Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 622, Task ID: 2433

Task ID:	2433
Risk Level:	8
Date Processed:	2016-02-22 05:29:43 (UTC)
Processing Time:	62.84 seconds
Virtual Environment:	IntelliVM

Execution Arguments:
`"c:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe"`

Sample ID:	622
Type:	basic
Owner:	admin
Label:	33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99
Date Added:	2016-02-22 05:26:49 (UTC)
File Type:	PE32:win32:gui
File Size:	54272 bytes
MD5:	75984f5cee7f9e64b9ffe44f60df8764
SHA256:	33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99
Description:	None

Pattern Matching Results

7 Writes to memory of system processes
4 Reads process memory
3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]
1 SSL traffic on standard port
6 Contacts service to find external IP address
8 Starts svchost.exe

Process/Thread Events

Creates process:
`C:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe`
`["C:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe" ]`

Creates process:	C:\Windows\SysWOW64\svchost.exe [svchost.exe]
Reads from process:	PID:1712 C:\Windows\SysWOW64\svchost.exe
Writes to process:	PID:1712 C:\Windows\SysWOW64\svchost.exe

Terminates process:
`C:\Windows\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe`

Named Object Events

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

File System Events

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\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XYGC8IM2\icanhazip_com[1].txt
Opens:	C:\Windows\Prefetch\33A18D17F6F150459E8EB2593A364-EB28559C.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll

Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\svchost.exe
Opens: C:\
Opens: C:\Windows\Prefetch\SVCHOST.EXE-672DEC87.pf
Opens: C:\Windows\SysWOW64\secur32.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\SHCore.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
Opens: C:\Windows\SysWOW64\wininet.dll
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\SysWOW64\winhttp.dll
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens: C:\Windows\SysWOW64\winnsi.dll
Opens: C:\Windows\SysWOW64\dnsapi.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\Windows\SysWOW64\clbcatq.dll
Opens: C:\Windows\SysWOW64\rasadhlp.dll
Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens: C:\Windows\SysWOW64\dhcpcsvc.dll
Opens: C:\Windows\System32\Drivers\etc\hosts
Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\AppContainerUserCertRead
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\SysWOW64\schannel.dll
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My
Opens: C:\Windows\SysWOW64\gpapi.dll
Opens: C:\Windows\SysWOW64\en-US\crypt32.dll.mui
Opens: C:\Windows\SysWOW64\ncrypt.dll
Opens: C:\Windows\SysWOW64\bcrypt.dll
Opens: C:\Windows\SysWOW64\ntasn1.dll
Opens: C:\Windows\SysWOW64\cryptnet.dll
Opens: C:\Users\Admin\AppData\LocalLow
Opens: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
Opens: C:\Windows\SysWOW64\en-US\winhttp.dll.mui
Opens: C:\Windows\SysWOW64\webio.dll
Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
Opens: C:\Windows\SysWOW64\en-US\mswsock.dll.mui
Opens: C:\Windows\SysWOW64\wshqos.dll
Opens: C:\Windows\SysWOW64\en-US\wshqos.dll.mui
Opens: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData
Opens: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content
Opens: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
Opens: C:\Windows\SysWOW64\ncryptsslp.dll
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XYGC8IM2\icanhazip_com[1].txt
Writes to: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
Writes to: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
Reads from: C:\Windows\SysWOW64\svchost.exe
Reads from: C:\Windows\System32\Drivers\etc\hosts
Reads from: C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
Deletes: C:\Windows\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe

Network Events

DNS query: icanhazip.com
DNS query: ctldl.windowsupdate.com
DNS response: icanhazip.com ⇒ 64.182.208.181
DNS response: a1621.g.akamai.net ⇒ 58.27.86.223
DNS response: a1621.g.akamai.net ⇒ 58.27.22.137
Connects to: 64.182.208.181:80

Connects to: 197.149.90.166:12232
Connects to: 208.117.68.78:443
Connects to: 67.222.201.61:443
Connects to: 209.27.49.117:443
Connects to: 58.27.86.223:80
Sends data to: 0.0.0.0:53
Sends data to: icanhazip.com:80 (64.182.208.181)
Sends data to: 209.27.49.117:443
Sends data to: a1621.g.akamai.net:80 (58.27.86.223)
Receives data from: 0.0.0.0:53
Receives data from: icanhazip.com:80 (64.182.208.181)
Receives data from: 209.27.49.117:443
Receives data from: a1621.g.akamai.net:80 (58.27.86.223)

