

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Task ID:	481	Host: mag2, Sample ID: 470, Task ID: 481
Risk Level:	10	
Date Processed:	2016-03-24 14:07:58 (UTC)	
Processing Time:	62.55 seconds	
Virtual Environment:	IntelliVM	
Execution Arguments:	"c:\windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe"	

Sample ID:	470
Type:	basic
Owner:	admin
Label:	755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63
Date Added:	2016-03-24 14:07:57 (UTC)
File Type:	PE32:win32:gui
File Size:	1580101 bytes
MD5:	cba74e507e9741740d251b1fb34a1874
SHA256:	755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63
Description:	None

## Pattern Matching Results

3	Writes to a log file [Info]
5	Possible process injection
1	SSL traffic on standard port
3	Long sleep detected
7	Attempts to connect to dynamic DNS
6	Modifies registry autorun entries
8	Starts svchost.exe
5	Accesses Filesystem keys
3	Connects to local host
10	Creates malicious events: Bookworm [Worm]
1	YARA score 1
5	Opens Copy Hook Handlers key
4	Reads process memory
3	HTTP connection - response code 200 (success)
5	Installs service

## Static Events

YARA rule hit:	Nonexecutable
Anomaly:	PE: Contains a virtual section

## Process/Thread Events

Creates process:	
C:\windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe	
["C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe" "C:\Program Files (x86)\install.exe" ]	
Creates process: C:\Program Files (x86)\flashplayer18_a_install.exe ["C:\Program Files (x86)\flashplayer18_a_install.exe" ]	
Creates process: C:\Program Files (x86)\install.exe ["C:\Program Files (x86)\install.exe"	
]	
Creates process: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe	
["C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe" "C:\Program Files (x86)\install.exe" ]	
Creates process: C:\ProgramData\Microsoft\DeviceSync\MsMpEng.exe	
[C:\ProgramData\Microsoft\DeviceSync\MsMpEng.exe]	
Creates process: C:\Windows\SysWOW64\svchost.exe [ -main]	
Creates process: C:\Windows\SysWOW64\svchost.exe [ -protect]	
Creates process: C:\Windows\SysWOW64\dlldllhost.exe [C:\Windows\SysWOW64\dlldllhost.exe -user]	
Reads from process: PID:2240 C:\Windows\SysWOW64\dlldllhost.exe	
Writes to process: PID:1568 C:\Windows\SysWOW64\svchost.exe	
Writes to process: PID:2216 C:\Windows\SysWOW64\svchost.exe	
Writes to process: PID:2240 C:\Windows\SysWOW64\dlldllhost.exe	
Terminates process:	
C:\Windows\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe	
Terminates process: C:\ProgramData\Microsoft\DeviceSync\MsMpEng.exe	
Terminates process: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe	
Terminates process: C:\Program Files (x86)\install.exe	

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0	
Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfdMonitorInstMutexDefault1	
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCounterMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\Adobe_ADM.log	
Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\_!MSFTHISTORY!_	
Creates mutex: \Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!	
Creates mutex: \Sessions\1\BaseNamedObjects\c:\users\admin!appdata!roaming!microsoft!windows!cookies!	
Creates mutex: \Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!history!history.ie5!	
Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\!PrivacIE!SharedMemory!Mutex	
Creates mutex: \BaseNamedObjects\BB6cmqyHzy8kkcJ	
Creates mutex: \BaseNamedObjects\DBWinMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\__DDrawExclMode__	
Creates mutex: \Sessions\1\BaseNamedObjects\__DDrawCheckExclMode__	
Creates mutex: \Sessions\1\BaseNamedObjects\DDrawWindowListMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex	
Creates mutex: \Sessions\1\BaseNamedObjects\Adobe_GDE.log	
Creates mutex: \BaseNamedObjects\_!MSFTHISTORY!_	

```
Creates mutex:
\BaseNamedObjects\c:\users\admin\appdata\local\microsoft\windows\temporary internet
files\content.ie5!
Creates mutex:
\BaseNamedObjects\c:\users\admin\appdata\roaming\microsoft\windows\cookies!
Creates mutex:
\BaseNamedObjects\c:\users\admin\appdata\local\microsoft\windows\history\history.ie5!
Creates mutex: \BaseNamedObjects\WininetStartupMutex
Creates mutex: \BaseNamedObjects\WininetProxyRegistryMutex
Creates mutex: \BaseNamedObjects\RasPbFile
Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates mutex: \Sessions\1\BaseNamedObjects\MSIMGSIZECacheMutex
Creates event: \KernelObjects\MaximumCommitCondition
Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfaActivated.Default1
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event: \BaseNamedObjects\SvcctlStartEvent_A3752DX
Creates event: \BaseNamedObjects\TermSrvReadyEvent
Creates event: \Sessions\1\BaseNamedObjects\CancelPort{4B0D4ADE-4CD1-4C14-B91F-
0B81B3658FD4}
Creates event: \BaseNamedObjects\BFE_Notify_Event_{2b7b2c24-181c-42ec-aaca-
0cea60941d33}
Creates event: \BaseNamedObjects\BFE_Notify_Event_{6580be35-3ce6-4645-8d0d-
ae7fefcdb845}
Creates event: \Sessions\1\BaseNamedObjects\CancelPort{F073E758-E77B-4DE5-9054-
56981D839D4B}
Creates semaphore: \BaseNamedObjects\{61410B1E-728E-4E96-96DD-9BE271228D74}
Creates semaphore: \BaseNamedObjects\{A925355A-7A05-4070-B3BC-3D323F229F91}}
```

## File System Events

```
Creates: C:\Users\Admin\AppData\Local\Temp\${inst}
Creates: C:\Users\Admin\AppData\Local\Temp\${inst}\2.tmp
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
Creates: C:\Users\Admin\AppData\Local\Temp\${inst}\temp_0.tmp
Creates: C:\Program Files (x86)\install.exe
Creates: C:\Program Files (x86)\flashplayer18_a_install.exe
Creates: C:\Program Files (x86)\Adobe\NewProduct
Creates: C:\Program Files (x86)\Adobe\NewProduct\Uninstall.exe
Creates: C:\Program Files (x86)\Adobe\NewProduct\Uninstall.ini
Creates: C:\Users\Admin\AppData\Local\Adobe\90B1C0A0-AE40-4E63-B002-A2B73E17B61A
Creates: C:\Users\Admin\AppData\Local\Temp\Adobe_ADMLogs
Creates: C:\Users\Admin\AppData\Local\Temp\Adobe_ADMLogs\Adobe_ADM.log
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:\Program Files (x86)
Creates: C:\Users
Creates: C:\Users\Admin\AppData
Creates: C:\Users\Admin\AppData\Local\Temp
Creates: C:\Users\Admin\AppData\Local\Temp\RarSFX0
Creates: C:\Users\Admin\AppData\Local\Temp\RarSFX0\_tmp_rar_sfx_access_check_105109
Creates: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe
Creates: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MpSvc.dll
Creates: C:\Users\Admin\AppData\Local\Temp\RarSFX0\readme.txt
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\160[1]
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD
Creates: C:\ProgramData
Creates: C:\ProgramData\Microsoft
Creates: C:\ProgramData\Microsoft\DeviceSync
Creates: C:\ProgramData\Mozilla
Creates: C:\ProgramData\Mozilla\Crypto
Creates: C:\ProgramData\Mozilla\Crypto\RSA
Creates: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys
Creates: C:\ProgramData\Microsoft\DeviceSync\MsMpEng.exe
Creates: C:\ProgramData\Microsoft\DeviceSync\MpSvc.dll
Creates: C:\ProgramData\Microsoft\DeviceSync\delete.txt
Creates: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
Creates: C:\ProgramData\Microsoft\DeviceSync\MpSvc
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\warning_icon_200.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_caution_200.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_caution_100.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_caution_125.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_caution_150.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_x_200.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_x_100.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_x_125.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_x_150.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_check_200.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_check_100.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_check_125.png
Creates: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys\E88B57F2
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\status_icon_check_150.png
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
```

E0FA51EC05AD\progressbar\_darkgray\_base\_200.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_darkgray\_base\_100.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_200.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_100.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_125.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_150.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\transparent.gif  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\gray\_button\_200.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\close\_200.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_200.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_100.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_125.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_150.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_200.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_100.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_125.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_150.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_200.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_100.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_125.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_150.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_200.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_100.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_125.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_150.png  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\info\_icon\_100.png  
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet  
Files\Content.IE5\266VNL5S\SC[1]  
Creates: C:\Users\Admin\AppData\Local\Temp\Adobe\_ADMLogs\Adobe\_GDE.log  
Creates: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\6a870d84bk  
Creates: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\2CF773DE-1707-4EAA-AF32-33313EDA1593  
Creates:  
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@adobe[1].txt  
Creates:  
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@adobe[2].txt  
Opens: C:\Windows\Prefetch\755A4B2EC15DA6BB01248B2DFBAD2-B591EB4C.pf  
Opens: C:\Windows  
Opens: C:\Windows\System32\wow64.dll  
Opens: C:\Windows\System32\wow64win.dll  
Opens: C:\Windows\System32\wow64cpu.dll  
Opens: C:\Windows\system32\wow64log.dll  
Opens: C:\Windows\SysWOW64  
Opens: C:\Windows\SysWOW64\sechost.dll  
Opens: C:\Windows\temp\winmm.dll  
Opens: C:\Windows\SysWOW64\winmm.dll  
Opens:  
C:\Windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe.Local\  
Opens: C:\Windows\winsxs\x86\_microsoft.windows.common-  
controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2  
Opens: C:\Windows\winsxs\x86\_microsoft.windows.common-  
controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2\comctl32.dll  
Opens: C:\Windows\temp\cabinet.dll  
Opens: C:\Windows\SysWOW64\cabinet.dll  
Opens: C:\Windows\SysWOW64\imm32.dll  
Opens: C:\Windows\WindowsShell.Manifest  
Opens: C:\Windows\SysWOW64\uxtheme.dll  
Opens: C:\Windows\temp\dwmmapi.dll  
Opens: C:\Windows\SysWOW64\dwmmapi.dll  
Opens: C:\Windows\Fonts\StaticCache.dat  
Opens: C:\Windows\SysWOW64\en-US\User32.dll.mui  
Opens: C:\Users\Admin\AppData\Local\Temp\\$inst  
Opens: C:\Users\Admin\AppData\Local\Temp  
Opens:  
C:\Windows\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe  
Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\2.tmp  
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls  
Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\7.tmp  
Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\9.tmp  
Opens: C:\Windows\SysWOW64\rpcss.dll  
Opens: C:\Windows\temp\msftedit.DLL  
Opens: C:\Windows\SysWOW64\msftedit.dll  
Opens: C:\Windows\win.ini  
Opens: C:\Windows\SysWOW64\uxtheme.dll.Config  
Opens: C:\Program Files (x86)  
Opens: C:\Windows\SysWOW64\shell32.dll  
Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui

Opens: C:\  
Opens: C:\Windows\SysWOW64\propsys.dll  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db  
Opens: C:\Windows\temp\ntmarta.dll  
Opens: C:\Windows\SysWOW64\ntmarta.dll  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000001.db  
Opens: C:\Program Files (x86)\desktop.ini  
Opens: C:\Windows\SysWOW64\ole32.dll  
Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\temp\_0.tmp  
Opens: C:\Program Files (x86)\install.exe  
Opens: C:\Program Files (x86)\flashplayer18\_a\_install.exe  
Opens: C:\Program Files (x86)\adobe\NewProduct\Uninstall.exe  
Opens: C:\Program Files (x86)\adobe\NewProduct  
Opens: C:\Program Files (x86)\Adobe  
Opens: C:\Program Files (x86)\Adobe\NewProduct\Uninstall.exe  
Opens: C:\Windows\temp\imageres.dll  
Opens: C:\Windows\SysWOW64\imageres.dll  
Opens: C:\Windows\SysWOW64\en-US\imageres.dll.mui  
Opens: C:\Program Files (x86)\Adobe\NewProduct  
Opens: C:\Users\Admin\Desktop\desktop.ini  
Opens: C:\Windows\temp\profapi.dll  
Opens: C:\Windows\SysWOW64\profapi.dll  
Opens: C:\Windows\System32\propsys.dll  
Opens: C:\Windows\SysWOW64\en-US\propsys.dll.mui  
Opens: C:\Windows\SysWOW64\urlmon.dll  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies  
Opens: C:\Program Files (x86)\flashplayer18\_a\_install.exe:Zone.Identifier  
Opens: C:\Windows\SysWOW64\apphelp.dll  
Opens: C:\Windows\AppPatch\sysmain.sdb  
Opens: C:\Program Files (x86)\ui\SwDRM.dll  
Opens: C:\Windows\Prefetch\FLASHPLAYER18\_A\_INSTALL.EXE-B865460F.pf  
Opens: C:\Program Files (x86)\NETAPI32.dll  
Opens: C:\Windows\SysWOW64\netapi32.dll  
Opens: C:\Program Files (x86)\netutils.dll  
Opens: C:\Windows\SysWOW64\netutils.dll  
Opens: C:\Program Files (x86)\srvcli.dll  
Opens: C:\Windows\SysWOW64\srvcli.dll  
Opens: C:\Program Files (x86)\wkscli.dll  
Opens: C:\Windows\SysWOW64\wkscli.dll  
Opens: C:\Program Files (x86)\SAMCLI.DLL  
Opens: C:\Windows\SysWOW64\samcli.dll  
Opens: C:\Program Files (x86)\WINHTTP.dll  
Opens: C:\Windows\SysWOW64\winhttp.dll  
Opens: C:\Program Files (x86)\webio.dll  
Opens: C:\Windows\SysWOW64\webio.dll  
Opens: C:\Program Files (x86)\msi.dll  
Opens: C:\Windows\SysWOW64\msi.dll  
Opens: C:\Program Files (x86)\VERSION.dll  
Opens: C:\Windows\SysWOW64\version.dll  
Opens: C:\Program Files (x86)\VMSIMG32.dll  
Opens: C:\Windows\SysWOW64\msimg32.dll  
Opens: C:\Program Files (x86)\WINSPOOL.DRV  
Opens: C:\Windows\SysWOW64\winspool.drv  
Opens: C:\Program Files (x86)\flashplayer18\_a\_install.exe.Local\  
Opens: C:\Program Files (x86)\UxTheme.dll  
Opens: C:\Program Files (x86)\oledlg.dll  
Opens: C:\Windows\SysWOW64\oledlg.dll  
Opens: C:\Windows\winsxs\x86\_microsoft.windows.gdiplus\_6595b64144ccf1df\_1.1.7601.17514\_none\_72d18a4386696c80  
Opens: C:\Windows\winsxs\x86\_microsoft.windows.gdiplus\_6595b64144ccf1df\_1.1.7601.17514\_none\_72d18a4386696c80\GdiPlus.dll  
Opens: C:\Program Files (x86)\MPR.dll  
Opens: C:\Windows\SysWOW64\mpr.dll  
Opens: C:\Program Files (x86)\OLEACC.dll  
Opens: C:\Windows\SysWOW64\oleacc.dll  
Opens: C:\Program Files (x86)\install.exe:Zone.Identifier  
Opens: C:\Program Files (x86)\WINMM.dll  
Opens: C:\Program Files (x86)\OLEACCRD.DLL  
Opens: C:\Windows\SysWOW64\oleaccrc.dll  
Opens: C:\Windows\Fonts\arial.ttf  
Opens: C:\Program Files (x86)\flashplayer18\_a\_installENU.dll  
Opens: C:\Program Files (x86)\flashplayer18\_a\_installENU.dll.DLL  
Opens: C:\Program Files (x86)\flashplayer18\_a\_installLOC.dll  
Opens: C:\Program Files (x86)\flashplayer18\_a\_installLOC.dll.DLL  
Opens: C:\Program Files (x86)\win\setup\iPlayer.ico  
Opens: C:\Users\Admin\AppData\Local  
Opens: C:\Program Files (x86)\lotus\approach\approach.exe  
Opens: C:\CARS.url  
Opens: C:\Users\Admin\AppData\Local\Adobe\90B1C0A0-AE40-4E63-B002-A2B73E17B61A  
Opens: C:\Program Files (x86)\ntmarta.dll  
Opens: C:\Users\Admin\AppData\Local\Temp\Adobe\_ADMLogs  
Opens: C:\Program Files (x86)\QW\_WIN95\SETUP.PKG  
Opens: C:\Program Files (x86)\Inspiration Documentation\Getting Started.pdf  
Opens: C:\Program Files (x86)\exe\org6.exe  
Opens: C:\Program Files (x86)\SMARTCTR\SUITEST.EXE  
Opens: C:\Program Files (x86)\x86\System32\PDBoot.exe  
Opens: C:\Program Files (x86)\x64\System64\PDBoot.exe  
Opens: C:\Users\Admin\AppData\Local\Temp\00BE.trace  
Opens: C:\Users\Admin\AppData\Local\Temp\00BE.debug  
Opens: C:\Users\Admin\AppData\Local\Temp\adm.trace  
Opens: C:\DISK2\DATA2.CAB  
Opens: C:\Program Files (x86)\Install\data1.cab  
Opens: C:\Users\Admin\AppData\Local\Temp\adm.debug  
Opens: C:\Users\Admin\AppData\Local\Temp\Adobe\_ADMLogs\Adobe\_ADM.log  
Opens: C:\Users\Admin\AppData\Local\Temp\Adobe\_ADM.trace  
Opens: C:\Users\Admin\AppData\Local\Temp\Adobe\_ADM.debug  
Opens: C:\Program Files (x86)\CATALOG\Children\landbeforetime\LBTlogo.gif  
Opens: C:\Windows\SysWOW64\tzres.dll  
Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui  
Opens: C:\Program Files (x86)\StoneAge\StoneAge.exe

