Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 4, Task ID: 14

Task ID:	14
Risk Level:	6
Date Processed:	2016-03-29 03:27:45 (UTC)
Processing Time:	61.54 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\test12.jar.exe"
Sample ID:	4
Type:	basic
Owner:	admin
Label:	test12.jar
Date Added:	2016-03-29 03:27:44 (UTC)
File Type:	archive:jar:applet
File Size:	6213 bytes
MD5:	0fa3c06281d3b260bfccbb5a22dd74c5
SHA256:	1b7e0322a81be961ebce33aaeb395124544cfb01a3ab54f23cf64400fb2b04c7
Description:	None

Pattern Matching Results

6 Writes to system32 folder
2 ZIP archive format
3 Long sleep detected

Process/Thread Events

Creates process: C:\Program Files\Internet Explorer\iexplore.exe ["C:\Program Files\Internet Explorer\iexplore.exe" "c:\windows\temp\test12.jar.html"]
Creates process: C:\Program Files\Internet Explorer\iexplore.exe ["C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:652 CREDAT:79873]
Creates process: C:\Program Files\Java\jre7\bin\java.exe ["C:\Program Files\Java\jre7\bin\java.exe" -D__jvm_launched=11225877405 -D__applet_launched=11225800879 -Xbootclasspath/a:C:\PROGRA~1\Java\jre7\lib\deploy.jar;C:\PROGRA~1\Java\jre7\lib\javaws.jar;C:\PROGRA~1\Java\jre7\lib\plugin.jar -Djava.class.path=C:\PROGRA~1\Java\jre7\classes -Dsun.awt.warmup=true sun.plugin2.main.client.PluginMain write_pipe_name=jpi2_pid1628_pipe3,read_pipe_name=jpi2_pid1628_pipe2]
Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]

Named Object Events

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\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\!BrowserEmulation!SharedMemory!Mutex
Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex: \BaseNamedObjects\ConnHashTable<652>_HashTable_Mutex
Creates mutex: \BaseNamedObjects\oleacc-msaa-loaded
Creates mutex: \BaseNamedObjects\ZonesCounterMutex
Creates mutex: \BaseNamedObjects\!PrivacIE!SharedMemory!Mutex
Creates mutex: \BaseNamedObjects_!SHMSFTHISTORY!_
Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local settings!history!history.ie5!mshist012016032920160330!
Creates mutex: \BaseNamedObjects\DDrawWindowListMutex
Creates mutex: \BaseNamedObjects__DDrawExclMode__
Creates mutex: \BaseNamedObjects__DDrawCheckExclMode__
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EIH
Creates event: \BaseNamedObjects\Isolation Signal Registry Event (3AF75141-F55E-11E5-AE32-08002719344D, 0)
Creates event: \BaseNamedObjects\IE_EarlyTabStart_0xfc
Creates event: \BaseNamedObjects\Isolation Signal Registry Event (3AF75142-F55E-11E5-AE32-08002719344D, 0)
Creates event: \BaseNamedObjects\userenv: User Profile setup event

Creates event: \BaseNamedObjects\IEFrame.EventCheckDefaultBrowser
Creates event: \BaseNamedObjects\jpi2_pid1628_evt1
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore: \BaseNamedObjects\IEFrame!GetAsyncKeyStateQuery!652
Creates semaphore: \BaseNamedObjects\IEFrame!GetAsyncKeyStateReply!652
Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore: \BaseNamedObjects\shell.{090851A5-EB96-11D2-8BE4-00C04FA31A66}
Creates semaphore: \BaseNamedObjects\OleDfRoot000023217
Creates semaphore: \BaseNamedObjects\OleDfRoot0000235CA

