Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 469, Task ID: 475

Task ID:	475
Risk Level:	10
Date Processed:	2016-03-24 13:55:15 (UTC)
Processing Time:	61.79 seconds
Virtual Environment:	IntelliVM

Execution Arguments:
"c:\windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe"

Sample ID:	469
Type:	basic
Owner:	admin
Label:	755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63
Date Added:	2016-03-24 13:55:14 (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]
1 SSL traffic on standard port
10 Creates malicious events: Bookworm [Worm]
5 Creates process in suspicious location
7 Attempts to connect to dynamic DNS
6 Creates executable in application data folder
6 Modifies registry autorun entries
8 Starts svchost.exe
3 Connects to local host
5 Possible process injection
5 Installs service
5 Opens Copy Hook Handlers key
3 Long sleep detected
6 Starts process from Application Data folder
1 YARA score 1
2 Terminates third-party processes
3 HTTP connection - response code 200 (success)

Static Events

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

Process/Thread Events

Creates process: C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe ["c:\windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe"]
Creates process: C:\Program Files\flashplayer18_a_install.exe ["C:\Program Files\flashplayer18_a_install.exe"]
Creates process: C:\Program Files\install.exe ["C:\Program Files\install.exe"]
Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe ["C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe" "C:\Program Files\install.exe"]
Creates process: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MsMpEng.exe ["C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MsMpEng.exe"]
Creates process: C:\WINDOWS\system32\svchost.exe [-main]
Creates process: C:\WINDOWS\system32\svchost.exe [-protect]
Creates process: C:\WINDOWS\system32\dllhost.exe [C:\WINDOWS\System32\dllhost.exe -user]
Writes to process: PID:1112 C:\WINDOWS\system32\svchost.exe
Writes to process: PID:1032 C:\WINDOWS\system32\svchost.exe
Writes to process: PID:1092 C:\WINDOWS\system32\dllhost.exe
Terminates process: C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
Terminates process: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MsMpEng.exe
Terminates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe
Terminates process: C:\Program Files\install.exe

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\ZonesCounterMutex
Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex: \BaseNamedObjects\oleacc-msaa-loaded
Creates mutex: \BaseNamedObjects\Adobe_ADM.log

Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local settings!temporary internet files!content.ie5!
Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!cookies!
Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local settings!history!history.ie5!
Creates mutex: \BaseNamedObjects\WininetConnectionMutex
Creates mutex: \BaseNamedObjects\!PrivacIE!SharedMemory!Mutex
Creates mutex: \BaseNamedObjects_SHuassist.mtx
Creates mutex: \BaseNamedObjects\BB6cmqyHzy8kkcJ
Creates mutex: \BaseNamedObjects\SHIMLIB_LOG_MUTEX
Creates mutex: \BaseNamedObjects\DDrawWindowListMutex
Creates mutex: \BaseNamedObjects\DDrawDriverObjectListMutex
Creates mutex: \BaseNamedObjects__DDrawExclMode__
Creates mutex: \BaseNamedObjects__DDrawCheckExclMode__
Creates mutex: \BaseNamedObjects\Adobe_GDE.log
Creates mutex: \BaseNamedObjects\MSIMGSIZECacheMutex
Creates event: \BaseNamedObjects\DINPUTWINMM
Creates event: \BaseNamedObjects\userenv: User Profile setup event
Creates event: \BaseNamedObjects\ShellCopyEngineRunning
Creates event: \BaseNamedObjects\ShellCopyEngineFinished
Creates event: \BaseNamedObjects\CancelPort{A91D59EC-724C-4209-9B91-75BDF5A5A275}
Creates event: \BaseNamedObjects\CancelPort{581E55A3-F365-4B2A-86CF-B362AF84DBE8}
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore: \BaseNamedObjects\{61410B1E-728E-4E96-96DD-9BE271228D74}
Creates semaphore: \BaseNamedObjects\{A925355A-7A05-4070-B3BC-3D323F229F91}}

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\$inst
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
Creates: C:\Program Files\install.exe
Creates: C:\Program Files\flashplayer18_a_install.exe
Creates: C:\Program Files\Adobe\NewProduct
Creates: C:\Program Files\Adobe\NewProduct\Uninstall.exe
Creates: C:\Program Files\Adobe\NewProduct\Uninstall.ini
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\E431E95C-97F5-44D2-A2D6-07B00F1A955B
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
Creates: C:\Program Files
Creates: C:\DOCUME~1
Creates: C:\DOCUME~1\Admin
Creates: C:\DOCUME~1\Admin\LOCALS~1
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0__tmp_rar_sfx_access_check_86975
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MpSvc.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\160[1]
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0
Creates: C:\Documents and Settings
Creates: C:\Documents and Settings\All Users
Creates: C:\Documents and Settings\All Users\Application Data
Creates: C:\Documents and Settings\All Users\Application Data\Microsoft
Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync
Creates: C:\Documents and Settings\All Users\Application Data\Mozilla
Creates: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto
Creates: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA
Creates: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys
Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MsMpEng.exe
Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc.dll
Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\delete.txt
Creates: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB
Creates: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys\889EC630
Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys\5227f4c3bk
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\warning_icon_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_125.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_150.png

Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_125.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_150.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_125.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_150.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_darkgray_base_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_darkgray_base_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_125.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_150.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\transparent.gif
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\gray_button_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\close_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_125.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_150.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_125.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_150.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_125.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_150.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_200.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_125.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_150.png
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\info_icon_100.png
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\SC[1]
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\Adobe_ADMLogs
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\6FBB2978-428C-49A1-976F-5CC584689783
Creates: C:\Documents and Settings\Admin\Cookies\admin@adobe[1].txt
Creates: C:\Documents and Settings\Admin\Cookies\admin@adobe[2].txt
Opens: C:\WINDOWS\Prefetch\755A4B2EC15DA6BB01248B2DFBAD2-0DD218E0.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\winmm.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\system32\cabinet.dll
Opens: C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\shell32.dll.124.Manifest
Opens: C:\WINDOWS\system32\shell32.dll.124.Config
Opens: C:\WINDOWS\system32\MSCTF.dll

Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\$inst
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\7.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\9.tmp
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\msftedit.dll
Opens: C:\WINDOWS\win.ini
Opens: C:\WINDOWS\system32\setupapi.dll
Opens: C:\
Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
Opens: C:\Program Files\install.exe
Opens: C:\Program Files\flashplayer18_a_install.exe
Opens: C:\Program Files\Adobe\NewProduct\Uninstall.exe
Opens: C:\WINDOWS\Temp\a87ac59b-3272-4219-9012-1b18fb4128b2
Opens: C:\Program Files\Adobe\NewProduct
Opens: C:\WINDOWS\system32\netapi32.dll
Opens: C:\Documents and Settings
Opens: C:\Documents and Settings\Admin\My Documents\desktop.ini
Opens: C:\Documents and Settings\All Users
Opens: C:\Documents and Settings\All Users\Documents\desktop.ini
Opens: C:\WINDOWS\system32\clbcatq.dll
Opens: C:\WINDOWS\system32\comres.dll
Opens: C:\WINDOWS\Registration\R000000000007.clb
Opens: C:\WINDOWS\system32\urlmon.dll
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\systest.sdb
Opens: C:\Program Files
Opens: C:\Program Files\flashplayer18_a_install.exe.Manifest
Opens: C:\Program Files\flashplayer18_a_install.exe.Config
Opens: C:\WINDOWS\Prefetch\FLASHPLAYER18_A_INSTALL.EXE-0B6F0919.pf
Opens: C:\WINDOWS\system32\winhttp.dll
Opens: C:\WINDOWS\system32\msi.dll
Opens: C:\WINDOWS\system32\psapi.dll
Opens: C:\WINDOWS\system32\msimg32.dll
Opens: C:\WINDOWS\system32\winspool.drv
Opens: C:\WINDOWS\system32\oledlg.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-
ww_dfb54e0c\GdiPlus.dll
Opens: C:\WINDOWS\system32\crypt32.dll
Opens: C:\WINDOWS\system32\msasn1.dll
Opens: C:\WINDOWS\system32\wintrust.dll
Opens: C:\WINDOWS\system32\oleacc.dll
Opens: C:\WINDOWS\system32\msvcp60.dll
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\Program Files\install.exe.Manifest
Opens: C:\Program Files\install.exe.Config
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\0.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\1.tmp
Opens: C:\WINDOWS\system32\oleaccrc.dll
Opens: C:\WINDOWS\Prefetch\INSTALL.EXE-199863BB.pf
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\3.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\4.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\5.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\6.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\8.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\10.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\11.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\12.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\13.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\14.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\15.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\16.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\17.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\20.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\50.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\21.tmp
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\51.tmp
Opens: C:\WINDOWS\system32\riched32.dll
Opens: C:\WINDOWS\system32\riched20.dll
Opens: C:\WINDOWS\Fonts\SEGOEUI.TTF
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\E431E95C-97F5-44D2-A2D6-07B00F1A955B
Opens: C:\WINDOWS\system32\ntmarta.dll
Opens: C:\WINDOWS\system32\samlib.dll
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\Adobe_ADMLogs\Adobe_ADM.log
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
Opens: C:\Program Files\flashplayer18_a_install.exe.3.Manifest
Opens: C:\WINDOWS\system32\browseui.dll
Opens: C:\WINDOWS\system32\browseui.dll.123.Manifest
Opens: C:\WINDOWS\system32\browseui.dll.123.Config
Opens: C:\WINDOWS\system32\ieframe.dll
Opens: C:\Program Files\Internet Explorer\iexplore.exe
Opens: C:\WINDOWS\system32\ieframe.dll.123.Manifest

