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
10 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

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" "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
Reads from process:	PID:3116 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3168 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3220 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3264 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3324 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3352 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3392 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3440 C:\Windows\System32\rundll32.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
Reads from process:	PID:2820 C:\Windows\System32\rundll32.exe

Reads from process:	PID:2908 C:\Windows\System32\rundll32.exe
Writes to process:	PID:1092 C:\Windows\explorer.exe
Writes to process:	PID:360 C:\Windows\System32\wininit.exe
Writes to process:	PID:396 C:\Windows\System32\winlogon.exe
Writes to process:	PID:464 C:\Windows\System32\lsass.exe
Writes to process:	PID:472 C:\Windows\System32\lsm.exe
Writes to process:	PID:572 C:\Windows\System32\svchost.exe
Writes to process:	PID:640 C:\Windows\System32\svchost.exe
Writes to process:	PID:688 C:\Windows\System32\svchost.exe
Writes to process:	PID:816 C:\Windows\System32\svchost.exe
Writes to process:	PID:860 C:\Windows\System32\svchost.exe
Writes to process:	PID:968 C:\Windows\System32\svchost.exe
Writes to process:	PID:1144 C:\Windows\System32\dwm.exe
Writes to process:	PID:1276 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:1348 C:\Windows\System32\spoolsv.exe
Writes to process:	PID:1388 C:\Windows\System32\taskhost.exe
Writes to process:	PID:1396 C:\Windows\System32\svchost.exe
Writes to process:	PID:1468 C:\Windows\System32\svchost.exe
Writes to process:	PID:1556 C:\Windows\System32\svchost.exe
Writes to process:	PID:1932 C:\Windows\System32\UIODetect.exe
Writes to process:	PID:280 C:\Windows\System32\svchost.exe
Writes to process:	PID:1508 C:\Windows\System32\mobsync.exe
Writes to process:	PID:1064 C:\Windows\System32\taskhost.exe
Writes to process:	PID:2308 C:\Windows\System32\wbem\unsecapp.exe
Writes to process:	PID:2420 C:\Windows\System32\wbem\WmiPrvSE.exe
Writes to process:	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:	PID:3168 C:\Windows\System32\rundll32.exe
Writes to process:	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:	PID:3352 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3392 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3440 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3532 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3588 C:\Windows\System32\rundll32.exe
Writes to process:	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:	PID:3928 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3976 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2148 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2248 C:\Windows\System32\rundll32.exe
Writes to process:	PID:1968 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2088 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2124 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2608 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2668 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2820 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2908 C:\Windows\System32\rundll32.exe
Terminates process:	C:\WinOldFileq\83A494219A6.exe
Terminates process:	C:\Windows\Temp\spyeye_injector.exe
Terminates process:	C:\Windows\System32\rundll32.exe
Terminates process:	C:\Windows\System32\mobsync.exe
Creates remote thread:	C:\Windows\System32\rundll32.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
Creates remote thread:	C:\Windows\System32\svchost.exe
Creates remote thread:	C:\Windows\System32\wbem\WmiPrvSE.exe
Creates remote thread:	C:\Windows\System32\taskhost.exe
Creates remote thread:	C:\Windows\System32\lsass.exe
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
Creates remote thread:	C:\Windows\System32\UIODetect.exe
Creates remote thread:	C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
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|00000000
Creates mutex:	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_
Creates mutex:	

\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!
Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex: \Sessions\1\BaseNamedObjects_!MSFTHISTORY!_LOW!_
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}
Creates event: \BaseNamedObjects\BFE_Notify_Event_{70064256-b57a-4a42-920e-9e57be0b48ab}
Creates semaphore: \Sessions\1\BaseNamedObjects\4FBEA4B1