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{3AF75143-F55E-11E5-AE32-08002719344D}.dat
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\~DF321B.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Active\{3AF75145-F55E-11E5-AE32-08002719344D}.dat
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\~DF35CE.tmp
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\hsperfdata_Admin
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin\1628
Creates: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012016032920160330
Creates: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012016032920160330\index.dat
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin\1252
Creates: C:\WINDOWS\system32\d3d9caps.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\0
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\1
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\2
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\3
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\4
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\5
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\6
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\7
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\8
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\9
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\10
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\11
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\12
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\13
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\14
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\15
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\16
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\17
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\18
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\19
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\20
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\21
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\22
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\23
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\24
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\25
Creates: C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\26
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\27
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\28
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\29
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\30
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\31
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\32
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\33
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\34
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\35
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\36
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\37
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\38
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\39
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\40
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\41
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\42
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\43
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\44
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\45
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\46
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\47
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\48
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\49
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\50
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\51
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\52
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\53
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\54
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\55
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\56
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\57
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\58
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\59
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\60
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\61
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\62
  Creates: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\63
  Opens: C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf
  Opens: C:
  Opens: C:\
  Opens: C:\Documents and Settings
  Opens: C:\Documents and Settings\Admin
  Opens: C:\Documents and Settings\Admin\Cookies
  Opens: C:\Documents and Settings\Admin\Local Settings
  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
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X
Opens: C:\Program Files
Opens: C:\Program Files\Internet Explorer
Opens: C:\WINDOWS
Opens: C:\WINDOWS\Registration
Opens: C:\WINDOWS\system32
Opens: C:\WINDOWS\system32\en-US
Opens: C:\WINDOWS\WinSxS
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\system32\ntdll.dll
Opens: C:\WINDOWS\system32\kernel32.dll
Opens: C:\WINDOWS\system32\unicode.nls
Opens: C:\WINDOWS\system32\locale.nls
Opens: C:\WINDOWS\system32\sorttbls.nls
Opens: C:\Program Files\Internet Explorer\iexplore.exe
Opens: C:\WINDOWS\system32\advapi32.dll
Opens: C:\WINDOWS\system32\rpcrt4.dll
Opens: C:\WINDOWS\system32\secur32.dll
Opens: C:\WINDOWS\system32\user32.dll
Opens: C:\WINDOWS\system32\gdi32.dll
Opens: C:\WINDOWS\system32\msvcrt.dll
Opens: C:\WINDOWS\system32\shlwapi.dll
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\ole32.dll
Opens: C:\WINDOWS\system32\iertutil.dll
Opens: C:\WINDOWS\system32\urlmon.dll
Opens: C:\WINDOWS\system32\oleaut32.dll
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\ctype.nls
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\sortkey.nls
Opens: C:\WINDOWS\system32\ieframe.dll
Opens: C:\WINDOWS\system32\en-US\ieframe.dll.mui
Opens: C:\WINDOWS\system32\comdlg32.dll
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\Program Files\Internet Explorer\sqmapi.dll
Opens: C:\WINDOWS\system32\winlogon.exe
Opens: C:\WINDOWS\system32\setupapi.dll
Opens: C:\WINDOWS\system32\xpsp2res.dll
Opens: C:\WINDOWS\system32\clbcatq.dll
Opens: C:\WINDOWS\system32\comres.dll
Opens: C:\WINDOWS\system32\version.dll
Opens: C:\WINDOWS\Registration\R000000000007.clb
Opens: C:\Program Files\Internet Explorer\ieproxy.dll
Opens: C:\WINDOWS\system32\wininet.dll
Opens: C:\WINDOWS\system32\normaliz.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\index.dat
Opens: C:\Documents and Settings\Admin\Cookies\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\index.dat
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\mlang.dll
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\system32\sxs.dll
Opens: C:\WINDOWS\system32\actxprxy.dll
Opens: C:\WINDOWS\system32\rasapi32.dll
Opens: C:\WINDOWS\system32\rasman.dll
Opens: C:\WINDOWS\system32\netapi32.dll
Opens: C:\WINDOWS\system32\tapi32.dll
Opens: C:\WINDOWS\system32\rtutils.dll
Opens: C:\WINDOWS\system32\winmm.dll
Opens: C:\WINDOWS\system32\userenv.dll
Opens: C:\WINDOWS\system32\sensapi.dll
Opens: C:\WINDOWS\system32\msv1_0.dll
Opens: C:\WINDOWS\system32\iphlpapi.dll
Opens: C:\WINDOWS\system32\narrhook.dll
Opens: C:\WINDOWS\system32\oleacc.dll