Opens: C:\WINDOWS\system32\ieframe.dll.123.Config
Opens: C:\WINDOWS\system32\en-US\ieframe.dll.mui
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0__tmp_rar_sfx_access_check_86975
Opens: C:\WINDOWS\system32\WININET.dll.123.Manifest
Opens: C:\WINDOWS\system32\WININET.dll.123.Config
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MpSvc.dll
Opens: C:\Documents and Settings\Admin\Local Settings\History
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\index.dat
Opens: C:\Documents and Settings\Admin\Cookies
Opens: C:\Documents and Settings\Admin\Cookies\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\mshtml.dll
Opens: C:\WINDOWS\system32\msls31.dll
Opens: C:\Documents and Settings\Admin\Local Settings
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe.Manifest
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe.Config
Opens: C:\WINDOWS\Prefetch\MSMPENG.EXE-13EF2649.pf
Opens: C:\WINDOWS\system32\shdocvw.dll
Opens: C:\WINDOWS\system32\cryptui.dll
Opens: C:\WINDOWS\system32\CRYPTUI.dll.2.Manifest
Opens: C:\WINDOWS\system32\CRYPTUI.dll.2.Config
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
Opens: C:\WINDOWS\system32\iphlpapi.dll
Opens: C:\WINDOWS\system32\SHDOCVW.dll.123.Manifest
Opens: C:\WINDOWS\system32\SHDOCVW.dll.123.Config
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MsMpEng.exe
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc.dll
Opens: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys
Opens: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
Opens: C:\WINDOWS\system32\mlang.dll
Opens: C:\WINDOWS\system32\MLANG.dll.123.Manifest
Opens: C:\WINDOWS\system32\MLANG.dll.123.Config
Opens: C:\WINDOWS\Prefetch\MSMPENG.EXE-1806D63D.pf
Opens: C:\WINDOWS\system32
Opens: C:\WINDOWS\system32\msxml3.dll
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\readme.txt
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc
Opens: C:\WINDOWS\system32\svchost.exe
Opens: C:\WINDOWS
Opens: C:\WINDOWS\System32\svchost.exe.Manifest
Opens: C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
Opens: C:\WINDOWS\system32\shimeng.dll
Opens: C:\WINDOWS\AppPatch\AcGenral.dll
Opens: C:\WINDOWS\system32\msacm32.dll
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\delete.txt
Opens: C:\WINDOWS\system32\mydocs.dll
Opens: C:\WINDOWS\system32\msxml3r.dll
Opens: C:\WINDOWS\system32\mydocs.dll.123.Manifest
Opens: C:\WINDOWS\system32\mydocs.dll.123.Config
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\ntshrui.dll
Opens: C:\WINDOWS\system32\ntshrui.dll
Opens: C:\WINDOWS\system32\atl.dll
Opens: C:\WINDOWS\system32\ntshrui.dll.123.Manifest
Opens: C:\WINDOWS\system32\ntshrui.dll.123.Config
Opens: C:\WINDOWS\system32\jscript.dll
Opens: C:\WINDOWS\system32\winlogon.exe
Opens: C:\WINDOWS\system32\xpsp2res.dll
Opens: C:\WINDOWS\system32\dxtrans.dll
Opens: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys\889EC630
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\F45C8A7E
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\s5227f4c3
Opens: C:\WINDOWS\system32\wtsapi32.dll
Opens: C:\WINDOWS\system32\winsta.dll
Opens: C:\WINDOWS\system32\ddrawex.dll
Opens: C:\WINDOWS\system32\mswsock.dll

Opens: C:\WINDOWS\system32\hnetcfg.dll
Opens: C:\WINDOWS\system32\wshtcpip.dll
Opens: C:\WINDOWS\system32\msv1_0.dll
Opens: C:\AUTOEXEC.BAT
Opens: C:\WINDOWS\system32\dllhost.exe
Opens: C:\WINDOWS\system32\ddraw.dll
Opens: C:\WINDOWS\system32\dciman32.dll
Opens: C:\WINDOWS\System32\dllhost.exe.Manifest
Opens: C:\WINDOWS\Prefetch\DLLHOST.EXE-45A368CC.pf
Opens: C:\WINDOWS\system32\dxtmsft.dll
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys\u5227f4c3
Opens: C:\WINDOWS\system32\sxs.dll
Opens: C:\WINDOWS\system32\rasapi32.dll
Opens: C:\WINDOWS\system32\rasman.dll
Opens: C:\WINDOWS\system32\tapi32.dll
Opens: C:\WINDOWS\system32\rtutils.dll
Opens: C:\WINDOWS\system32\stdole2.tlb
Opens: C:\WINDOWS\System32\TAPI32.dll.124.Manifest
Opens: C:\WINDOWS\System32\TAPI32.dll.124.Config
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk
Opens: C:\WINDOWS\system32\ras
Opens: C:\Documents and Settings\Admin\Application Data\Mozilla\Firefox\profiles.ini
Opens: C:\Documents and Settings\Admin\Application Data\Mozilla\Firefox\prefs.js
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Network\Connections\Pbk\
Opens: C:\WINDOWS\system32\sensapi.dll
Opens: C:\WINDOWS\system32\rasadhlp.dll
Opens: C:\WINDOWS\system32\dnsapi.dll
Opens: C:\WINDOWS\system32\drivers\etc\hosts
Opens: C:\WINDOWS\system32\rsaenh.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR
Opens: C:\WINDOWS\Fonts\arialbd.ttf
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\Adobe_ADMLogs\Adobe_GDE.log
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
Opens: C:\WINDOWS\system32\TAPI32.dll.124.Manifest
Opens: C:\WINDOWS\system32\TAPI32.dll.124.Config
Opens: C:\WINDOWS\system32\schannel.dll
Opens: C:\WINDOWS\system32\dssenh.dll
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\SystemCertificates\My\Certificates
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\SystemCertificates\My\CRLs
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\SystemCertificates\My\CTLs
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\SystemCertificates\My
Opens: C:\WINDOWS\system32\iepeers.dll
Opens: C:\WINDOWS\system32\iepeers.dll.123.Manifest
Opens: C:\WINDOWS\system32\iepeers.dll.123.Config
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
Opens: C:\WINDOWS\system32\imgutil.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_100.png
Opens: C:\WINDOWS\system32\pngfilt.dll
Opens: C:\Documents and Settings\Admin\Cookies\admin@adobe[1].txt
Opens: C:\Documents and Settings\Admin\Cookies\admin@adobe[2].txt
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
Writes to: C:\Program Files\install.exe
Writes to: C:\Program Files\flashplayer18_a_install.exe
Writes to: C:\Program Files\Adobe\NewProduct\Uninstall.exe
Writes to: C:\Program Files\Adobe\NewProduct\Uninstall.ini
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MpSvc.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\160[1]
Writes to: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MsMpEng.exe
Writes to: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc.dll
Writes to: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\delete.txt
Writes to: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
Writes to: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc
Writes to: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys\889EC630
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\warning_icon_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_200.png

Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_125.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_150.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_125.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_150.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_125.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_150.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_darkgray_base_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_darkgray_base_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_125.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_150.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\transparent.gif
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\gray_button_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\close_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_125.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_150.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_125.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_150.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_125.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_150.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_200.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_125.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_150.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\info_icon_100.png
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\SC[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
Writes to: C:\Documents and Settings\Admin\Cookies\admin@adobe[1].txt
Writes to: C:\Documents and Settings\Admin\Cookies\admin@adobe[2].txt
Reads from: C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
Reads from: C:\WINDOWS\win.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
Reads from: C:\Documents and Settings\Admin\My Documents\desktop.ini
Reads from: C:\Documents and Settings\All Users\Documents\desktop.ini
Reads from: C:\WINDOWS\Registration\R000000000007.clb
Reads from: C:\Program Files\flashplayer18_a_install.exe
Reads from: C:\Program Files\install.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt

Reads from: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc
Reads from: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
Reads from: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\delete.txt
Reads from: C:\AUTOEXEC.BAT
Reads from: C:\WINDOWS\system32\dxtmsft.dll
Reads from: C:\WINDOWS\system32\stdole2.tlb
Reads from: C:\WINDOWS\system32\dxtrans.dll
Reads from: C:\WINDOWS\system32\drivers\etc\hosts
Reads from: C:\WINDOWS\system32\rsaenh.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
Reads from: C:\WINDOWS\system32\dssenh.dll
Reads from: C:\WINDOWS\system32\iepeers.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_100.png
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\$inst
Deletes: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\E431E95C-97F5-44D2-A2D6-07B00F1A955B
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0__tmp_rar_sfx_access_check_86975
Deletes: C:\Program Files\install.exe
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MpSvc.dll
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0
Deletes: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\delete.txt
Deletes: C:\Documents and Settings\Admin\Cookies\admin@adobe[1].txt

Network Events

DNS query: linuxdns.sytes.net
DNS query: get.adobe.com
DNS query: systeminfothai.gotdns.ch
DNS query: sysnc.sytes.net
DNS query: dlmping2.adobe.com
DNS query: stats.adobe.com
DNS response: linuxdns.sytes.net ⇒ 0.0.0.0
DNS response: get.wip4.adobe.com ⇒ 193.104.215.66
DNS response: systeminfothai.gotdns.ch ⇒ 0.0.0.0
DNS response: sysnc.sytes.net ⇒ 0.0.0.0
DNS response: e4578.g.akamaiedge.net ⇒ 118.214.80.175
DNS response: adobe.com.d1.sc.omtrdc.net ⇒ 192.243.250.16
DNS response: adobe.com.d1.sc.omtrdc.net ⇒ 192.243.250.65
Connects to: 0.0.0.0:80
Connects to: 127.0.0.1:1048
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: 193.104.215.66:443
Connects to: 0.0.0.0:21
Connects to: 127.0.0.1:1121
Connects to: 127.0.0.1:1138
Connects to: 118.214.80.175:443
Connects to: 192.243.250.16:80
Sends data to: 8.8.8.8:53
Sends data to: 127.0.0.1:1048
Sends data to: get.wip4.adobe.com:443 (193.104.215.66)
Sends data to: 127.0.0.1:1121
Sends data to: e4578.g.akamaiedge.net:443 (118.214.80.175)
Sends data to: 127.0.0.1:1138
Sends data to: adobe.com.d1.sc.omtrdc.net:80 (192.243.250.16)
Receives data from: sysnc.sytes.net:0 (0.0.0.0)
Receives data from: get.wip4.adobe.com:443 (193.104.215.66)
Receives data from: e4578.g.akamaiedge.net:443 (118.214.80.175)
Receives data from: 127.0.0.1:1138
Receives data from: adobe.com.d1.sc.omtrdc.net:80 (192.243.250.16)

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Creates key: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached
Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\userassist
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{75048700-ef1f-11d0-9888-