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\
Creates key: HKLM\system\currentcontrolset\control\securityproviders\schannel
Creates key: HKCU\software\microsoft\windows\currentversion\wintrust\trust providers\software publishing
Creates key: HKCU\software\microsoft\systemcertificates\ca
Creates key: HKCU\software\microsoft\systemcertificates\ca\certificates
Creates key: HKCU\software\microsoft\systemcertificates\ca\crls
Creates key: HKCU\software\microsoft\systemcertificates\ca\ctls
Creates key: HKCU\software\policies\microsoft\systemcertificates\ca
Creates key: HKCU\software\policies\microsoft\systemcertificates\ca\certificates
Creates key: HKCU\software\policies\microsoft\systemcertificates\ca\crls
Creates key: HKCU\software\policies\microsoft\systemcertificates\ca\ctls
Creates key: HKLM\software\wow6432node\microsoft\systemcertificates\ca
Creates key: HKLM\software\microsoft\systemcertificates\ca
Creates key: HKLM\software\microsoft\systemcertificates\ca\certificates
Creates key: HKLM\software\microsoft\systemcertificates\ca\crls
Creates key: HKLM\software\microsoft\systemcertificates\ca\ctls
Creates key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\ca
Creates key: HKLM\software\policies\microsoft\systemcertificates\ca
Creates key: HKLM\software\policies\microsoft\systemcertificates\ca\certificates
Creates key: HKLM\software\policies\microsoft\systemcertificates\ca\crls
Creates key: HKLM\software\policies\microsoft\systemcertificates\ca\ctls
Creates key: HKLM\software\wow6432node\microsoft\enterprisecertificates\ca
Creates key: HKLM\software\microsoft\enterprisecertificates\ca
Creates key: HKLM\software\microsoft\enterprisecertificates\ca\certificates
Creates key: HKLM\software\microsoft\enterprisecertificates\ca\crls
Creates key: HKLM\software\microsoft\enterprisecertificates\ca\ctls
Creates key: HKCU\software\microsoft\systemcertificates\disallowed
Creates key: HKCU\software\microsoft\systemcertificates\disallowed\certificates
Creates key: HKCU\software\microsoft\systemcertificates\disallowed\crls
Creates key: HKCU\software\microsoft\systemcertificates\disallowed\ctls
Creates key: HKCU\software\policies\microsoft\systemcertificates\disallowed
Creates key: HKCU\software\policies\microsoft\systemcertificates\disallowed\certificates
Creates key: HKCU\software\policies\microsoft\systemcertificates\disallowed\crls
Creates key: HKCU\software\policies\microsoft\systemcertificates\disallowed\ctls
Creates key: HKLM\software\wow6432node\microsoft\systemcertificates\disallowed
Creates key: HKLM\software\microsoft\systemcertificates\disallowed
Creates key: HKLM\software\microsoft\systemcertificates\disallowed\certificates
Creates key: HKLM\software\microsoft\systemcertificates\disallowed\crls
Creates key: HKLM\software\microsoft\systemcertificates\disallowed\ctls
Creates key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\disallowed
Creates key: HKLM\software\policies\microsoft\systemcertificates\disallowed
Creates key: HKLM\software\policies\microsoft\systemcertificates\disallowed\certificates
Creates key: HKLM\software\policies\microsoft\systemcertificates\disallowed\crls
Creates key: HKLM\software\policies\microsoft\systemcertificates\disallowed\ctls
Creates key: HKLM\software\wow6432node\microsoft\enterprisecertificates\disallowed
Creates key: HKLM\software\microsoft\enterprisecertificates\disallowed
Creates key: HKLM\software\microsoft\enterprisecertificates\disallowed\certificates
Creates key: HKLM\software\microsoft\enterprisecertificates\disallowed\crls
Creates key: HKLM\software\microsoft\enterprisecertificates\disallowed\ctls
Creates key: HKCU\software\microsoft\systemcertificates\root
Creates key: HKCU\software\microsoft\systemcertificates\root\certificates
Creates key: HKCU\software\microsoft\systemcertificates\root\crls
Creates key: HKCU\software\microsoft\systemcertificates\root\ctls
Creates key: HKLM\software\wow6432node\microsoft\systemcertificates\root
Creates key: HKLM\software\microsoft\systemcertificates\root
Creates key: HKLM\software\microsoft\systemcertificates\root\certificates
Creates key: HKLM\software\microsoft\systemcertificates\root\crls
Creates key: HKLM\software\microsoft\systemcertificates\root\ctls

