries value:
                         \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[dnscacheentries]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonzonecrossing]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonbadcertrecving]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[alwaysdrainonredirect]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonhttpstohttpredirect]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\wpad[wpadoverride]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nonetautodial]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[globaluseroffline]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[badproxyexpirestime]
                         HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablebranchcache]
 Queries value:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[explorer.exe]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[*]
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
 Oueries value:
c19ce8a73253}[enabledhcp]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\compatibility32[spyeye_injector]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
 Oueries value:
c19ce8a73253}[registeradaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
 Oueries value:
c19ce8a73253}[dhcpdomain]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
 Queries value:
c19ce8a73253}[nameserver]
 Queries value:
                         HKCU\appevents\schemes[]
 Queries value:
                         HKCU\appevents\schemes\apps\.default\open\.current[]
 Oueries value:
                         HKCU\appevents\schemes\apps\.default\open\.current[default flags]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
 Queries value:
                         HKLM\system\currentcontrolset\services\crypt32[diaglevel]
```

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

2160590473-689474908-1361669368-1002[profileimagepath]

Queries value

 $\label{lem:hklmsystem} Hklm \end{area} Hklm \end{area} The substitution of the subst$ 

Queries value:

 $\label{lem:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [registration enabled]$ 

Oueries value:

 $\label{lem:hklm} HKLM \system \current controls et \services \tcpip \parameters \ interfaces \end{6e} e29 ac6 c2-7037-11 de-816 d-806 e6f6 e6963 \end{6e} [register adapter name]$ 

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [domain]$ 

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{e29ac6c2-7037-11de-816d-806e6f6e6963\}[dhcpdomain]$ 

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [nameserver]$ 

Queries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{e29ac6c2-7037-11de-816d-806e6f6e6963\} \ [dhcpnameserver]$ 

Queries value: HKCU\appevents\schemes\apps\.default\close\.current[]

Queries value: HKCU\appevents\schemes\apps\.default\close\.current[default flags]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\compatibility assistant[logignoremonitorreason] Oueries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Queries value: HKLM\system\currentcontrolset\services\eventlog\system[type] Queries value: HKLM\system\currentcontrolset\services\eventlog\system[filemax] Queries value:  ${\tt HKLM \ } system \verb| current control set \verb| services \verb| eventlog \verb| system[file counter]|$ Queries value:  ${\tt HKLM \ } system \verb| current control set \verb| services \verb| eventlog \verb| system [buffer size]|$ Queries value: HKLM\system\currentcontrolset\services\eventlog\system[minbuffers] Oueries value: HKLM\system\currentcontrolset\services\eventlog\system[maxbuffers] Queries value: HKLM\system\currentcontrolset\services\eventlog\system[latency] Queries value: HKLM\system\currentcontrolset\services\eventlog\system[clocktype] Oueries value: HKLM\system\currentcontrolset\services\eventlog\system[level]

 Queries value:
 HKLM\system\currentcontrolset\services\eventlog\system[level]

 Queries value:
 HKLM\system\currentcontrolset\services\eventlog\system[controlguid]

 Queries value:
 HKLM\system\currentcontrolset\services\eventlog\system[maxsize]

 Queries value:
 HKLM\system\currentcontrolset\services\eventlog\system[maxsizeupper]

 Queries value:
 HKLM\system\currentcontrolset\services\eventlog\system[retention]

Queries value:

 ${\tt HKLM \ } system \verb| current control set \verb| services \verb| eventlog \verb| system [autobackuplog files]| \\$ 

 Queries value:
 HKLM\system\currentcontrolset\services\eventlog\system[file]

 Queries value:
 HKLM\system\currentcontrolset\services\eventlog\system[flags]

 Queries value:
 HKLM\system\currentcontrolset\services\eventlog\system[filterid]

Queries value: HKLM\system\currentcontrolset\services\eventlog\system[owningpublisher]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[customsd]

Oueries value:

 $\label{lem:hklmsoftwaremicrosoftwindows\currentversion\winevt\publishers\\ \{eef54e71-0661-422d-9a98-82fd4940b820\}\\ \channel{lem:hklmsoftware}$ 

Queries value:

 $\label{thm:local-pages} $$HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820\}\channelreferences\0[]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\0[flags]

Queries value:

 $\label{limit} $HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820\}\channelreferences\0[id]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\1[]

Queries value:

 $HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\lifelags\}$ 

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows\currentversion\winevt\publishers\\ \{eef54e71-0661-422d-9a98-82fd4940b820\}\\ \channel{lem:hklmsoftware} \label{lem:hklmsoftware} \label{lem:hklmsoftware}$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{eef54e71-0661-422d-9a98-82fd4940b820\} \ channel \ references \ []$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{eef54e71-0661-422d-9a98-82fd4940b820\} \ \ channel \ references \ [flags]$ 

Queries value:

 $\label{limited-basis} HKLM\software\microsoft\windows\currentversion\winevt\publishers\effields with the sum of the sum$ 

Queries value:

 $\label{limited-basis} HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820\}\channelreferences\3[]$ 

Queries value:

```
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\3[flags]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\3[id]
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\4[]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\4[flags]
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\4[id]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\5[]
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\5[flags]
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\5[id]
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\6[]
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\6[flags]
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\6[id]
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\7[]