006097deacf9}
Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{75048700-ef1f-11d0-9888-
006097deacf9}\count
Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-
00aa004ae837}
Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-
00aa004ae837}\count
Creates key: HKLM\software\classes
Creates key: HKU\.default\software\microsoft\windows\currentversion\internet settings
Creates key: HKU\.default\software\microsoft\multimedia\audio
Creates key: HKU\.default\software\microsoft\multimedia\audio compression manager\
Creates key: HKU\.default\software\microsoft\multimedia\audio compression
manager\msacm
Creates key: HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00
Creates key: HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows nt\currentversion\winlogon
Creates key: HKLM\software\microsoft\directdraw\mostrecentapplication
Creates key: HKCU\software\microsoft\multimedia\audio
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00
Creates key: HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKLM\software\microsoft\tracing
Creates key: HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\internet settings\connections
Creates key: HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\internet settings
Creates key: HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows nt\currentversion\network\location awareness
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key: HKCU\software\microsoft\windows script\settings
Creates key: HKCU\software\microsoft\windows\currentversion\wintrust\trust
providers\software publishing
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\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\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\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\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: 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\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\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\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\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\policies\microsoft\systemcertificates\disallowed
Creates key: HKLM\software\policies\microsoft\systemcertificates\disallowed\certificates
Creates key: HKLM\software\policies\microsoft\systemcertificates\disallowed\crls
Creates key: HKLM\software\policies\microsoft\systemcertificates\disallowed\ctls
Creates key: HKLM\software\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\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\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\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\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: HKCU\software\microsoft\systemcertificates\my
Creates key: HKCU\software\microsoft\windows nt\currentversion\winlogon
Creates key: HKLM\software\microsoft\systemcertificates\authroot\certificates\5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25
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: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings[proxyserver]
Deletes value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings[proxyoverride]
Deletes value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings[autoconfigurl]
Deletes value: HKLM\software\microsoft\systemcertificates\authroot\certificates[5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25]
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\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winmm.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cabinet.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32
Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\system\setup
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
Opens key:
HKLM\software\microsoft\ctf\compatibility\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
Opens key: HKCU\software\microsoft\ctf
Opens key: HKLM\software\microsoft\ctf\systemshared
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msftedit.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
Opens key: HKLM\system\currentcontrolset\control\minint
Opens key: HKLM\system\wpa\pnp
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\software\microsoft\rpc\pagedbuffers
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}\
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\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\
Opens key: HKCU\software\microsoft\windows\currentversion\policies\system
Opens key: HKCU\software\classes\directory\shellex\iconhandler
Opens key: HKCR\directory\shellex\iconhandler
Opens key: HKCU\software\classes\directory\clsid
Opens key: HKCR\directory\clsid
Opens key: HKCU\software\classes\folder

Opens key: HKCR\folder
Opens key: HKCU\software\classes\folder\clsid
Opens key: HKCR\folder\clsid
Opens key: HKLM\software\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netapi32.dll
Opens key: HKCU\software\classes\drive\shellex\folderextensions
Opens key: HKCR\drive\shellex\folderextensions
Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe
Opens key: HKCU\software\classes\.exe
Opens key: HKCR\.exe
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\application
Opens key: HKCR\systemfileassociations\application
Opens key: HKCU\software\classes\exefile\clsid
Opens key: HKCR\exefile\clsid
Opens key: HKCU\software\classes*
Opens key: HKCR*
Opens key: HKCU\software\classes*\clsid
Opens key: HKCR*\clsid
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks
Opens key: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
Opens key: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
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: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comres.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\clbcatq.dll
Opens key: HKLM\software\microsoft\com3\debug
Opens key: HKLM\software\classes
Opens key: HKU\
Opens key: HKCR\clsid
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}\treatas
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll
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
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
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\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\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\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key: HKLM\software\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software
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\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zonemap\domains\msn.com
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zonemap\domains\msn.com\related
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKCU\software\microsoft\internet explorer\ietld
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
Opens key: HKLM\software\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\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\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
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\policies\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
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\microsoft\windows\currentversion\policies\explorer\restrictrun
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\flashplayer18_a_install.exe
Opens key: HKCU\software\classes\exefile\shell\open\ddeexec
Opens key: HKCR\exefile\shell\open\ddeexec
Opens key: HKCU\software\classes\applications\flashplayer18_a_install.exe
Opens key: HKCR\applications\flashplayer18_a_install.exe
Opens key: HKCU\software\microsoft\windows\shellnoroam
Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache
Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\apphelp.dll
Opens key: HKLM\system\wpa\tabletpc
Opens key: HKLM\system\wpa\mediacenter
Opens key: HKLM\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\policies\microsoft\windows\safer\levelobjects
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\flashplayer18_a_install.exe
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\install.exe
Opens key: HKCU\software\classes\applications\install.exe
Opens key: HKCR\applications\install.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\install.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winhttp.dll
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\winhttp\tracing
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\psapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msimg32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winspool.drv
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oledlg.dll
Opens key: HKCU\software\classes\clsid
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\gdiplus.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
Opens key: HKLM\system\currentcontrolset\services\crypt32\performance
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imagehlp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mpr.dll
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleacc.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\install.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\riched20.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\riched32.dll
Opens key: HKCU\software\microsoft\windows\currentversion\policies\network
Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32
Opens key: HKLM\software\microsoft\ctf\compatibility\flashplayer18_a_install.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\samlib.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntmarta.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\autocomplete
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}\treatas
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserverx86
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\localserver32
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver32
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandlerx86
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\localserver
Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserverx86
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver32
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandlerx86
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\browseui.dll
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver
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}\treatas
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserverx86
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver32
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver32
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandler32
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandler32
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandlerx86
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandlerx86
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ieframe.dll
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
Opens key: HKLM\software\microsoft\internet explorer\setup
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver
Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver
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}\treatas
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
Opens key: HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
Opens key: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32
Opens key: HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32
Opens key: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver
Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver
Opens key: HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\flashplayer18_a_install.exe\rpcthreadpoolthrottle
Opens key: HKCU\software\microsoft\internet explorer\main
Opens key: HKLM\software\microsoft\internet explorer\main
Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKCU\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
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}\treatas
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_iedde_register_protocol
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe\rpcthreadpoolthrottle
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe\starcraft
1.03
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2help.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
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: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: 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\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\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}\treatas
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msls31.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mshtml.dll
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
Opens key: HKLM\software\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\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\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
Opens key: HKLM\software\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\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\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\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\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\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\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
Opens key: HKLM\software\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\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\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\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
Opens key: HKLM\software\microsoft\internet explorer\application compatibility
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\microsoft\internet explorer\domstorage
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\microsoft\internet explorer\safety\privacie
Opens key: HKLM\software\microsoft\internet explorer\mediatypeclass
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
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\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
Opens key: HKCU\software\classes\exefile\shell
Opens key: HKCR\exefile\shell
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\msmpeng.exe
Opens key: HKCU\software\classes\applications\msmpeng.exe
Opens key: HKCR\applications\msmpeng.exe
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: HKCU\software\microsoft\internet explorer
Opens key: HKLM\software\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_res_to_lmz
Opens key: HKLM\software\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\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\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_feeds
Opens key: HKLM\software\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\microsoft\windows nt\currentversion\appcompatflags\custom\msmpeng.exe
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msmpeng.exe
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_manage_script_circular_refs
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_manage_script_circular_refs
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserverx86
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload
Opens key: HKLM\software\microsoft\internet explorer\security\floppy access
Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof detection
Opens key: HKLM\software\microsoft\internet explorer\security\adv addrbar spoof detection
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\localserver32
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\localserver32
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandlerx86
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\localserver
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mpsvc.dll
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\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}\treatas
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{75048700-ef1f-11d0-9888-006097deacf9}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-00aa004ae837}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\userassist\settings
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iphlpapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cryptui.dll
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_document_compatible_mode
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_document_compatible_mode
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shdocvw.dll
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\policies\microsoft\internet explorer\zoom
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key: HKCU\software\policies\microsoft\internet explorer\zoom
Opens key: HKCU\software\microsoft\internet explorer\zoom
Opens key: HKLM\software\microsoft\internet explorer\zoom
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_weboc_document_zoom
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_weboc_document_zoom
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
Opens key: HKLM\software\microsoft\internet explorer\registration
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enable_compat_logging
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_compat_logging
Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msmpeng.exe\rpcthreadpoolthrottle
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\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\microsoft\internet explorer\settings
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: 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\system\currentcontrolset\services\devicesync
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mlang.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKLM\software\microsoft\internet explorer\version vector
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_sslux
Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_sslux
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones
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: HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}
Opens key: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}
Opens key: HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\treatas
Opens key: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\treatas
Opens key: HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprocserver32
Opens key: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32
Opens key: HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprocserverx86
Opens key: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\localserver32
Opens key: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\localserver32
Opens key: HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprochandler32
Opens key: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler32
Opens key: HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprochandlerx86
Opens key: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\localserver
Opens key: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\localserver
Opens key: HKU\.default\software\policies\microsoft\control panel\desktop
Opens key: HKU\.default\control panel\desktop
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKCR\protocols\name-space handler\
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKU\.default\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKU\.default\software\policies\microsoft\internet
explorer\main\featurecontrol
Opens key: HKU\.default\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKU\.default\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
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: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm
Opens key: HKLM\system\currentcontrolset\control\productoptions
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKU\.default\software\microsoft\windows\currentversion\thememanager