Opens: C:\Program Files (x86)\data\jars\BcdSharedLib.jar  
 Opens: C:\Program Files (x86)\data\jars\BcdChildApp.jar  
 Opens: C:\Program Files (x86)\Intro95\Clabs\_logo.bmp  
 Opens: C:\Program Files (x86)\INSTALL\DATA.TAG  
 Opens: C:\Program Files (x86)\Runimage\delphi50\bin\coride50.bpl  
 Opens: C:\Program Files (x86)\RUNIMAGE\DELPHI40\BIN\DFWEDIT.DLL  
 Opens: C:\Program Files (x86)\flashplayer18\_a\_install.exe.3.Manifest  
 Opens: C:\Program Files (x86)\dwmapi.dll  
 Opens: C:\install.exe  
 Opens: C:\Program Files (x86)\jdk\java\jre\bin\java.exe  
 Opens: C:\Program Files (x86)\SETUP\ANTIVIR\ENU\SERVER\WINNT\SETUPEX.EXE  
 Opens: C:\Program Files (x86)\TRIAL\ANTIVIR\ENU\WORKSTAT\WINNT\FSAVNTWS.EXE  
 Opens: C:\Resource1.zip  
 Opens: C:\Program Files (x86)\setup\images\jbuilder.ico  
 Opens: C:\Program Files (x86)\INSTALL\SHGM.INF  
 Opens: C:\Program Files (x86)\help\bcd\win\2003-dlx.chm  
 Opens: C:\Program Files (x86)\DATA\DISK\LEGOISLE.EXE  
 Opens: C:\vewolf.ico  
 Opens: C:\WINNT\WMSSET.INF  
 Opens: C:\Windows\SysWOW64\ieframe.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\0.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\1.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\3.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\4.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\5.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\6.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\8.tmp  
 Opens: C:\Windows\Prefetch\INSTALL.EXE-D4AD4950.pf  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\10.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\11.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\12.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\13.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\14.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\15.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\16.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\17.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\20.tmp  
 Opens: C:\Program Files (x86)\install.exe.Local\  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\50.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\21.tmp  
 Opens: C:\Users\Admin\AppData\Local\Temp\\$inst\51.tmp  
 Opens: C:\Program Files (x86)\apphelp.dll  
 Opens: C:\Windows\AppPatch\AcLayers.dll  
 Opens: C:\Program Files (x86)\USERENV.dll  
 Opens: C:\Windows\SysWOW64\userenv.dll  
 Opens: C:\Program Files (x86)\profapi.dll  
 Opens: C:\Program Files (x86)\riched32.dll  
 Opens: C:\Windows\SysWOW64\riched32.dll  
 Opens: C:\Program Files (x86)\RICHED20.dll  
 Opens: C:\Windows\SysWOW64\riched20.dll  
 Opens: C:\Windows\SysWOW64\wininet.dll  
 Opens: C:\Windows\Fonts\simsun.ttc  
 Opens: C:\Users\Admin  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet  
 Files\desktop.ini  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet  
 Files\Content.IE5  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet  
 Files\Content.IE5\desktop.ini  
 Opens: C:\Windows\Fonts\mingliu.ttc  
 Opens: C:\Windows\Fonts\msmincho.ttc  
 Opens: C:\Windows\Fonts\batang.ttc  
 Opens: C:\Windows\Fonts\msgothic.ttc  
 Opens: C:\Windows\Fonts\gulim.ttc  
 Opens: C:\Users\Admin\AppData\Roaming  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet  
 Files\Content.IE5\index.dat  
 Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat  
 Opens: C:\Program Files (x86)\Common Files\microsoft shared\ink\iptisf.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0  
 Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\\_tmp\_rar\_sfx\_access\_check\_105109  
 Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe  
 Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MpSvc.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\readme.txt  
 Opens: C:\Program Files (x86)\PROPSYS.dll  
 Opens: C:\Program Files (x86)\HELP\STAR.HTM  
 Opens: C:\Program Files (x86)\dnsapi.DLL  
 Opens: C:\Windows\SysWOW64\dnsapi.dll  
 Opens: C:\Program Files (x86)\iphlpapi.DLL  
 Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL  
 Opens: C:\Program Files (x86)\WINNSI.DLL  
 Opens: C:\Windows\SysWOW64\winnsi.dll  
 Opens: C:\Windows\SysWOW64\en-US\ieframe.dll.mui  
 Opens: C:\Windows\SysWOW64\mshtml.dll  
 Opens: C:\Windows\SysWOW64\msls31.dll  
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet  
 Files\Content.IE5\TZILKL9J\160[1]  
 Opens: C:\Windows\SysWOW64\en-US\urlmon.dll.mui  
 Opens: C:\Windows\SysWOW64\msxml3.dll  
 Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui  
 Opens: C:\Windows\SysWOW64\msxml3r.dll  
 Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD  
 Opens: C:\Windows\SysWOW64\msimtf.dll  
 Opens: C:\Users\desktop.ini

Opens: C:\Users  
Opens: C:\Users\Admin\Searches\desktop.ini  
Opens: C:\Users\Admin\Videos\desktop.ini  
Opens: C:\Users\Admin\Pictures\desktop.ini  
Opens: C:\Users\Admin\Contacts\desktop.ini  
Opens: C:\Program Files (x86)\CRYPTSP.dll  
Opens: C:\Windows\SysWOW64\cryptsp.dll  
Opens: C:\Windows\SysWOW64\rsaenh.dll  
Opens: C:\Program Files (x86)\RpcRtRemote.dll  
Opens: C:\Windows\SysWOW64\RpcRtRemote.dll  
Opens: C:\Program Files (x86)\SXS.DLL  
Opens: C:\Windows\SysWOW64\sxs.dll  
Opens: C:\Program Files (x86)\MLANG.dll  
Opens: C:\Windows\SysWOW64\mlang.dll  
Opens: C:\Windows\SysWOW64\jscript.dll  
Opens: C:\Users\Admin\Favorites\desktop.ini  
Opens: C:\Users\Admin\Music\desktop.ini  
Opens: C:\Users\Admin\Downloads\desktop.ini  
Opens: C:\Users\Admin\Documents\desktop.ini  
Opens: C:\Users\Admin\Links\desktop.ini  
Opens: C:\Users\Admin\Saved Games\desktop.ini  
Opens: C:\Windows\SysWOW64\shdocvw.dll  
Opens: C:\Windows\SysWOW64\en-US\shdocvw.dll.mui  
Opens: C:\Users\Admin\AppData  
Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe:Zone.Identifier  
Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\ui\SwDRM.dll  
Opens: C:\Windows\Prefetch\MSMPENG.EXE-21EA2863.pf  
Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\USERENV.dll  
Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\profapi.dll  
Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\WINSPOOL.DRV  
Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MPR.dll  
Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\IPHlpApi.dll  
Opens: C:\Users\Admin\AppData\Local\Temp\RarSFX0\WINNSI.DLL  
Opens: C:\ProgramData\Microsoft\DeviceSync\MsMpEng.exe  
Opens: C:\ProgramData\Microsoft\DeviceSync\MpSvc.dll  
Opens: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys\sgkey.data  
Opens: C:\Windows\SysWOW64\dxtrans.dll  
Opens: C:\Windows\SysWOW64\atl.dll  
Opens: C:\Windows\Prefetch\MSMPENG.EXE-E3190967.pf  
Opens: C:\ProgramData\Microsoft\DeviceSync\readme.txt  
Opens: C:\ProgramData\Microsoft\DeviceSync\MpSvc  
Opens: C:\ProgramData\Microsoft\DeviceSync\IPHlpApi.dll  
Opens: C:\ProgramData\Microsoft\DeviceSync\WINNSI.DLL  
Opens: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys\sg.setting  
Opens: C:\Windows\SysWOW64\svchost.exe  
Opens: C:\Windows\SysWOW64\ui\SwDRM.dll  
Opens: C:\Windows\Prefetch\SVCHOST.EXE-51F5DA2F.pf  
Opens: C:\Windows\SysWOW64\ddrawex.dll  
Opens: C:\Windows\SysWOW64\en-US\svchost.exe.mui  
Opens: C:\Windows\SysWOW64\ddraw.dll  
Opens: C:\Windows\SysWOW64\dciman32.dll  
Opens: C:\Windows\SysWOW64\en-US\ddraw.dll.mui  
Opens: C:\ProgramData\Microsoft\DeviceSync\delete.txt  
Opens: C:\Windows\SysWOW64\en-US\shell32.dll.mui  
Opens: C:\Windows\SysWOW64\ntshrui.dll  
Opens: C:\Windows\SysWOW64\en-US\ntshrui.dll.mui  
Opens: C:\Program Files (x86)\cscapi.dll  
Opens: C:\Windows\SysWOW64\cscapi.dll  
Opens: C:\Program Files (x86)\slc.dll  
Opens: C:\Windows\SysWOW64\slc.dll  
Opens: C:\Windows\SysWOW64\dxtransft.dll  
Opens: C:\Users\Public  
Opens: C:\Windows\SysWOW64\kernel32.dll  
Opens: C:\Windows\SysWOW64\stdole2.tlb  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\warning\_icon\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_caution\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_caution\_100.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_caution\_125.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_caution\_150.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_x\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_x\_100.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_x\_125.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_x\_150.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_check\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_check\_100.png  
Opens: C:\Windows\Prefetch\SVCHOST.EXE-D4143593.pf  
Opens: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys\E88B57F2  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_check\_125.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\status\_icon\_check\_150.png  
Opens: C:\ProgramData\Microsoft\DeviceSync\F45C8A7E  
Opens: C:\ProgramData\Microsoft\DeviceSync\s6a870d84  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\progressbar\_darkgray\_base\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\progressbar\_darkgray\_base\_100.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-E0FA51EC05AD\progressbar\_blue\_active\_200.png  
Opens: C:\Windows\SysWOW64\wtsapi32.dll  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-

E0FA51EC05AD\progressbar\_blue\_active\_100.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_125.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_150.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\transparent.gif  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\gray\_button\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\close\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_200.png  
Opens: C:\Windows\SysWOW64\winsta.dll  
Opens: C:\Windows\Temp  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_100.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_125.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_150.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_100.png  
Opens: C:\Windows\SysWOW64\dlhhost.exe  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_125.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_150.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_100.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_125.png  
Opens: C:\Windows\Prefetch\DLLHOST.EXE-99F4EFBD.pf  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_150.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_200.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_100.png  
Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_125.png  
Opens: C:\Windows\SysWOW64\dhcpcsvc.dll  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_150.png  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\info\_icon\_100.png  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet  
Files\Content.IE5\266VNL5S\SC[1]  
Opens: C:\Windows\Fonts\arialbd.ttf  
Opens: C:\Users\Admin\AppData\Local\Temp\Adobe\_ADMLogs\Adobe\_GDE.log  
Opens: C:\Users\Admin\AppData\Local\Temp\Adobe\_GDE.trace  
Opens: C:\Users\Admin\AppData\Local\Temp\Adobe\_GDE.debug  
Opens: C:\Windows\SysWOW64\mswsock.dll  
Opens: C:\Program Files (x86)\dhcpcsvc6.DLL  
Opens: C:\Program Files (x86)\dhcpcsvc.DLL  
Opens: C:\Windows\SysWOW64\WSH\_TCPIP.DLL  
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\u6a870d84  
Opens: C:\Windows\SysWOW64\svchost.exe.Local\  
Opens: C:\Program Files (x86)\credssp.dll  
Opens: C:\Windows\SysWOW64\credssp.dll  
Opens: C:\Windows\SysWOW64\wship6.dll  
Opens: C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\profiles.ini  
Opens: C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\prefs.js  
Opens: C:\Program Files (x86)\rasadhlp.dll  
Opens: C:\Windows\SysWOW64\rasadhlp.dll  
Opens: C:\Windows\System32\drivers\etc\hosts  
Opens: C:\Windows\SysWOW64\FWPULNT.DLL  
Opens: C:\Windows\SysWOW64\rasapi32.dll  
Opens: C:\Windows\SysWOW64\rasman.dll  
Opens: C:\Windows\SysWOW64\rtutils.dll  
Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\  
Opens: C:\Windows\SysWOW64\ras  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk  
Opens: C:\Windows\SysWOW64\SensApi.dll  
Opens: C:\Windows\SysWOW64\nlaapi.dll  
Opens: C:\Windows\SysWOW64\schannel.dll  
Opens: C:\Program Files (x86)\secur32.dll  
Opens: C:\Windows\SysWOW64\secur32.dll  
Opens: C:\Program Files (x86)\ncrypt.dll  
Opens: C:\Windows\SysWOW64\ncrypt.dll  
Opens: C:\Program Files (x86)\bcrypt.dll  
Opens: C:\Windows\SysWOW64\bcrypt.dll  
Opens: C:\Windows\SysWOW64\bcryptprimitives.dll  
Opens: C:\Windows\SysWOW64\p2pollab.dll  
Opens: C:\Windows\SysWOW64\qagentrt.dll  
Opens: C:\Windows\SysWOW64\en-US\crypt32.dll.mui  
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:\Program Files (x86)\GPAPI.dll  
Opens: C:\Windows\SysWOW64\gpapi.dll  
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My  
Opens: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\2CF773DE-1707-4EAA-AF32-33313EDA1593  
Opens: C:\Windows\SysWOW64\iepeers.dll  
Opens: C:\Program Files (x86)\RASAPI32.dll

Opens: C:\Program Files (x86)\rasman.dll  
Opens: C:\Program Files (x86)\rtutils.dll  
Opens: C:\Program Files (x86)\sensapi.dll  
Opens: C:\Users\Admin\AppData\Local\Microsoft  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer  
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer\MSIMGSI.DAT  
Opens: C:\Program Files (x86)\ImgUtil.dll  
Opens: C:\Windows\SysWOW64\imgutil.dll  
Opens: C:\Windows\SysWOW64\pngfilt.dll  
Opens:  
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@adobe[1].txt  
Opens:  
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@adobe[2].txt  
Writes to: C:\Users\Admin\AppData\Local\Temp\\$inst\2.tmp  
Writes to: C:\Users\Admin\AppData\Local\Temp\\$inst\temp\_0.tmp  
Writes to: C:\Program Files (x86)\install.exe  
Writes to: C:\Program Files (x86)\flashplayer18\_a\_install.exe  
Writes to: C:\Program Files (x86)\Adobe\NewProduct\Uninstall.exe  
Writes to: C:\Program Files (x86)\Adobe\NewProduct\Uninstall.ini  
Writes to: C:\Users\Admin\AppData\Local\Temp\Adobe\_ADMLogs\Adobe\_ADM.log  
Writes to: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe  
Writes to: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MpSvc.dll  
Writes to: C:\Users\Admin\AppData\Local\Temp\RarSFX0\readme.txt  
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet  
Files\Content.IE5\TZILKL9J\160[1]  
Writes to: C:\ProgramData\Microsoft\DeviceSync\MsMpEng.exe  
Writes to: C:\ProgramData\Microsoft\DeviceSync\MpSvc.dll  
Writes to: C:\ProgramData\Microsoft\DeviceSync\delete.txt  
Writes to: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys\sgkey.data  
Writes to: C:\ProgramData\Microsoft\DeviceSync\MpSvc  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\warning\_icon\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_caution\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_caution\_100.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_caution\_125.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_caution\_150.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_x\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_x\_100.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_x\_125.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_x\_150.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_check\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_check\_100.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_check\_125.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\status\_icon\_check\_150.png  
Writes to: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys\E88B57F2  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_darkgray\_base\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_darkgray\_base\_100.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_100.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_125.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_blue\_active\_150.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\transparent.gif  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\gray\_button\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\close\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_100.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_125.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\progressbar\_pole\_null\_150.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_100.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_125.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_150.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_100.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_125.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_mini\_150.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-  
E0FA51EC05AD\yellow\_button\_short\_200.png  
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-



```
E0FA51EC05AD\yellow_button_short_100.png
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\yellow_button_short_125.png
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\yellow_button_short_150.png
Writes to: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\info_icon_100.png
Writes to: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\SC[1]
Writes to: C:\Users\Admin\AppData\Local\Temp\Adobe_ADMLogs\Adobe_GDE.log
Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@adobe[1].txt
Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@adobe[2].txt
Reads from: C:\Windows\Fonts\StaticCache.dat
Reads from:
C:\Windows\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
Reads from: C:\Users\Admin\AppData\Local\Temp\$_inst\2.tmp
Reads from: C:\Windows\win.ini
Reads from: C:\Program Files (x86)\desktop.ini
Reads from: C:\Users\Admin\AppData\Local\Temp\$_inst\temp_0.tmp
Reads from: C:\Users\Admin\Desktop\desktop.ini
Reads from: C:\Program Files (x86)\flashplayer18_a_install.exe
Reads from: C:\Program Files (x86)\install.exe
Reads from: C:\Users\Admin\AppData\Local\Temp\Adobe_ADMLogs\Adobe_ADM.log
Reads from: C:\Users\desktop.ini
Reads from: C:\Users\Admin\Searches\desktop.ini
Reads from: C:\Users\Admin\Videos\desktop.ini
Reads from: C:\Users\Admin\Pictures\desktop.ini
Reads from: C:\Users\Admin\Contacts\desktop.ini
Reads from: C:\Users\Admin\Favorites\desktop.ini
Reads from: C:\Users\Admin\Music\desktop.ini
Reads from: C:\Users\Admin\Downloads\desktop.ini
Reads from: C:\Users\Admin\Documents\desktop.ini
Reads from: C:\Users\Admin\Links\desktop.ini
Reads from: C:\Users\Admin\Saved Games\desktop.ini
Reads from: C:\Windows\SysWOW64\shdocvw.dll
Reads from: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe
Reads from: C:\Users\Admin\AppData\Local\Temp\RarSFX0\readme.txt
Reads from: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MpSvc.dll
Reads from: C:\ProgramData\Microsoft\DeviceSync\MpSvc
Reads from: C:\ProgramData\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
Reads from: C:\Windows\SysWOW64\svchost.exe
Reads from: C:\ProgramData\Microsoft\DeviceSync\delete.txt
Reads from: C:\Windows\SysWOW64\ntshrui.dll
Reads from: C:\Windows\SysWOW64\dxtmsft.dll
Reads from: C:\Windows\SysWOW64\stdole2.tlb
Reads from: C:\Windows\SysWOW64\dxtrans.dll
Reads from: C:\Users\Admin\AppData\Local\Temp\Adobe_ADMLogs\Adobe_GDE.log
Reads from: C:\Windows\System32\drivers\etc\hosts
Reads from: C:\Windows\SysWOW64\iepeers.dll
Reads from: C:\Users\Admin\AppData\Local\Adobe\F9B5B628-A559-4282-B35A-
E0FA51EC05AD\yellow_button_100.png
Deletes: C:\Users\Admin\AppData\Local\Temp\$_inst\temp_0.tmp
Deletes: C:\Users\Admin\AppData\Local\Adobe\90B1C0A0-AE40-4E63-B002-A2B73E17B61A
Deletes: C:\Users\Admin\AppData\Local\Temp\$_inst\2.tmp
Deletes: C:\Users\Admin\AppData\Local\Temp\$_inst
Deletes:
C:\Users\Admin\AppData\Local\Temp\RarSFX0\_tmp_rar_sfx_access_check_105109
Deletes: C:\Program Files (x86)\install.exe
Deletes: C:\Users\Admin\AppData\Local\Temp\RarSFX0
Deletes: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MpSvc.dll
Deletes: C:\Users\Admin\AppData\Local\Temp\RarSFX0\MsMpEng.exe
Deletes: C:\Users\Admin\AppData\Local\Temp\RarSFX0\readme.txt
Deletes: C:\ProgramData\Microsoft\DeviceSync\delete.txt
Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@adobe[1].txt
```