Creates key: HKLM\software\wow6432node\microsoft\systemcertificates\authroot
Creates key: HKLM\software\microsoft\systemcertificates\authroot
Creates key: HKLM\software\microsoft\systemcertificates\authroot\certificates
Creates key: HKLM\software\microsoft\systemcertificates\authroot\crls
Creates key: HKLM\software\microsoft\systemcertificates\authroot\ctls
Creates key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\root
Creates key: HKLM\software\policies\microsoft\systemcertificates\root
Creates key: HKLM\software\policies\microsoft\systemcertificates\root\certificates
Creates key: HKLM\software\policies\microsoft\systemcertificates\root\crls
Creates key: HKLM\software\policies\microsoft\systemcertificates\root\ctls
Creates key: HKLM\software\wow6432node\microsoft\enterprisecertificates\root
Creates key: HKLM\software\microsoft\enterprisecertificates\root
Creates key: HKLM\software\microsoft\enterprisecertificates\root\certificates
Creates key: HKLM\software\microsoft\enterprisecertificates\root\crls
Creates key: HKLM\software\microsoft\enterprisecertificates\root\ctls
Creates key: HKLM\software\wow6432node\microsoft\systemcertificates\smartcardroot
Creates key: HKLM\software\microsoft\systemcertificates\smartcardroot
Creates key: HKLM\software\microsoft\systemcertificates\smartcardroot\certificates
Creates key: HKLM\software\microsoft\systemcertificates\smartcardroot\crls
Creates key: HKLM\software\microsoft\systemcertificates\smartcardroot\ctls
Creates key: HKCU\software\microsoft\systemcertificates\smartcardroot
Creates key: HKCU\software\microsoft\systemcertificates\smartcardroot\certificates
Creates key: HKCU\software\microsoft\systemcertificates\smartcardroot\crls
Creates key: HKCU\software\microsoft\systemcertificates\smartcardroot\ctls
Creates key: HKCU\software\microsoft\systemcertificates\trustedpeople
Creates key: HKCU\software\microsoft\systemcertificates\trustedpeople\certificates
Creates key: HKCU\software\microsoft\systemcertificates\trustedpeople\crls
Creates key: HKCU\software\microsoft\systemcertificates\trustedpeople\ctls
Creates key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople
Creates key:
HKCU\software\policies\microsoft\systemcertificates\trustedpeople\certificates
Creates key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople\crls
Creates key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople\ctls
Creates key: HKLM\software\wow6432node\microsoft\systemcertificates\trustedpeople
Creates key: HKLM\software\microsoft\systemcertificates\trustedpeople
Creates key: HKLM\software\microsoft\systemcertificates\trustedpeople\certificates
Creates key: HKLM\software\microsoft\systemcertificates\trustedpeople\crls
Creates key: HKLM\software\microsoft\systemcertificates\trustedpeople\ctls
Creates key:
HKLM\software\wow6432node\policies\microsoft\systemcertificates\trustedpeople
Creates key: HKLM\software\policies\microsoft\systemcertificates\trustedpeople
Creates key:
HKLM\software\policies\microsoft\systemcertificates\trustedpeople\certificates
Creates key: HKLM\software\policies\microsoft\systemcertificates\trustedpeople\crls
Creates key: HKLM\software\policies\microsoft\systemcertificates\trustedpeople\ctls
Creates key: HKLM\software\wow6432node\microsoft\enterprisecertificates\trustedpeople
Creates key: HKLM\software\microsoft\enterprisecertificates\trustedpeople
Creates key:
HKLM\software\microsoft\enterprisecertificates\trustedpeople\certificates
Creates key: HKLM\software\microsoft\enterprisecertificates\trustedpeople\crls
Creates key: HKLM\software\microsoft\enterprisecertificates\trustedpeople\ctls
Creates key: HKCU\software\microsoft\systemcertificates\trust
Creates key: HKCU\software\microsoft\systemcertificates\trust\certificates
Creates key: HKCU\software\microsoft\systemcertificates\trust\crls
Creates key: HKCU\software\microsoft\systemcertificates\trust\ctls
Creates key: HKCU\software\policies\microsoft\systemcertificates\trust
Creates key: HKCU\software\policies\microsoft\systemcertificates\trust\certificates
Creates key: HKCU\software\policies\microsoft\systemcertificates\trust\crls
Creates key: HKCU\software\policies\microsoft\systemcertificates\trust\ctls
Creates key: HKLM\software\wow6432node\microsoft\systemcertificates\trust
Creates key: HKLM\software\microsoft\systemcertificates\trust
Creates key: HKLM\software\microsoft\systemcertificates\trust\certificates
Creates key: HKLM\software\microsoft\systemcertificates\trust\crls
Creates key: HKLM\software\microsoft\systemcertificates\trust\ctls
Creates key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\trust
Creates key: HKLM\software\policies\microsoft\systemcertificates\trust
Creates key: HKLM\software\policies\microsoft\systemcertificates\trust\certificates
Creates key: HKLM\software\policies\microsoft\systemcertificates\trust\crls
Creates key: HKLM\software\policies\microsoft\systemcertificates\trust\ctls
Creates key: HKLM\software\wow6432node\microsoft\enterprisecertificates\trust
Creates key: HKLM\software\microsoft\enterprisecertificates\trust
Creates key: HKLM\software\microsoft\enterprisecertificates\trust\certificates
Creates key: HKLM\software\microsoft\enterprisecertificates\trust\crls
Creates key: HKLM\software\microsoft\enterprisecertificates\trust\ctls
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[autodetect]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[proxybypass]
Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\svchost.exe
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\svchost.exe
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKU\
Opens key: HKU\.default
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_handling
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\wow6432node\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software\wow6432node
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main
Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
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_disable_notify_unverified_spn_kb2385266
Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\27daf4d1
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\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\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\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\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\software\policies\microsoft\peerdist\service
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\service
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\system\currentcontrolset\services\dns
Opens key: HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\winhttp
Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\zonemap\ranges\
Opens key: HKCU\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer
Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\appid\svchost.exe
Opens key: HKCR\appid\svchost.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat

Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}
Opens key: HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}
Opens key: HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32
Opens key: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windowsruntime\clsid
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
Opens key: HKCR\activatableclasses\clsid
Opens key: HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler
Opens key: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprochandler
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip
Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-25b8d56dd1d8}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-8a6dc56e0da9}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov\#16
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov\ldap
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\certdllopenstoreprov
Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores
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: HKLM\system\currentcontrolset\control\securityproviders
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0\cryptdlldecodeobjectex
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certificate\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\wow6432node\microsoft\cryptography\providers\trust\finalpolicy\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\wow6432node\microsoft\cryptography\providers\trust\initialization\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\wow6432node\microsoft\cryptography\providers\trust\message\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\wow6432node\microsoft\cryptography\providers\trust\signature\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certcheck\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\wow6432node\microsoft\cryptography\providers\trust\diagnosticpolicy\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\wow6432node\microsoft\cryptography\providers\trust\cleanup\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft enhanced rsa and aes cryptographic provider
Opens key: HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKCU\software\microsoft\internet explorer\security
Opens key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKLM\software\policies\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKLM\software\wow6432node\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKLM\software\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\root\protectedroots
Opens key: HKLM\software\policies\microsoft\systemcertificates\root\protectedroots
Opens key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\authroot
Opens key: HKLM\software\policies\microsoft\systemcertificates\authroot
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config
Opens key: HKLM\software\microsoft\systemcertificates\authroot\autoupdate
Opens key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\chainengine\config
Opens key: HKLM\software\policies\microsoft\systemcertificates\chainengine\config
Opens key: HKCU\software\microsoft\systemcertificates\ca\physicalstores
Opens key: HKCU\software\microsoft\systemcertificates\ca\
Opens key: HKLM\software\wow6432node\microsoft\systemcertificates\ca\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\ca\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\ca\
Opens key:

HKLM\software\microsoft\systemcertificates\ca\certificates\109f1caed645bb78b3ea2b94c0697c740733031c
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\d559a586669b08f46a30a133f8a9ed3d038e2ea8
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\fee449ee0e3965a5246f000e87fde2a065fd89d4
Opens key:
HKLM\software\microsoft\systemcertificates\ca\crls\a377d1b1c0538833035211f4083d00fecc414dab
Opens key:
HKLM\software\wow6432node\microsoft\enterprisecertificates\ca\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\ca\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\ca\
Opens key: HKCU\software\microsoft\systemcertificates\disallowed\physicalstores
Opens key: HKCU\software\microsoft\systemcertificates\disallowed\
Opens key:
HKLM\software\wow6432node\microsoft\systemcertificates\disallowed\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\disallowed\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\disallowed\
Opens key:
HKLM\software\microsoft\systemcertificates\disallowed\ctls\27748148bbe67a43cdbfec6c3784862ce134e6ea
Opens key:
HKLM\software\wow6432node\microsoft\enterprisecertificates\disallowed\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\
Opens key: HKCU\software\microsoft\systemcertificates\root\physicalstores
Opens key: HKCU\software\microsoft\systemcertificates\root\protectedroots
Opens key: HKCU\software\microsoft\systemcertificates\root\
Opens key:
HKLM\software\wow6432node\microsoft\systemcertificates\root\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\root\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\root\
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\18f7c1fcc3090203fd5baa2f861a754976c8dd25
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\245c97df7514e7cf2df8be72ae957b9e04741e85
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\3b1efd3a66ea28b16697394703a72ca340a05bd5
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\7f88cd7223f3c813818c994614a89c99fa3b5247
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\8f43288ad272f3103b6fb1428485ea3014c0bcfe
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\a43489159a520f0d93d032ccaf37e7fe20a8b419
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\be36a4562fb2ee05dbb3d32323adf445084ed656
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\cdd4eeae6000ac7f40c3802c171e30148030c072
Opens key: HKLM\software\microsoft\systemcertificates\authroot\
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4eb6d578499b1ccf5f581ead56be3d9b6744a5e5
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4f65566336db6598581d584a596c87934d5f2ab4
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\742c3192e607e424eb4549542be1bbc53e6174e2
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\97817950d81c9670cc34d809cf794431367ef474
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d23209ad23d314232174e40d7f9d62139786633a
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d4de20d05e66fc53fe1a50882c78db2852cae474
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\de28f4a4ffe5b92fa3c503d1a349a7f9962a8212
Opens key:
HKLM\software\wow6432node\microsoft\enterprisecertificates\root\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\root\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\root\
Opens key: HKLM\software\microsoft\systemcertificates\smartcardroot\
Opens key: HKCU\software\microsoft\systemcertificates\smartcardroot\
Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople\physicalstores
Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople\
Opens key:
HKLM\software\wow6432node\microsoft\systemcertificates\trustedpeople\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\trustedpeople\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\trustedpeople\
Opens key:
HKLM\software\wow6432node\microsoft\enterprisecertificates\trustedpeople\physicalstores
Opens key:
HKLM\software\microsoft\enterprisecertificates\trustedpeople\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\trustedpeople\
Opens key: HKCU\software\microsoft\systemcertificates\trust\physicalstores
Opens key: HKCU\software\microsoft\systemcertificates\trust\
Opens key:
HKLM\software\wow6432node\microsoft\systemcertificates\trust\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\trust\physicalstores