Opens: C:\WINDOWS\system32\msvcp60.dll
Opens: C:\WINDOWS\system32\oleaccrc.dll
Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\WINDOWS\system32\stdole2.tlb
Opens: C:\WINDOWS\system32\msimg32.dll
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\WINDOWS\system32\IEFRAME.dll.123.Manifest
Opens: C:\WINDOWS\system32\IEFRAME.dll.123.Config
Opens: C:\WINDOWS\system32\WININET.dll.123.Manifest
Opens: C:\WINDOWS\system32\WININET.dll.123.Config
Opens: C:\Documents and Settings\Admin\Desktop
Opens: C:\Program Files\Common Files
Opens: C:\Program Files\Common Files\Adobe
Opens: C:\Program Files\Common Files\Adobe\Acrobat
Opens: C:\Program Files\Java
Opens: C:\Program Files\Java\jre7
Opens: C:\Program Files\Java\jre7\bin
Opens: C:\WINDOWS\Temp
Opens: C:\Program Files\Internet Explorer\iexplore.exe.Manifest
Opens: C:\WINDOWS\system32\TAPI32.dll.124.Manifest
Opens: C:\WINDOWS\system32\TAPI32.dll.124.Config
Opens: C:\AUTOEXEC.BAT
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\Microsoft\Network\Connections\Pbk\
Opens: C:\WINDOWS\system32\ieui.dll
Opens: C:\Program Files\Internet Explorer\xpshims.dll
Opens: C:\WINDOWS\system32\cscui.dll
Opens: C:\WINDOWS\system32\cscdll.dll
Opens: C:\WINDOWS\System32\cscui.dll.124.Manifest
Opens: C:\WINDOWS\System32\cscui.dll.124.Config
Opens: C:\WINDOWS\system32\url.dll
Opens: C:\Documents and Settings\Admin\Favorites\Desktop.ini
Opens: C:\WINDOWS\system32\xmllite.dll
Opens: C:\WINDOWS\system32\xpsp3res.dll
Opens: C:\Program Files\Messenger\msmsgs.exe
Opens: C:\WINDOWS\Fonts\SEGOEUI.TTF
Opens: C:\WINDOWS\system32\MLANG.dll.123.Manifest
Opens: C:\WINDOWS\system32\MLANG.dll.123.Config
Opens: C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
Opens: C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll.2.Manifest
Opens: C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll.2.Config
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcr80.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcp80.dll
Opens: C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
Opens: C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll.2.Manifest
Opens: C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll.2.Config
Opens: C:\Program Files\Java\jre7\bin\jp2ssv.dll
Opens: C:\Program Files\Java\jre7\bin\msvcr100.dll
Opens: C:\WINDOWS\system32\en-US\urlmon.dll.mui
Opens: C:\WINDOWS\Temp\test12.jar.html
Opens: C:\WINDOWS\system32\mshtml.dll
Opens: C:\WINDOWS\system32\msls31.dll
Opens: C:\WINDOWS\system32\psapi.dll
Opens: C:\Program Files\Java\jre7\bin\jp2iexp.dll
Opens: C:\Program Files\Java\jre7\bin\client
Opens: C:\Program Files\Java\jre7\bin\client\jvm.dll
Opens: C:\PROGRA~1\Java\jre7\bin\client\jvm.dll.2.Manifest
Opens: C:\PROGRA~1\Java\jre7\bin\client\jvm.dll.2.Config
Opens: C:\WINDOWS\system32\wsock32.dll
Opens: C:\Program Files\Java\jre7\bin\verify.dll
Opens: C:\Program Files\Java\jre7\bin\java.dll
Opens: C:.hotspotrc
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
Opens: C:\Program Files\Java\jre7\bin\zip.dll