File System Events

Creates: C:\WinOldFileq
Creates: C:\WinOldFileq\
Creates: C:\WinOldFileq\83A494219A6.exe
Creates: C:\WinOldFileq\9C413B7B23C1D6D
Creates: C:\Users\Admin
Creates: C:\Users\Admin\AppData\Local
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates: C:\Users\Admin\AppData\Roaming
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates: C:\Users\Admin\Favorites
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Creates: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Creates: C:\Windows\Prefetch\MOBSYNC.EXE-C5E2284F.pf
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}
Creates: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}
Creates: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}\snapshot.etl
Creates: C:\Windows\system32\wdi\{86432a0b-3c7d-4ddf-a89c-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
Opens: C:\Windows\System32\sechost.dll
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
Opens: C:\Windows\MSIMG32.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\System32\wininet.dll
Opens: C:\Windows\System32\ws2_32.dll
Opens: C:\Windows\System32\advapi32.dll
Opens: C:\Windows\System32\crypt32.dll
Opens: C:\Windows\System32\tzres.dll
Opens: C:\Windows\System32\en-US\tzres.dll.mui

Opens: C:\Windows\System32\mswsock.dll
Opens: C:\Windows\System32\WSHTCPIP.DLL
Opens: C:\Windows\Explorer.EXE.Local\
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
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\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:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
Opens: C:\Windows\System32\Sens.dll
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\PrivacIE\Low
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\Low
Opens: C:\Users\Admin\AppData\Local\Temp\Low
Opens: C:\Users\Admin\AppData\Local\Temp
Opens: C:\Windows\System32\rundll32.exe
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

Opens: C:\Windows\System32\KernelBase.dll
Opens: C:\Windows\System32\locale.nls
Opens: C:\Windows\System32\gdi32.dll
Opens: C:\Windows\System32\lpk.dll
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
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\index.dat
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
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
Opens: 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 Files\Low\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\desktop.ini
Opens: C:\Windows\System32\drivers\etc\hosts
Opens: C:\Windows\System32\FWPUCLNT.DLL
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
Opens: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf
Opens: C:\Windows\System32\calc.exe
Opens: C:\Windows\Prefetch\PARANORMAL.EXE-7FD43081.pf
Opens: C:\Windows\Prefetch
Opens: C:\Windows\Prefetch\CALC.EXE-77FDF17F.pf
Opens: C:\$Extend
Opens: C:\dump.pcap
Opens: C:\Windows\system32\wdi\{86432a0b-3c7d-4ddf-a89c-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
Opens: C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\{d1f2f9e5-d532-4869-b3a9-54da1cb4eba2}\snapshot.etl

Opens: C:\Windows\System32\wdi\LogFiles\WdiContextLog.etl.002
Opens: C:\Windows\System32\wdi\LogFiles\BootCKCL.etl
Opens: C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics_SystemData.bin
Opens: C:\Windows\System32\diagperf.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Opens: C:\Windows\System32\wdi\BootPerformanceDiagnostics_SystemData.bin
Writes to: C:\WinOldFileq\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%4Operational.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
Reads from: C:\WinOldFileq\9C413B7B23C1D6D
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.etl.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
Reads from: C:\Windows\System32\wdi\ShutdownPerformanceDiagnostics_SystemData.bin
Reads from: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Reads from: C:\Windows\System32\wdi\BootPerformanceDiagnostics_SystemData.bin
Deletes: C:\Windows\Temp\spyeye_injector.exe

Network Events

DNS query: alexeyartemov.com
DNS query: wpad
DNS query: www.msftncsi.com
DNS query: teredo.ipv6.microsoft.com
DNS response: alexeyartemov.com ⇒ 198.105.244.11
DNS response: alexeyartemov.com ⇒ 104.239.213.7
DNS response: a1961.g2.akamai.net ⇒ 58.27.86.16
DNS response: a1961.g2.akamai.net ⇒ 58.27.86.67
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
Connects to: 104.239.213.7:80
Sends data to: 8.8.8.8:53
Sends data to: 4.2.2.1:53
Sends data to: 88.198.13.147:443
Sends data to: 224.0.0.252:5355
Sends data to: alexeyartemov.com:80 (198.105.244.11)
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
Receives data from: 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)