Opens key: HKLM\software\microsoft\systemcertificates\trust\
Opens key:
HKLM\software\wow6432node\microsoft\enterprisecertificates\trust\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\trust\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\trust\
Opens key: HKCU\software\microsoft\systemcertificates\root\certificates
Opens key: HKCU\software\microsoft\systemcertificates\root\crls
Opens key: HKCU\software\microsoft\systemcertificates\root\ctls
Opens key: HKLM\software\microsoft\systemcertificates\root\certificates
Opens key: HKLM\software\microsoft\systemcertificates\root\crls
Opens key: HKLM\software\microsoft\systemcertificates\root\ctls
Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates
Opens key: HKLM\software\microsoft\systemcertificates\authroot\crls
Opens key: HKLM\software\microsoft\systemcertificates\authroot\ctls
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\system
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKLM\software\wow6432node\policies\microsoft\systemcertificates
Opens key: HKLM\software\policies\microsoft\systemcertificates
Opens key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\root
Opens key: HKLM\software\policies\microsoft\systemcertificates\root
Opens key: HKLM\software\policies\microsoft\systemcertificates\root\certificates
Opens key: HKLM\software\policies\microsoft\systemcertificates\root\crls
Opens key: HKLM\software\policies\microsoft\systemcertificates\root\ctls
Opens key: HKLM\software\microsoft\enterprisecertificates\root\certificates
Opens key: HKLM\software\microsoft\enterprisecertificates\root\crls
Opens key: HKLM\software\microsoft\enterprisecertificates\root\ctls
Opens key: HKLM\software\microsoft\systemcertificates\smartcardroot\certificates
Opens key: HKLM\software\microsoft\systemcertificates\smartcardroot\crls
Opens key: HKLM\software\microsoft\systemcertificates\smartcardroot\ctls
Opens key: HKCU\software\microsoft\systemcertificates\smartcardroot\certificates
Opens key: HKCU\software\microsoft\systemcertificates\smartcardroot\crls
Opens key: HKCU\software\microsoft\systemcertificates\smartcardroot\ctls
Opens key: HKCU\software\microsoft\systemcertificates\trust\certificates
Opens key: HKCU\software\microsoft\systemcertificates\trust\crls
Opens key: HKCU\software\microsoft\systemcertificates\trust\ctls
Opens key: HKCU\software\policies\microsoft\systemcertificates
Opens key: HKCU\software\policies\microsoft\systemcertificates\trust
Opens key: HKCU\software\policies\microsoft\systemcertificates\trust\certificates
Opens key: HKCU\software\policies\microsoft\systemcertificates\trust\crls
Opens key: HKCU\software\policies\microsoft\systemcertificates\trust\ctls
Opens key: HKLM\software\microsoft\systemcertificates\trust\certificates
Opens key: HKLM\software\microsoft\systemcertificates\trust\crls
Opens key: HKLM\software\microsoft\systemcertificates\trust\ctls
Opens key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\trust
Opens key: HKLM\software\policies\microsoft\systemcertificates\trust
Opens key: HKLM\software\policies\microsoft\systemcertificates\trust\certificates
Opens key: HKLM\software\policies\microsoft\systemcertificates\trust\crls
Opens key: HKLM\software\policies\microsoft\systemcertificates\trust\ctls
Opens key: HKLM\software\microsoft\enterprisecertificates\trust\certificates
Opens key: HKLM\software\microsoft\enterprisecertificates\trust\crls
Opens key: HKLM\software\microsoft\enterprisecertificates\trust\ctls
Opens key: HKCU\software\microsoft\systemcertificates\ca\certificates
Opens key: HKCU\software\microsoft\systemcertificates\ca\crls
Opens key: HKCU\software\microsoft\systemcertificates\ca\ctls
Opens key: HKCU\software\policies\microsoft\systemcertificates\ca
Opens key: HKCU\software\policies\microsoft\systemcertificates\ca\certificates
Opens key: HKCU\software\policies\microsoft\systemcertificates\ca\crls
Opens key: HKCU\software\policies\microsoft\systemcertificates\ca\ctls
Opens key: HKLM\software\microsoft\systemcertificates\ca\certificates
Opens key: HKLM\software\microsoft\systemcertificates\ca\crls
Opens key: HKLM\software\microsoft\systemcertificates\ca\ctls
Opens key: HKLM\software\wow6432node\policies\microsoft\systemcertificates\ca
Opens key: HKLM\software\policies\microsoft\systemcertificates\ca
Opens key: HKLM\software\policies\microsoft\systemcertificates\ca\certificates
Opens key: HKLM\software\policies\microsoft\systemcertificates\ca\crls
Opens key: HKLM\software\policies\microsoft\systemcertificates\ca\ctls
Opens key: HKLM\software\microsoft\enterprisecertificates\ca\certificates
Opens key: HKLM\software\microsoft\enterprisecertificates\ca\crls
Opens key: HKLM\software\microsoft\enterprisecertificates\ca\ctls
Opens key: HKCU\software\microsoft\systemcertificates\disallowed\certificates
Opens key: HKCU\software\microsoft\systemcertificates\disallowed\crls
Opens key: HKCU\software\microsoft\systemcertificates\disallowed\ctls
Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed
Opens key:
HKCU\software\policies\microsoft\systemcertificates\disallowed\certificates
Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed\crls
Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed\ctls
Opens key: HKLM\software\microsoft\systemcertificates\disallowed\certificates
Opens key: HKLM\software\microsoft\systemcertificates\disallowed\crls
Opens key: HKLM\software\microsoft\systemcertificates\disallowed\ctls