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\7[flags]
  Queries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{eef54e71-0661-422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1422d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-1420d-9a98-142
82fd4940b820}\channelreferences\7[id]
                                     HKLM\software\microsoft\tracing[enableconsoletracing]
  Oueries value:
                                     HKLM\software\microsoft\tracing\explorer_rasapi32[enablefiletracing]
  Queries value:
                                     HKLM\software\microsoft\tracing\explorer_rasapi32[filetracingmask]
                                     HKLM\software\microsoft\tracing\explorer_rasapi32[enableconsoletracing]
  Oueries value:
  Queries value:
                                     HKLM\software\microsoft\tracing\explorer_rasapi32[consoletracingmask]
  Queries value:
                                     HKLM\software\microsoft\tracing\explorer_rasapi32[maxfilesize]
  Queries value:
                                     HKLM\software\microsoft\tracing\explorer_rasapi32[filedirectory]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
                                     HKLM\software\microsoft\tracing\explorer_rasmancs[enablefiletracing]
  Oueries value:
  Oueries value:
                                     HKLM\software\microsoft\tracing\explorer_rasmancs[filetracingmask]
  Queries value:
                                     HKLM\software\microsoft\tracing\explorer_rasmancs[enableconsoletracing]
  Queries value:
                                     HKLM\software\microsoft\tracing\explorer_rasmancs[consoletracingmask]
  Oueries value:
                                     HKLM\software\microsoft\tracing\explorer_rasmancs[maxfilesize]
  Queries value:
                                     HKLM\software\microsoft\tracing\explorer_rasmancs[filedirectory]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Oueries value:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyenable]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                                     HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[]
  Queries value:
                                     HKCR\clsid\{d5978620-5b9f-11d1-8dd2-
  Queries value:
00aa004abd5e}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[]
  Oueries value:
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[autoconfigurl]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\connections[savedlegacysettings]
  Queries value:
                                     HKCR\clsid\{d5978620-5b9f-11d1-8dd2-
00aa004abd5e}\inprocserver32[threadingmodel]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\connections[defaultconnectionsettings]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigcustomua]
  Queries value:
                                     HKCR\autoproxytypes\application/x-internet-signup[dllfile]
```

```
HKCR\autoproxytypes\application/x-internet-signup[fileextensions]
 Oueries value:
                      HKCR\autoproxytypes\application/x-internet-signup[default]
 Oueries value:
 Oueries value:
                      HKCR\autoproxytypes\application/x-internet-signup[flags]
                      HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]
 Queries value:
 Oueries value:
                      HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
 Queries value:
                      HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]
                      HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]
 Oueries value:
                      HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
 Oueries value:
Oueries value:
                      HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
 Oueries value:
Oueries value:
                      HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Oueries value:
                     HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
 Oueries value:
Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
 Oueries value:
Queries value:
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[]
 Oueries value:
 Queries value:
                      HKCR \land (d597bab1-5b9f-11d1-8dd2-00aa004abd5e) \land (d597bab1-6b9f-11d1-8dd2-00aa004abd5e) \land (d597bab1-6b9f-11d1-6b9f-11d
 Queries value:
                      HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32[]
 Oueries value:
                      HKCR\interface\{d597bab1-5b9f-11d1-8dd2-
00aa004abd5e}[interfacehelperdisabletypelib]
 Queries value:
                      HKCR\interface\{d597bab1-5b9f-11d1-8dd2-
00aa004abd5e}[interfacehelperdisableall]
                      HKCR\interface\{d597bab1-5b9f-11d1-8dd2-
 Oueries value:
00aa004abd5e}[interfacehelperuser]
                      HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
 Oueries value:
                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[explorer.exe]
 Queries value:
HKLM\software\policies\microsoft\windows\ipsec\policy\local[activepolicy]
 Oueries value:
                      HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
 Queries value:
                      HKLM\software\microsoft\windows
nt\currentversion\compatibilitv32[rundll32]
 Queries value:
                      HKLM\system\currentcontrolset\control\cmf\config[system]
                      HKLM\sam\sam\domains\account\users\000003ea[v]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
                      HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
 Oueries value:
```

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

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] 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: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]$ Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Queries value:

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

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

Queries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Queries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout] HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts] Oueries value:  $\label{lem:hklm} \verb+Kklm/system/currentcontrolset/services/tcpip/parameters[dnsquerytimeouts]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\lowcache[signature] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\lowcache\content[peruseritem] Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6[winsock 2.0 provider id] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} = \{ parameters \setminus winsock [minsock addrlength] \} \} = \{ parameters \setminus winsock [minsock addrlength] \} = \{ param$ Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname] Queries value: ba85-6007caedcf9d}[category] Oueries value: ba85-6007caedcf9d}[name] ba85-6007caedcf9d}[parentfolder] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251ba85-6007caedcf9d}[description] ba85-6007caedcf9d}[relativepath] Queries value: ba85-6007caedcf9d}[parsingname] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251ba85-6007caedcf9d}[infotip] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle] Queries value: ba85-6007caedcf9d}[localizedname] Oueries value:

ba85-6007caedcf9d}[icon]

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '{352481e8-33be-4251-ba85-6007} caed \ cf9d \ [stream resource]$ 

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '{352481e8-33be-4251-ba85-6007} caed \ 'folder \ 'folder \ 'folder \ 'explorer' \ 'folder \ 'folde$ 

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '{352481e8-33be-4251-ba85-6007} caed \ 'folder \ 'folder \ 'folder \ 'explorer' \ 'folder \ 'folde$ 

Queries value:

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

Queries value:

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

Queries value:

Oueries value:

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

Oueries value

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

Queries value:

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{352481e8-33be-4251-ba85-6007 caed \ folder \ 'handler' \ 'explorer' \ 'folder \ 'handler' \ 'explorer' \ 'folder \ 'explorer' \ 'folder \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer'' \ 'expl$ 

Oueries value

 $\label{thm:local-problem} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}(category)$ 

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

Queries value:

 $\label{thm:local-problem} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifthfully folderdescriptions \fifth a 2785-6 fba-4 fcf-9 d55-7 b8e7 f157091\fifth parsing name]$ 

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 1532785-6 fba-4fcf-9d55-7b8e7f157091 \cite{1}{1} \cite{1} \cite{1}{1} \cite{1}{1}$ 

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}[icon]$ 

Queries value:

 $\label{thm:hklm} $$HKL^M\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[security]$$ 

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}treamresource\figure{1}{2}$ 

Queries value:

 $\label{thm:hk.mass} $$HKL^M\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[streamresourcetype]$$ 

Queries value:

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \find 2785-6 fba-4 fcf-9 d55-7 b8e7 f157091 \find \cite{157091} [stream]$ 

Queries value:

Oueries value:

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

Queries value:

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

Queries value:

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

folders[local appdata]
 Queries value:

 $HKLM \ software \ `microsoft \ 'encountersion' \ explorer \ 'folder descriptions' \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [category]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ forme1$ 

Queries value:

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

Oueries value

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

Queries value

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

Oueries value:

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

Oueries value:

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

Oueries value

 $HKLM \ software \ `microsoft \ 'enclosed \ 'enclosed$ 

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value

 $\label{thm:hklm} $$HKL^M\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[foldertypeid]$$ 

Queries value:

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

Oueries value: HKCU\software\

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\lowcache\content[cacheprefix]

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

settings\5.0\lowcache\content[cachelimit]

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

settings\5.0\lowcache\cookies[peruseritem]

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folder descriptions \currentversion\explorer\folder \currentversion\explorer\folder \currentversion\explorer\folder\currentversion\explorer\folder\currentversion\explorer\folder\currentversion\explorer\folder\currentversion\explorer\folder\currentversion\explorer\explorer\folder\currentversion\explorer\exp$ 

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'endows \ 'en$ 

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsoftwaremicrosoftwindows} Label{lem:hklmsof$ 

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

a03a-e3ef65729f3d}[security]

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

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

settings\5.0\lowcache\cookies[cacheprefix]

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

settings\5.0\lowcache\cookies[cachelimit]

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

settings\5.0\lowcache\history[peruseritem]

Queries value:

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \ [queryadaptername]$ 

Queries value:

 $\label{thm:hklm} HKL^{M} system \current controlset \services \trip\parameters \ interfaces \ \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} [disable adapter domain name]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \interfaces \{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \cite{lem:hklmsystem} \end{subarray} \end{subarray} \end{subarray} \label{lem:hklmsystem}$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{128919e8-8a5e-41d1-ac17-c19ce8a73253\} \ [maxnumber of addresses to register]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

a781-5a1130a75963}[streamresource] Oueries value: a781-5a1130a75963}[streamresourcetype] HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}[localredirectonly] Queries value: a781-5a1130a75963}[roamable] Queries value: a781-5a1130a75963}[precreate] Queries value: a781-5a1130a75963}[stream] Queries value: a781-5a1130a75963}[publishexpandedpath] a781-5a1130a75963}[attributes] 806e6f6e6963}[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disableadapterdomainname]  $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-d9dc8a4b-b784-432e-d9dc8a4b-b784-432e-d9dc8a400-d9dc8a4b-b784-432e-d9dc8a4b-b784-4360-d9dc8a4b-b784-4360-d9dc$ a781-5a1130a75963}[foldertypeid] a781-5a1130a75963}[initfolderhandler] HKLM\svstem\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disabledynamicupdate] Queries value: 806e6f6e6963}[enableadapterdomainnameregistration] HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[maxnumberofaddressestoregister] 806e6f6e6963}[enablemulticast] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ Oueries value: settings\5.0\lowcache\history[cacheprefix] Queries value:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$ settings\5.0\lowcache\history[cachelimit] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cacherepair] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\lowcache\extensible cache\feedplat[cachepath] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\lowcache\extensible cache\feedplat[cacheprefix] Queries value:  $\label{lem:hkcu} \verb+KCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\$ settings\5.0\lowcache\extensible cache\feedplat[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\lowcache\extensible cache\feedplat[cacheoptions] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacherepair] Queries value:  $\label{lem:hkcu} \verb+KCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\$ settings\5.0\lowcache\extensible cache\iecompat[cachepath] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacheprefix] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cachelimit]