Network Events

DNS query:	linuxdns.sytes.net
DNS query:	get.adobe.com
DNS query:	dlmping2.adobe.com
DNS query:	stats.adobe.com
DNS query:	systeminfothai.gotdns.ch
DNS query:	sysnc.sytes.net
DNS response:	linuxdns.sytes.net ⇒ 0.0.0.0
DNS response:	get.wip4.adobe.com ⇒ 192.150.16.58
DNS response:	e4578.g.akamaiedge.net ⇒ 23.197.61.24
DNS response:	adobe.com.d1.sc.omtrdc.net ⇒ 192.243.250.65
DNS response:	adobe.com.d1.sc.omtrdc.net ⇒ 192.243.250.16
DNS response:	systeminfothai.gotdns.ch ⇒ 0.0.0.0
DNS response:	sysnc.sytes.net ⇒ 0.0.0.0
Connects to:	0.0.0.0:80
Connects to:	192.150.16.58:443
Connects to:	0.0.0.0:1433
Connects to:	0.0.0.0:8080
Connects to:	0.0.0.0:53
Connects to:	0.0.0.0:443
Connects to:	0.0.0.0:21
Connects to:	127.0.0.1:60446
Connects to:	192.243.250.65:80
Connects to:	23.197.61.24:443
Sends data to:	8.8.8.8:53
Sends data to:	get.wip4.adobe.com:443 (192.150.16.58)
Sends data to:	127.0.0.1:60446
Sends data to:	e4578.g.akamaiedge.net:443 (23.197.61.24)
Sends data to:	adobe.com.d1.sc.omtrdc.net:80 (192.243.250.65)
Receives data from:	linuxdns.sytes.net:0 (0.0.0.0)
Receives data from:	8.8.8.8:53
Receives data from:	get.wip4.adobe.com:443 (192.150.16.58)
Receives data from:	127.0.0.1:60446

Receives data from: e4578.g.akamaiedge.net:443 (23.197.61.24)  
Receives data from: adobe.com.d1.sc.omtrdc.net:80 (192.243.250.65)

## Windows Registry Events

Creates key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00  
Creates key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer  
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings  
Creates key: HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication  
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters  
Creates key: HKCU\software\microsoft\windows\_script\settings  
Creates key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings  
Creates key: HKLM\software\wow6432node\microsoft\tracing  
Creates key: HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32  
Creates key: HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs  
Creates key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\connections  
Creates key: HKLM\system\currentcontrolset\control\securityproviders\schannel  
Creates key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows nt\currentversion\network\location awareness  
Creates key: HKCU\software\microsoft\systemcertificates\my  
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\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\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\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  
 Creates key: HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32  
 Creates key: HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasmancs  
 Creates key: HKCU\software\microsoft\windows\currentversion\internet  
 settings\connections  
 Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location  
 awareness  
 Creates key: HKCU\software\microsoft\windows\currentversion\internet  
 settings\p3p\history  
 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]  
 Deletes value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
 1001\software\microsoft\windows\currentversion\internet settings[proxyserver]  
 Deletes value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
 1001\software\microsoft\windows\currentversion\internet settings[proxyoverride]  
 Deletes value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
 1001\software\microsoft\windows\currentversion\internet settings[autoconfigurl]  
 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]  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options  
 Opens key: HKLM\system\currentcontrolset\control\session manager  
 Opens key: HKLM\software\microsoft\wow64  
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file  
 execution options  
 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\locale  
 Opens key: HKLM\system\currentcontrolset\control\language  
 Opens key: HKLM\system\currentcontrolset\control\mui\languages  
 Opens key: HKLM\system\currentcontrolset\control\mui\languages\en-us  
 Opens key: HKLM\system\currentcontrolset\control\mui\languages\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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions  
Opens key: HKLM\  
Opens key: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\diagnostics  
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\software\wow6432node\microsoft\windows nt\currentversion\windows  
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\oleaut  
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
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\software\microsoft\windows nt\currentversion\fontlink\systemlink  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\datastore\_v1.0  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback\segoe ui  
Opens key: HKLM\system\currentcontrolset\control\cmf\config  
Opens key: HKCU\software\microsoft\windows nt\currentversion\windows  
Opens key: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced  
Opens key: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\fontsubstitutes  
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback\tahoma  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}\propertybag  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer  
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer  
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer  
Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder  
Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder  
Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum  
Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}\  
Opens key: HKCU\software\classes\drive\shellex\folderextensions  
Opens key: HKCR\drive\shellex\folderextensions  
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup  
Opens key: HKLM\software\microsoft\windows\currentversion\setup  
Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}  
4442-804e-409d6c4515e9}  
Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}  
409d6c4515e9}  
Opens key: HKLM\software\wow6432node\microsoft\rpc  
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername  
Opens key: HKLM\system\setup  
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

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\microsoft\com3  
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}  
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}  
Opens key: HKLM\software\policies\microsoft\windows nt\rpc  
Opens key: HKLM\software\policies\microsoft\sqlclient\windows  
Opens key: HKLM\software\microsoft\sqlclient\windows  
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas  
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid  
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid  
Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}  
Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}  
Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid  
Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}\  
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler  
Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders  
Opens key: HKLM\system\currentcontrolset\services\ldap  
Opens key: HKLM\software\wow6432node\microsoft\ctf\compatibility\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe  
Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}  
Opens key: HKLM\software\microsoft\ctf\tip\{000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}  
Opens key: HKLM\software\wow6432node\microsoft\ctf\  
Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\  
Opens key: HKCU\software\classes\\*.exe  
Opens key: HKCR\\*.exe  
Opens key: HKCU\software\classes\\*.exe\openwithprogid  
Opens key: HKCR\\*.exe\openwithprogid  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\\*.exe\openwithprogid  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\\*.exe  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\\*.exe\  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\\*.exe\userchoice  
Opens key: HKCU\software\classes\exefile  
Opens key: HKCR\exefile  
Opens key: HKCU\software\classes\exefile\curver  
Opens key: HKCR\exefile\curver  
Opens key: HKCR\exefile\  
Opens key: HKCU\software\classes\exefile\shellex\iconhandler  
Opens key: HKCR\exefile\shellex\iconhandler  
Opens key: HKCU\software\classes\systemfileassociations\\*.exe  
Opens key: HKCR\systemfileassociations\\*.exe  
Opens key: HKCU\software\classes\systemfileassociations\\*.exe\shellex\iconhandler  
Opens key: HKCR\systemfileassociations\\*.exe\shellex\iconhandler  
Opens key: HKCU\software\classes\exefile\docobject  
Opens key: HKCR\exefile\docobject  
Opens key: HKCU\software\classes\systemfileassociations\\*.exe\docobject  
Opens key: HKCR\systemfileassociations\\*.exe\docobject  
Opens key: HKCU\software\classes\exefile\browseinplace  
Opens key: HKCR\exefile\browseinplace  
Opens key: HKCU\software\classes\systemfileassociations\\*.exe\browseinplace  
Opens key: HKCR\systemfileassociations\\*.exe\browseinplace  
Opens key: HKCU\software\classes\exefile\clsid  
Opens key: HKCR\exefile\clsid  
Opens key: HKCU\software\classes\systemfileassociations\\*.exe\clsid  
Opens key: HKCR\systemfileassociations\\*.exe\clsid  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}\propertybag  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}\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:  
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\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\shell\registeredapplications\urlassociations\directory\openwithprogids  
Opens key:  
HKCU\software\microsoft\windows\shell\associations\urlassociations\directory  
Opens key:  
HKCU\software\classes\directory  
Opens key:  
HKCR\directory  
Opens key:  
HKCU\software\classes\directory\curver  
Opens key:  
HKCR\directory\curver  
Opens key:  
HKCR\directory\  
Opens key:  
HKCU\software\classes\directory\shellex\iconhandler  
Opens key:  
HKCR\directory\shellex\iconhandler  
Opens key:  
HKCU\software\classes\folder  
Opens key:  
HKCR\folder  
Opens key:  
HKCU\software\classes\folder\shellex\iconhandler  
Opens key:  
HKCR\folder\shellex\iconhandler  
Opens key:  
HKCU\software\classes\allfilesystemobjects  
Opens key:  
HKCR\allfilesystemobjects  
Opens key:  
HKCU\software\classes\allfilesystemobjects\shellex\iconhandler  
Opens key:  
HKCR\allfilesystemobjects\shellex\iconhandler  
Opens key:  
HKCU\software\classes\directory\docobject  
Opens key:  
HKCR\directory\docobject  
Opens key:  
HKCU\software\classes\folder\docobject  
Opens key:  
HKCR\folder\docobject  
Opens key:  
HKCU\software\classes\allfilesystemobjects\docobject  
Opens key:  
HKCR\allfilesystemobjects\docobject  
Opens key:  
HKCU\software\classes\directory\browseinplace  
Opens key:  
HKCR\directory\browseinplace  
Opens key:  
HKCU\software\classes\folder\browseinplace  
Opens key:  
HKCR\folder\browseinplace  
Opens key:  
HKCU\software\classes\allfilesystemobjects\browseinplace  
Opens key:  
HKCR\allfilesystemobjects\browseinplace  
Opens key:  
HKCU\software\classes\directory\clsid  
Opens key:  
HKCR\directory\clsid  
Opens key:  
HKCU\software\classes\folder\clsid  
Opens key:  
HKCR\folder\clsid  
Opens key:  
HKCU\software\classes\allfilesystemobjects\clsid  
Opens key:  
HKCR\allfilesystemobjects\clsid  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\kindmap  
Opens key:  
HKCU\software\classes\exefile\shell\open  
Opens key:  
HKCR\exefile\shell\open  
Opens key:  
HKCU\software\classes\exefile\shell\open\command  
Opens key:  
HKCR\exefile\shell\open\command  
Opens key:  
HKCU\software\classes\exefile\shell\open\droptarget  
Opens key:  
HKCR\exefile\shell\open\droptarget  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\associations  
Opens key:  
HKLM\software\microsoft\windows\currentversion\policies\associations  
Opens key:  
HKCU\software\microsoft\windows\currentversion\policies\associations  
Opens key:  
HKCU\software\classes\ade  
Opens key:  
HKCR\ade  
Opens key:  
HKCU\software\classes\adp  
Opens key:  
HKCR\adp  
Opens key:  
HKCU\software\classes\app  
Opens key:  
HKCR\app  
Opens key:  
HKCU\software\classes\asp  
Opens key:  
HKCR\asp  
Opens key:  
HKCU\software\classes\bas  
Opens key:  
HKCR\bas  
Opens key:  
HKCU\software\classes\bat  
Opens key:  
HKCR\bat  
Opens key:  
HKCU\software\classes\cer  
Opens key:  
HKCR\cer  
Opens key:  
HKCU\software\classes\chm  
Opens key:  
HKCR\chm  
Opens key:  
HKCU\software\classes\cmd  
Opens key:  
HKCR\cmd  
Opens key:  
HKCU\software\classes\com  
Opens key:  
HKCR\com  
Opens key:  
HKCU\software\classes\cpl  
Opens key:  
HKCR\cpl  
Opens key:  
HKCU\software\classes\crt  
Opens key:  
HKCR\crt  
Opens key:  
HKCU\software\classes\csh  
Opens key:  
HKCR\csh  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}  
Opens key:  
HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas  
Opens key:  
HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid  
Opens key:  
HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid  
Opens key:  
HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}  
Opens key:  
HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}  
Opens key:  
HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler  
Opens key: HKLM\system\currentcontrolset\services\crypt32  
Opens key: HKLM\software\wow6432node\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\windows\currentversion\internet settings\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  
Opens key: HKLM\software\wow6432node\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\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\  
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges  
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_unc\_savedfilecheck  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_unc\_savedfilecheck  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\  
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  
Opens key: HKCU\software\policies  
Opens key: HKCU\software  
Opens key: HKLM\software\wow6432node  
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  
Opens key: HKCU\software\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: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_initialize\_urlaction\_shellexecute\_to\_allow\_kb936610  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_initialize\_urlaction\_shellexecute\_to\_allow\_kb936610  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings  
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\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\policies\microsoft\internet explorer  
Opens key: HKLM\software\policies\microsoft\internet explorer  
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

[illegible]



33be-4251-ba85-6007caedcf9d}\propertybag  
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:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_protocol\_lockdown  
Opens key:  
HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_protocol\_lockdown  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0  
Opens key:  
HKCU\software\classes\exefile\progid  
Opens key:  
HKCR\exefile\progid  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\proguids\exefile  
Opens key:  
HKCU\software\classes\exefile\shell\open\ddeexec  
Opens key:  
HKCR\exefile\shell\open\ddeexec  
Opens key:  
HKCU\software\microsoft\windows\currentversion\app  
paths\flashplayer18\_a\_install.exe  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\app  
paths\flashplayer18\_a\_install.exe  
Opens key:  
HKLM\software\microsoft\windows\currentversion\app  
paths\flashplayer18\_a\_install.exe  
Opens key:  
HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\flashplayer18\_a\_install.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\currentversion\explorer\shell folders  
Opens key:  
HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers  
Opens key:  
HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers  
Opens key:  
HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\flashplayer18\_a\_install.exe  
Opens key:  
HKLM\software\microsoft\windows nt\currentversion\appcompatflags  
Opens key:  
HKCU\software\microsoft\windows nt\currentversion\appcompatflags  
Opens key:  
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters  
Opens key:  
HKCU\software\microsoft\windows\currentversion\app\_paths\install.exe  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\app  
paths\install.exe  
Opens key:  
HKLM\software\microsoft\windows\currentversion\app\_paths\install.exe  
Opens key:  
HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\install.exe  
Opens key:  
HKLM\system\currentcontrolset\control\filesystem  
Opens key:  
HKCU\software\classes\wow6432node\clsid  
Opens key:  
HKCR\wow6432node\clsid  
Opens key:  
HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\install.exe  
Opens key:  
HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1  
Opens key:  
HKLM\system\currentcontrolset\control\networkprovider\hworder  
Opens key:  
HKCU\software\microsoft\windows\currentversion\policies\network  
Opens key:  
HKCU\software\microsoft\windows\currentversion\policies\comdlg32  
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\shellcompatibility\applications\flashplayer18\_a\_install.exe  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}  
Opens key:  
HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas  
Opens key:  
HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid  
Opens key:  
HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32  
Opens key:  
HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32  
Opens key:  
HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler  
Opens key:  
HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler  
Opens key:  
HKCU\software\microsoft\internet explorer\main  
Opens key:  
HKLM\software\wow6432node\microsoft\internet explorer\main  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\internet explorer\main  
Opens key:  
HKLM\software\policies\microsoft\internet explorer\main  
Opens key:  
HKCU\software\policies\microsoft\internet explorer\main  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder  
Opens key:  
HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder  
Opens key:  
HKCU\software\microsoft\windows\currentversion\app  
paths\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\app  
paths\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe  
Opens key:  
HKLM\software\microsoft\windows\currentversion\app  
paths\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe  
Opens key:  
HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shell extensions\blocked

Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked

Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-a2ea-08002b30309d}

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_iedde\_register\_protocol

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_iedde\_register\_protocol

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache

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

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

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\content

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

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\cookies

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

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

Opens key: HKLM\software\policies\microsoft\windows\currentversion\explorer\autocomplete

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

Opens key: HKLM\software\wow6432node\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\autocomplete

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid

Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler

Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}

Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}

Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas

Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\progid

Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\progid

Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}

Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}

00aa005b4383}\progid  
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\progid  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\domstore  
Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprocserver32  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\feedplat  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\iecompat  
Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprochandler  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\ietld  
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}  
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}  
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\treatas  
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\progid  
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:  
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}  
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}  
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\progid  
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprochandler32  
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\_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\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprochandler  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client\  
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}  
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}  
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}\treatas  
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}\progid  
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}\inprocserver32  
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\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-  
b61bb7cdd997}\inprochandler  
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings\5.0\cache  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289  
Opens key: HKLM\software\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: HKLM\software\wow6432node\microsoft\rpc\extensions

Opens key: HKLM\software\microsoft\rpc\extensions  
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\_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\_release\_keys\_on\_unload\_kb975619  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_release\_keys\_on\_unload\_kb975619  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_security\_flag\_ignore\_revocation\_kb2275828  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_security\_flag\_ignore\_revocation\_kb2275828  
Opens key: HKLM\software\wow6432node\microsoft\ctf\compatibility\install.exe  
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\0a35f3af  
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\00000028  
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\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe\  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe\starcraft