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msxml3.dll
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers
Opens key: HKCR\directory\shellex\copyhookhandlers
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\cdf
Opens key: HKCR\directory\shellex\copyhookhandlers\cdf
Opens key: HKLM\software\microsoft\msxml30
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\treatas
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\treatas
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserverx86
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\localserver32
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\localserver32
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprochandler32
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprochandler32
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprochandlerx86
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\localserver
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\localserver
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{67ea19a0-ccef-11d0-8024-00c04fd75d13}
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\filesystem
Opens key: HKCR\directory\shellex\copyhookhandlers\filesystem
Opens key: HKCU\software\classes\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32
Opens key: HKCR\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\mydocuments
Opens key: HKCR\directory\shellex\copyhookhandlers\mydocuments
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\treatas
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\treatas
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserverx86
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver32
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver32
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprochandler32
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprochandler32
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprochandlerx86
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mydocs.dll
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ecf03a33-103d-11d2-854d-006008059367}
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\sharing
Opens key: HKCR\directory\shellex\copyhookhandlers\sharing
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\treatas
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\treatas
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserverx86
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\localserver32
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\localserver32
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandler32
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandler32
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandlerx86
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\localserver
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\atl.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntshrui.dll
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\software\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msimtf.dll
Opens key: HKLM\software\microsoft\ctf\tip
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile
Opens key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\localserver32
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandler32
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandlerx86
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\localserver
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
Opens key: HKLM\software\microsoft\ctf\tip\
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKCU\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
Opens key: HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
Opens key: HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
Opens key: HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
Opens key: HKCU\software\policies\microsoft\internet explorer\control panel
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\url
history
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserverx86
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver32
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandlerx86
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jscript.dll
Opens key: HKLM\software\microsoft\windows script\features
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
Opens key: HKLM\software\microsoft\internet explorer\activex compatibility
Opens key: HKLM\software\microsoft\internet explorer\activex
compatibility\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
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: HKCU\software\classes\appid\flashplayer18_a_install.exe
Opens key: HKCR\appid\flashplayer18_a_install.exe
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\treatas
Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32
Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserverx86
Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\localserver32
Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver32
Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler32
Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler32
Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandlerx86
Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\localserver
Opens key: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dxtrans.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
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}\treatas
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas
Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32
Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserverx86
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\localserver32
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\localserver32
Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler32
Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandlerx86
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\localserver
Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\localserver
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
Opens key: HKLM\software\microsoft\internet explorer\default behaviors
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}\treatas
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas
Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe\rpcthreadpoolthrottle
Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserverx86
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\localserver32
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver32
Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winsta.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler32

Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandlerx86
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver
Opens key: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKLM\system\currentcontrolset\control\securityproviders
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mswsock.dll
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\hnetcfg.dll
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wshtcpip.dll
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msv1_0.dll
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\environment
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\volatile environment
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\dllhost.exe
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\control panel\desktop
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\control panel\desktop
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dciman32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ddraw.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ddrawex.dll
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\software\microsoft\directdraw\compatibility
Opens key: HKLM\software\microsoft\directdraw\compatibility\bug!
Opens key: HKLM\software\microsoft\directdraw\compatibility\demolitionderby2
Opens key: HKLM\software\microsoft\directdraw\compatibility\mortalkombat3
Opens key: HKLM\software\microsoft\directdraw\compatibility\msgolf98
Opens key: HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
Opens key: HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
Opens key: HKLM\software\microsoft\directdraw\compatibility\rogue squadron
Opens key: HKLM\software\microsoft\directdraw\compatibility\savage
Opens key: HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
Opens key: HKLM\software\microsoft\directdraw\compatibility\silentthunder
Opens key: HKLM\software\microsoft\directdraw\compatibility\terracide
Opens key: HKLM\software\microsoft\directdraw\compatibility\thirddimension
Opens key: HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark
Opens key: HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark
Opens key: HKLM\software\microsoft\directdraw\gammacalibrator
Opens key: HKLM\software\microsoft\directdraw
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key: HKLM\software\microsoft\direct3d

Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllhost.exe
Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
Opens key: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
Opens key: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
Opens key: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserverx86
Opens key: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver32
Opens key: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver32
Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32
Opens key: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandlerx86
Opens key: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver
Opens key: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver
Opens key: HKLM\software\policies\microsoft\internet explorer\dxtrans
Opens key: HKCU\software\microsoft\internet explorer\dxtrans
Opens key: HKLM\software\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: HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}
Opens key: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}
Opens key: HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\treatas
Opens key: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\treatas
Opens key: HKLM\software\microsoft\internet explorer\activex compatibility\{623e2882-fc0e-11d1-9a77-0000f8756a10}
Opens key: HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32
Opens key: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32
Opens key: HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserverx86
Opens key: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\localserver32
Opens key: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\localserver32
Opens key: HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandler32
Opens key: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandler32
Opens key: HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandlerx86
Opens key: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\localserver
Opens key: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllhost.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\microsoft\ctf\compatibility\dllhost.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dxtmsft.dll
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet settings
Opens key: HKU\.default\software\policies
Opens key: HKU\.default\software
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}\treatas
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\treatas
Opens key: HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32
Opens key: HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserverx86
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\localserver32
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\localserver32
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache
Opens key: HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandler32
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandler32
Opens key: HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandlerx86
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-

00c04fd9189d}\localserver
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\localserver
Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\treatas
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32
Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserverx86
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\localserver32
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver32
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler32
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler32
Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandlerx86
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\localserver
Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012013122320131224
Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\treatas
Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas
Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32
Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32
Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserverx86
Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\localserver32
Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver32
Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler32
Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler32
Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandlerx86
Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\localserver
Opens key: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll
Opens key: HKCU\software\classes\typelib
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\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0
Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\0\win32
Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet
settings\wpad
Opens key: HKU\.default\software\microsoft\windows\currentversion\internet
settings\http filters\rpa
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
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\0
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
Opens key: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasman.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtutils.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tapi32.dll
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: HKLM\software\microsoft\windows\currentversion\telephony
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasapi32.dll
Opens key: HKLM\software\microsoft\tracing\rasapi32
Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
Opens key: HKCU\software\opera software
Opens key: HKCU\software\microsoft\ftp
Opens key: HKLM\software\policies\microsoft\internet explorer\services
Opens key: HKCU\software\microsoft\internet explorer\services
Opens key: HKLM\software\microsoft\internet explorer\services
Opens key: HKLM\software\policies\microsoft\internet explorer\activities
Opens key: HKCU\software\microsoft\internet explorer\activities
Opens key: HKLM\software\microsoft\internet explorer\activities
Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\microsoft\internet explorer\suggested sites
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sensapi.dll
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}\treatas
Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas
Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32
Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32
Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserverx86
Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver32
Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver32
Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler32
Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler32
Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandlerx86
Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver
Opens key: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasadhlp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation

Opens key: HKLM\software\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\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_script
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\ua tokens
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\pre platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\pre platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent\pre platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\post platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform
Opens key: HKCU\software\classes\http\shell\open\command
Opens key: HKCR\http\shell\open\command
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\connections
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\winhttp\unsafesslapps
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\connections
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\schannel.dll
Opens key: HKCU\software\microsoft\cryptography\providers\type 012
Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 012
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKCU\software\microsoft\cryptography\providers\type 018
Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 018
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft dh schannel cryptographic provider
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dssenh.dll
Opens key: HKLM\software\microsoft\cryptography\oid
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov\#16
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllopenstoreprov\ldap
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\certdllopenstoreprov
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdlldecodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
Opens key: HKLM\software\microsoft\cryptography\providers\trust\certificate\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\finalpolicy\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\initialization\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\message\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}

Opens key:
HKLM\software\microsoft\cryptography\providers\trust\signature\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key:
HKLM\software\microsoft\cryptography\providers\trust\certcheck\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key:
HKLM\software\microsoft\cryptography\providers\trust\diagnosticpolicy\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\cleanup\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}
Opens key: HKCU\software\microsoft\cryptography\providers\type 001
Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 001
Opens key: HKCU\software\microsoft\internet explorer\security
Opens key:
HKLM\software\policies\microsoft\systemcertificates\trustedpublisher\safer
Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKLM\software\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\certdllcreatecertificatechainengine\config
Opens key: HKCU\software\microsoft\systemcertificates\root\physicalstores
Opens key: HKLM\software\policies\microsoft\systemcertificates\root\protectedroots
Opens key: HKCU\software\microsoft\systemcertificates\root\protectedroots
Opens key: HKCU\software\microsoft\systemcertificates\root\
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\a43489159a520f0d93d032ccaf37e7fe20a8b419
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\cdd4eeae6000ac7f40c3802c171e30148030c072
Opens key: HKLM\software\microsoft\systemcertificates\authroot\
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\0048f8d37b153f6ea2798c323ef4f318a5624a9e
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\00ea522c8a9c06aa3ecce0b4fa6cdc21d92e8099
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\02faf3e291435468607857694df5e45b68851868
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\0483ed3399ac3608058722edbc5e4600e3bef9d7
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\049811056afe9fd0f5be01685aace6a5d1c4454c
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\0b77bebbcb7aa24705decc0fbd6a02fc7abd9b52
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\1331f48a5da8e01daaca1bb0c17044acfef755bb
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\1f55e8839bac30728be7108ede7b0bb0d3298224
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\209900b63d955728140cd13622d8c687a4eb0085
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\216b2a29e62a00ce820146d8244141b92511b279
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\23e594945195f2414803b4d564d2a3a3f5d88b8c
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\24a40a1f573643a67f0a4b0749f6a22bf28abb6b
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\24ba6d6c8a5b5837a48db5fae919ea675c94d217
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\273ee12457fdc4f90c55e82b56167f62f532e547
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\284f55c41a1a7a3f8328d4c262fb376ed6096f24
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\2f173f7de99667afa57af80aa2d1b12fac830338
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\317a2ad07f2b335ef5a1c34e4b57e8b7d8f1fca6
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\36863563fd5128c7bea6f005cfe9b43668086cce
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\394ff6850b06be52e51856cc10e180e882b385cc
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\3f85f2bb4a62b0b58be1614abb0d4631b4bef8ba
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4072ba31fec351438480f62e6cb95508461eab2f
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\40e78c1d523d1cd9954fac1a1ab3bd3cbaa15bfc
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\43ddb1fff3b49b73831407f6bc8b975023d07c50
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\43f9b110d5bafd48225231b0d0082b372fef9a54
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4463c531d7ccc1006794612bb656d3bf8257846f
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\47afb915cda26d82467b97fa42914468726138dd
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4b421f7515f6ae8a6ecef97f6982a400a4d9224e
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4ba7b9ddd68788e12ff852e1a024204bf286a8f6

Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4c95a9902abe0777ced18d6accc3372d2748381e
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4eb6d578499b1ccf5f581ead56be3d9b6744a5e5
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4ef2e6670ac9b5091fe06be0e5483eaad6ba32d9
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4efced9c6bdd0c985ca3c7d253063c5be6fc620c
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4f65566336db6598581d584a596c87934d5f2ab4
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\54f9c163759f19045121a319f64c2d0555b7e073
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\58119f0e128287ea50fdd987456f4f78dcfad6d4
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5b4e0ec28ebd8292a51782241281ad9feedd4e4c
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5d989cdb159611365165641b560fdbea2ac23ef1
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5e5a168867bfff00987d0b1dc2ab466c4264f956
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5e997ca5945aab75ffd14804a974bf2ae1dfe7e1
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\627f8d7827656399d27d7f9044c9feb3f33efa9a
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\6372c49da9fff051b8b5c7d4e5aae30384024b9c
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\6782aae0edeee21a5839d3c0cd14680a4f60142a
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\67eb337b684ceb0ec2b0760ab488278cdd9597dd
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\687ec17e0602e3cd3f7dfbd7e28d57a0199a3f44
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\688b6eb807e8eda5c7b17c4393d0795f0fae155f
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\68ed18b309cd5291c0d3357c1d1141bf883866b1
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\69bd8cf49cd300fb592e1793ca556af3ecaa35fb
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\6a174570a916fbe84453eed3d070a1d8da442829
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\720fc15ddc27d456d098fabf3cdd78d31ef5a8da
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\74207441729cdd92ec7931d823108dc28192e2bb
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\742c3192e607e424eb4549542be1bbc53e6174e2
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7639c71847e151b5c7ea01c758fbf12aba298f7a
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\78e9dd0650624db9cb36b50767f209b843be15b3
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7a74410fb0cd5c972a364b71bf031d88a6510e9e
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7ac5fff8dcbc5583176877073bf751735e9bd358
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7ca04fd8064c1caa32a37aa94375038e8df8ddc0
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7e784a101c8265cc2de1f16d47b440cad90a1945
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\81968b3aef1cdc70f5fa3269c292a3635bd123d3
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\838e30f77fdd14aa385ed145009c0e2236494faa
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\85371ca6e550143dce2803471bde3a09e8f8770f
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\85a408c09c193e5d51587dcdd61330fd8cde37bf
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\879f4bee05df98583be360d633e70d3ffe9871af
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\8eb03fc3cf7bb292866268b751223db5103405cb
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\9078c5a28f9a4325c2a7c73813cdfe13c20f934e
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\90aea26985ff14804c434952ece9608477af556f
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\90dede9e4c4e9f6fd88617579dd391bc65a68964
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\96974cd6b663a7184526b1d648ad815cf51e801a
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\97817950d81c9670cc34d809cf794431367ef474
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\97e2e99636a547554f838fba38b82e74f89a830a
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\99a69be61afe886b4d2b82007cb854fc317e1539
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\9bacf3b664eac5a17bed08437c72e4acda12f7e7
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\9e6ceb179185a29ec6060ca53e1974af94af59d4
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\9fc796e8f8524f863ae1496d381242105f1b78f5
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\a399f76f0cbf4c9da55e4ac24e8960984b2905b6

Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\a3e31e20b2e46a328520472d0cde9523e7260c6d
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\a5ec73d48c34fcbef1005aeb85843524bbfab727
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\ab48f333db04abb9c072da5b0cc1d057f0369b46
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\aced5f6553fd25ce015f1f7a483b6a749f6178c6
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b172b1a56d95f91fe50287e14d37ea6a4463768a
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b19dd096dcd4e3e0fd676885505a672c438d4e9c
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b3eac44776c9c81ceaf29d95b6cca0081b67ec9d
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b5d303bf8682e152919d83f184ed05f1dce5370c
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b6af5be5f878a00114c3d7fef8c775c34ccd17b6
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b72fff92d2ce43de0a8d4c548c503726a81e2b93
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\bc9219ddc98e14bf1a781f6e280b04c27f902712
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\be36a4562fb2ee05dbb3d32323adf445084ed656
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cabb51672400588e6419f1d40878d0403aa20264
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cfdefe102fda05bbe4c78d2e4423589005b2571d
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cff360f524cb20f1fead89006f7f586a285b2d5b
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cff810fb2c4ffc0156bfe1e1fabcb418c68d31c5
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d23209ad23d314232174e40d7f9d62139786633a
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d29f6c98befc6d986521543ee8be56cebc288cf3
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d2edf88b41b6fe01461d6e2834ec7c8f6c77721e
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d4de20d05e66fc53fe1a50882c78db2852cae474
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\da40188b9189a3edeeaeda97fe2f9df5b7d18a41
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\dbac3c7aa4254da1aa5caad68468cb88eeddeea8
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\de28f4a4ffe5b92fa3c503d1a349a7f9962a8212
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e12dfb4b41d7d9c32b30514bac1d81d8385e2d46
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e392512f0acff505dff6de067f7537e165ea574b
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e4554333ca390e128b8bf81d90b70f4002d1d6e9
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e5df743cb601c49b9843dcab8ce86a81109fe48e
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\ebbc0e2d020ca69b222c2bffd203cb8bf5a82766
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\ec0c3716ea9edfadd35dfbd55608e60a05d3cbf3
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\ef2daccbeabb682d32ce4abd6cb90025236c07bc
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\f44095c238ac73fc4f77bf8f98df70f8f091bc52
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\f88015d3f98479e1da553d24fd42ba3f43886aef
Opens key: HKLM\software\microsoft\enterprisecertificates\root\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\root\
Opens key: HKCU\software\microsoft\systemcertificates\ca\physicalstores
Opens key: HKCU\software\microsoft\systemcertificates\ca\
Opens key: HKLM\software\microsoft\systemcertificates\ca\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\ca\
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\063da67748f0eccc690d319bcdcd0e72ac8d48d5
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\109f1caed645bb78b3ea2b94c0697c740733031c
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\12519ae9cd777a560184f1fbd54215222e95e71f
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\189271e573fed295a8c130eaf357a20c4a9f115e
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\2d69a20ec4f0cd19037fd6d6246b1ee0ec41ba22
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\7b02312bacc59ec388feae12fd277f6a9fb4fac1
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\8b24cd8d8b58c6da72ace097c7b1e3cea4dc3dc6
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\9f025d9f58711a605eb0694b0e8bc0ca4f25fd6f
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\ba9e3c32562a67128caabd4ab0c500bee1d0c256
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\e5215d3460c2c20bbe2d9fe5fb665daa2c0e225c
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\f6357239b7c39725bd8000646e4a0d18ebce4cfa
Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\fe622ea7b33ca46519ab39736a66b8f6e41ff157

Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\fee449ee0e3965a5246f000e87fde2a065fd89d4
Opens key:
HKLM\software\microsoft\systemcertificates\ca\crls\a377d1b1c0538833035211f4083d00fecc414dab
Opens key: HKLM\software\microsoft\enterprisecertificates\ca\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\ca\
Opens key: HKCU\software\microsoft\systemcertificates\disallowed\physicalstores
Opens key: HKCU\software\microsoft\systemcertificates\disallowed\
Opens key: HKLM\software\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\microsoft\enterprisecertificates\disallowed\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\
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
Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed
Opens key:
HKCU\software\policies\microsoft\systemcertificates\disallowed\certificates
Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed\crls
Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed\ctls
Opens key: HKLM\software\microsoft\systemcertificates\disallowed\certificates
Opens key: HKLM\software\microsoft\systemcertificates\disallowed\crls
Opens key: HKLM\software\microsoft\systemcertificates\disallowed\ctls
Opens key: HKLM\software\policies\microsoft\systemcertificates
Opens key: HKLM\software\policies\microsoft\systemcertificates\disallowed
Opens key:
HKLM\software\policies\microsoft\systemcertificates\disallowed\certificates
Opens key: HKLM\software\policies\microsoft\systemcertificates\disallowed\crls
Opens key: HKLM\software\policies\microsoft\systemcertificates\disallowed\ctls
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\certificates
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\crls
Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\ctls
Opens key: HKCU\software\microsoft\systemcertificates\trust\physicalstores
Opens key: HKCU\software\microsoft\systemcertificates\trust\
Opens key: HKLM\software\microsoft\systemcertificates\trust\physicalstores
Opens key: HKLM\software\microsoft\systemcertificates\trust\
Opens key: HKLM\software\microsoft\enterprisecertificates\trust\physicalstores
Opens key: HKLM\software\microsoft\enterprisecertificates\trust\
Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores
Opens key: HKCU\environment
Opens key: HKCU\volatile environment
Opens key: HKCU\software\microsoft\systemcertificates\my
Opens key: HKCU\software\microsoft\systemcertificates\my\
Opens key: HKCU\software\microsoft\systemcertificates\my\certificates
Opens key: HKCU\software\microsoft\systemcertificates\my\crls
Opens key: HKCU\software\microsoft\systemcertificates\my\ctls
Opens key: HKCU\software\microsoft\systemcertificates\my\keys
Opens key: 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\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: 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\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\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\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: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllimportpublickeyinfoex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllimportpublickeyinfoex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllconvertpublickeyinfo
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllconvertpublickeyinfo
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllverifycertificatechainpolicy
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\certdllverifycertificatechainpolicy
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\treatas
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandlerx86
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\localserver
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iepeers.dll
Opens key: HKCU\software\policies\microsoft\internet explorer\persistence
Opens key: HKLM\software\policies\microsoft\internet explorer\persistence
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: 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\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
Opens key: HKCU\software\microsoft\windows\currentversion\urlmon settings
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
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\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\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
Opens key: HKLM\software\\macromedia\\flashplayerplugin
Opens key: HKLM\software\policies\microsoft\internet explorer\recovery
Opens key: HKCU\software\microsoft\internet explorer\recovery
Opens key: HKLM\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: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imgutil.dll
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}

Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandlerx86
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
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\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\pngfilt.dll
Opens key: HKCU\software\microsoft\cryptography\providers\type 024

Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 024
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft enhanced rsa and aes cryptographic provider (prototype)
Opens key: HKCU\software\microsoft\internet explorer\ietld\lowmic
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\p3p\history\adobe.com
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
Opens key: HKCU\software\microsoft\internet explorer\searchproviders\
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
Queries value: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]