settings\5.0\lowcache\extensible cache\iecompat[cacheoptions] HKCU\software\microsoft\windows\currentversion\internet Oueries value:

HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\lowcache\extensible cache\ietld[cacherepair]

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

settings\5.0\lowcache\extensible cache\ietld[cachepath]

Queries value:

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

settings\5.0\lowcache\extensible cache\ietld[cacheprefix]

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

settings\5.0\lowcache\extensible cache\ietld[cachelimit]

Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacheoptions] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadlastnetwork] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[autoproxydetecttype] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback[rundll32.exe] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespace\_callout] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[next\_catalog\_entry\_id] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[num\_catalog\_entries] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000001[packedcatalogitem] Oueries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 00000000000002 \ [packed catalog item]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000003[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000006[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000007[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem] Oueries value: Oueries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ catalog\_entries \ 0000000000013 \ [packed catalog item]$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000015[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000016[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000017[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000018[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath] Oueries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[displaystring]) \ displaystring \ (catalog\_entries \ name space\_catalog 5) \ displays$ Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[addressfamily] Queries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]]$ Queries value: Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000001[version]$ Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 1000000000001 \ [storesservice classinfo]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerinfo] Queries 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] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000002 [address family])$ Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
   Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 0000000000003 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[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\000000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
   Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 00000000000004 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerid]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[enabled]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[storesserviceclassinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]
  Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries \namespace\_catalog5 \catalog5 \$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[version]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]
  Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2\_32 numhandle buckets]$

Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32spincount1 Oueries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6] Queries value: Oueries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling] Oueries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession] Oueries value: HKLM\system\currentcontrolset\enum\root\ms\_agilevpnminiport\0000[phantom] HKLM\system\currentcontrolset\enum\root\ms\_agilevpnminiport\0000[driver] Oueries value: Queries value: 08002be10318}\0001[componentid] HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-Oueries value: 08002be10318}\0001\ndi\interfaces[upperrange] Oueries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi\interfaces[lowerrange] Queries value: HKLM\system\currentcontrolset\enum\root\\*isatap\0000[phantom] Oueries value: HKLM\system\currentcontrolset\enum\root\\*isatap\0000[driver] Oueries value: 08002be10318}\0009[componentid] Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009\ndi\interfaces[upperrange] HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-Queries value: 08002be10318}\0009\ndi\interfaces[lowerrange] HKLM\system\currentcontrolset\enum\root\ms 12tpminiport\0000[phantom] Queries value: Queries value: HKLM\system\currentcontrolset\enum\root\ms\_12tpminiport\0000[driver] Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002[componentid] HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-Queries value: 08002be10318}\0002\ndi\interfaces[upperrange] HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-Queries value: 08002be10318}\0002\ndi\interfaces[lowerrange] Queries value: HKLM\system\currentcontrolset\enum\root\\*teredo\0000[phantom] HKLM\system\currentcontrolset\enum\root\\*teredo\0000[driver] Oueries value: Queries value: 08002be10318}\0011[componentid] Oueries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011\ndi\interfaces[upperrange] HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-Queries value: 08002be10318}\0011\ndi\interfaces[lowerrange] HKLM\system\currentcontrolset\enum\root\ms\_ndiswanbh\0000[phantom] Queries value: HKLM\system\currentcontrolset\enum\root\ms\_ndiswanbh\0000[driver] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006[componentid] Queries value: 08002be10318}\0006\ndi\interfaces[upperrange] Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006\ndi\interfaces[lowerrange] Queries value:  $HKLM \setminus system \setminus current control set \setminus enum \setminus pci \setminus ven\_8086 \& dev\_100e \& subsys\_001e 8086 \& rev\_02 \setminus 3 \& 267a616a \& 0 \& 18[phantom]$ Oueries value:  $HKLM \setminus system \setminus current control set \setminus enum \setminus pci \setminus ven\_8086 \& dev\_100e \& subsys\_001e 8086 \& rev\_02 \setminus 3 \& 267a616a \& 0 \& 18 [driver]$ Queries value: 08002be10318}\0007[componentid] Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi\interfaces[upperrange] Oueries value: HKLM\system\currentcontrolset\enum\pci\ven\_8086&dev\_100e&subsys\_001e8086&rev\_02\3&267a616a&0&18[capabilities] HKLM\system\currentcontrolset\enum\pci\ven\_8086&dev\_100e&subsys\_001e8086&rev\_02\3&267a616a&0&18[configflags] Oueries value: 08002be10318}\0007[netcfginstanceid] HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-Oueries value: 08002be10318}\0007[characteristics] HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[mediasubtype] HKLM\system\currentcontrolset\control\network[config] Queries value: Queries value: 08002be10318}\0007\ndi[clsid] Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi[service] HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-Oueries value: 08002be10318}\0007\ndi[coservices] Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi[bindform] Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi[helptext] HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-Oueries value: 08002be10318}\0007\ndi[filterclass]

Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

Queries value:

08002be10318}\0007\ndi[filtertype]

```
08002be10318}\0007\ndi[timestamp]
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318}\0007\ndi[filterruntype]
 Queries value:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi\interfaces[lowerrange]
 Queries value:
                      08002be10318}\0007\ndi\interfaces[lowerexclude]
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318}\0007\ndi\interfaces[filtermediatypes]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[devicedesc]
                      HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
 Queries value:
                      HKLM\software\microsoft\network\media[mediamanager]
                      Oueries value:
b16d-46121d0255aa]
 Queries value:
                      HKLM\system\currentcontrolset\control\wmi\security[5b23f342-8421-42ef-
87eb-3b686f5a1b2a1
 Queries value:
                      HKLM\system\currentcontrolset\control\wmi\security[253f4cd1-9475-4642-
88e0-6790d7a86cde]
                      Oueries value:
8afe-0bb2ab92997a]
 Queries value:
                      HKLM\system\currentcontrolset\control\wmi\security[ab0d8ef9-866d-4d39-
b83f-453f3b8f63251
                      HKLM \verb|\system| current controls et \verb|\enum| root \verb|\ms_ndiswanip| 0000 [phantom]
 Queries value:
                      HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
 Queries value:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318}\0008[componentid]
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318}\0008\ndi\interfaces[upperrange]
                      Queries value:
08002be10318}\0008\ndi\interfaces[lowerrange]
 Oueries value:
                      HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[phantom]
                      HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[driver]
 Queries value:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318}\0005[componentid]
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value:
08002be10318}\0005\ndi\interfaces[upperrange]
 Oueries value:
                      08002be10318}\0005\ndi\interfaces[lowerrange]
                      HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[phantom]
 Oueries value:
 Oueries value:
                      HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
                      Oueries value:
08002be10318}\0004[componentid]
 Queries value:
                      08002be10318}\0004\ndi\interfaces[upperrange]
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318}\0004\ndi\interfaces[lowerrange]
 Oueries value:
                      HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[phantom]
 Oueries value:
                      HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[driver]
 Queries value:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003[componentid]
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318}\0003\ndi\interfaces[upperrange]
 Oueries value:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\ndi\interfaces[lowerrange]
 Queries value:
                      HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000[phantom]
                      HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000[driver]
 Queries value:
 Queries value:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000[componentid]
                      Queries value:
08002be10318}\0000\ndi\interfaces[upperrange]
 Oueries value:
                      HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\ndi\interfaces[lowerrange]
                      HKU\s-1-5-21-2160590473-689474908-1361669368-
 Queries value:
1002\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
 Queries value:
                      HKU\s-1-5-21-2160590473-689474908-1361669368-1002\control
panel\international[localename]
 Queries value:
                      HKU\s-1-5-21-2160590473-689474908-1361669368-1002\software\microsoft\ras
autodial\default[defaultinternet]
                      HKLM\software\microsoft\ras autodial\default[defaultinternet]
 Oueries value:
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\networklist\profiles\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[category]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\networklist\profiles\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[profilename]
 Oueries value:
                      HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[]
                      HKCR\clsid\{7007acc7-3202-11d1-aad2-
 Oueries value:
00805fc1270e}\inprocserver32[loadwithoutcom]
 Queries value:
                      HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
```

 $HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e\}[sortorderindex]$ 

HKCR\clsid\{2227a280-3aea-1069-a2de-

Queries value: Queries value:

```
08002b30309d}[system.itemnamedisplay]
                                HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[{b725f130-47ef-101a-
  Oueries value:
a5f1-02608c9eebac} 101
  Queries value:
                                 HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
  Oueries value:
Oueries value:
                                 HKCU\software\classes\local
settings\muicache\27\52c64b7e[@c:\windows\system32\prnfldr.dll,-8036]
  Queries value:
                                 HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}[system.itemnamedisplay]
                                HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[{b725f130-47ef-101a-
  Oueries value:
a5f1-02608c9eebac} 10]
  Oueries value:
                                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
                                HKCU\software\classes\local