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\run
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
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
Creates key: HKU\s-1-5-21-2160590473-689474908-1361669368-1002\software\microsoft\ras 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 key: HKLM\system\currentcontrolset\control\diagnostics\performance
Creates key: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot
Creates key: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot
Creates key: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot
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: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-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\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpdefaultgateway]
Deletes value: HKLM\system\currentcontrolset\services\netbt\parameters[dhcpscopeid]
Deletes value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpnetbiosoptions]
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\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\currentcontrolset\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\currentversion\appcompatflags\custom\83a494219a6.exe
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-fd27e3774e32}\0000
Opens key:
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-9dd4432fa2e9}\0000
Opens key: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-0d8e74595f78}\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\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\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 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\currentcontrolset\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 key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\user agent
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet 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
Opens key: HKCU\software\microsoft\windows\currentversion\internet 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
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software
Opens key: HKLM\software\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
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
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies
Opens key: HKCU\software\microsoft\windows\currentversion\internet 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
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet 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
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\microsoft\internet
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
Opens key: HKCU\software\microsoft\internet
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
Opens key: HKLM\software\microsoft\internet
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
Opens key: HKCU\software\microsoft\internet
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
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\microsoft\internet
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
Opens key: HKCU\software\microsoft\internet
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
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
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 key: HKLM\system\currentcontrolset\control\cryptography\configuration
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{f3229805-869e-479e-ba76-
dd643f1d1b80}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{72dd97a9-e544-4915-88d8-
44e829c34f68}

Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{72dd97a9-e544-4915-88d8-44e829c34f68}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{0aab3bce-41ed-11e5-bf5b-080027dfc114}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{0aab3bce-41ed-11e5-bf5b-080027dfc114}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{69d2510e-6c18-11e3-b3bc-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:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7c5653f0-144a-4534-9e34-28ac99cba85e}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{69d2510f-6c18-11e3-b3bc-a199dcc7ccd3}
Opens key: HKLM\software\microsoft\cryptography\oid
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 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
Opens key: HKCU\software\microsoft\systemcertificates\my
Opens key: HKCU\software\microsoft\systemcertificates\my\
Opens key: HKCU\software\microsoft\systemcertificates\my\certificates
Opens key: HKCU\software\microsoft\systemcertificates\my\crls
Opens key: HKCU\software\microsoft\systemcertificates\my\ctls
Opens key: HKCU\software\microsoft\systemcertificates\my\keys
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{69d2510f-6c18-11e3-b3bc-a199dcc7ccd3}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-1709a0196aed}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-a68f334c8d34}
Opens key: HKCU\appevents\schemes\apps\.default\close\.current
Opens key: HKCU\appevents\schemes\apps\.default\close\.current\active
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6fe-7037-11de-816d-001c23e25b76}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6fe-7037-11de-816d-001c23e25b76}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac701-7037-11de-816d-001c23e25b76}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac701-7037-11de-816d-

001c23e25b76}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac700-7037-11de-816d-
001c23e25b76}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac700-7037-11de-816d-
001c23e25b76}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{db2b4279-b5cf-4626-9dba-
32d0ece44c87}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{db2b4279-b5cf-4626-9dba-
32d0ece44c87}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e2f8a220-af88-446c-9a55-
453e58dd3a33}
Opens key: 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}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{483c9ff8-503d-414b-b402-
e4c1f1f568cb}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{483c9ff8-503d-414b-b402-
e4c1f1f568cb}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{c0de3e38-8ba7-479f-8b75-
833f294c5aa8}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{c0de3e38-8ba7-479f-8b75-
833f294c5aa8}
Opens key: HKLM\system\currentcontrolset\services\eventlog\system
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\0
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\1
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\2
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\3
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\4
Opens key:
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 key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-
82fd4940b820}\channelreferences\7
Opens key: HKLM\software\microsoft\tracing\explorer_rasapi32
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\software\microsoft\tracing\explorer_rasmancs
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\treatas
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\progid
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprochandler32
Opens key: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprochandler
Opens key: HKCU\software\classes\
Opens key: HKLM\software\classes
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: HKCU\software\classes\autoproxytypes\application/x-ns-proxy-autoconfig
Opens key: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig

Opens key: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}
Opens key: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib
Opens key: HKCR\typelib
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0
Opens key: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32
Opens key: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rundll32.exe
Opens key: HKLM\software\microsoft\windows 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
Opens key: HKCU\software\microsoft\internet 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\sam\domains\account\groups\000003ea
Opens key: HKLM\sam\sam\domains\account\aliases\000003ea
Opens key: HKLM\sam\sam\domains\account\users\000003ea
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
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: HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\content
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-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: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key: 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 key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-

908e-08a611b84ff6}\propertybag
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\history
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld
Opens key: HKLM\software\microsoft\windows
nt\currentversion\networklist\profiles\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\307bda19-07de87e0
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\307bda19
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
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:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\control\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}\0001\ndi\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_l2tpminiport\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\currentcontrolset\control\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}\0006\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\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\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}\0005\ndi\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\currentcontrolset\control\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-1-5-21-2160590473-689474908-1361669368-
1002\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

Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-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\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\controlpanel\namespace\namecustomizations
Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings
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: HKCU\system\currentcontrolset\control\network\showwirelessconnectingonstart
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKU\.default\control panel\international
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\connections
Opens key: HKLM\system\currentcontrolset\services\nlasvc\parameters\internet
Opens key: HKU\s-1-5-20
Opens key: HKU\s-1-5-20\control panel\international
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{128919e8-8a5e-41d1-ac17-c19ce8a73253}
Opens key: HKLM\system\currentcontrolset\services\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\parameters\tcpip
Opens key: HKLM\system\currentcontrolset\services\netbt\adapters\{128919e8-8a5e-41d1-ac17-c19ce8a73253}
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key: HKLM\software\policies\microsoft\windows\networkconnectivitystatusindicator
Opens key: HKLM\software\microsoft\ctf\knownclasses
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: HKLM\system\currentcontrolset\services\netlogon\parameters
Opens key: HKLM\software\policies\microsoft\windows\reliability analysis\wmi
Opens key: HKLM\software\microsoft\reliability analysis\wmi
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\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-diagnostics-performance/operational
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-diagnostics-performance/diagnostic

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-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-diagnostics-performance/diagnostic/loopback
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers[c:\winoldfileq\83a494219a6.exe]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]
Queries value: HKLM\hardware\devicemap\video[\device\video3]
Queries value: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-fd27e3774e32}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video0]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video1]
Queries value: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-0d8e74595f78}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video2]
Queries value: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-8ed0c8eb59a8}\0000[pruningmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[83a494219a6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security_hklm_only]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\psched[winsock 2.0 provider id]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[lsass]
Queries value: HKLM\software\microsoft\internet explorer[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version]
Queries value: HKLM\software\microsoft\windows\currentversion\internet 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]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[explorer.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation[*]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-a3fe-553973d0b723]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-b924-d51178a59ce4]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[fromcachetimeout]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[certificaterevocation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablekeepalive]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablepassport]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cachemode]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablenegotiate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablebasicoverclearchannel]
Queries value: HKCU\software\microsoft\internet 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]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[syncmode5]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache[sessionstarttimedefaultdeltasecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
Queries 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]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
Queries value: 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]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[keepalivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[maxhttpredirects]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[maxconnectionsperserver]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[maxconnectionsper1_0server]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[maxconnectionsper1_0server]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[maxconnectionsperproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[serverinfotimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[connecttimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[connecttimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[connectretries]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[connectretries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sendtimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[sendtimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[receivetimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[receivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablentlmpreauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[scavengecachelowerbound]
Queries value: HKCU\software\microsoft\windows\currentversion\internet 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]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelimit]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[httpdefaultexpirytimesecs]
Queries 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[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[perusercookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[leashlegacycookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sendextracrlf]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[wpadsearchalldomains]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypassssl nocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[bypassssl nocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[enablehttptrace]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[dontusednsloadbalancing]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[explorer.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[spyeye_injector]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
Queries value: HKCU\appevents\schemes[]
Queries value: HKCU\appevents\schemes\apps\.default\open\.current[]
Queries 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]
Queries 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: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enabledhcp]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationenabled]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registeradaptername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[domain]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[dhcpdomain]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[nameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\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]
Queries 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: HKLM\system\currentcontrolset\services\eventlog\system[filecounter]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[buffersize]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[minbuffers]
Queries 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]
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: HKLM\system\currentcontrolset\services\eventlog\system[autobackuplogfiles]
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]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences[count]
Queries value: 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: 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\1[flags]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\1[id]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\2[]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\2[flags]
Queries value: HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\2[id]
Queries value: 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]
Queries 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[]
Queries 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]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\5[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\5[flags]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\5[id]
Queries value:
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]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\6[id]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\7[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\7[flags]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}\channelreferences\7[id]
Queries value: HKLM\software\microsoft\tracing[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[enableconsoletracing]
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]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[enablefiletracing]
Queries 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]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[filedirectory]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxysettingsperuser]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigcustomua]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[dllfile]