Opens key:
HKLM\software\wow6432node\policies\microsoft\systemcertificates\disallowed
Opens key: HKLM\software\policies\microsoft\systemcertificates\disallowed
Opens key:
HKLM\software\policies\microsoft\systemcertificates\disallowed\certificates
Opens key: HKLM\software\policies\microsoft\systemcertificates\disallowed\crls
Opens key: HKLM\software\policies\microsoft\systemcertificates\disallowed\ctls
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\certificates
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\crls
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\ctls
Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople\certificates
Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople\crls
Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople\ctls
Opens key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople
Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpeople\certificates
Opens key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople\crls
Opens key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople\ctls
Opens key: HKLM\software\microsoft\systemcertificates\trustedpeople\certificates
Opens key: HKLM\software\microsoft\systemcertificates\trustedpeople\crls
Opens key: HKLM\software\microsoft\systemcertificates\trustedpeople\ctls
Opens key:
HKLM\software\wow6432node\policies\microsoft\systemcertificates\trustedpeople
Opens key: HKLM\software\policies\microsoft\systemcertificates\trustedpeople
Opens key:
HKLM\software\policies\microsoft\systemcertificates\trustedpeople\certificates
Opens key: HKLM\software\policies\microsoft\systemcertificates\trustedpeople\crls
Opens key: HKLM\software\policies\microsoft\systemcertificates\trustedpeople\ctls
Opens key:
HKLM\software\microsoft\enterprisecertificates\trustedpeople\certificates
Opens key: HKLM\software\microsoft\enterprisecertificates\trustedpeople\crls
Opens key: HKLM\software\microsoft\enterprisecertificates\trustedpeople\ctls
Opens key: HKCU\software\microsoft\systemcertificates\authroot\autoupdate
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7
Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings
Opens key: HKCU\software\classes\local settings\muicache\13\52c64b7e
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\system\currentcontrolset\control\cryptography\providers
Opens key: HKLM\system\currentcontrolset\control\cryptography\configuration
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\software\wow6432node\microsoft\cryptography\tvo
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\schemedllretrieveencodedobjectw
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
1\schemedllretrieveencodedobjectw
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\connections
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\connections
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllverifyencodedsignature
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
1\cryptdllverifyencodedsignature
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllimportpublickeyinfoex2
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
1\cryptdllimportpublickeyinfoex2
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllimportpublickeyinfoex
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
1\cryptdllimportpublickeyinfoex
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllconvertpublickeyinfo
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
1\cryptdllconvertpublickeyinfo
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\certdllverifycertificatechainpolicy
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
1\certdllverifycertificatechainpolicy
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[svchost]
Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\software\microsoft\rpc[idletimerwindow]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[syncmode5]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache[sessionstarttimedefaultdeltasecs]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsingname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[mbcsapiforcrack]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security_hklm_only]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable[svchost.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_http_username_password_disable[*]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[svchost.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[*]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[svchost.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[fromcachetimeout]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols]
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[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[preconnectlimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[preresolvelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sqmhttpstreamrandomuploadpoolsize]
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\windows\currentversion\internet settings[clientauthbuiltinui]
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[utf8servernameres]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disableworkerthreadhibernation]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[maxconnectionsper1_0server]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[maxconnectionsper1_0server]
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\wow6432node\microsoft\windows\currentversion\internet settings[connecttimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[connectretries]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[connectretries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sendtimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[sendtimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[receivetimeout]
Queries value: HKLM\software\wow6432node\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\wow6432node\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: HKCU\software\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[leashlegacycookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypassssl nocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypassssl nocachecheck]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
Queries value: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\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\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\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[usefirstavailable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[combinefalsestartdata]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablefalsestartblacklist]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enforcep3pvalidity]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\service[enable]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
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: 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: 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[autodetect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
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[disablesmartnameresolution]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value:
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[newdhcpsrvregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
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: HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
Queries value:
HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[winhttplowercasehost]
Queries value: HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[svchost.exe]
Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[svchost.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet

settings[createuricachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
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:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[name]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cachelimit]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localizedname]
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cookies]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[history]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cachelimit]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]

Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
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[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpdomain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlockcount]
Queries value:
HKLM\system\currentcontrolset\control\securityproviders\schannel[usercontextlistcount]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certificate\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certificate\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\finalpolicy\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\finalpolicy\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\initialization\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\initialization\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\message\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:

HKLM\software\wow6432node\microsoft\cryptography\providers\trust\message\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\signature\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\signature\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certcheck\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certcheck\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\cleanup\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\cleanup\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft enhanced rsa and aes cryptographic provider[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft enhanced rsa and aes cryptographic provider[image path]
Queries value: HKCU\software\microsoft\windows\currentversion\wintrust\trust providers\software publishing[state]
Queries value: HKCU\software\microsoft\internet explorer\security[safety warning level]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\autoupdate[disallowedcertsyncdeltatime]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[disablemandatorybasicconstraints]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[disablecanameconstraints]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[disableunsupportedcriticalextensions]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[maxaiaurlcountincert]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[maxaiaurlretrievalcountperchain]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[maxurlretrievalbytecount]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[maxaiaurlretrievalbytecount]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[maxaiaurlretrievalcertcount]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[cryptnetprefetchtriggerperiodseconds]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[enableweaksignatureflags]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[minrsapubkeybitlength]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[weakrsapubkeytime]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config[chaincacheresyncfiletime]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\109f1caed645bb78b3ea2b94c0697c740733031c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\d559a586669b08f46a30a133f8a9ed3d038e2ea8[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\fee449ee0e3965a5246f000e87fde2a065fd89d4[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\crls\a377d1b1c0538833035211f4083d00fecc414dab[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\disallowed\ctls\27748148bbe67a43cdbfec6c3784862ce134e6ea[blob]
Queries value:
HKCU\software\microsoft\systemcertificates\root\protectedroots[certificates]
Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\18f7c1fcc3090203fd5baa2f861a754976c8dd25[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\245c97df7514e7cf2df8be72ae957b9e04741e85[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\3b1efd3a66ea28b16697394703a72ca340a05bd5[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\7f88cd7223f3c813818c994614a89c99fa3b5247[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\8f43288ad272f3103b6fb1428485ea3014c0bcfe[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\a43489159a520f0d93d032ccaf37e7fe20a8b419[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\be36a4562fb2ee05dbb3d32323adf445084ed656[blob]

Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\cdd4eeae6000ac7f40c3802c171e30148030c072[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4eb6d578499b1ccf5f581ead56be3d9b6744a5e5[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4f65566336db6598581d584a596c87934d5f2ab4[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\742c3192e607e424eb4549542be1bbc53e6174e2[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\97817950d81c9670cc34d809cf794431367ef474[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d23209ad23d314232174e40d7f9d62139786633a[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d4de20d05e66fc53fe1a50882c78db2852cae474[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\de28f4a4ffe5b92fa3c503d1a349a7f9962a8212[blob]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]
Queries value: HKLM\system\currentcontrolset\control\notifications[0d891e2aa3bc10f5]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\autoupdate[disallowedcertlastsynctime]
Queries value:
HKCU\software\microsoft\systemcertificates\authroot\autoupdate[disallowedcertlastsynctime]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\autoupdate[disallowedcertencodedctl]
Queries value: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7[name]
Queries value:
HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
Queries value: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7[name]
Queries value: HKCU\software\classes\local
settings\muicache\13\52c64b7e[@%systemroot%\system32\dnsapi.dll,-103]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\autoupdate[rootdirurl]
Queries value: HKLM\software\microsoft\systemcertificates\authroot\autoupdate[flags]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugflags]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllcreatecertificatechainengine\config[enableinetunknownauth]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[08f93b14-1608-4a72-
9cfa-457eecedbba7]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[50b3e73c-9370-461d-
bb9f-26f32d68887d]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
Value changes: HKCU\software\classes\local settings\muicache\13\52c64b7e[languagelist]