  Oueries value:
settings\muicache\27\52c64b7e[@c:\windows\system32\netshell.dll,-1200]
  Queries value:
                                 HKLM\system\currentcontrolset\services\netbt\linkage[export]
  Oueries value:
                                 HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:
                                 HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
  Queries value:
HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activewebprobehost]
  Queries value:
HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activewebprobepath]
  Queries value:
Queries value:
                                 HKU\s-1-5-20\control panel\international[localename]
  Queries value:
                                 HKLM\system\currentcontrolset\control\wmi\security[981f2d7e-b1f3-11d0-
8dd7-00c04fc3358c]
                                 HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
  Oueries value:
0000-0000000000000]
                                 HKLM\system\currentcontrolset\control\wmi\security[981f2d7d-b1f3-11d0-
  Oueries value:
8dd7-00c04fc3358c1
  Queries value:
Queries value:
                                 HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zonemap[autodetect]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zones\3[1a10]
                                 \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecision]
                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisiontime]
                                 HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\wpad[wpadexpirationdays]
  Queries value:
                                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisionreason]
  Oueries value:
HKLM\software\policies\microsoft\windows\networkconnectivitystatusindicator[noactiveprobe]
                                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
  Oueries value:
  Oueries value:
9926f41749ea}\count[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
  Oueries value:
HKLM\system\currentcontrolset\services\netlogon\parameters[expecteddialupdelay]
  Queries value:
                                 HKLM\software\microsoft\reliability analysis\wmi[wmienable]
  Oueries value:
                                 HKLM\system\currentcontrolset\control\wmi\security[f52ac1cc-b92d-4d8e-
8cf5-699ca40a73d2]
  Queries value:
HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
  Oueries value:
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
  Oueries value:
HKLM \setminus system \setminus current control \setminus diagnostics \setminus performance [active shutdown dcl]
                                 HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
  Oueries value:
  Queries value:
                                 HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
  Oueries value:
HKLM \label{lem:hklm} Which is a substitute of the substitute of
  Oueries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[postboot_timetoaccumulate_sec]
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[hardthresholds_critserviceslist]
  Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[mindelaypercentagetoidentify]
  Oueries value:
Oueries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[distantsize]
  Oueries value:
Oueries value:
```

Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[distantquorum]

Queries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[recentquorum]
Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[currentquorum]
Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[flatthresholdingconfig]
Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[distantsize]
Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[recentsize]
Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[currentsize]
Queries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[distantquorum]
 Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[recentquorum]
Queries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[currentquorum]
Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[flatthresholdingconfig]

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[distantsize]
Queries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[recentsize]

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[currentsize]
Queries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[distantquorum]
 Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[recentquorum]

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[currentquorum]
 Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[numinitialshutdownstoignore]
 Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[flatthresholdingconfig]
 Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[shutdownminorthreshold\_sec]
Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[shutdownmajorthreshold\_sec]
 Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[logoffminorthreshold\_sec]
 Oueries value:

HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[logoffmajorthreshold\_sec]

Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a7098685]

Queries value:

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-

622caee05b0a}[messagefilename]

Queries value:

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[resourcefilename]

Oueries value

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{cfc18ec0-96b1-4eba-961b-622caee05b0a\} \ [parameter filename]$ 

Queries value:

 $\label{limit} $HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}\ [helplink]$ 

Queries value

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ publishers \ \{cfc18ec0-96b1-4eba-961b-622caee05b0a\} \ [enabled]$ 

Queries value:

 $\label{limit} HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a\}[categorycount]}$ 

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance/operational[type]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows-diagnostics-performance/operational \cite{lem:hklmsoftware} enabled]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/operational[filemax]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \- diagnostic s-performance/operational [filecounter]$ 

Oueries value:

 $HKLM \ software \ `microsoft\ `windows \ `current version \ `winevt\ `channels\ `microsoft-windows-diagnostics-performance/operational[buffersize]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows - diagnostic speciform and \cite{linear} winevalue \cite{linear} winevalue \cite{linear} his linear \cite{line$ 

Queries value:

 $\label{lem:hammelsmicrosoft-windows-diagnostics-performance/operational[maxbuffers]} HKLM\software\mbox{\converted} winevt\channels\mbox{\converted} microsoft-windows-diagnostics-performance/operational[maxbuffers]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows - diagnostic speciform and constant and constant$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -diagnostic sperformance/operational[clocktype]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/operational[sidtype]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows-diagnostics-performance/operational [level]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \- current version \winevt \channels \microsoft \- windows \- diagnostic s-performance \- operational \cite{lem:hklmsoftware} \ \mbox{ and } \mbox{ in the lem of the lem$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} HKLM \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hkllm} winevt \label{lem:hkllm} hkll \label{lem:hkllm} winevt \label{lem:hkllm} hkll \label{lem:hkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkklllm} hkll \label{lkkllm} hkll \label{lkklllm} hkll \labellh{lkklllm} hkll \$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/operational[maxsizeupper]

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \- current version \winevt \channels \microsoft \- windows \- diagnostic s-performance \- operational \[retention]$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} hkll \label{lem:hkklm} hkll \label{lkklm} hkll \label{lkklm$ 

Oueries value:

 $\label{lem:hammelsmicrosoft-windows-diagnostics-performance/operational[file]} HKLM\software\mbox{\constraints} winevt\channels\mbox{\constraints} microsoft-windows-diagnostics-performance/operational[file]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \winevt \channels \microsoft \-windows \-diagnostics-performance/operational \[filterid]\]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows-diagnostics-performance/operational \cite{lisolation} is observed as the lisolation \cite{lisolation}.$ 

Queries value:

 $\label{lem:hammelsmicrosoft-windows-diagnostics-performance/operational[owningpublisher]} HKLM \software \microsoft-windows-diagnostics-performance/operational[owningpublisher]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\-currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance/operational[channelaccess]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \- diagnostic s-performance \/ diagnostic \[ type \]$ 

Queries value:

 $\label{thm:local-performance} HKLM \software \microsoft \windows \- diagnostic s-performance \// diagnostic \[ enabled \] \\$ 

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance/diagnostic[filemax]$ 

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\-currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance\slabel{lem:hklm} diagnostic[filecounter]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[buffersize]

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft-windows-diagnostics-performance/diagnostic[minbuffers]$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} winevt \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hklm} hkll \label{lem:hkklm} hkll \label{lkklm} hkll \lab$ 

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\-current version\winevt\channels\microsoft\-windows\-diagnostics-performance\/diagnostic[latency]$ 

Queries value:

 $HKLM \ software \ `microsoft\ `windows \ `current version \ `winevt\ `channels\ `microsoft-windows-diagnostics-performance/diagnostic[clocktype]$ 

Queries value:

 $\label{lem:hammelsmicrosoft-windows-diagnostics-performance/diagnostic[sidtype]} HKLM \software \microsoft-windows-diagnostic[sidtype]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-

performance/diagnostic[level]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[keywordslower]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \- diagnostic s-performance \/ diagnostic \[ keyword supper \] \\$ 

Oueries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \la$ 

Oueries value:

 $HKLM \ software \ `microsoft\ `windows \ `current version \ `winevt\ `channels\ `microsoft-windows-diagnostics-performance/diagnostic \ [max size]$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[maxsizeupper]

Queries value:

 $\label{lem:hammelsmicrosoft-windows-diagnostics-performance/diagnostic[retention]} HKLM \software \microsoft-windows-diagnostic[retention]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[autobackuplogfiles]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[file]

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[filterid]

Oueries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic[isolation]

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance\slashed\currentversion\sla$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft - windows - diagnostic s-performance \ / diagnostic \ [channel access]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft-windows - diagnostic s-performance \slight / diagnostic / loop back [type]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \- diagnostics-performance \/ diagnostic \/ loop back \[ enabled \]$ 

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ - diagnostic \ - performance \ / diagnostic \ / loop back \ [filemax]$ 

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance/diagnostic/loopback[filecounter]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance\/diagnostic\/loopback\[buffersize\]$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance\/diagnostic\/loopback\/[minbuffers\]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic/loopback[maxbuffers]

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance\/diagnostic\/loopback\[latency\]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic/loopback[clocktype]

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} his cross ft-windows-diagnostic \label{lem:hklm} experience \label{lem:hklm} diagnostic \label{lem:hklm} experience \label{lem:hklm} winevt \label{lem:hklm} his cross ft-windows-diagnostic \label{lem:hklm} winevt \label{lem:hklm} his cross ft-windows-diagnostic \label{lem:hklm} experience \label{lem:hklm} diagnostic \label{lem:hklm} his cross ft-windows-diagnostic \label{lem:hklm} his cross ft-windows-diagnost$ 

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} winevt \label{lem:hklm} his cross ft-windows-diagnostic separate \label{lem:hklm} winevt \label{lem:hklm} his cross ft-windows-diagnostic separate \label{lem:hklm} winevt \label{lem:hklm} his cross ft-windows-diagnostic separate \labe$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft\-windows\-diagnostics-performance\/diagnostic\/loopback\[keywordslower\]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnosticsperformance/diagnostic/loopback[keywordsupper]

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \- current version \winevt \channels \microsoft \- windows \- diagnostics \- performance \/ diagnostic \/ loop back \[ control guid \]$ 

Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxsize]

Queries value:

```
HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -diagnostic s - wind