1.03  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
explorer\browseremulation  
Opens key: HKLM\software\policies\microsoft\internet explorer\browseremulation  
Opens key: HKCU\software\policies\microsoft\internet explorer\browseremulation  
Opens key: HKCU\software\classes\protocols\name-space handler\  
Opens key: HKCR\protocols\name-space handler  
Opens key: HKCU\software\classes\protocols\name-space handler\res\  
Opens key: HKCR\protocols\name-space handler\res  
Opens key: HKCU\software\classes\protocols\name-space handler\\*\  
Opens key: HKCR\protocols\name-space handler\\*  
Opens key: HKCU\software\classes\protocols\handler\res  
Opens key: HKCR\protocols\handler\res  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}  
Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\treatas  
Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\progid  
Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\progid  
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}  
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}  
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\progid  
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprochandler  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_css\_data\_respects\_xss\_zone\_setting\_kb912120  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_css\_data\_respects\_xss\_zone\_setting\_kb912120  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_external\_style\_sheet\_fix\_for\_smartnavigation\_kb926131  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_aria\_support  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_aria\_support  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_legacy\_dispparams  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_legacy\_dispparams  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_private\_font\_setting  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_private\_font\_setting  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_css\_show\_hide\_events  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_css\_show\_hide\_events  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_display\_node\_advise\_kb833311  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_display\_node\_advise\_kb833311  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_allow\_expanduri\_bypass  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_allow\_expanduri\_bypass  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_body\_size\_in\_editable\_iframe\_kb943245  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_body\_size\_in\_editable\_iframe\_kb943245  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_databinding\_support  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_databinding\_support  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_enforce\_bstr  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_enforce\_bstr  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_dynamic\_object\_caching  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_dynamic\_object\_caching  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_object\_caching  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_object\_caching  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_legacy\_tostring\_in\_compatview  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_legacy\_tostring\_in\_compatview  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_on\_screen\_origin\_display\_pixels

Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_om\_screen\_origin\_display\_pixels  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_crash\_recovery\_save\_kb978454  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_crash\_recovery\_save\_kb978454  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_cleanup\_at\_fl  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_cleanup\_at\_fl  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}\propertybag  
Opens key: HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder  
Opens key: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app  
paths\outlook.exe  
Opens key: HKLM\software\microsoft\windows\currentversion\app\_paths\outlook.exe  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\application  
compatibility  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
explorer\domstorage  
Opens key: HKLM\software\policies\microsoft\internet explorer\domstorage  
Opens key: HKCU\software\policies\microsoft\internet explorer\domstorage  
Opens key: HKCU\software\microsoft\internet explorer\domstorage  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\domstorage  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
explorer\safety\privacie  
Opens key: HKLM\software\policies\microsoft\internet explorer\safety\privacie  
Opens key: HKCU\software\policies\microsoft\internet explorer\safety\privacie  
Opens key: HKCU\software\microsoft\internet explorer\safety\privacie  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\safety\privacie  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\mediatypeclass  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\accepted documents  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\ratings  
Opens key: HKLM\software\microsoft\windows\currentversion\policies\ratings  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_show\_failed\_connect\_content\_kb942615  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_show\_failed\_connect\_content\_kb942615  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder  
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}  
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}  
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas  
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\progid  
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\progid  
Opens key: HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}  
Opens key: HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}  
Opens key: HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\progid  
Opens key: HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}\propertybag  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}\propertybag  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}\propertybag  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}\propertybag

Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{48daf80b-e6cf-4f4e-b800-0e69d84ee384}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{48daf80b-e6cf-4f4e-b800-0e69d84ee384}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9e52ab10-f80d-49df-acb8-4330f5687855}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9e52ab10-f80d-49df-acb8-4330f5687855}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{98ec0e18-2098-4d44-8644-66979315a281}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{98ec0e18-2098-4d44-8644-66979315a281}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{cac52c1a-b53d-4edc-92d7-6b2e8ac19434}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{cac52c1a-b53d-4edc-92d7-6b2e8ac19434}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{18989b1d-99b5-455b-841c-ab7c74e4ddfc}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{18989b1d-99b5-455b-841c-ab7c74e4ddfc}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}  
Opens key: HKCU\software\classes\protocols\name-space handler\c\  
Opens key: HKCR\protocols\name-space handler\c\  
Opens key: HKCU\software\classes\protocols\handler\c\  
Opens key: HKCR\protocols\handler\c\  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{6f0cd92b-2e97-45d1-88ff-b0d186b8dedd}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{6f0cd92b-2e97-45d1-88ff-b0d186b8dedd}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{76fc4e2d-d6ad-4519-a663-37bd5608185}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{76fc4e2d-d6ad-4519-a663-37bd5608185}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a75d362e-50fc-4fb7-ac2c-a8beaa314493}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a75d362e-50fc-4fb7-ac2c-a8beaa314493}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{491e922f-5643-4af4-a7eb-4e7a138d8174}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{491e922f-5643-4af4-a7eb-4e7a138d8174}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}  
Opens key: HKCU\software\microsoft\internet explorer  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}  
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:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}  
Opens key:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_res\_to\_lmz  
Opens key:  
HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_res\_to\_lmz  
Opens key:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_load\_shdoclc\_resources  
Opens key:  
HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_load\_shdoclc\_resources  
Opens key:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_sniffing  
Opens key:  
HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_sniffing  
Opens key:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_feeds  
Opens key:  
HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_feeds  
Opens key:  
HKCU\software\classes\protocols\filter\text/html  
Opens key:  
HKCR\protocols\filter\text/html  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}  
Opens key:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_safe\_bindtoobject  
Opens key:  
HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_safe\_bindtoobject  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}  
Opens key:  
HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas  
Opens key:  
HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid  
Opens key:  
HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32  
Opens key:  
HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32  
Opens key:  
HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler  
Opens key:  
HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler  
Opens key:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_manage\_script\_circular\_refs  
Opens key:  
HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_manage\_script\_circular\_refs  
Opens key:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_filedownload  
Opens key:  
HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_filedownload  
Opens key:  
HKLM\software\wow6432node\microsoft\internet explorer\security\floppy  
access  
Opens key:  
HKCU\software\microsoft\internet explorer\security\adv addrbar spoof  
detection  
Opens key:  
HKLM\software\wow6432node\microsoft\internet explorer\security\adv  
addrbar spoof detection  
Opens key:  
HKCU\software\classes\protocols\name-space handler\about\  
Opens key:  
HKCR\protocols\name-space handler\about  
Opens key:  
HKCU\software\classes\protocols\handler\about  
Opens key:  
HKCR\protocols\handler\about  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}  
Opens key:  
HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas  
Opens key:  
HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid  
Opens key:  
HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid  
Opens key:  
HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}  
Opens key:  
HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}  
Opens key:  
HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}  
Opens key:  
HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32  
Opens key:  
HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32  
Opens key:  
HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32  
Opens key:  
HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler  
Opens key:  
HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler  
Opens key:  
HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_document\_compatible\_mode



Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_document\_compatible\_mode

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

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

Opens key: HKCU\software\policies\microsoft\internet explorer\zoom

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_weboc\_document\_zoom

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_weboc\_document\_zoom

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_ipersistmoniker\_load\_redirected\_url\_kb976425

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_ipersistmoniker\_load\_redirected\_url\_kb976425

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2400183a-6185-49fb-a2d8-4a392a602ba3}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2400183a-6185-49fb-a2d8-4a392a602ba3}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4900540-2379-4c75-844b-64e6faf8716b}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4900540-2379-4c75-844b-64e6faf8716b}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{289a9a43-be44-4057-a41b-587a76d7e7f9}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{289a9a43-be44-4057-a41b-587a76d7e7f9}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bfebf45-347d-4006-a5be-ac0cb0567192}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bfebf45-347d-4006-a5be-ac0cb0567192}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}

Opens key: HKCU\software\policies\microsoft\internet explorer

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}

Opens key: HKCU\software\microsoft\internet explorer\international

Opens key: HKLM\software\policies\microsoft\internet explorer\international\scripts

Opens key: HKCU\software\microsoft\internet explorer\international\scripts

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

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

Opens key: HKCU\software\microsoft\internet explorer\settings

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

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}

Opens key: HKCU\software\microsoft\internet explorer\styles

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

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

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

Opens key: HKCU\software\microsoft\internet explorer\menuext

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{56784854-c6cb-462b-8169-88e350acb882}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{56784854-c6cb-462b-8169-88e350acb882}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7b396e54-9ec5-4300-be0a-2482ebae1a26}

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7b396e54-9ec5-4300-be0a-2482ebae1a26}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bcbd3057-ca5c-4622-b42d-bc56db0ae516}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bcbd3057-ca5c-4622-b42d-bc56db0ae516}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a302545d-deff-464b-abe8-61c8648d939b}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a302545d-deff-464b-abe8-61c8648d939b}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2a00375e-224c-49de-b8d1-440df7ef3ddc}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2a00375e-224c-49de-b8d1-440df7ef3ddc}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{e555ab60-153b-4d17-9f04-a5fe99fc15ec}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{e555ab60-153b-4d17-9f04-a5fe99fc15ec}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b250c668-f57d-4ee1-a63c-290ee7d1aa1f}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b250c668-f57d-4ee1-a63c-290ee7d1aa1f}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52528a6b-b9e3-4add-b60d-588c2dba842d}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52528a6b-b9e3-4add-b60d-588c2dba842d}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8983036c-27c0-404b-8f08-102d10cdf74}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8983036c-27c0-404b-8f08-102d10cdf74}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bcb5256f-79f6-4cee-b725-dc34e402fd46}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bcb5256f-79f6-4cee-b725-dc34e402fd46}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{724ef170-a42d-4fef-9f26-b60e846fba4f}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{724ef170-a42d-4fef-9f26-b60e846fba4f}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4d9f7874-4e0c-4904-967b-40b0d20c3e4b}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4d9f7874-4e0c-4904-967b-40b0d20c3e4b}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a77f5d77-2e2b-44c3-a6a2-aba601054a51}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}  
Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d0384e7d-bac3-4797-8f14-cba229b392b5}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d0384e7d-bac3-4797-8f14-cba229b392b5}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7b0db17d-9cd2-4a93-9733-46cc89022e7c}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7b0db17d-9cd2-4a93-9733-46cc89022e7c}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b6ebfb86-6907-413c-9af7-4fc2abf07cc5}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b6ebfb86-6907-413c-9af7-4fc2abf07cc5}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9274bd8d-cfd1-41c3-b35e-b13f55a758f4}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9274bd8d-cfd1-41c3-b35e-b13f55a758f4}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{69d2cf90-fc33-4fb7-9a0c-ebb0f0fcb43c}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{69d2cf90-fc33-4fb7-9a0c-ebb0f0fcb43c}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}\propertybag  
Opens key: HKCU\software\microsoft\internet explorer\menuext\%s  
Opens key: HKLM\system\currentcontrolset\control\nls\codepage  
Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\travellog  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\travellog  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\version vector  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_sslux  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_sslux  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}  
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_browser\_emulation  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{dfdf76a2-c82a-4d63-906a-5644ac457385}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{dfdf76a2-c82a-4d63-906a-5644ac457385}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1a6fdb2a-f42d-4358-a798-b74d745926c5}

Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1a6fdb2-f42d-4358-a798-b74d745926c5}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b88f4daa-e7bd-49a9-b74d-02885a5dc765}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b88f4daa-e7bd-49a9-b74d-02885a5dc765}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2c36c0aa-5812-4b87-bfd0-4cd0dfb19b39}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2c36c0aa-5812-4b87-bfd0-4cd0dfb19b39}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9e3995ab-1f9c-4f13-b827-48b24b6c7174}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{df7266ac-9274-4867-8d55-3bd661de872d}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{df7266ac-9274-4867-8d55-3bd661de872d}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ed4824af-dce4-45a8-81e2-fc7965083634}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ed4824af-dce4-45a8-81e2-fc7965083634}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{15ca69b3-30ee-49c1-ace1-6b5ec372afb5}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{15ca69b3-30ee-49c1-ace1-6b5ec372afb5}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3214fab5-9757-4298-bb61-92a9deaa44ff}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3214fab5-9757-4298-bb61-92a9deaa44ff}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b97d20bb-f46a-4c97-ba10-5e3608430854}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b97d20bb-f46a-4c97-ba10-5e3608430854}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de92c1c7-837f-4f69-a3bb-86e631204a23}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de92c1c7-837f-4f69-a3bb-86e631204a23}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c1bae2d0-10df-4334-bedd-7aa20b227a9d}

Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_xssfilter  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_xssfilter  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c1bae2d0-10df-4334-bedd-7aa20b227a9d}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{190337d1-b8ca-4121-a639-6d472d16972a}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{190337d1-b8ca-4121-a639-6d472d16972a}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{54eed2e0-e7ca-4fdb-9148-0f4247291cfa}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{54eed2e0-e7ca-4fdb-9148-0f4247291cfa}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones  
Opens key: HKLM\software\policies\microsoft\internet explorer\low rights  
Opens key: HKCU\software\microsoft\internet explorer\low rights  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\low rights  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_read\_zone\_strings\_from\_registry  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_read\_zone\_strings\_from\_registry  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\1  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\2  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\3  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\4  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\ctf\compatibility\flashplayer18\_a\_install.exe  
Opens key: HKCU\software\classes\msxml2.domdocument.3.0  
Opens key: HKCR\msxml2.domdocument.3.0  
Opens key: HKCU\software\classes\msxml2.domdocument.3.0\clsid  
Opens key: HKCR\msxml2.domdocument.3.0\clsid  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-664e-48db-a079-df759e0509f7}  
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}  
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}  
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\treatas  
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\progid  
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\progid  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-664e-48db-a079-df759e0509f7}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}  
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}\propertybag  
Opens key: HKLM\software\wow6432node\microsoft\msxml30  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mshtml\_autoload\_ieframe  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mshtml\_autoload\_ieframe  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_compat\_logging

Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_enable\_compat\_logging  
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings\  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\  
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings\zonemap\  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
explorer\restrictions  
Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions  
Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}  
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\treatas  
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\progid  
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}\progid  
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}  
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}  
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\progid  
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaaf59cfc}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-  
f4ceaaaf59cfc}\inprochandler  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-  
aeb4-465c-a014-d097ee346d63}\propertybag  
Opens key: HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-  
00aa00389b71}\proxystubclsid32  
Opens key: HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-  
00aa00389b71}\proxystubclsid32  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-  
c14e-49b2-97c9-747784d784b7}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-  
c14e-49b2-97c9-747784d784b7}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-  
9efe-4bda-8fd7-f78dca774f87}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-  
9efe-4bda-8fd7-f78dca774f87}\propertybag  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-  
bb9d-43b0-b5b4-2d72e54eaaa4}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-  
bb9d-43b0-b5b4-2d72e54eaaa4}\propertybag  
Opens key: HKCU\software\classes\appid\flashplayer18\_a\_install.exe  
Opens key: HKCR\appid\flashplayer18\_a\_install.exe  
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat  
Opens key: HKLM\software\microsoft\ole\appcompat  
Opens key: HKLM\system\currentcontrolset\control\lsa  
Opens key:  
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic  
provider  
Opens key: HKLM\system\currentcontrolset\control\lsa\ipsalgorithmpolicy  
Opens key:  
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration  
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\{332c4425-26cb-11d0-b483-  
00c04fd90119}  
Opens key: HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119}  
Opens key: HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-  
00c04fd90119}\proxystubclsid32  
Opens key: HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-  
00c04fd90119}\proxystubclsid32  
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}  
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}  
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}\treatas  
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-

000000000046}\progid  
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\progid  
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}  
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}  
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-  
000000000046}\progid  
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-  
000000000046}\inprochandler  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_binary\_caller\_service\_provider  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_binary\_caller\_service\_provider  
Opens key: HKCU\software\policies\microsoft\internet explorer\control panel  
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings\url history  
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings\url history  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\url  
history  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\url history  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_iedde\_register\_urlecho  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_iedde\_register\_urlecho  
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}  
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}  
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}\treatas  
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}\progid  
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-  
00aa00bbb58}\inprochandler  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders  
Opens key:  
HKCU\software\microsoft\windows\currentversion\explorer\usersfiles\namespace  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders\{dffacd5-  
679f-4156-8947-c5c76bc0b67f}  
Opens key:  
HKCU\software\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders  
Opens key:  
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\usersfiles\namespace  
Opens key:  
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\usersfiles\namespace\delegatefolders  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacd5-679f-4156-8947-  
c5c76bc0b67f}\shellfolder  
Opens key: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-  
c5c76bc0b67f}\shellfolder  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{dffacd5-  
679f-4156-8947-c5c76bc0b67f}\shellfolder  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{dffacd5-679f-4156-  
8947-c5c76bc0b67f}\shellfolder  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacd5-679f-4156-8947-  
c5c76bc0b67f}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-  
c5c76bc0b67f}\inprocserver32  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\shdocvw.dll  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacd5-679f-4156-8947-  
c5c76bc0b67f}  
Opens key: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacd5-679f-4156-8947-  
c5c76bc0b67f}\treatas  
Opens key: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacd5-679f-4156-8947-  
c5c76bc0b67f}\progid  
Opens key: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\progid  
Opens key: HKCU\software\classes\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}  
Opens key: HKCR\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}  
Opens key: HKCU\software\classes\clsid\{dffacd5-679f-4156-8947-  
c5c76bc0b67f}\progid  
Opens key: HKCR\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacd5-679f-4156-8947-

c5c76bc0b67f}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-  
c5c76bc0b67f}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-  
c5c76bc0b67f}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-  
c5c76bc0b67f}\inprochandler  
Opens key: HKLM\software\wow6432node\microsoft\windows script\features  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_respect\_objectsafety\_policy\_kb905547  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_respect\_objectsafety\_policy\_kb905547  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activex  
compatibility  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activex  
compatibility\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}  
Opens key: HKLM\software\wow6432node\microsoft\com3  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-  
c5c76bc0b67f}\instance  
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance  
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}  
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}  
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\treatas  
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\progid  
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\progid  
Opens key: HKCU\software\classes\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}  
Opens key: HKCR\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}  
Opens key: HKCU\software\classes\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\progid  
Opens key: HKCR\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-  
c66de400274e}\inprochandler  
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-  
c5c76bc0b67f}\instance\initpropertybag  
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-  
c5c76bc0b67f}\instance\initpropertybag  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{dffacdc5-  
679f-4156-8947-c5c76bc0b67f}  
Opens key: HKCU\software\classes\exefile\shell  
Opens key: HKCR\exefile\shell  
Opens key: HKCU\software\microsoft\windows\currentversion\app\_paths\msmpeng.exe  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app  
paths\msmpeng.exe  
Opens key: HKLM\software\microsoft\windows\currentversion\app\_paths\msmpeng.exe  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\msmpeng.exe  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\msmpeng.exe  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_shim\_mshelp\_combine  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_shim\_mshelp\_combine  
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\system  
Opens key: HKLM\software\policies\microsoft\windows\system  
Opens key: HKLM\software\microsoft\internet explorer\registration  
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}  
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}  
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}\treatas  
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}\progid  
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-  
dc030521aabd}\inprochandler  
Opens key: HKLM\system\currentcontrolset\services\devicesync  
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist  
Opens key: HKU\default\control  
panel\desktop\muicached\machinelanguageconfiguration  
Opens key: HKU\default\software\policies\microsoft\control panel\desktop  
Opens key: HKU\default\control panel\desktop\languageconfiguration  
Opens key: HKU\default\control panel\desktop  
Opens key: HKU\default\control panel\desktop\muicached  
Opens key: HKU\default\control panel\international  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\3791cfa2



Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\svchost.exe  
Opens key: HKU\.\default\software\microsoft\windows\currentversion\explorer\shell  
folders  
Opens key: HKU\.\default\software\microsoft\windows  
nt\currentversion\appcompatflags\layers  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\svchost.exe  
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}  
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}  
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\treatas  
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\progid  
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid  
Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}  
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}  
Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\progid  
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-  
3c8b00c10000}\inprochandler  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_behaviors  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_behaviors  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\default behaviors  
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}  
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}  
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\treatas  
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\progid  
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid  
Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}  
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}  
Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\progid  
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-  
00c04fd9189d}\inprochandler  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\27daf4d1-1069d532  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\27daf4d1  
Opens key: HKLM\hardware\devicemap\video  
Opens key: HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-  
1e1a187c13e9}\0000  
Opens key: HKLM\system\currentcontrolset\enum\pci\ven\_80ee&dev\_beef&subsys\_00000000&rev\_00\_3&267a616a&0&10  
Opens key: HKCU\software\classes\directory\shellex\propertyhandler  
Opens key: HKCR\directory\shellex\propertyhandler  
Opens key: HKCU\software\classes\folder\shellex\propertyhandler  
Opens key: HKCR\folder\shellex\propertyhandler  
Opens key: HKCU\software\classes\allfilesystemobjects\shellex\propertyhandler  
Opens key: HKCR\allfilesystemobjects\shellex\propertyhandler  
Opens key: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-  
9dd4432fa2e9}\0000  
Opens key: HKCU\software\classes\wow6432node\clsid\{72eb61e0-8672-4303-9175-  
f2e4c68b2e7c}  
Opens key: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}  
Opens key: HKCU\software\classes\wow6432node\clsid\{72eb61e0-8672-4303-9175-  
f2e4c68b2e7c}\treatas  
Opens key: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{72eb61e0-8672-4303-9175-  
f2e4c68b2e7c}\progid  
Opens key: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\progid  
Opens key: HKCU\software\classes\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}  
Opens key: HKCR\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}  
Opens key: HKCU\software\classes\clsid\{72eb61e0-8672-4303-9175-  
f2e4c68b2e7c}\progid  
Opens key: HKCR\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\progid  
Opens key: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-  
0d8e74595f78}\0000  
Opens key: HKCU\software\classes\wow6432node\clsid\{72eb61e0-8672-4303-9175-  
f2e4c68b2e7c}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-  
f2e4c68b2e7c}\inprocserver32

Opens key: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-8ed0c8eb59a8}\0000

Opens key: HKCU\software\classes\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\inprochandler

Opens key: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\inprochandler

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug!

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\user

shell folders

Opens key: HKCU\software\classes\.dll

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98

Opens key: HKCR\.dll

Opens key: HKCU\software\classes\.dll\openwithprogids

Opens key: HKCR\.dll\openwithprogids

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dll\openwithprogids

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dll

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dll

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.dll\userchoice

Opens key: HKCU\software\classes\dllfile

Opens key: HKCR\dllfile

Opens key: HKCU\software\classes\dllfile\curver

Opens key: HKCR\dllfile\curver

Opens key: HKCR\dllfile\

Opens key: HKCU\software\classes\dllfile\shellex\iconhandler

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue

squadron

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage

Opens key: HKCR\dllfile\shellex\iconhandler

Opens key: HKCU\software\classes\systemfileassociations\.dll

Opens key: HKCR\systemfileassociations\.dll

Opens key: HKCU\software\classes\systemfileassociations\.dll\shellex\iconhandler

Opens key: HKCR\systemfileassociations\.dll\shellex\iconhandler

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder

Opens key: HKCU\software\classes\dllfile\docobject

Opens key: HKCR\dllfile\docobject

Opens key: HKCU\software\classes\systemfileassociations\.dll\docobject

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115

Opens key: HKCR\systemfileassociations\.dll\docobject

Opens key: HKCU\software\classes\dllfile\browseinplace

Opens key: HKCR\dllfile\browseinplace

Opens key: HKCU\software\classes\systemfileassociations\.dll\browseinplace

Opens key: HKCR\systemfileassociations\.dll\browseinplace

HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracedemo

Opens key: HKCU\software\classes\dllfile\clsid

Opens key: HKCR\dllfile\clsid

Opens key: HKCU\software\classes\systemfileassociations\.dll\clsid

Opens key: HKCR\systemfileassociations\.dll\clsid

HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark

Opens key: HKLM\software\wow6432node\microsoft\directdraw\gammacalibrator

Opens key: HKCU\software\classes\.txt

Opens key: HKCR\.txt

Opens key: HKCU\software\classes\.txt\openwithprogids

Opens key: HKCR\.txt\openwithprogids

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.txt\openwithprogids

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.txt

Opens key: HKLM\software\wow6432node\microsoft\direct3d

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.txt\

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.txt\userchoice

Opens key: HKCU\software\classes\txtfile

Opens key: HKCR\txtfile

Opens key: HKCU\software\classes\txtfile\curver

Opens key: HKCR\txtfile\curver

Opens key: HKCR\txtfile\

Opens key: HKCU\software\classes\txtfile\shellex\iconhandler

Opens key: HKCR\txtfile\shellex\iconhandler

Opens key: HKCU\software\classes\systemfileassociations\.txt

Opens key: HKCR\systemfileassociations\.txt

Opens key: HKCU\software\classes\systemfileassociations\.txt\shellex\iconhandler

Opens key: HKCR\systemfileassociations\.txt\shellex\iconhandler

Opens key: HKCU\software\classes\systemfileassociations\text

Opens key: HKCR\systemfileassociations\text  
Opens key: HKCU\software\classes\systemfileassociations\text\shellx\iconhandler  
Opens key: HKCR\systemfileassociations\text\shellx\iconhandler  
Opens key: HKCU\software\classes\txtfile\docobject  
Opens key: HKCR\txtfile\docobject  
Opens key: HKCU\software\classes\systemfileassociations\.txt\docobject  
Opens key: HKCR\systemfileassociations\.txt\docobject  
Opens key: HKCU\software\classes\systemfileassociations\text\docobject  
Opens key: HKCR\systemfileassociations\text\docobject  
Opens key: HKCU\software\classes\txtfile\browseinplace  
Opens key: HKCR\txtfile\browseinplace  
Opens key: HKCU\software\classes\systemfileassociations\.txt\browseinplace  
Opens key: HKCR\systemfileassociations\.txt\browseinplace  
Opens key: HKCU\software\classes\systemfileassociations\text\browseinplace  
Opens key: HKCR\systemfileassociations\text\browseinplace  
Opens key: HKCU\software\classes\txtfile\clsid  
Opens key: HKCR\txtfile\clsid  
Opens key: HKCU\software\classes\systemfileassociations\.txt\clsid  
Opens key: HKCR\systemfileassociations\.txt\clsid  
Opens key: HKCU\software\classes\systemfileassociations\text\clsid  
Opens key: HKCR\systemfileassociations\text\clsid  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\advanced  
Opens key: HKCU\software\classes\directory\shellx\copyhookhandlers  
Opens key: HKCR\directory\shellx\copyhookhandlers  
Opens key: HKCU\software\classes\directory\shellx\copyhookhandlers\filesystem  
Opens key: HKCR\directory\shellx\copyhookhandlers\filesystem  
Opens key: HKCU\software\classes\wow6432node\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32  
Opens key: HKCU\software\classes\directory\shellx\copyhookhandlers\sharing  
Opens key: HKCR\directory\shellx\copyhookhandlers\sharing  
Opens key: HKCU\software\classes\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\ntshrui.dll  
Opens key: HKCU\software\classes\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}  
Opens key: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}  
Opens key: HKCU\software\classes\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\treatas  
Opens key: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\progid  
Opens key: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\progid  
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}  
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}  
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}  
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas  
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid  
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandler  
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}  
Opens key: HKCU\software\classes\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}  
Opens key: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}  
Opens key: HKCU\software\classes\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\treatas  
Opens key: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\progid  
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler  
Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\progid  
Opens key: HKCU\software\classes\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}  
Opens key: HKCR\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}  
Opens key: HKCU\software\classes\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\progid  
Opens key: HKCR\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprocserver32  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\dxtrans

Opens key: HKLM\software\policies\microsoft\internet explorer\dxtrans  
Opens key: HKCU\software\microsoft\internet explorer\dxtrans  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\dxtrans  
Opens key: HKCU\software\classes\dximagetransform.microsoft.gradient  
Opens key: HKCR\dximagetransform.microsoft.gradient  
Opens key: HKCU\software\classes\dximagetransform.microsoft.gradient\clsid  
Opens key: HKCR\dximagetransform.microsoft.gradient\clsid  
Opens key: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}  
0000f8756a10}  
Opens key: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}  
Opens key: HKCU\software\classes\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprochandler  
Opens key: HKCU\software\classes\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\treatas  
Opens key: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\progid  
Opens key: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\progid  
Opens key: HKLM\system\currentcontrolset\services\lanmanserver\defaultsecurity  
Opens key: HKCU\software\classes\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}  
c7289fd10169}  
Opens key: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}  
Opens key: HKCU\software\classes\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\treatas  
c7289fd10169}\treatas  
Opens key: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\progid  
Opens key: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\progid  
Opens key: HKCU\software\classes\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}  
Opens key: HKCR\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}  
Opens key: HKCU\software\classes\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\progid  
Opens key: HKCR\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandler  
Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activexcompatibility\{623e2882-fc0e-11d1-9a77-0000f8756a10}  
Opens key: HKCU\software\classes\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprochandler  
Opens key: HKCU\software\classes\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprochandler  
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist  
Opens key: HKLM\system\currentcontrolset\control\computername  
Opens key: HKCU\software\classes\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}  
00c04fd9189d}  
Opens key: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}  
Opens key: HKCU\software\classes\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\treatas  
00c04fd9189d}\treatas  
Opens key: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\progid  
00c04fd9189d}\progid  
Opens key: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\progid  
Opens key: HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}  
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}  
Opens key: HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\progid  
00c04fd9189d}\progid  
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\progid  
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18  
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19  
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-20  
Opens key: HKCU\software\classes\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}  
54a6827f513c}  
Opens key: HKCU\software\classes\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32  
00c04fd9189d}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}  
Opens key: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\treatas  
54a6827f513c}\treatas  
Opens key: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\progid  
54a6827f513c}\progid  
Opens key: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\progid  
Opens key: HKCU\software\classes\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}  
Opens key: HKCR\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}

Opens key: HKCU\software\classes\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\progid

Opens key: HKCR\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandler

Opens key: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandler

Opens key: HKCU\software\classes\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}

Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}

Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas

Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid

Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}

Opens key: HKCU\software\classes\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprochandler

Opens key: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprochandler

Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}

Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid

Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\sharing

Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler

Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler

Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\propertyssystem\propertyhandlers\dl1

Opens key: HKCU\software\classes\wow6432node\clsid\{66742402-f9b9-11d1-a202-0000f81fedee}\overridefilesystemproperties

Opens key: HKCR\wow6432node\clsid\{66742402-f9b9-11d1-a202-0000f81fedee}\overridefilesystemproperties

Opens key: HKCU\software\classes\wow6432node\clsid\{66742402-f9b9-11d1-a202-0000f81fedee}

Opens key: HKCR\wow6432node\clsid\{66742402-f9b9-11d1-a202-0000f81fedee}

Opens key: HKCU\software\classes\explorer\clsid\flags\{66742402-f9b9-11d1-a202-0000f81fedee}

Opens key: HKCR\explorer\clsid\flags\{66742402-f9b9-11d1-a202-0000f81fedee}

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid

HKLM\software\wow6432node\microsoft\windows\currentversion\propertyssystem\propertyhandlers\exe

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\propertyssystem\propertyhandlers\txt

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler

Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler

Opens key: HKCU\software\classes\typelib

Opens key: HKCU\software\classes\txtfile\shellex\propertyhandler

Opens key: HKCR\typelib

Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}

Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1

Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409

Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9

Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9

Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0

Opens key: HKCR\txtfile\shellex\propertyhandler  
 Opens key: HKCU\software\classes\.txt\shellex\propertyhandler  
 Opens key: HKCR\.txt\shellex\propertyhandler  
 Opens key:  
 HKCU\software\classes\systemfileassociations\.txt\shellex\propertyhandler  
 Opens key: HKCR\systemfileassociations\.txt\shellex\propertyhandler  
 Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\O  
 Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-  
 00aa003b6061}\1.1\O\win32  
 Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\O\win32  
 Opens key:  
 HKCU\software\classes\systemfileassociations\text\shellex\propertyhandler  
 Opens key: HKCR\systemfileassociations\text\shellex\propertyhandler  
 Opens key: HKCU\software\classes\  
 Opens key: HKCR\  
 Opens key: HKCU\software\classes\\*\shellex\propertyhandler  
 Opens key: HKCR\\*\shellex\propertyhandler  
 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}  
 Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}  
 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0  
 Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0  
 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-  
 000000000046}\2.0\O  
 Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\O  
 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-  
 000000000046}\2.0\O\win32  
 Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\O\win32  
 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}  
 Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}  
 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1  
 Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1  
 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-  
 0000f87557db}\1.1\409  
 Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409  
 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-  
 0000f87557db}\1.1\9  
 Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9  
 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-  
 0000f87557db}\1.1\O  
 Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\O  
 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-  
 0000f87557db}\1.1\O\win32  
 Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\O\win32  
 Opens key: HKCU\software\microsoft\internet  
 explorer\main\featurecontrol\feature\_disable\_behaviors\_draw\_reentrancy  
 Opens key: HKLM\software\wow6432node\microsoft\internet  
 explorer\main\featurecontrol\feature\_disable\_behaviors\_draw\_reentrancy  
 Opens key: HKCU\software\microsoft\internet  
 explorer\main\featurecontrol\feature\_scripturl\_mitigation  
 Opens key: HKLM\software\wow6432node\microsoft\internet  
 explorer\main\featurecontrol\feature\_scripturl\_mitigation  
 Opens key: HKCU\software\microsoft\internet  
 explorer\main\featurecontrol\feature\_subdownload\_lockdown  
 Opens key: HKLM\software\wow6432node\microsoft\internet  
 explorer\main\featurecontrol\feature\_subdownload\_lockdown  
 Opens key: HKCU\software\microsoft\ftp  
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\services  
 Opens key: HKLM\software\policies\microsoft\internet explorer\services  
 Opens key: HKCU\software\microsoft\internet explorer\services  
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
 explorer\activities  
 Opens key: HKLM\software\policies\microsoft\internet explorer\activities  
 Opens key: HKCU\software\microsoft\internet explorer\activities  
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\activities  
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
 explorer\infodeliveryrestrictions  
 Opens key: HKLM\software\policies\microsoft\internet  
 explorer\infodeliveryrestrictions  
 Opens key: HKCU\software\policies\microsoft\internet  
 explorer\infodeliveryrestrictions  
 Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\suggested  
 sites  
 Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites  
 Opens key: HKCU\software\microsoft\internet explorer\suggested sites  
 Opens key: HKCU\software\classes\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}  
 Opens key: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}  
 Opens key: HKCU\software\classes\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\treatas  
 Opens key: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas  
 Opens key: HKCU\software\classes\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\progid  
 Opens key: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\progid  
 Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}  
 Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}  
 Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\progid  
 Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\progid  
 Opens key: HKCU\software\classes\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\inprocserver32  
 Opens key: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\inprocserver32  
 Opens key: HKCU\software\classes\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\inprochandler32  
 Opens key: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\inprochandler32  
 Opens key: HKCU\software\classes\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\inprochandler  
 Opens key: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-  
 00c04fd9189d}\inprochandler  
 Opens key: HKCU\software\microsoft\windows nt\currentversion  
 Opens key: HKU.\default\software\microsoft\windows nt\currentversion