Opens: C:\WINDOWS\Fonts\times.ttf
Opens: C:\Program Files\Java\jre7\lib
Opens: C:\Program Files\Java\jre7\lib\meta-index
Opens: C:\Program Files\Java\jre7\bin\client\classes.jsa
Opens: C:\WINDOWS\system32\en-US\mshtml.dll.mui
Opens: C:\Program Files\Java\jre7\lib\rt.jar
Opens: C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014033120140407\index.dat
Opens: C:\WINDOWS\Temp\404ddfd0-b2d3-4483-abb5-cc3aec4357f3
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016032920160330
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016032920160330\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\frameiconcache.dat
Opens: C:\Program Files\Java\jre7\lib\deploy.jar
Opens: C:\Program Files\Java\jre7\lib\javaws.jar
Opens: C:\Program Files\Java\jre7\lib\plugin.jar
Opens: C:.hotspot_compiler
Opens: C:\WINDOWS\system32\rsaenh.dll
Opens: C:\WINDOWS\system32\crypt32.dll
Opens: C:\Program Files\Java\jre7\lib\ext\meta-index
Opens: C:\WINDOWS\system32\msasn1.dll
Opens: C:\Program Files\Java\jre7\lib\ext
Opens: C:\Program Files\Java\jre7\bin\deploy.dll
Opens: C:\Program Files\Java\jre7\bin\jp2native.dll
Opens: C:\WINDOWS\system32\netmsg.dll
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\deployment.properties
Opens: C:\Program Files\Java\jre7\bin\net.dll
Opens: C:\Program Files\Java\jre7\bin\nio.dll
Opens: C:\Program Files\Java\jre7\lib\security\java.security
Opens: C:\Program Files\Java\jre7\bin\java.exe
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\systest.sdb
Opens: C:\Program Files\Java\jre7\bin\java.exe.Manifest
Opens: C:\Program Files\Java\jre7\bin\java.exe.Config
Opens: C:\WINDOWS\Prefetch\JAVA.EXE-1E21D4DA.pf
Opens: C:\Documents and Settings\Admin\Application Data
Opens: C:\Documents and Settings\Admin\Application Data\Sun
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
Opens: C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Program Files\Java\jre7\lib\i386
Opens: C:\Program Files\Java\jre7\lib\security
Opens: C:\System Volume Information
Opens: C:\System Volume Information_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}
Opens: C:\System Volume Information_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP24
Opens: C:\WINDOWS\AppPatch
Opens: C:\WINDOWS\system32\shimeng.dll
Opens: C:\Program Files\Java\jre7\lib\i386\jvm.cfg
Opens: C:\Program Files\Java\jre7\bin\awt.dll
Opens: C:\DOCUME~1\ADMIN\LOCALS~1\TEMP\HSPERFDATA_ADMIN\2912
Opens: C:\WINDOWS\system32\d3d9.dll
Opens: C:\WINDOWS\system32\d3d8thk.dll
Opens: C:\WINDOWS\system32\vga.dll
Opens: C:\WINDOWS\system32\d3d9caps.dat
Opens: C:\WINDOWS\SYSTEM32\D3D9CAPS.TMP
Opens: C:\WINDOWS\system32\vga256.dll
Opens: C:\WINDOWS\system32\vga64k.dll
Opens: C:\Program Files\Java\jre7\lib\net.properties
Opens: C:\SYSTEM VOLUME INFORMATION_RESTORE{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP24\CHANGE.LOG
Opens: C:\Program Files\Java\jre7\lib\security\java.policy
Opens: C:\Program Files\Java\jre7\bin\client\jvm.dll.2.Manifest

Opens: C:\Program Files\Java\jre7\bin\client\jvm.dll.2.Config
Opens: C:\WINDOWS\system32\d3d9caps.tmp
Opens: C:\Documents and Settings\Admin\.accessibility.properties
Opens: C:\Program Files\Java\jre7\lib\accessibility.properties
Opens: C:\WINDOWS\Sun
Opens: C:\WINDOWS\Sun\Java
Opens: C:\Documents and Settings\Admin\.java.policy
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\security\java.policy
Opens: C:\Program Files\Java\jre7\lib\management
Opens: C:\WINDOWS\Fonts\coure.fon
Opens: C:\WINDOWS\Fonts\sserife.fon
Opens: C:\WINDOWS\Fonts\vgafix.fon
Opens: C:\Program Files\Java\jre7\lib\fonts
Opens: C:\Program Files\Java\jre7\bin\fontmanager.dll
Opens: C:\Program Files\Java\jre7\lib\fontconfig.bfc
Opens: C:\WINDOWS\Fonts
Opens: C:\Program Files\Java\jre7\lib\applet
Opens: C:\WINDOWS\Sun\Java\Deployment
Opens: C:\Program Files\Java\jre7\lib\currency.data
Opens: C:\WINDOWS\Temp\test12.jar.exe
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\security
Opens: C:\Program Files\Java\jre7\lib\security\blacklist
Opens: C:\Program Files\Java\jre7\lib\security\trusted.libraries
Opens: C:\Program Files\Java\jre7\lib\jsse.jar
Opens: C:\WINDOWS\Fonts\arial.ttf
Opens: C:\Program Files\Java\jre7\bin\t2k.dll
Opens: C:\WINDOWS\Fonts\wingding.ttf
Opens: C:\WINDOWS\Fonts\symbol.ttf
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{3AF75143-F55E-11E5-AE32-08002719344D}.dat
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\~DF321B.tmp
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Active\{3AF75145-F55E-11E5-AE32-08002719344D}.dat
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\~DF35CE.tmp
Writes to: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012016032920160330\index.dat
Writes to: C:\WINDOWS\system32\d3d9caps.tmp
Reads from: C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf
Reads from: C:\AUTOEXEC.BAT
Reads from: C:\WINDOWS\Registration\R000000000007.clb
Reads from: C:\WINDOWS\system32\url.dll
Reads from: C:\Documents and Settings\Admin\Favorites\Desktop.ini
Reads from: C:\WINDOWS\system32\oleacc.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\~DF321B.tmp
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{3AF75143-F55E-11E5-AE32-08002719344D}.dat
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\~DF35CE.tmp
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Active\{3AF75145-F55E-11E5-AE32-08002719344D}.dat
Reads from: C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
Reads from: C:\WINDOWS\Temp\test12.jar.html
Reads from: C:\WINDOWS\system32\ieframe.dll
Reads from: C:\WINDOWS\system32\stdole2.tlb
Reads from: C:\Program Files\Java\jre7\lib\meta-index
Reads from: C:\Program Files\Java\jre7\bin\client\classes.jsa
Reads from: C:\Program Files\Java\jre7\lib\rt.jar
Reads from: C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\frameiconcache.dat
Reads from: C:\Program Files\Java\jre7\lib\deploy.jar
Reads from: C:\Program Files\Java\jre7\lib\javaws.jar
Reads from: C:\Program Files\Java\jre7\lib\plugin.jar
Reads from: C:\WINDOWS\system32\rsaenh.dll
Reads from: C:\Program Files\Java\jre7\lib\ext\meta-index
Reads from: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\deployment.properties
Reads from: C:\Program Files\Java\jre7\lib\security\java.security
Reads from: C:\WINDOWS\Prefetch\JAVA.EXE-1E21D4DA.pf
Reads from: C:\Program Files\Java\jre7\lib\i386\jvm.cfg
Reads from: C:\WINDOWS\system32\d3d9caps.dat
Reads from: C:\Program Files\Java\jre7\lib\net.properties
Reads from: C:\Program Files\Java\jre7\lib\security\java.policy
Reads from: C:\Program Files\Java\jre7\lib\fontconfig.bfc
Reads from: C:\Program Files\Java\jre7\lib\currency.data
Reads from: C:\WINDOWS\Temp\test12.jar.exe
Reads from: C:\Program Files\Java\jre7\lib\security\blacklist
Reads from: C:\Program Files\Java\jre7\lib\security\trusted.libraries
Reads from: C:\Program Files\Java\jre7\lib\jsse.jar
Reads from: C:\WINDOWS\Fonts\arial.ttf