performance/diagnostic/loopback[maxsizeupper]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/diagnostic/loopback[retention]
    Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/diagnostic/loopback[autobackuplogfiles]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/diagnostic/loopback[file]
    Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/diagnostic/loopback[filterid]
    Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -diagnostic s - wind
performance/diagnostic/loopback[isolation]
    Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-
performance/diagnostic/loopback[owningpublisher]
HKLM \ software \ microsoft \ windows \ current version \ winevt \ channels \ microsoft \ windows \ -diagnostic s - wind
performance/diagnostic/loopback[channelaccess]
    Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fwvux1exfmpbqaa]
    Sets/Creates value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1409]
                                                              HKCU\software\microsoft\windows\currentversion\internet
    Sets/Creates value:
settings\zones\0[1609]
    Sets/Creates value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1406]
                                                             \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
    Sets/Creates value:
settings\lockdown_zones\1[1406]
    Sets/Creates value:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2[1406]
                                                              \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
    Sets/Creates value:
settings\lockdown zones\3[1406]
    Sets/Creates value:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4[1406]
                                                             HKCU\software\microsoft\internet
    Sets/Creates value:
explorer\phishingfilter[shownservicedownballoon]
                                                             HKCU\software\microsoft\internet
    Sets/Creates value:
explorer\recovery[clearbrowsinghistoryonexit]
    Sets/Creates value:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
                                                              HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver]
    Sets/Creates value:
    Sets/Creates value:
-HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17
c19ce8a73253}[dhcpnameserver]
    Sets/Creates value:
-HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17
c19ce8a73253}[dhcpsubnetmaskopt]
    Sets/Creates value:
-HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17
c19ce8a73253}[dhcpdefaultgateway]
    Sets/Creates value:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisionreason]
                                                             HKCU\software\microsoft\windows\currentversion\internet
    Sets/Creates value:
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisiontime]
    Sets/Creates value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecision]
    Sets/Creates value:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpadnetworkname]
                                                             HKCU\software\microsoft\windows\currentversion\internet
    Sets/Creates value:
settings\wpad\ae-54-c5-b6-a2-81[wpaddecisionreason]
    Sets/Creates value:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\ae-54-c5-b6-a2-81[wpaddecisiontime]
    Sets/Creates value:
                                                             \label{lem:hkcu} \verb+KCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\wpad\ae-54-c5-b6-a2-81[wpaddecision]
    Value changes:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
    Value changes:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
    Value changes:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                                                              HKCU\software\microsoft\windows\currentversion\internet
    Value changes:
settings[warnonpostredirect]
    Value changes:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
    Value changes:
                                                             HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1409]
```

HKCU\software\microsoft\windows\currentversion\internet

Value changes: settings\zones\1[1609]

```
HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\zones\1[1406]
 Value changes:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1409]
                         HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
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]
                         HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\zones\3[1609]
 Value changes:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1406]
 Value changes:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1409]
                         HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\zones\4[1609]
 Value changes:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1406]
 Value changes:
                         HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
 Value changes:
                         HKLM\software\microsoft\windows
nt\corrent version\network list\nla\cache \ intranet [\{128919e8-8a5e-41d1-ac17-c19ce8a73253\}]
 Value changes:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
                         HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\connections[savedlegacysettings]
 Value changes:
                         HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[pnpinstanceid]
                         HKCU\software\classes\local settings\muicache\27\52c64b7e[languagelist]
 Value changes:
 Value changes:
Value changes:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpinterfaceoptions]
                         HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\connections[defaultconnectionsettings]
                        HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\wpad[wpadlastnetwork]
                        HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisionreason]
                        HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisiontime]
 Value changes:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecision]
                        HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings \verb|\wpad|{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpadnetworkname]|
 Value changes:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\ae-54-c5-b6-a2-81[wpaddecisionreason]
 Value changes:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\ae-54-c5-b6-a2-81[wpaddecisiontime]
                        HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\wpad\ae-54-c5-b6-a2-81[wpaddecision]
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
 Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[hrzr_pgyfrffvba]
                         HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
```

settings[globaluseroffline]