Opens key: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\appcompatflags  
Opens key: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\appcompatflags\custom\svchost.exe  
Opens key: HKLM\system\currentcontrolset\services\dnsclient\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\system\currentcontrolset\control\session manager\environment  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\27daf4d1-2e01084b  
Opens key: HKU\  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-1001  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\explorer\user shell folders  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\environment  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\volatile environment  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\volatile environment\0  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\dlldllhost.exe  
Opens key: HKLM\system\currentcontrolset\control\session manager\quota system\s-1-  
5-21-980053277-1733835069-2361817685-1001  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\policies\microsoft\windows\safer\codeidentifiers  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows nt\currentversion  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows nt\currentversion\appcompatflags\layers  
Opens key: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\appcompatflags\custom\dlldllhost.exe  
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\{22873b3e-c4d3-495a-8165-  
e1e01c1f69b5}  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-  
e1e01c1f69b5}  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_activex\_inactivate\_mode\_removal\_revert  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_activex\_inactivate\_mode\_removal\_revert  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_cross\_domain\_redirect\_mitigation  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_cross\_domain\_redirect\_mitigation  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_block\_lmz\_script  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_block\_lmz\_script  
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user  
agent  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\user agent  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\user agent  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\user agent  
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings\user agent  
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings\user agent  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\user agent\ua tokens  
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-  
806e6f6e6963}  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-  
806e6f6e6963}  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\user agent\pre platform  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\user agent\pre platform  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\user agent\pre platform  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\user agent\post platform  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\user agent\post platform  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\user agent\post platform  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-  
127795cce47a}  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-  
65fee5bae0b1}  
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\0d2ab2aa-00c20a66  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\0d2ab2aa  
Opens key: HKCU\software\classes\http\shell\open\command  
Opens key: HKCR\http\shell\open\command  
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters  
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters  
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\winhttp\tracing  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\winhttp  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\policies\microsoft\windows\currentversion\internet settings  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\software\policies  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\software  
Opens key: HKU\software\microsoft\windows\currentversion\internet  
settings\connections  
Opens key: HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli  
Opens key: HKLM\system\currentcontrolset\control\securityproviders  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\policies\microsoft\internet explorer\main\featurecontrol  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet explorer\main\featurecontrol  
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache  
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\content  
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles  
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\connections  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\explorer  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\explorer\sessioninfo\0  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip6  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\control  
panel\international  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\policies\microsoft\windows\explorer  
Opens key: HKLM\software\wow6432node\policies\microsoft\windows  
nt\dnsc\client\dnspolicyconfig  
Opens key: HKLM\software\policies\microsoft\windows nt\dnsc\client\dnspolicyconfig  
Opens key: HKLM\software\policies\microsoft\windows nt\dnsc\client\dnspolicyconfig  
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig  
Opens key: HKU\software\opera software  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies  
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\history  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\domstore  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\feedplat  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\iecompat  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\privacie:  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet explorer\main\featurecontrol\feature\_bufferbreaking\_818408  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\policies\microsoft\windows\currentversion\internet settings\5.0\cache  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_fix\_chunked\_proxy\_script\_download\_kb843289  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet explorer\main\featurecontrol\feature\_use\_cname\_for\_spn\_kb911149  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_notify\_unverified\_spn\_kb2385266  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_compat\_use\_connection\_based\_negotiate\_auth\_kb2151543  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_allow\_long\_international\_filenames  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_permit\_cache\_for\_authenticated\_ftp\_kb910274  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disallow\_null\_in\_response\_headers  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet explorer\main\featurecontrol\feature\_digest\_no\_extras\_in\_uri  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet



explorer\main\featurecontrol\feature\_exclude\_invalid\_client\_cert\_kb929477  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_utf8\_for\_basic\_auth\_kb967545  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_release\_keys\_on\_unload\_kb975619  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_security\_flag\_ignore\_revocation\_kb2275828  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet\_settings\wpad  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_return\_failed\_connect\_content\_kb942615  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable  
Opens key: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\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: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet explorer\main\featurecontrol\feature\_mime\_handling  
Opens key: HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32  
Opens key: HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs  
Opens key: HKLM\system\currentcontrolset\control\cryptography\providers  
Opens key: HKLM\system\currentcontrolset\control\cryptography\configuration  
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\cryptdlldecodeobjectex  
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1  
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 1  
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\cryptography\oid\encodingtype  
0\cryptdllfindoidinfo  
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype  
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7  
Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings  
Opens key: HKCU\software\classes\local\_settings\muicache\16\52c64b7e  
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\software\wow6432node\microsoft\cryptography\oid\encodingtype  
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7  
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype  
0\certdllcreatecertificatechainengine\config  
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\chainengine\config  
Opens key: HKLM\software\policies\microsoft\systemcertificates\chainengine\config  
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\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\ctl  
Opens key: HKCU\software\microsoft\systemcertificates\my\keys  
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\d559a58669b08f46a30a133f8a9ed3d038e2ea8  
Opens key:  
HKLM\software\microsoft\systemcertificates\ca\certificates\fee449ee0e3965a5246f000e87fde2a065fd89d4  
Opens key:  
HKLM\software\microsoft\systemcertificates\ca\crls\va377d1b1c0538833035211f4083d00fecc414dab  
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:

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: 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\certificates\637162cc59a3a1e25956fa5fa8f60d2e1c52eac6  
Opens key:  
HKLM\software\microsoft\systemcertificates\disallowed\certificates\7d7f4414ccef168adf6bf40753b5becd78375931  
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\7f88cd7223f3c813818c994614a89c99fa3b5247  
Opens key:  
HKLM\software\microsoft\systemcertificates\root\certificates\aa43489159a520f0d93d032ccaf37e7fe20a8b419  
Opens key:  
HKLM\software\microsoft\systemcertificates\root\certificates\be36a4562fb2ee05dbb3d3232adfa445084ed656  
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\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: 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\winlogon  
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\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: 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: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft enhanced rsa and aes cryptographic provider  
Opens key: HKLM\software\wow6432node\microsoft\cryptography\desahashsessionkeybackward  
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  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}  
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-  
00aa00bdce0b}\treatas  
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-  
00aa00bdce0b}\progid  
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-  
00aa00bdce0b}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-  
00aa00bdce0b}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-  
00aa00bdce0b}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-  
00aa00bdce0b}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-  
00aa00bdce0b}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-  
00aa00bdce0b}\inprochandler  
Opens key: HKCU\software\policies\microsoft\internet explorer\persistance  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet  
explorer\persistance  
Opens key: HKLM\software\policies\microsoft\internet explorer\persistance  
Opens key: HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}  
Opens key: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}  
Opens key: HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0  
Opens key: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0  
Opens key: HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-  
00c04fb6bfc4}\1.0\0  
Opens key: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0  
Opens key: HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-  
00c04fb6bfc4}\1.0\0\win32  
Opens key: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32  
Opens key: HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32  
Opens key: HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasmancs  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_ietldlist\_for\_domain\_determination  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_ietldlist\_for\_domain\_determination  
Opens key: HKCU\software\microsoft\internet explorer\ietld  
Opens key: HKCU\software\classes\protocols\name-space handler  
Opens key: HKCU\software\classes\protocols\name-space handler\http\  
Opens key: HKCR\protocols\name-space handler\http  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_maxconnectionsperserver  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_maxconnectionsperserver  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_maxconnectionsper1\_0server  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_maxconnectionsper1\_0server  
Opens key: HKCU\software\microsoft\windows\currentversion\urlmon settings  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_include\_port\_in\_spn\_kb908209  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_legacy\_compression  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_legacy\_compression  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_block\_lmz\_img  
Opens key: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_block\_lmz\_img  
Opens key: HKLM\software\wow6432node\macromedia\flashplayerplugin  
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\recovery  
Opens key: HKLM\software\policies\microsoft\internet explorer\recovery  
Opens key: HKCU\software\microsoft\internet explorer\recovery  
Opens key: HKCU\software\classes\protocols\name-space handler\file\  
Opens key: HKCR\protocols\name-space handler\file  
Opens key: HKCU\software\classes\.png  
Opens key: HKCR\.png  
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}  
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}  
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}\treatas  
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}\progid  
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-  
00aa006c1a01}\inprochandler  
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-  
00aa006c1a01}  
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}  
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-  
00aa006c1a01}\treatas  
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-  
00aa006c1a01}\progid

Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler  
Opens key: HKCU\software\classes\mime\database\content type  
Opens key: HKCR\mime\database\content type  
Opens key: HKCU\software\classes\mime\database\content type\image\bmp\bits  
Opens key: HKCR\mime\database\content type\image\bmp\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/gif\bits  
Opens key: HKCR\mime\database\content type\image/gif\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/jpeg\bits  
Opens key: HKCR\mime\database\content type\image/jpeg\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/pjpeg\bits  
Opens key: HKCR\mime\database\content type\image/pjpeg\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/png\bits  
Opens key: HKCR\mime\database\content type\image/png\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/tiff\bits  
Opens key: HKCR\mime\database\content type\image/tiff\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/x-icon\bits  
Opens key: HKCR\mime\database\content type\image/x-icon\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/x-jg\bits  
Opens key: HKCR\mime\database\content type\image/x-jg\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/x-png\bits  
Opens key: HKCR\mime\database\content type\image/x-png\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/x-wmf\bits  
Opens key: HKCR\mime\database\content type\image/x-wmf\bits  
Opens key: HKCU\software\classes\mime\database\content type\image/x-png  
Opens key: HKCR\mime\database\content type\image/x-png  
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}  
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}  
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas  
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas  
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid  
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid  
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32  
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32  
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32  
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32  
Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler  
Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler  
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype  
0\cryptdllverifyencodesignature  
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype  
1\cryptdllverifyencodesignature  
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype  
0\cryptdllimportpublickeyinfoex2  
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype  
1\cryptdllimportpublickeyinfoex2  
Opens key: HKCU\software\microsoft\windows\currentversion\internet  
settings\p3p\history\adobe.com  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options[disableusermodecallbackfilter]  
Queries value: HKLM\system\currentcontrolset\control\session  
manager[cwdillegalindllsearch]  
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]  
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
Queries value: HKLM\system\currentcontrolset\control\locale\customlocale[empty]  
Queries value:  
HKLM\system\currentcontrolset\control\locale\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\locale\sorting\versions[]  
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\gre\_initialize[disablemetafiles]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\compatibility32[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f046cedf5e99d63]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]  
Queries value: HKLM\system\currentcontrolset\control\locale\customlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\locale\extendedlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\locale\locale[00000409]  
Queries value: HKLM\system\currentcontrolset\control\locale\language groups[1]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\datastore\_v1.0[disable]

Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\datastore\_v1.0[datafilepath]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane1]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane2]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane3]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane4]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane5]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane6]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane7]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane8]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane9]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane10]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane11]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane12]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane13]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane14]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane15]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane16]  
Queries value: HKLM\system\currentcontrolset\control\cmf\config\system]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\windows[scrollinterval]  
Queries value: HKCU\control panel\desktop[smoothscroll]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe  
ui]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\fontsubstitutes[tahoma]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-  
c1bf-494e-b29c-65b732d3d21a}[precreate]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[attributes]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[callforattributes]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[restrictedattributes]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsfordisplay]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hidefolderverbs]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[usedrophandler]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsforparsing]

Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsparsedisplayname]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforoverlay]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[mapnetdriveverbs]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforinfotip]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideinwebview]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideondesktopperuser]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsaliasednotifications]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsuniversaldelegate]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[nofilefolderjunction]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[pintonamespacetree]  
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hasnavigationenum]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-08002b30309d}]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}[data]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}[generation]  
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable]  
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]  
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]  
Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]  
Queries value: HKLM\system\setup[oobeinprogress]  
Queries value: HKLM\system\setup\systemsetupinprogress  
Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask]  
Queries value: HKLM\software\microsoft\com3[com+enabled]  
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]  
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]  
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[inprocserver32]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}[data]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}[generation]  
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\microsoft\ole[maxsxsshcount]  
Queries value: HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]  
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]  
Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]  
Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnamealiases]  
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]  
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[maximizeapps]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[enableshellexecutehooks]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]



Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[icononly]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]  
Queries value: HKCR\.exe[]  
Queries value: HKCR\exefile[docobject]  
Queries value: HKCR\systemfileassociations\.exe[docobject]  
Queries value: HKCR\exefile[browseinplace]  
Queries value: HKCR\systemfileassociations\.exe[browseinplace]  
Queries value: HKCR\.exe[content type]  
Queries value: HKCR\exefile[isshortcut]  
Queries value: HKCR\systemfileassociations\.exe[isshortcut]  
Queries value: HKCR\exefile[alwaysshowext]  
Queries value: HKCR\systemfileassociations\.exe[alwaysshowext]  
Queries value: HKCR\exefile[nevershowext]  
Queries value: HKCR\systemfileassociations\.exe[nevershowext]  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[initfolderhandler]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[desktop]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]  
Queries value:

[illegible]

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:  
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-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]  
Queries value: HKCR\directory[docobject]  
Queries value: HKCR\folder[docobject]  
Queries value: HKCR\allfilesystemobjects[docobject]  
Queries value: HKCR\directory[browseinplace]  
Queries value: HKCR\folder[browseinplace]  
Queries value: HKCR\allfilesystemobjects[browseinplace]  
Queries value: HKCR\directory[isshortcut]  
Queries value: HKCR\folder[isshortcut]  
Queries value: HKCR\allfilesystemobjects[isshortcut]  
Queries value: HKCR\directory[alwaysshowext]  
Queries value: HKCR\directory[nevershowext]  
Queries value: HKCR\folder[nevershowext]  
Queries value: HKCR\allfilesystemobjects[nevershowext]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.exe]  
Queries value: HKCR\exefile\shell\open\command[delegateexecute]  
Queries value: HKCR\ .asp[]  
Queries value: HKCR\ .bas[]  
Queries value: HKCR\ .bat[]  
Queries value: HKCR\ .cer[]  
Queries value: HKCR\ .chm[]  
Queries value: HKCR\ .cmd[]  
Queries value: HKCR\ .com[]  
Queries value: HKCR\ .cp1[]  
Queries value: HKCR\ .crt[]  
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]  
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel]  
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings[security\_hklm\_only]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_unc\_savedfilecheck[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_unc\_savedfilecheck[\*]  
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: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable[\*]  
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[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.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[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings[specialfolderscachesize]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[specialfolderscachesize]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[specialfolderscachesize]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[specialfolderscachesize]  
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: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[cache]  
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}[streamresourcectype]  
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\internet  
explorer\main\featurecontrol\feature\_protocol\_lockdown[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_protocol\_lockdown[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\0[1806]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0[1806]  
Queries value: HKCR\exefile\shell\open\command[command]  
Queries value: HKCR\exefile\shell\open\command[]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[restrictrun]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[disallowrun]  
Queries value: HKCR\exefile\shell\open[setworkingdirectoryfromtarget]  
Queries value: HKCR\exefile\shell\open[noworkingdirectory]  
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\microsoft\windows  
nt\currentversion\appcompatflags[{6c3dff7f-feff-4e9b-9eb1-252651df86d4}]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\appcompatflags[{6c3dff7f-feff-4e9b-9eb1-252651df86d4}]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options[disablelocaloverride]