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\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewwatermark]
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[usedoubleclicktimer]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
Queries value: HKLM\system\wpa\pnp[seed]
Queries value: HKLM\system\setup[osloaderpath]
Queries value: HKLM\system\setup[systempartition]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[generation]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value:
HKCU\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: HKCR\directory[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
Queries value: HKCR\.exe[]
Queries value: HKCR\exefile[docobject]
Queries value: HKCR\exefile[browseinplace]
Queries value: HKCR\exefile[isshortcut]
Queries value: HKCR\exefile[alwaysshowext]
Queries value: HKCR\exefile[nevershowext]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32[loadwithoutcom]
Queries value: HKCR\.asp[]
Queries value: HKCR\.bat[]
Queries value: HKCR\.cer[]
Queries value: HKCR\.chm[]
Queries value: HKCR\.cmd[]
Queries value: HKCR\.com[]
Queries value: HKCR\.cpl[]
Queries value: HKCR\.crt[]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
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\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1806]
Queries value: HKCR\exefile\shell\open\command[]
Queries value: HKCR\exefile\shell\open\command[command]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program files\flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]
Queries value: HKLM\system\currentcontrolset\control\session manager\appcompatibility[disableappcompat]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[itemdata]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[saferflags]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemdata]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[hashalg]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemsize]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[saferflags]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemdata]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[hashalg]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemsize]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[saferflags]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemsize]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[saferflags]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemdata]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsize]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemdata]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[hashalg]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemsize]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[saferflags]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
Queries value: HKLM\software\microsoft\windows\currentversion\app
paths\install.exe[runascommand]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program
files\install.exe]
Queries value: HKLM\software\microsoft\windows\currentversion\app
paths\install.exe[useshortname]
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\microsoft\windows\currentversion\app
paths\install.exe[runasonnonadmininstall]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[flashplayer18_a_install]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[flashplayer18_a_install]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[debugger]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[executeoptions]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[disableheaplookaside]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[shutdownflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[minimumstackcommitinbytes]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[globalflag]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[debugprocessheaponly]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[applicationgoo]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[install]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[install]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norun]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nodrives]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetconnectdisconnect]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[norecentdocshistory]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[appid]
Queries value: HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
Queries value: HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
Queries value: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[appid]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
Queries value: HKCR\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
Queries value: HKLM\software\microsoft\internet explorer\setup[installstarted]
Queries value: HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
Queries value: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
Queries value: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
Queries value: HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]

Queries value: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[appid]
Queries value: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[alwaysdropup]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[flashplayer18_a_install.exe]
Queries value: HKCU\software\microsoft\internet explorer\main[frametabwindow]
Queries value: HKLM\software\microsoft\internet explorer\main[frametabwindow]
Queries value: HKCU\software\microsoft\internet explorer\main[framemerging]
Queries value: HKLM\software\microsoft\internet explorer\main[framemerging]
Queries value: HKCU\software\microsoft\internet explorer\main[sessionmerging]
Queries value: HKLM\software\microsoft\internet explorer\main[sessionmerging]
Queries value: HKCU\software\microsoft\internet explorer\main[admintabprocs]
Queries value: HKLM\software\microsoft\internet explorer\main[admintabprocs]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
Queries value: HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
Queries value: HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
Queries value: HKLM\software\microsoft\internet explorer\main[navigationdelay]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046} 0x401]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046} 0x401]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[fromcachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[secureprotocols]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[security_hklm_only]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[certificaterevocation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablekeepalive]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablepassport]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cachemode]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablenegotiate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablebasicoverclearchannel]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[syncmode5]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache[sessionstarttimedefaultdeltasecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\cache\history[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[history]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[requiredfile]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[version]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[contextmenu]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[corelinternetenum]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[oldcreateviewwnd]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[win95defview]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[docobject]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[flushnowaitalways]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[mycomputerfirst]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[oldregitemgdn]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[loadcolumnhandler]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[ansi]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[staroffice5printer]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[novalidatefsids]
Queries value: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[win95shlexec]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[fileopenneedsext]
Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[win95bindtoobject]
Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[ignoreenumreset]
Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[ansidisplaynames]
Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[fileopenbogusctrlid]
Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[forcelfnidlist]
Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe\starcraft
1.03[requiredfile]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[leashlegacycookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablent4rascheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[sendextracrlf]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypassftptimecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[releasesocketduringauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[releasesocketduring401auth]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[releasesocketduring401auth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[wpadsearchalldomains]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[disablelegacypreauthasserver]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disablelegacypreauthasserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[bypassssl nocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[bypassssl nocachecheck]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[enablehttptrace]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[sharecredswithwinhttp]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[mimeexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[headerexclusionlistforcache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscacheenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscacheentries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscachetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnalwaysonpost]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonzonecrossing]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonbadcertsending]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonbadcertrecving]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpostredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[alwaysdrainonredirect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonhttpstohttpredirect]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
Queries value: HKCR\protocols\handler\res[clsid]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[appid]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[install.exe]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
Queries value: HKLM\software\microsoft\internet explorer\application
compatibility[flashplayer18_a_install.exe]
Queries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit]

Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[install.exe]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[urlencoding]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[flashplayer18_a_install.exe]
Queries value: HKCR\exefile\shell[]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[flashplayer18_a_install.exe]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\rarsfx0\msmpeng.exe]
Queries value: HKCU\software\microsoft\internet explorer[no3dborder]
Queries value: HKLM\software\microsoft\internet explorer[no3dborder]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[*]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[istextplainhonored]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_feeds[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_feeds[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject[*]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
Queries value: HKCR\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[dragscrolldelay]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragscrollinterval]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[inprocserver32]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[*]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
Queries value: HKCR\protocols\handler\about[clsid]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[appid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[msmpeng]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[msmpeng]
Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{75048700-ef1f-11d0-9888-006097deacf9}[version]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-00aa004ae837}[version]
Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2106]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3[2106]
Queries value: HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
Queries value: HKLM\software\microsoft\internet explorer\registration[productid]
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: HKLM\software\policies\microsoft\internet explorer\main[usecleartype]
Queries value: HKCU\software\microsoft\internet explorer\main[usecleartype]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[page_transitions]
Queries value: HKCU\software\microsoft\internet explorer\main[page_transitions]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[use_dlgbox_colors]

Queries value: HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[anchor underline]
Queries value: HKCU\software\microsoft\internet explorer\main[anchor underline]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noinstrumentation]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{75048700-ef1f-11d0-9888-006097deacf9}\count[hrzr_pgyfrffvba]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-00aa004ae837}\count[hrzr_pgyfrffvba]
Queries value: HKCU\software\microsoft\internet explorer\main[css_compat]
Queries value: HKCU\software\microsoft\internet explorer\main[expand alt text]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[display inline images]
Queries value: HKCU\software\microsoft\internet explorer\main[display inline images]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[display inline videos]
Queries value: HKCU\software\microsoft\internet explorer\main[display inline videos]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[play_background_sounds]
Queries value: HKCU\software\microsoft\internet explorer\main[play_background_sounds]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[play_animations]
Queries value: HKCU\software\microsoft\internet explorer\main[play_animations]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[print_background]
Queries value: HKCU\software\microsoft\internet explorer\main[print_background]
Queries value: HKCU\software\microsoft\internet explorer\main[use stylesheets]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[smoothscroll]
Queries value: HKCU\software\microsoft\internet explorer\main[smoothscroll]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[xmlhttp]
Queries value: HKCU\software\microsoft\internet explorer\main[xmlhttp]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[show image placeholders]
Queries value: HKCU\software\microsoft\internet explorer\main[show image placeholders]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[disable script debugger]
Queries value: HKCU\software\microsoft\internet explorer\main[disable script debugger]
Queries value: HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
Queries value: HKCU\software\microsoft\internet explorer\main[move system caret]
Queries value: HKCU\software\microsoft\internet explorer\main[force offscreen composition]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[enable autoimageresize]
Queries value: HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
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: HKCU\software\microsoft\internet explorer\main[cleanup htcs]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest]
Queries value: HKCU\software\microsoft\internet explorer\main[xdomainrequest]
Queries value: HKLM\software\microsoft\internet explorer\main[xdomainrequest]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[domstorage]
Queries value: HKCU\software\microsoft\internet explorer\main[domstorage]
Queries value: HKLM\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: 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: 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\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefontsize]
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: HKCU\software\microsoft\internet explorer\international[acceptlanguage]
Queries value: HKLM\software\microsoft\internet explorer\version vector[vml]
Queries value: HKLM\software\microsoft\internet explorer\version vector[ie]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[2700]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[2700]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones[securitysafe]
Queries value: HKCR\msxml2.domdocument.3.0\clsid[]
Queries value: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32[]
Queries value: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}[appid]
Queries value: HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32[threadingmodel]
Queries value: HKU\.default\control panel\desktop[multiuilanguageid]
Queries value: HKU\.default\control panel\desktop[smoothscroll]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[msmpeng.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[svchost]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[svchost]
Queries value: HKU\.default\software\microsoft\multimedia\audio[systemformats]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.imaadpcm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msadpcm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg711]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msgsm610]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.trspch]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg723]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.sl_anet]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
Queries value: HKU\.default\software\microsoft\multimedia\audio compression manager\msacm[nopcmconverter]
Queries value: HKU\.default\software\microsoft\multimedia\audio compression manager\priority v4.00[priority1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[chkaccdebuglevel]
Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders[personal]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders[local settings]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsopdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
Queries value: HKU\.default\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKU\.default\control panel\desktop[lamebuttontext]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[svchost.exe]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[nofilefolderconnection]
Queries value: HKCR\directory\shellex\copyhookhandlers\cdf[]
Queries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[]
Queries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked[{67ea19a0-ccef-11d0-8024-00c04fd75d13}]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked[{67ea19a0-ccef-11d0-8024-00c04fd75d13}]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\cached[{67ea19a0-ccef-11d0-8024-00c04fd75d13} {00000000-0000-0000-c000-000000000046} 0x401]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{67ea19a0-ccef-11d0-8024-00c04fd75d13} {00000000-0000-0000-c000-000000000046} 0x401]
Queries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}[appid]
Queries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[threadingmodel]
Queries value: HKCR\directory\shellex\copyhookhandlers\filesystem[]
Queries value: HKCR\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32[]
Queries value: HKCR\directory\shellex\copyhookhandlers\mydocuments[]
Queries value: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32[]
Queries value: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked[{ecf03a33-103d-11d2-854d-006008059367}]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked[{ecf03a33-103d-11d2-854d-006008059367}]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\cached[{ecf03a33-103d-11d2-854d-006008059367} {00000000-0000-0000-c000-000000000046} 0x401]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{ecf03a33-103d-11d2-854d-006008059367} {00000000-0000-0000-c000-000000000046} 0x401]
Queries value: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}[appid]
Queries value: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32[threadingmodel]
Queries value: HKCR\directory\shellex\copyhookhandlers\sharing[]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-