Queries value: HKCR\autoproxytypes\application/x-internet-signup[fileextensions]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[default]
Queries value: HKCR\autoproxytypes\application/x-internet-signup[flags]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]
Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassname]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[ownersid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[firinginterfaceiid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[customconfigclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[description]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[typelib]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[multiinterfacepublisherfilterclsid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowinprocactivation]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[fireinparallel]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclasspartitionid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassapplicationid]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[parallelfiringtimeout]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowperuserinprocactivation]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowperuseractivateasactivator]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[allowperusermoniker]
Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-{00000000-0000-0000-0000-000000000000}[serialfiringtimeout]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[version]
Queries value: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32[]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}[interfacehelperdisableall]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}[interfacehelperuser]
Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[explorer.exe]
Queries value: HKLM\software\policies\microsoft\windows\ipsec\policy\local[activepolicy]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[rundll32]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\sam\sam\domains\account\users\000003ea[v]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
Queries 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]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
Queries 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]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
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\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[infotip]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[icon]
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]

Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: 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\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]

Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-

a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
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:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localizedname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[enablemulticast]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[security]
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[initfolderhandler]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\history[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\feedplat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\iecompat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cachelimit]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\ietld[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadlastnetwork]
Queries value: HKCU\software\microsoft\windows\currentversion\internet 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]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
Queries 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]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
Queries 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]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries 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]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries 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:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
Queries value:
HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[phantom]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces[upperrange]
Queries 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]
Queries value: HKLM\system\currentcontrolset\enum\root*isatap\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000[phantom]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\enum\root*teredo\0000[phantom]
Queries value: HKLM\system\currentcontrolset\enum\root*teredo\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[phantom]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\ndi\interfaces[lowerrange]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[phantom]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi\interfaces[upperrange]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[capabilities]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[configflags]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[characteristics]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[mediasubtype]
Queries value: HKLM\system\currentcontrolset\control\network[config]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[clsid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[service]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
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]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[filterclass]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[filtertype]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-

08002be10318}\0007\ndi[timestamp]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi[filterruntype]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi\interfaces[lowerexclude]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi\interfaces[filtermediatypes]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[friendlyname]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[devicedesc]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\network\media[mediamanager]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5f31090b-d990-4e91-b16d-46121d0255aa]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5b23f342-8421-42ef-87eb-3b686f5a1b2a]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[253f4cd1-9475-4642-88e0-6790d7a86cde]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[7076bf7a-db99-4a63-8afe-0bb2ab92997a]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[ab0d8ef9-866d-4d39-b83f-453f3b8f6325]
Queries value: HKLM\system\currentcontrolset\enum\root\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-bfc1-08002be10318}\0008[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[phantom]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[phantom]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[phantom]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003\ndi\interfaces[upperrange]
Queries 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]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000[componentid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000\ndi\interfaces[lowerrange]
Queries value: HKU\s-1-5-21-2160590473-689474908-1361669368-1002\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]
Queries value: HKLM\software\microsoft\ras autodial\default[defaultinternet]
Queries value: HKLM\software\microsoft\windows nt\currentversion\networklist\profiles\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[category]
Queries value: HKLM\software\microsoft\windows nt\currentversion\networklist\profiles\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[profilename]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[loadwithoutcom]
Queries value: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[sortorderindex]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-