Queries value:  
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]  
Queries value: HKLM\software\microsoft\windows\currentversion\app  
paths\install.exe[appendpath]  
Queries value: HKLM\software\microsoft\windows\currentversion\app  
paths\install.exe[path]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\compatibility32[flashplayer18\_a\_install]  
Queries value: HKLM\system\currentcontrolset\control\filesystem[win31filesystem]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags[{d472e9bd-0225-4926-a79c-51ce1da8d7a5}]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\appcompatflags[{d472e9bd-0225-4926-a79c-51ce1da8d7a5}]  
Queries value: HKLM\system\currentcontrolset\control\locale[en]  
Queries value: HKLM\system\currentcontrolset\control\locale[en]  
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}[parsiname]  
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: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]  
Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]  
Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-  
00c04fd705a2}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-  
00c04fd705a2}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-  
00c04fd705a2}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_http\_username\_password\_disable[flashplayer18\_a\_install.exe]  
Queries value: HKCU\software\microsoft\internet explorer\main[frametabwindow]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[frametabwindow]  
Queries value: HKCU\software\microsoft\internet explorer\main[framemerging]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[framemerging]  
Queries value: HKCU\software\microsoft\internet explorer\main[sessionmerging]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[sessionmerging]  
Queries value: HKCU\software\microsoft\internet explorer\main[admintabprocs]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[admintabprocs]  
Queries value: HKCU\software\microsoft\internet explorer\main[tabprocgrowth]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[tabprocgrowth]  
Queries value: HKLM\software\wow6432node\microsoft\internet

```
explorer\main[navigationdelay]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[callforattributes]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[restrictedattributes]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsfordisplay]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hidefolderverbs]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[usedrophandler]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsforparsing]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsparsedisplayname]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[queryforoverlay]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[mapnetdriveverbs]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[queryforinfotip]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hideinwebview]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hideondesktopperuser]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsaliasednotifications]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsuniversaldelegate]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[nofilefolderjunction]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[globalassocchangedcounter]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[pintonamespacetree]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hasnavigationenum]
  Queries value: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
  Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-08002b30309d}]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[loadwithoutcom]
  Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046} 0xffff]
  Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[threadingmodel]
  Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[install]
  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[disablekeepalive]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablepassport]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[idnenabled]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cachemode]
  Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1]
  Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablenegotiate]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablebasiccoverclearchannel]
  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: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui]
  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: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache[signature]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\content[peruseritem]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\cache\content[peruseritem]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\content[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\content[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\cookies[peruseritem]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\cache\cookies[peruseritem]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\cookies[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\cookies[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\history[peruseritem]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\cache\history[peruseritem]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab]  
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}[streamresourcecetype]  
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: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[ ]  
Queries value: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-  
00c04fd7d062}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-  
00c04fd7d062}\inprocserver32[ ]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[history]  
Queries value: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-



00c04fd7d062}\inprocserver32[threadingmodel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\history[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\history[cachelimit]  
Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\domstore[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\domstore[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\domstore[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\domstore[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\domstore[cacheoptions]  
Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprocserver32[]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\feedplat[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\feedplat[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\feedplat[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\feedplat[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\feedplat[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\iecompat[cacherepair]  
Queries value: HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-  
00aa005b4383}\inprocserver32[threadingmodel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\iecompat[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\iecompat[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\iecompat[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\iecompat[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\ietld[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\ietld[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\ietld[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\ietld[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\ietld[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cacheprefix]  
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cacheoptions]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[enableautopxyresultcache]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[displayscriptdownloadfailureui]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[mcscsservername]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[mbscapiforcrack]  
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-  
00c04fd7d062}\inprocserver32[threadingmodel]  
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: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]  
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: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]  
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: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]  
Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[]  
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: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\inprocserver32[threadingmodel]  
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: HKLM\software\microsoft\rpc\extensions[ndroleextdll]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[httpdefaultexpirytimesecs]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[ftpdefaultexpirytimesecs]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback[flashplayer18\_a\_install.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[disablecachingofsslpages]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[perusercookies]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[leashlegacycookies]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[dialupuselansettings]  
Queries value: HKLM\software\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[bypasshttpproxycheck]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[bypasshttpproxycheck]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[bypasssslproxycheck]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[bypasssslproxycheck]  
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]

[illegible]

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\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[requiredfile]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[version]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[contextmenu]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[corelinternetenum]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[oldcreateviewwnd]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[win95defview]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[docobject]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[flushnowaitalways]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[mycomputerfirst]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[oldregitemgdn]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[loadcolumnhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[ansi]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[staroffice5printer]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[novalidatefsids]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[win95shlexec]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[win95bindtoobject]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[ignoreenumreset]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[ansidisplaynames]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[fileopenbogusctrlid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[forcelfnidlist]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[returnallattrs]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[nodefviewmsgpump]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[stripfolderbit]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[returnnonurlsasurls]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[notheadusechecks]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[forcelibraryparse]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[staticjumplistsize]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[appisoffice]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[ignoredefaulttoken]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[coinitalize\_compareids]  
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\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\install.exe\starcraft

1.03[requiredfile]  
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[storiesserviceclassinfo]  
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: HKCU\software\microsoft\windows\currentversion\internet  
settings\wpad[wpadoverride]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[enableautodial]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[nonetautodial]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[globaluseroffline]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[badproxyexpiretime]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings[disablebranchcache]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]  
Queries value: HKCR\protocols\handler\res[clsid]  
Queries value: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[]  
Queries value: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{3050f3bc-98b5-11cf-bb82-  
00aa00bdce0b}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_legacy\_dispparams[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_legacy\_dispparams[\*]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_object\_caching[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_object\_caching[\*]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-  
4901-4acc-8648-d5d44b04ef8f}[attributes]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-  
91a2-7b624e0e7244]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[initfolderhandler]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[attributes]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\application compatibility[flashplayer18\_a\_install.exe]  
Queries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[callforattributes]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[restrictedattributes]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsfordisplay]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hidefolderverbs]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[usedrophandler]  
Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsforparsing]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsparsedisplayname]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[queryforoverlay]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[mapnetdriveverbs]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[queryforinfotip]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hideinwebview]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hideondesktopperuser]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsaliasednotifications]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsuniversaldelegate]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[nofilefolderjunction]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[pintonamespacetree]  
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hasnavigationenum]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-5595fe6b30ee}]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[urlencoding]  
Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}[]  
Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_unc\_savedfilecheck[flashplayer18\_a\_install.exe]  
Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[threadingmodel]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[roamable]

[illegible]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[localizedname]  
Queries value: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_localmachine\_lockdown[flashplayer18\_a\_install.exe]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[attributes]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_localmachine\_lockdown[flashplayer18\_a\_install.exe]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[parsiname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}[initfolderhandler]



[illegible]

[illegible]

[illegible]

[illegible]

Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{18989b1d-99b5-455b-841c-ab7c74e4ddfc}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{18989b1d-99b5-455b-841c-ab7c74e4ddfc}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{18989b1d-99b5-455b-841c-ab7c74e4ddfc}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{18989b1d-99b5-455b-841c-ab7c74e4ddfc}[initfolderhandler]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[my video]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[security]  
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-

[illegible]

[illegible]

[illegible]



4e1e-4676-835a-98395c3bc3bb}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[initfolderhandler]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[my pictures]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[parsingsname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[publishexpandedpath]  
Queries value: HKCU\software\microsoft\internet explorer[no3dborder]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer[no3dborder]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings[urlencoding]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[urlencoding]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[name]

Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[description]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[\*]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[streamresourcecetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[parsingname]  
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_res\_to\_lmz[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_res\_to\_lmz[\*]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[streamresourcecetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[localredirectonly]

Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[stream]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_sniffing[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_sniffing[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\istextplainhonored]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_feeds[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_feeds[\*]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}[initfolderhandler]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\proxyenable]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_safe\_bindtoobject[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_safe\_bindtoobject[\*]  
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]  
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]  
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[threadingmodel]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\windows[dragscrollinset]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\windows[dragscrollldelay]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\windows[dragscrollinterval]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[parentfolder]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_filedownload[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_restrict\_filedownload[\*]  
Queries value: HKCR\protocols\handler\about[clsid]  
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[]  
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_protocol\_lockdown[flashplayer18\_a\_install.exe]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\3[2106]  
Queries value: HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}[streamresource]  
Queries value:

[illegible]

[illegible]

[illegible]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}[initfolderhandler]  
Queries value: HKLM\software\policies\microsoft\internet explorer[smartdithering]  
Queries value: HKCU\software\microsoft\internet explorer[smartdithering]  
Queries value: HKCU\software\microsoft\internet explorer[rtfconverterflags]  
Queries value: HKCU\software\microsoft\internet explorer\main[usecleartype]  
Queries value: HKCU\software\microsoft\internet explorer\main[page\_transitions]  
Queries value: HKCU\software\microsoft\internet explorer\main[use\_dlgbox\_colors]  
Queries value: HKCU\software\microsoft\internet explorer\main[anchor\_underline]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[relativepath]

Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[security]  
Queries value: HKCU\software\microsoft\internet explorer\main[css\_compat]  
Queries value: HKCU\software\microsoft\internet explorer\main[expand alt text]  
Queries value: HKCU\software\microsoft\internet explorer\main[display inline images]  
Queries value: HKCU\software\microsoft\internet explorer\main[display inline videos]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[display inline videos]  
Queries value: HKCU\software\microsoft\internet explorer\main[play\_background\_sounds]  
Queries value: HKCU\software\microsoft\internet explorer\main[play\_animations]  
Queries value: HKCU\software\microsoft\internet explorer\main[print\_background]  
Queries value: HKCU\software\microsoft\internet explorer\main[use\_stylesheets]  
Queries value: HKCU\software\microsoft\internet explorer\main[smoothscroll]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}[initfolderhandler]  
Queries value: HKCU\software\microsoft\internet explorer\main[xmlhttp]  
Queries value: HKCU\software\microsoft\internet explorer\main[show image placeholders]  
Queries value: HKCU\software\microsoft\internet explorer\main[disable script debugger]  
Queries value: HKCU\software\microsoft\internet explorer\main[disablescripdebuggerie]  
Queries value: HKCU\software\microsoft\internet explorer\main[move system caret]  
Queries value: HKCU\software\microsoft\internet explorer\main[force offscreen composition]  
Queries value: HKCU\software\microsoft\internet explorer\main[enable autoimagesize]  
Queries value: HKCU\software\microsoft\internet explorer\main[usethemes]  
Queries value: HKCU\software\microsoft\internet explorer\main[usehr]  
Queries value: HKCU\software\microsoft\internet explorer\main[q300829]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[infotip]  
Queries value: HKCU\software\microsoft\internet explorer\main[cleanup htcs]  
Queries value: HKCU\software\microsoft\internet explorer\main[xdomainrequest]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main[xdomainrequest]  
Queries value: HKCU\software\microsoft\internet explorer\main[domstorage]  
Queries value: HKCU\software\microsoft\internet explorer\international[default\_codepage]  
Queries value: HKCU\software\microsoft\internet explorer\international[autodetect]  
Queries value: HKCU\software\microsoft\internet explorer\international\scripts[default\_iefontsizeprivate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[localizedname]  
Queries value:



HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[publishexpandedpath]  
Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color]  
Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color visited]  
Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color hover]  
Queries value: HKCU\software\microsoft\internet explorer\settings[always use my colors]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[description]  
Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font size]  
Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font face]  
Queries value: HKCU\software\microsoft\internet explorer\settings[disable visited hyperlinks]  
Queries value: HKCU\software\microsoft\internet explorer\settings[use anchor hover color]  
Queries value: HKCU\software\microsoft\internet explorer\settings[miscflags]  
Queries value: HKCU\software\microsoft\windows\currentversion\policies[allow programmatic cut\_copy\_paste]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[roamable]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]  
Queries value: HKCU\software\microsoft\internet explorer\pagesetup[print\_background]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-

[illegible]

[illegible]

[illegible]

[illegible]

```

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}[initfolderhandler]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[parsiname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{177ff761-68ad-4d8a-87bd-30b759fa33dd}[initfolderhandler]
    Queries value:
        HKCU\software\microsoft\windows\currentversion\explorer\user_shell_folders[favorites]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b250c668-f57d-4ee1-a63c-290ee7d1aa1f}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b250c668-f57d-4ee1-a63c-290ee7d1aa1f}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b250c668-f57d-4ee1-a63c-290ee7d1aa1f}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b250c668-f57d-4ee1-a63c-290ee7d1aa1f}[description]
    Queries value:

```

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]

fc33-4fb7-9a0c-ebb0f0fcb43c}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{69d2cf90-fc33-4fb7-9a0c-ebb0f0fcb43c}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{69d2cf90-fc33-4fb7-9a0c-ebb0f0fcb43c}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}[initfolderhandler]  
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]  
Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefontsize]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{374de290-123f-4565-9164-39c4925e467b}]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[parsingname]  
Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefontsizeprivate]  
Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iepropfontname]  
Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefixedfontname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[localizedname]

Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}[initfolderhandler]  
Queries value: HKCU\software\microsoft\internet explorer\international[acceptlanguage]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version  
vector[vm1]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version vector[ie]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\version  
vector[windowsedition]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[icon]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_zone\_elevation[\*]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-

f527-492b-8b1a-7e76fa98d6e4}[foldertypeid]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_sslux[flashplayer18\_a\_install.exe]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[parsiname]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_sslux[\*]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_browser\_emulation[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_browser\_emulation[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\0[2700]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[stream]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0[2700]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}[parsiname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```
e9f1-4567-b850-448b77cb37f9}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}[initfolderhandler]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[initfolderhandler]
    Queries value:
        HKCU\software\microsoft\windows\currentversion\explorer\user_shell
folders[personal]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c1bae2d0-10df-4334-bedd-7aa20b227a9d}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c1bae2d0-10df-4334-bedd-7aa20b227a9d}[name]
```

[illegible]



[illegible]

c6a9-404c-b2b2-ae6db6af4968}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}[initfolderhandler]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[category]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones[securitysafe]  
Queries value: HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\low  
rights[protectedmodeoffforallzones]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[roamable]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\0[icon]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0[minlevel]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0[recommendedlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\0[currentlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\1[icon]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\1[minlevel]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\1[recommendedlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\1[currentlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\1[2500]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zones\1[2500]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\2[icon]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\2[minlevel]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[category]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\2[recommendedlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\2[currentlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\2[2500]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\2[2500]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\3[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[parsiname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[streamresource]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\3[minlevel]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\3[recommendedlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\3[currentlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\3[2500]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\3[2500]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-

57ac-4347-9151-b08c6c32d1f7}[initfolderhandler]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\4[icon]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\4[minlevel]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\4[recommendedlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\4[currentlevel]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\4[2500]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\4[2500]  
Queries value: HKCR\msxml2.domdocument.3.0\clsid[]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[attributes]  
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\progid[]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-  
664e-48db-a079-df759e0509f7}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-  
e4eb-479d-b89f-130c02886155}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-  
e4eb-479d-b89f-130c02886155}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-  
e4eb-479d-b89f-130c02886155}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-  
e4eb-479d-b89f-130c02886155}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-  
e4eb-479d-b89f-130c02886155}[relativepath]  
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}[]  
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-  
0000f81fe221}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-  
0000f81fe221}\inprocserver32[]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-  
e4eb-479d-b89f-130c02886155}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-  
e4eb-479d-b89f-130c02886155}[infotip]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[precreate]  
Queries value: HKCR\wow6432node\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32[threadingmodel]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[icon]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mshtml\_autoload\_iframe[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_mshtml\_autoload\_iframe[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\0[2106]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0[2106]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[localredirectonly]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\0[1400]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[publishexpandedpath]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[foldertypeid]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings[warnonintranet]  
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet  
settings[warnonintranet]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[warnonintranet]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zonemap[autodetect]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}[initfolderhandler]  
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\[]  
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaf59cfc}\inprocserver32[threadingmodel]  
Queries value: HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[parsingname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}[initfolderhandler]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-9efe-4bda-8fd7-f78dca774f87}[category]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-9efe-4bda-8fd7-f78dca774f87}[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-9efe-4bda-8fd7-f78dca774f87}[parentfolder]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-9efe-4bda-8fd7-f78dca774f87}[description]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-9efe-4bda-8fd7-f78dca774f87}[relativepath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-

[illegible]

```
bb9d-43b0-b5b4-2d72e54eaaa4}[initfolderhandler]
  Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user_shell
folders[{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}]
  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\system\currentcontrolset\control\lsa\fpisalgorithmpolicy[enabled]
  Queries value: HKLM\system\currentcontrolset\control\lsa\fpisalgorithmpolicy]
  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: HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[d0fe44be]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value: HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-
00c04fd90119}\proxystubclsid32[]
  Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}[]
  Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[url_history[daystokeep]
  Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\progid[]
  Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}[]
  Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbb58}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbb58}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbb58}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders[suppressionpolicy]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders[]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders\{dffacdc5-
679f-4156-8947-c5c76bc0b67f}[suppressionpolicy]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[attributes]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[callforattributes]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[restrictedattributes]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[wantsfordisplay]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[hidefolderverbs]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[usedrophandler]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[wantsforparsing]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[wantsparsedisplayname]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[queryforoverlay]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[mapnetdriveverbs]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[queryforinfotip]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[hideinwebview]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[hideondesktopperuser]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[wantsaliasednotifications]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[wantsuniversaldelegate]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[nofilefolderjunction]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[pintonamespacetree]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\shellfolder[hasnavigationenum]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{dffacdc5-679f-4156-8947-
c5c76bc0b67f}]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\inprocserver32[loadwithoutcom]
  Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{dffacdc5-679f-4156-8947-c5c76bc0b67f} {add8ba80-002b-11d0-8f0f-00c04fd7d062}
0xfffff]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}[]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\inprocserver32[inprocserver32]
```



Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\inprocserver32[threadingmodel]

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

settings\zones\0[1201]

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

settings\zones\0[1201]

Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance[clsid]

Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprocserver32[loadwithoutcom]

Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}[]

Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprocserver32[threadingmodel]

Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance\initpropertybag[attributes]

Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance\initpropertybag[descriptionid]

Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance\initpropertybag[helptopic]

Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance\initpropertybag[recursiveearch]

Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance\initpropertybag[targetknownfolder]

Queries value: HKCR\exefile[nostaticdefaultverb]

Queries value: HKCR\exefile\shell[]

Queries value: HKCR\exefile\shell\open[neverdefault]

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

explorer\main\featurecontrol\feature\_unc\_savedfilecheck[install.exe]

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

explorer\main\featurecontrol\feature\_http\_username\_password\_disable[install.exe]

Queries value: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_localmachine\_lockdown[install.exe]

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

explorer\main\featurecontrol\feature\_localmachine\_lockdown[install.exe]

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

explorer\main\featurecontrol\feature\_protocol\_lockdown[install.exe]

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

settings[cointernetcombineiuricachesize]

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

settings[cointernetcombineiuricachesize]

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

settings[cointernetcombineiuricachesize]

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

settings[cointernetcombineiuricachesize]

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

explorer\main\featurecontrol\feature\_shim\_mshelp\_combine[flashplayer18\_a\_install.exe]

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

explorer\main\featurecontrol\feature\_shim\_mshelp\_combine[\*]

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

nt\currentversion\compatibility32[msmpeng]

Queries value: HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronosio]

Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksiz]

Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]

Queries value: HKLM\software\microsoft\internet explorer\registration[productid]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[threadingmodel]

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

Queries value: HKU\default\control panel\desktop[preferreduilanguages]

Queries value: HKU\default\control

panel\desktop\muicached[machinepreferreduilanguages]

Queries value: HKU\default\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

Queries value: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[]

Queries value: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[threadingmodel]

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

explorer\main\featurecontrol\feature\_behaviors[flashplayer18\_a\_install.exe]

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

explorer\main\featurecontrol\feature\_behaviors[\*]

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

settings\zones\0[2000]

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

settings\zones\0[2000]

Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default

behaviors[dxtfilterbehavior]

Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[]

Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[threadingmodel]

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

nt\currentversion\compatibility32[svchost]

Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[confirmfiledelete]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer[nofilefolderconnection]  
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]  
Queries value: HKLM\hardware\devicemap\video[\device\video3]  
Queries value: HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000[pruningmode]  
Queries value:  
HKLM\system\currentcontrolset\enum\pci\ven\_80ee&dev\_beef&subsys\_00000000&rev\_00\38267a616a80&10[hardwareid]  
Queries value: HKLM\hardware\devicemap\video[\device\video0]  
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[pruningmode]  
Queries value: HKLM\hardware\devicemap\video[\device\video1]  
Queries value: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}[]  
Queries value: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\inprocserver32[]  
Queries value: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-0d8e74595f78}\0000[pruningmode]  
Queries value: HKLM\hardware\devicemap\video[\device\video2]  
Queries value: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-8ed0c8eb59a8}\0000[pruningmode]  
Queries value: HKCR\wow6432node\clsid\{72eb61e0-8672-4303-9175-f2e4c68b2e7c}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![name]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![flags]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![id]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user\_shell  
folders[start menu]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionorderby2[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionorderby2[flags]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionorderby2[id]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[flags]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[id]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\user\_shell  
shell folders[common start menu]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user\_shell  
folders[recent]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[flags]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[id]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[flags]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[id]  
Queries value: HKCR\.dll[]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[flags]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[id]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[flags]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[id]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue\_squadron[name]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue\_squadron[flags]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue\_squadron[id]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[flags]  
Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[id]  
Queries value: HKCR\.dll[perceivedtype]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[flags]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[id]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[flags]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[id]  
Queries value: HKCR\systemfileassociations\.dll[perceivedtype]  
Queries value: HKCR\dllfile[docobject]  
Queries value: HKCR\systemfileassociations\.dll[docobject]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[name]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[flags]  
Queries value:  
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[id]  
Queries value:

```

HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[id]
Queries value: HKCR\dllfile[browseinplace]
Queries value: HKCR\systemfileassociations\.dll[browseinplace]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terraced[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terraced[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terraced[id]
Queries value: HKCR\.dll[content type]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[id]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
Queries value: HKCR\dllfile[isshortcut]
Queries value: HKCR\systemfileassociations\.dll[isshortcut]
Queries value: HKCR\dllfile[alwaysshowext]
Queries value: HKCR\dllfile[nevershowext]
Queries value: HKCR\systemfileassociations\.dll[nevershowext]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[modexonly]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[emulationonly]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[showframerate]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[enableprintscreen]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[forceagpsupport]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[disableagpsupport]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[disablemmx]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[disableddscapsinddsd]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[disablewidersurfaces]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[usenonlocalvidmem]
Queries value: HKCR\.txt[]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[forcerefreshrate]
Queries value: HKLM\software\wow6432node\microsoft\direct3d[flipnovsync]
Queries value: HKCR\.txt[perceivedtype]
Queries value: HKCR\txtfile[docobject]
Queries value: HKCR\systemfileassociations\.txt[docobject]
Queries value: HKCR\systemfileassociations\text[docobject]
Queries value: HKCR\txtfile[browseinplace]
Queries value: HKCR\systemfileassociations\.txt[browseinplace]
Queries value: HKCR\systemfileassociations\text[browseinplace]
Queries value: HKCR\.txt[content type]
Queries value: HKCR\txtfile[isshortcut]
Queries value: HKCR\systemfileassociations\.txt[isshortcut]
Queries value: HKCR\systemfileassociations\text[isshortcut]
Queries value: HKCR\txtfile[alwaysshowext]
Queries value: HKCR\systemfileassociations\.txt[alwaysshowext]
Queries value: HKCR\systemfileassociations\text[alwaysshowext]
Queries value: HKCR\txtfile[nevershowext]
Queries value: HKCR\systemfileassociations\.txt[nevershowext]
Queries value: HKCR\systemfileassociations\text[nevershowext]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[maxundoitems]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\advanced[maxundoitems]
Queries value: HKCR\directory\shellex\copyhookhandlers\filesystem[]
Queries value: HKCR\wow6432node\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32[]
Queries value: HKCR\directory\shellex\copyhookhandlers\sharing[]
Queries value: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[loadwithoutcom]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{40dd6e20-7c17-11ce-a804-00aa003ca9f6} {000214fc-0000-0000-c000-000000000046}
0xffff]
Queries value: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}[]
Queries value: HKLM\software\wow6432node\microsoft\directdraw[owndc]
Queries value: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
Queries value: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
Queries value: HKCR\wow6432node\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[threadingmodel]

```

Queries value: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}[]  
Queries value: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprocserver32[]  
Queries value: HKCR\dximagetransform.microsoft.gradient\clsid[]  
Queries value: HKCR\wow6432node\clsid\{edb5f444-cb8d-445a-a523-ec5ab6ea33c7}\inprocserver32[threadingmodel]  
Queries value: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\progid[]  
Queries value:  
HKLM\system\currentcontrolset\services\lanmanserver\defaultsecurity[srvsvcdefaultshareinfo]  
Queries value: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}[]  
Queries value: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32[threadingmodel]  
Queries value: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}[]  
Queries value: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{6311429e-2f1a-4777-880f-c7289fd10169}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[profilesdirectory]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18[profileimagepath]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19[profileimagepath]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-20[profileimagepath]  
Queries value: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}[]  
Queries value: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32[threadingmodel]  
Queries value: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}[]  
Queries value: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{49f371e1-8c5c-4d9c-9a3b-54a6827f513c}\inprocserver32[threadingmodel]  
Queries value: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\explorer\sharing[userssharename]  
Queries value: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[threadingmodel]  
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\install.exe[dontusedesktopchangerouter]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\propertyssystem\propertyhandlers\.dll[]  
Queries value: HKCR\wow6432node\clsid\{66742402-f9b9-11d1-a202-0000f81fedee}[disableprocessisolation]  
Queries value: HKCR\wow6432node\clsid\{66742402-f9b9-11d1-a202-0000f81fedee}[nooplock]  
Queries value: HKCR\wow6432node\clsid\{66742402-f9b9-11d1-a202-0000f81fedee}[useinprochandlercache]  
Queries value: HKCR\wow6432node\clsid\{66742402-f9b9-11d1-a202-0000f81fedee}[useoutofprochandlercache]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\propertyssystem\propertyhandlers\.exe[]  
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid[]  
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[]  
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[threadingmodel]  
Queries value: HKCR\type1lib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]  
Queries value: HKCR\type1lib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]  
Queries value: HKCR\type1lib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_subdownload\_lockdown[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_subdownload\_lockdown[\*]  
Queries value: HKCU\software\microsoft\ftp[use web based ftp]  
Queries value: HKCU\software\microsoft\internet explorer\services[selectionactivitybuttonisable]  
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]  
Queries value: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[]  
Queries value: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[inprocserver32]  
Queries value: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[]  
Queries value: HKCR\wow6432node\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[threadingmodel]  
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[screndefaultservers]  
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[usedns]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnssecurenamequeryfallback]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[enabledaforallnetworks]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[directaccessqueryorder]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]  
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[addrconfigcontrol]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressesstoregister]  
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[updateleveldomainzones]  
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[adapvertimeoutlimit]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[serverprioritytimelimit]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachedsockets]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[enablemulticast]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastresponderflags]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsenderflags]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendermaxtimeout]  
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[usecompartments]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[cacheallcompartments]  
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[usenewregistration]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistration]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistrationonly]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquerytimeouts]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquickquerytimeouts]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\profilelist[programdata]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir (x86)]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir (x86)]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion[programw6432dir]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion[commonw6432dir]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[searchlist]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enabledhcp]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationenabled]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registeradaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[domain]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpdomain]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpv6domain]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpnameserver]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_block\_lmz\_script[flashplayer18\_a\_install.exe]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main\featurecontrol\feature\_block\_lmz\_script[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\user agent[]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\user agent[]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\user agent[compatible]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\user agent[compatible]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\user agent[version]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\user agent[version]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enabledhcp]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user  
agent]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\user agent[platform]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\5.0\user agent[platform]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\compatibility32[dllhost]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[queryadaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[disableadapterdomainname]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationmaxaddresscount]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[maxnumberofaddressesstoregister]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enablemulticast]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[queryadaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disableadapterdomainname]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disabledynamicupdate]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enableadapterdomainnameregistration]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationmaxaddresscount]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[maxnumberofaddressesstoregister]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enablemulticast]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]  
Queries value: HKCU\software\microsoft\windows\_script\settings[jitdebug]  
Queries value: HKCR\http\shell\open\command[ ]  
Queries value: HKLM\software\wow6432node\microsoft\internet  
explorer\main[maxrenderline]  
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[nodetype]  
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[dhcpnodetype]  
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[scopeid]  
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[dhcpscopeid]  
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[enableproxy]  
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[enabledns]  
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\winhttp\tracing[enabled]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\winhttp[disablebranchcache]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]  
Queries value: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip[winsock 2.0 provider id]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[fromcachetimeout]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\policies\microsoft\windows\currentversion\internet settings[secureprotocols]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[secureprotocols]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings[proxysettingsperuser]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\connections[defaultconnectionsettings]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[certificaterevocation]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[disablekeepalive]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[disablepassport]  
Queries value:  
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignedll]  
Queries value:  
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[idnenabled]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[cachemode]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1\_1]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[enablehttp1\_1]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\policies\microsoft\windows\currentversion\internet settings[proxyhttp1.1]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-

1001\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[enablenegotiate]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[disablebasiccoverclearchannel]  
Queries value:  
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\internet explorer\main\featurecontrol[feature\_clientauthcertfilter]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[syncmode5]  
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: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature]  
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\software\wow6432node\microsoft\windows\currentversion\internet  
settings\connections[winhttpsettings]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\explorer\user shell folders[cache]  
Queries value: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip6[winsock 2.0 provider id]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\control  
panel\international[localename]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[proxyserver]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[autoconfigurl]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cacheprefix]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cachelimit]  
Queries value:  
HKLM\system\currentcontrolset\services\dns\cache\parameters\dns\cache[shutdownonidle]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\explorer\user shell folders[cookies]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cacheprefix]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[peruseritem]  
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\explorer\user shell folders[history]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cacheprefix]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cachelimit]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\domstore[cache\repair]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\domstore[cache\path]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\domstore[cache\prefix]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\domstore[cache\limit]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\domstore[cache\options]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\feedplat[cache\repair]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\feedplat[cache\path]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\feedplat[cache\prefix]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\feedplat[cache\limit]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\feedplat[cache\options]  
Queries value: HKU\s-1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible  
cache\lecompat[cache\repair]



[illegible]

explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback[svchost.exe]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[perusercookies]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[leashlegacycookies]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[sendextracrlf]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[wpadsearchalldomains]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[bypasssslnocheck]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[mimeexclusionlistforcache]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[headerexclusionlistforcache]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[dnscheenabled]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[dnscheentries]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[dnschetimeout]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[warnonpost]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[warnalwaysonpost]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[warnonzonecrossing]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[warnonbadcertecvng]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[warnonpostredirect]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[alwaysdrainonredirect]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[warnonhttpstohttpredirect]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\wpad\wpadoverride]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[enableautodial]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[netautodial]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[globaluseroffline]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings[badproxyexpiretime]  
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\_mime\_handling[svchost.exe]  
Queries value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]  
Queries value: HKLM\software\microsoft\sqlclient\windows\disabledprocesses[9882dba6]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[enablefiletracing]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[filetracingmask]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[enableconsoletracing]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[consoletracingmask]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[maxfilesize]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[filedirectory]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[enablefiletracing]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[filetracingmask]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[enableconsoletracing]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[consoletracingmask]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[maxfilesize]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[filedirectory]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet  
settings\connections[defaultconnectionsettings]  
Queries value: HKU\1-5-21-980053277-1733835069-2361817685-  
1001\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]  
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\oid\encodingtype  
0\cryptdllfindoidinfo\1.3.6.1.4.1.311.44.3.4!7[name]  
Queries value:  
HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]  
Queries value: HKCU\software\classes\local  
settings\mui.cache\16\52c64b7e[@%systemroot%\system32\p2collab.dll,-8042]  
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\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\16\52c64b7e[@%systemroot%\system32\dnsapi.dll,-103]  
Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel]  
Queries value: HKLM\system\currentcontrolset\services\crypt32[diagnatchanymask]  
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[maxaiaurcountincert]  
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype  
0\certdllcreatecertificatechainengine\config[maxaiaurretrievalcountperchain]  
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype  
0\certdllcreatecertificatechainengine\config[maxurlretrievalbytecount]  
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype  
0\certdllcreatecertificatechainengine\config[maxaiaurretrievalbytecount]  
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype  
0\certdllcreatecertificatechainengine\config[maxaiaurretrievalcertcount]  
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[chaincachesyncfiletime]  
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\fee449ee0e3965a5246f000e87fde2a065f8d9d4[blob]  
Queries value:  
HKLM\software\microsoft\systemcertificates\ca\crls\377d1b1c0538833035211f4083d00fecc414dab[blob]  
Queries value:  
HKLM\software\microsoft\systemcertificates\disallowed\certificates\637162cc59a3a1e25956fa5fa8f60d2e1c52eac6[blob]  
Queries value:  
HKLM\software\microsoft\systemcertificates\disallowed\certificates\7d7f4414ccef168adf6bf40753b5becd78375931[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\7f88cd7223f3c813818c994614a89c99fa3b5247[blob]  
Queries value:  
HKLM\software\microsoft\systemcertificates\root\certificates\4a3489159a520f0d93d032ccaf37e7fe20a8b419[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\wow6432node\microsoft\windows  
nt\currentversion\winlogon[userenvdebuglevel]  
Queries value: HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]  
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\internet  
settings\zones\0[1c00]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet  
settings\zones\0[1c00]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default  
behaviors[homepage]  
Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid[]  
Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[]  
Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32]  
00aa00bdce0b}\inprocserver32[  
Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]  
00aa00bdce0b}\inprocserver32[  
Queries value: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel]  
00aa00bdce0b}\inprocserver32[threadingmodel]  
Queries value: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\win32[]  
Queries value: HKCU\software\microsoft\internet explorer\main[start page]  
Queries value: HKLM\software\wow6432node\microsoft\internet explorer\default  
behaviors[clientcaps]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[enablefiletracing]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[filetracingmask]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[enableconsoletracing]  
Queries value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[consoletracingmask]  
Queries value:

```
HKLM\software\wow6432node\microsoft\tracing\flashplayer18_a_install_rasapi32[maxfilesize]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\flashplayer18_a_install_rasapi32[filedirectory]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\flashplayer18_a_install_rasmancs[enablefiletracing]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\flashplayer18_a_install_rasmancs[filetracingmask]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\flashplayer18_a_install_rasmancs[enableconsoletracing]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\flashplayer18_a_install_rasmancs[consoletracingmask]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\flashplayer18_a_install_rasmancs[maxfilesize]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\flashplayer18_a_install_rasmancs[filedirectory]
  Queries value:
HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:
HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:
HKCU\software\microsoft\windows\currentversion\internet
settings[connections[savedlegacysettings]
  Queries value:
HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Queries value:
HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Queries value:
HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
  Queries value:
HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
  Queries value:
HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[flashplayer18_a_install.exe]
  Queries value:
HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
  Queries value:
HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[flashplayer18_a_install.exe]
  Queries value:
HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
  Queries value:
HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
  Queries value:
HKLM\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:
HKCU\software\policies\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:
HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
  Queries value:
HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[flashplayer18_a_install.exe]
  Queries value:
HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
  Queries value:
HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[flashplayer18_a_install.exe]
  Queries value:
HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
  Queries value:
HKCU\software\microsoft\internet explorer\recovery[autorecover]
  Queries value:
HKCR\.png[content type]
  Queries value:
HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
  Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\progid[]
  Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
  Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
  Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
  Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
  Queries value:
HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:
HKCR\mime\database\content type\image/bmp/bits[0]
  Queries value:
HKCR\mime\database\content type\image/gif/bits[0]
  Queries value:
HKCR\mime\database\content type\image/jpeg/bits[0]
  Queries value:
HKCR\mime\database\content type\image/pjpeg/bits[0]
  Queries value:
HKCR\mime\database\content type\image/png/bits[0]
  Queries value:
HKCR\mime\database\content type\image/x-png/bits[0]
  Queries value:
HKCR\mime\database\content type\image/x-wmf/bits[0]
  Queries value:
HKCR\mime\database\content type\image/x-png[image filter clsid]
  Queries value:
HKCR\wow6432node\clsid\{a3ccdf7-2de2-11d0-86f4-00a0c913f750}\progid[]
  Queries value:
HKCR\wow6432node\clsid\{a3ccdf7-2de2-11d0-86f4-00a0c913f750}[]
  Queries value:
HKCR\wow6432node\clsid\{a3ccdf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[inprocserver32]
  Queries value:
HKCR\wow6432node\clsid\{a3ccdf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
  Queries value:
HKCR\wow6432node\clsid\{a3ccdf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[threadingmodel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{a8a88c49-5eb2-4990-a1a2-0876022c854f}]
  Queries value:
HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[displayname]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[displayversion]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[versionmajor]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[versionminor]
```

Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[publisher]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[displayicon]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[uninstallstring]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[urlinfoabout]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[helpink]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[installlocation]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[installsource]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[installdate]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[language]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[estimatedsize]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[nomodify]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\newproduct 1.00[norepair]  
Sets/Creates value: HKLM\system\currentcontrolset\services\devicesync[description]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[enablefiletracing]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[enableconsoletracing]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[filetracingmask]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[consoletracingmask]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[maxfilesize]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasapi32[filedirectory]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[enablefiletracing]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[enableconsoletracing]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[filetracingmask]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[consoletracingmask]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[maxfilesize]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\svchost\_rasmancs[filedirectory]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[enablefiletracing]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[enableconsoletracing]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[filetracingmask]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[consoletracingmask]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[maxfilesize]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasapi32[filedirectory]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasmancs[enablefiletracing]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasmancs[enableconsoletracing]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasmancs[filetracingmask]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasmancs[consoletracingmask]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasmancs[maxfilesize]  
Sets/Creates value:  
HKLM\software\wow6432node\microsoft\tracing\flashplayer18\_a\_install\_rasmancs[filedirectory]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[uncasintranet]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]  
Value changes:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[globalassocchangedcounter]  
Value changes: HKLM\system\currentcontrolset\services\devicesync[type]  
Value changes:  
HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[name]  
Value changes: HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[id]  
Value changes: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\software\microsoft\windows\currentversion\internet settings[proxyenable]  
Value changes: HKU\s-1-5-21-980053277-1733835069-2361817685-1001\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]  
Value changes: HKCU\software\classes\local settings\muicache\16\52c64b7e[language list]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]