00aa003ca9f6}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked[{40dd6e20-7c17-11ce-a804-00aa003ca9f6}]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked[{40dd6e20-7c17-11ce-a804-00aa003ca9f6}]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\cached[{40dd6e20-7c17-11ce-a804-00aa003ca9f6} {00000000-0000-0000-c000-000000000046} 0x401]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{40dd6e20-7c17-11ce-a804-00aa003ca9f6} {00000000-0000-0000-c000-000000000046} 0x401]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}[appid]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local settings]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileimagepath]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[fonts]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[startup]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[programs]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[start menu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[recent]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[sendto]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[favorites]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[nethood]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[printhood]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[templates]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common startup]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common programs]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common start menu]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common favorites]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common appdata]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common templates]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[altstartup]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common altstartup]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[my pictures]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[administrative tools]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common administrative tools]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[profilesdirectory]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[allusersprofile]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[my music]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[my video]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[commonpictures]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[commonmusic]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[commonvideo]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[oem links]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cd burning]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[2106]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[2106]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1400]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonintranet]
Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings[warnonintranet]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]
Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]
Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\url history[daystokeep]
Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]
Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1201]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]
Queries value: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]
Queries value: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[appid]
Queries value: HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]
Queries value: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[appid]
Queries value: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[2000]
Queries value: HKLM\software\microsoft\internet explorer\default behaviors[dxtfilterbehavior]
Queries value: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[inprocserver32]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[enabledhcp]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseobtainedtime]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseterminatestime]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserver]
Queries value: HKLM\software\microsoft\rpc\securityservice[10]
Queries value: HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
Queries value: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[appid]
Queries value: HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[threadingmodel]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]
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\tcpip\parameters[ipenablerouter]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[enableproxy]
Queries value: HKLM\system\currentcontrolset\services\netbt\parameters[enabledns]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[defaultuserprofile]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows nt\currentversion\winlogon[parseautoexec]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\control panel\desktop[multiuilanguageid]
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]
Queries value: HKLM\hardware\devicemap\video[\device\video0]
Queries value: HKLM\hardware\devicemap\video[\device\video1]
Queries value: HKLM\hardware\devicemap\video[\device\video2]
Queries value: HKLM\software\microsoft\directdraw\compatibility\bug![name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\bug![flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\bug![id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\msgolf98[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\savage[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\savage[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\savage[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\silentthunder[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\silentthunder[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\terracide[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\terracide[flags]
Queries value: HKLM\software\microsoft\directdraw\compatibility\terracide[id]
Queries value: HKLM\software\microsoft\directdraw\compatibility\thirddimension[name]
Queries value: HKLM\software\microsoft\directdraw\compatibility\thirddimension[flags]

Queries value: HKLM\software\microsoft\directdraw\compatibility\thirddimension[id]
Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
Queries value: HKLM\software\microsoft\directdraw[modexonly]
Queries value: HKLM\software\microsoft\directdraw[emulationonly]
Queries value: HKLM\software\microsoft\directdraw[showframerate]
Queries value: HKLM\software\microsoft\directdraw[enableprintscreen]
Queries value: HKLM\software\microsoft\directdraw[forceagpsupport]
Queries value: HKLM\software\microsoft\directdraw[disableagpsupport]
Queries value: HKLM\software\microsoft\directdraw[disablemmx]
Queries value: HKLM\software\microsoft\directdraw[disableddscapsinddsd]
Queries value: HKLM\software\microsoft\directdraw[disablewidersurfaces]
Queries value: HKLM\software\microsoft\directdraw[usenonlocalvidmem]
Queries value: HKLM\software\microsoft\directdraw[forcerefreshrate]
Queries value: HKLM\software\microsoft\direct3d[flipnovsync]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value: HKLM\software\microsoft\directdraw[owndc]
Queries value: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
Queries value: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[appid]
Queries value: HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[dllhost]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[dllhost]
Queries value: HKCR\dximagetransform.microsoft.gradient\clsid[]
Queries value: HKCR\clsid\{623e2882-fc0e-11d1-9a77-
0000f8756a10}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32[]
Queries value: HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}[appid]
Queries value: HKCR\clsid\{623e2882-fc0e-11d1-9a77-
0000f8756a10}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\multimedia\audio[systemformats]
Queries value: HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
Queries value: HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00[priority1]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[dllhost.exe]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablepassport]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[idnenabled]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[cachemode]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
Queries value: HKCR\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\inprocserver32[inprocserver32]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings[syncmode5]
Queries value: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32[]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-

1003\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}[appid]
Queries value: HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cacheprefix]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[cachelimit]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\explorer\user shell folders[cookies]
Queries value: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[appid]
Queries value: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[threadingmodel]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cacheprefix]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[cachelimit]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[peruseritem]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\explorer\user shell folders[history]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cacheprefix]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\history[cachelimit]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacherepair]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cachepath]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheprefix]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cachelimit]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheoptions]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012013122320131224[cacherepair]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012013122320131224[cachepath]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012013122320131224[cacheprefix]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012013122320131224[cachelimit]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012013122320131224[cacheoptions]
Queries value: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[inprocserver32]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[disableworkerthreadhibernation]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[disablereadrange]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[socketsendbufferlength]
Queries value: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[socketreceivebufferlength]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[keepalivetimeout]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[maxhttpredirects]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[maxconnectionsperserver]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[maxconnectionsper1_0server]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[maxconnectionsperproxy]
Queries value: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[appid]
Queries value: HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[threadingmodel]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[serverinfotimeout]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[connecttimeout]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[connectretries]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[sendtimeout]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[receivetimeout]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[disablentlmpreauth]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[scavengecachelowerbound]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[certcachenovalidate]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelifetime]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings\5.0\cache[scavengecachefilelimit]

Queries value: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[httpdefaultexpirytimesecs]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[ftpdefaultexpirytimesecs]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[svchost.exe]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disablecachingofsslpages]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[perusercookies]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[leashlegacycookies]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[disablent4rascheck]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[dialupuselansettings]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[sendextracrlf]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[bypassftptimecheck]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[releasesocketduringauth]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[releasesocketduring401auth]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[wpadsearchalldomains]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[disablelegacypreauthasserver]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[bypasshttpnocachecheck]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[bypassssslnocachecheck]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[mimeexclusionlistforcache]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[headerexclusionlistforcache]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[dnscacheenabled]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[dnscacheentries]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[dnscachetimeout]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[warnonpost]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[warnalwaysonpost]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[warnonzonecrossing]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[warnonbadcertsending]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[warnonbadcertrecving]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[warnonpostredirect]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[alwaysdrainonredirect]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[warnonhttpstohttpredirect]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[globaluseroffline]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[enableautodial]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[truncatefilename]
Queries value: HKU\.default\software\microsoft\windows\currentversion\internet settings[badproxyexpirestime]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[svchost.exe]
Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
Queries value: HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
Queries value: HKLM\software\microsoft\tracing[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
Queries value: HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
Queries value: HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
Queries value: HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
Queries value: HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
Queries value: HKLM\software\microsoft\tracing\rasapi32[filedirectory]
Queries value: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]

Queries value: HKCU\software\microsoft\ftp[use web based ftp]
Queries value: HKCU\software\microsoft\internet explorer\services[selectionactivitybuttondisable]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]
Queries value: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[]
Queries value: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[appid]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Queries value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Queries value: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[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[filterclusterip]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipautoconfigurationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user agent]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKCU\software\microsoft\windows script\settings[jitdebug]
Queries value: HKCR\http\shell\open\command[]
Queries value: HKLM\software\microsoft\internet explorer\main[maxrenderline]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\connections[winhttpsettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type 012[name]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider[image path]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type 018[name]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft dh schannel cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft dh schannel cryptographic provider[image path]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\certificate\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:

HKLM\software\microsoft\cryptography\providers\trust\certificate\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\finalpolicy\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\finalpolicy\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\initialization\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\initialization\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value: HKLM\software\microsoft\cryptography\providers\trust\message\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value: HKLM\software\microsoft\cryptography\providers\trust\message\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\signature\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\signature\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\certcheck\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value:
HKLM\software\microsoft\cryptography\providers\trust\certcheck\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value: HKLM\software\microsoft\cryptography\providers\trust\cleanup\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$dll]
Queries value: HKLM\software\microsoft\cryptography\providers\trust\cleanup\{573e31f8-aaba-11d0-8ccb-00c04fc295ee}[$function]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type 001[name]
Queries value: HKCU\software\microsoft\windows\currentversion\wintrust\trust providers\software publishing[state]
Queries value: HKCU\software\microsoft\internet explorer\security[safety warning level]
Queries value:
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\a43489159a520f0d93d032ccaf37e7fe20a8b419[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\root\certificates\cdd4eeae6000ac7f40c3802c171e30148030c072[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\0048f8d37b153f6ea2798c323ef4f318a5624a9e[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\00ea522c8a9c06aa3ecce0b4fa6cdc21d92e8099[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\02faf3e291435468607857694df5e45b68851868[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\0483ed3399ac3608058722edbc5e4600e3bef9d7[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\049811056afe9fd0f5be01685aace6a5d1c4454c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\0b77bebbcb7aa24705decc0fbd6a02fc7abd9b52[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\1331f48a5da8e01daaca1bb0c17044acfef755bb[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\1f55e8839bac30728be7108ede7b0bb0d3298224[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\209900b63d955728140cd13622d8c687a4eb0085[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\216b2a29e62a00ce820146d8244141b92511b279[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\23e594945195f2414803b4d564d2a3a3f5d88b8c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\24a40a1f573643a67f0a4b0749f6a22bf28abb6b[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\24ba6d6c8a5b5837a48db5fae919ea675c94d217[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\273ee12457fdc4f90c55e82b56167f62f532e547[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\284f55c41a1a7a3f8328d4c262fb376ed6096f24[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\2f173f7de99667afa57af80aa2d1b12fac830338[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\317a2ad07f2b335ef5a1c34e4b57e8b7d8f1fca6[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\36863563fd5128c7bea6f005cfe9b43668086cce[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\394ff6850b06be52e51856cc10e180e882b385cc[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\3f85f2bb4a62b0b58be1614abb0d4631b4bef8ba[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4072ba31fec351438480f62e6cb95508461eab2f[blob]
Queries value:

HKLM\software\microsoft\systemcertificates\authroot\certificates\40e78c1d523d1cd9954fac1a1ab3bd3cbaa15bfc[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\43ddb1fff3b49b73831407f6bc8b975023d07c50[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\43f9b110d5bafd48225231b0d0082b372fef9a54[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4463c531d7ccc1006794612bb656d3bf8257846f[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\47afb915cda26d82467b97fa42914468726138dd[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4b421f7515f6ae8a6ecef97f6982a400a4d9224e[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4ba7b9ddd68788e12ff852e1a024204bf286a8f6[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4c95a9902abe0777ced18d6accc3372d2748381e[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4eb6d578499b1ccf5f581ead56be3d9b6744a5e5[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4ef2e6670ac9b5091fe06be0e5483eaad6ba32d9[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4efced9c6bdd0c985ca3c7d253063c5be6fc620c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\4f65566336db6598581d584a596c87934d5f2ab4[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\54f9c163759f19045121a319f64c2d0555b7e073[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\58119f0e128287ea50fdd987456f4f78dcfad6d4[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5b4e0ec28ebd8292a51782241281ad9feedd4e4c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5d989cdb159611365165641b560fdbea2ac23ef1[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5e5a168867bfff00987d0b1dc2ab466c4264f956[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5e997ca5945aab75ffd14804a974bf2ae1dfe7e1[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\627f8d7827656399d27d7f9044c9feb3f33efa9a[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\6372c49da9fff051b8b5c7d4e5aae30384024b9c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\6782aae0edeee21a5839d3c0cd14680a4f60142a[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\67eb337b684ceb0ec2b0760ab488278cdd9597dd[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\687ec17e0602e3cd3f7dfbd7e28d57a0199a3f44[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\688b6eb807e8eda5c7b17c4393d0795f0fae155f[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\68ed18b309cd5291c0d3357c1d1141bf883866b1[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\69bd8cf49cd300fb592e1793ca556af3ecaa35fb[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\6a174570a916fbe84453eed3d070a1d8da442829[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\720fc15ddc27d456d098fabf3cdd78d31ef5a8da[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\74207441729cdd92ec7931d823108dc28192e2bb[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\742c3192e607e424eb4549542be1bbc53e6174e2[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7639c71847e151b5c7ea01c758fbf12aba298f7a[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\78e9dd0650624db9cb36b50767f209b843be15b3[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7a74410fb0cd5c972a364b71bf031d88a6510e9e[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7ac5fff8dcbc5583176877073bf751735e9bd358[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7ca04fd8064c1caa32a37aa94375038e8df8ddc0[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\7e784a101c8265cc2de1f16d47b440cad90a1945[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\81968b3aef1cdc70f5fa3269c292a3635bd123d3[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\838e30f77fdd14aa385ed145009c0e2236494faa[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\85371ca6e550143dce2803471bde3a09e8f8770f[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\85a408c09c193e5d51587dcdd61330fd8cde37bf[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\879f4bee05df98583be360d633e70d3ffe9871af[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\8eb03fc3cf7bb292866268b751223db5103405cb[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\9078c5a28f9a4325c2a7c73813cdfe13c20f934e[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\90aea26985ff14804c434952ece9608477af556f[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\90dede9e4c4e9f6fd88617579dd391bc65a68964[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\96974cd6b663a7184526b1d648ad815cf51e801a[blob]
Queries value:

HKLM\software\microsoft\systemcertificates\authroot\certificates\97817950d81c9670cc34d809cf794431367ef474[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\97e2e99636a547554f838fba38b82e74f89a830a[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\99a69be61afe886b4d2b82007cb854fc317e1539[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\9bacf3b664eac5a17bed08437c72e4acda12f7e7[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\9e6ceb179185a29ec6060ca53e1974af94af59d4[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\9fc796e8f8524f863ae1496d381242105f1b78f5[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\a399f76f0cbf4c9da55e4ac24e8960984b2905b6[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\a3e31e20b2e46a328520472d0cde9523e7260c6d[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\a5ec73d48c34fcbef1005aeb85843524bbfab727[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\ab48f333db04abb9c072da5b0cc1d057f0369b46[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\aced5f6553fd25ce015f1f7a483b6a749f6178c6[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b172b1a56d95f91fe50287e14d37ea6a4463768a[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b19dd096dcd4e3e0fd676885505a672c438d4e9c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b3eac44776c9c81ceaf29d95b6cca0081b67ec9d[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b5d303bf8682e152919d83f184ed05f1dce5370c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b6af5be5f878a00114c3d7fef8c775c34ccd17b6[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\b72fff92d2ce43de0a8d4c548c503726a81e2b93[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\bc9219ddc98e14bf1a781f6e280b04c27f902712[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\be36a4562fb2ee05dbb3d32323adf445084ed656[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cabb51672400588e6419f1d40878d0403aa20264[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cfdefe102fda05bbe4c78d2e4423589005b2571d[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cff360f524cb20f1fead89006f7f586a285b2d5b[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cff810fb2c4ffc0156bfe1e1fabcb418c68d31c5[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d23209ad23d314232174e40d7f9d62139786633a[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d29f6c98befc6d986521543ee8be56cebc288cf3[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d2edf88b41b6fe01461d6e2834ec7c8f6c77721e[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\d4de20d05e66fc53fe1a50882c78db2852cae474[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\da40188b9189a3edeeaaeda97fe2f9df5b7d18a41[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\dbac3c7aa4254da1aa5caad68468cb88eeddeea8[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\de28f4a4ffe5b92fa3c503d1a349a7f9962a8212[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e12dfb4b41d7d9c32b30514bac1d81d8385e2d46[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e392512f0acff505dff6de067f7537e165ea574b[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e4554333ca390e128b8bf81d90b70f4002d1d6e9[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e5df743cb601c49b9843dcab8ce86a81109fe48e[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\ebbc0e2d020ca69b222c2bffd203cb8bf5a82766[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\ec0c3716ea9edfadd35dfbd55608e60a05d3cbf3[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\ef2daccbeabb682d32ce4abd6cb90025236c07bc[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\f44095c238ac73fc4f77bf8f98df70f8f091bc52[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\f88015d3f98479e1da553d24fd42ba3f43886aef[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\063da67748f0eccc690d319bcdcd0e72ac8d48d5[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\109f1caed645bb78b3ea2b94c0697c740733031c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\12519ae9cd777a560184f1fbd54215222e95e71f[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\189271e573fed295a8c130eaf357a20c4a9f115e[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\2d69a20ec4f0cd19037fd6d6246b1ee0ec41ba22[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\7b02312bacc59ec388feae12fd277f6a9fb4fac1[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\8b24cd8d8b58c6da72ace097c7b1e3cea4dc3dc6[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\9f025d9f58711a605eb0694b0e8bc0ca4f25fd6f[blob]
Queries value:

HKLM\software\microsoft\systemcertificates\ca\certificates\ba9e3c32562a67128caabd4ab0c500bee1d0c256[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\e5215d3460c2c20bbe2d9fe5fb665daa2c0e225c[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\f6357239b7c39725bd8000646e4a0d18ebce4cfa[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\fe622ea7b33ca46519ab39736a66b8f6e41ff157[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\fee449ee0e3965a5246f000e87fde2a065fd89d4[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\ca\crls\a377d1b1c0538833035211f4083d00fecc414dab[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\disallowed\certificates\637162cc59a3a1e25956fa5fa8f60d2e1c52eac6[blob]
Queries value:
HKLM\software\microsoft\systemcertificates\disallowed\certificates\7d7f4414ccef168adf6bf40753b5becd78375931[blob]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates[5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1c00]
Queries value: HKLM\software\microsoft\internet explorer\default behaviors[homepage]
Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid]
Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
Queries value: HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[start page]
Queries value: HKCU\software\microsoft\internet explorer\main[start page]
Queries value: HKLM\software\microsoft\internet explorer\default behaviors[clientcaps]
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: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[flashplayer18_a_install.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
Queries value: HKCU\software\microsoft\internet explorer\recovery[autorecover]
Queries value: HKCR\.png[content type]
Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid]
Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
Queries value: HKCR\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\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type
024[name]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced rsa and aes cryptographic provider (prototype)[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced rsa and aes cryptographic provider (prototype)[image path]
Queries value: HKCU\software\microsoft\internet
explorer\ietld\lowmic[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet
explorer\ietld\lowmic[ietlddllversionhigh]
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]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1a00]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[160a]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[160a]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[displayname]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[displayversion]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[versionmajor]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[versionminor]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[publisher]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[displayicon]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[uninstallstring]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[urlinfoabout]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[helplink]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[installlocation]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[installsource]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[installdate]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[language]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[estimatedsize]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[nomodify]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00[norepair]
Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program files\flashplayer18_a_install.exe]
Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program files\install.exe]
Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\rarsfx0\msmpeng.exe]
Sets/Creates value: HKLM\system\currentcontrolset\services\devicesync[description]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[personal]
Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common documents]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[desktop]
Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common desktop]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[uncasintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cookies]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[local appdata]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[history]
Value changes: HKLM\system\currentcontrolset\services\devicesync[type]
Value changes: HKLM\software\microsoft\directdraw\mostrecentapplication[name]
Value changes: HKLM\software\microsoft\directdraw\mostrecentapplication[id]
Value changes: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Value changes: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\explorer\shell folders[cookies]
Value changes: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\explorer\shell folders[history]
Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common appdata]
Value changes: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\explorer\shell folders[appdata]
Value changes: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings[proxyenable]
Value changes: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Value changes: HKLM\software\microsoft\systemcertificates\authroot\certificates\5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25[blob]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[appdata]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]