08002b30309d}[system.itemnamedisplay]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[{b725f130-47ef-101a-a5f1-02608c9eebac} 10]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
Queries value: HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
Queries 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]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[{b725f130-47ef-101a-a5f1-02608c9eebac} 10]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
Queries value: HKCU\software\classes\local settings\muicache\27\52c64b7e[@c:\windows\system32\netshell.dll,-1200]
Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]
Queries 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: HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activewebprobecontent]
Queries value: HKU\s-1-5-20\control panel\international[localename]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[981f2d7e-b1f3-11d0-8dd7-00c04fc3358c]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[981f2d7d-b1f3-11d0-8dd7-00c04fc3358c]
Queries value: HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1a10]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecision]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisiontime]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadexpirationdays]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisionreason]
Queries value: HKLM\software\policies\microsoft\windows\networkconnectivitystatusindicator[noactiveprobe]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
Queries value: HKLM\system\currentcontrolset\services\netlogon\parameters[expecteddialupdelay]
Queries value: HKLM\software\microsoft\reliability analysis\wmi[wmienable]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[f52ac1cc-b92d-4d8e-8cf5-699ca40a73d2]
Queries value: HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
Queries value: HKLM\system\currentcontrolset\control\diagnostics\performance[activeshutdowndcl]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[postboot_busythreshold]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[postboot_timetoaccumulate_sec]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[hardthresholds_critserviceslist]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[mindelaypercentagetoidentify]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\boot[numinitialbootstoignore]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[distantsize]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[recentsize]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[currentsize]

Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[distantquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[recentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[currentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\systemboot[flatthresholdingconfig]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[distantsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[recentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[currentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[distantquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[recentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[currentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\userboot[flatthresholdingconfig]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[distantsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[recentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[currentsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[distantquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[recentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[currentquorum]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[numinitialshutdownstoignore]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[flatthresholdingconfig]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[shutdownminorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[shutdownmajorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[logoffminorthreshold_sec]
Queries value:
HKLM\software\microsoft\windows\currentversion\diagnostics\performance\shutdown[logoffmajorthreshold_sec]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a7098685]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[messagefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[categorymessagefile]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[resourcefilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[parameterfilename]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[helplink]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}[categorycount]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filecounter]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[level]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/operational[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[buffersize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[minbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[maxbuffers]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[latency]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/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-diagnostics-performance/diagnostic[keywordslower]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic[channelaccess]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[type]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[enabled]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[filemax]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[filecounter]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[buffersize]
Queries value:
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-diagnostics-performance/diagnostic/loopback[maxbuffers]
Queries value:
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-diagnostics-performance/diagnostic/loopback[clocktype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[sidtype]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[level]
Queries value:
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-diagnostics-performance/diagnostic/loopback[keywordsupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[controlguid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxsize]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[maxsizeupper]
Queries 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]
Queries 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]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-performance/diagnostic/loopback[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-diagnostics-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]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1609]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4[1406]
Sets/Creates value: HKCU\software\microsoft\internet explorer\phishingfilter[shownservicedownballoon]
Sets/Creates value: HKCU\software\microsoft\internet explorer\recovery[clearbrowsinghistoryonexit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]
Sets/Creates value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver]
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]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet 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]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet 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: HKCU\software\microsoft\windows\currentversion\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]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpostredirect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[warnonintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1609]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet 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]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1609]
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\currentversion\networklist\nla\cache\intranet[{128919e8-8a5e-41d1-ac17-c19ce8a73253}]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Value changes: HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[pnpinstanceid]
Value changes: HKCU\software\classes\local settings\muicache\27\52c64b7e[languagelist]
Value changes: HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection]
Value changes: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpinterfaceoptions]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\wpad[wpadlastnetwork]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisionreason]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecisiontime]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{af1709b3-b8ae-42fd-82e7-ca712dddaac3}[wpaddecision]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\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]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\ae-54-c5-b6-a2-81[wpaddecision]
Value changes: 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]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]