Reads from: C:\WINDOWS\Fonts\wingding.ttf
Reads from: C:\WINDOWS\Fonts\symbol.ttf
Deletes: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014033120140407\index.dat
Deletes: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014033120140407
Deletes: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014041220140413\index.dat
Deletes: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014041220140413
Deletes: C:\WINDOWS\system32\d3d9caps.dat
Deletes: C:\WINDOWS\system32\d3d9caps.tmp

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key: HKCU\software\microsoft\internet explorer\main
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Creates key: HKLM\software\microsoft\tracing
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKCU\software\microsoft\windows nt\currentversion\winlogon
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKCU\software\microsoft\internet explorer\recovery\active
Creates key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}
Creates key: HKCU\software
Creates key: HKCU\software\microsoft
Creates key: HKCU\software\microsoft\ctf
Creates key: HKCU\software\microsoft\ctf\tip
Creates key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}
Creates key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile
Creates key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000
Creates key: HKCU\software\microsoft\internet explorer\main\windowssearch
Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-4134-82b7-f2ba38496583}\iexplore
Creates key: HKCU\software\microsoft\internet explorer\lowregistry\extensions\cmdmapping
Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-11d2-bb9e-00c04f795683}\iexplore
Creates key: HKCU\software\microsoft\internet explorer\toolbar
Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore
Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}\iexplore
Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}
Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}\inprocserver32
Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}
Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32
Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}
Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}\inprocserver32
Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}
Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}\inprocserver32
Creates key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}
Creates key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}\inprocserver32
Creates key: HKCU\software\classes\javaplugin.1020
Creates key: HKCU\software\classes\javaplugin.1020\clsid
Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore
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\5.0\cache\extensible cache\mshist012016032920160330
Creates key: HKCU\software\microsoft\direct3d\mostrecentapplication
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\iexplore.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
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\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
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\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 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\msvcrt.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\shell32.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\iertutil.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\urlmon.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\currentversion\explorer\performance
Opens key: HKLM\system\setup
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
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: HKCU\software\classes\
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: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKLM\software\microsoft\internet explorer\main
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enablesafesearchpath_kb963027
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enablesafesearchpath_kb963027
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: 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\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\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
Opens key: HKLM\software\policies\microsoft\internet explorer
Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer
Opens key: HKLM\software\microsoft\internet explorer
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: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software
Opens key: HKLM\software\policies\microsoft\internet explorer\main
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: HKLM\software\microsoft\rpc\pagedbuffers
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iexplore.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
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: 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: HKU\
Opens key: HKCU\software\microsoft\internet explorer\main
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\safety\privacie
Opens key: HKCU\software\microsoft\internet explorer\safety\privacie
Opens key: HKLM\software\microsoft\internet explorer\safety\privacie
Opens key: HKCU\software\microsoft\internet explorer\new windows
Opens key: HKLM\software\microsoft\internet explorer\new windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\iexplore.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKCU\software\microsoft\internet explorer\sqm
Opens key: HKLM\software\microsoft\internet explorer\sqm
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sqmapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
Opens key: HKLM\software\policies\microsoft\internet explorer\sqm
Opens key: HKCU\software\policies\microsoft\internet explorer\sqm
Opens key: HKCU\software\microsoft\internet
explorer\browseremulation\clearablelistdata
Opens key: HKCU\software\microsoft\internet explorer\browseremulation
Opens key: HKLM\software\policies\microsoft\internet explorer\toolbars\restrictions
Opens key: HKCU\software\microsoft\internet explorer\toolbars\restrictions
Opens key: HKLM\software\microsoft\internet explorer\toolbars\restrictions
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\browser helper
objects
Opens key: HKLM\software\microsoft\internet explorer\extension
compatibility\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-
e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKLM\software\microsoft\windows\currentversion\ext\settings\{18df081c-
e8ad-4283-a596-fa578c2ebdc3}

Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\treatas
Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\treatas
Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32
Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32
Opens key: HKLM\software\microsoft\internet explorer\extension compatibility\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKLM\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\treatas
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\treatas
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32
Opens key: HKLM\software\microsoft\internet explorer\toolbar
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: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\
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\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\security
Opens key: HKLM\software\microsoft\internet explorer\security
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\objects\{20d04fe0-3aea-1069-a2d8-08002b30309d}
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\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient
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\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\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: HKCU\software\microsoft\windows\currentversion\explorer\fileexts
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html
Opens key: HKCU\software\classes\.html
Opens key: HKCR\.html
Opens key: HKCU\software\classes\htmlfile
Opens key: HKCR\htmlfile
Opens key: HKCU\software\classes\htmlfile\curver
Opens key: HKCR\htmlfile\curver
Opens key: HKCR\htmlfile\
Opens key: HKCU\software\classes\htmlfile\shellex\iconhandler
Opens key: HKCR\htmlfile\shellex\iconhandler
Opens key: HKCU\software\classes\systemfileassociations\.html
Opens key: HKCR\systemfileassociations\.html
Opens key: HKCU\software\classes\systemfileassociations\text
Opens key: HKCR\systemfileassociations\text
Opens key: HKCU\software\classes\htmlfile\clsid
Opens key: HKCR\htmlfile\clsid
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046}
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
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\netapi32.dll
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\winmm.dll
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 nt\currentversion\image file execution options\tapi32.dll
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: HKLM\software\microsoft\windows nt\currentversion\image file execution options\userenv.dll
Opens key: HKLM\system\currentcontrolset\control\productoptions
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003
Opens key: HKCU\environment
Opens key: HKCU\volatile environment
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sensapi.dll
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: 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\msimg32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ieui.dll
Opens key: HKLM\software\microsoft\directui
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: HKLM\software\microsoft\com3
Opens key: HKCU\software\classes\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}
Opens key: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}
Opens key: HKCU\software\classes\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32
Opens key: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32
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: HKCR\clsid
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserverx86
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\localserver32
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\localserver32
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandlerx86
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\localserver
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ieproxy.dll
Opens key: HKCU\software\classes\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}
Opens key: HKCR\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}
Opens key: HKCU\software\classes\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}\proxystubclsid32
Opens key: HKCR\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}\proxystubclsid32
Opens key: HKLM\software\policies\microsoft\internet explorer\tabbedbrowsing
Opens key: HKCU\software\microsoft\internet explorer\tabbedbrowsing
Opens key: HKLM\software\microsoft\internet explorer\tabbedbrowsing
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: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000
Opens key: HKCU\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: HKCU\software\policies\microsoft\internet explorer\main
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\windows nt\currentversion\image file execution options\xpshims.dll
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: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}
Opens key: HKCU\software\microsoft\internet explorer\main\windowssearch
Opens key: HKLM\software\policies\microsoft\internet explorer\feeds
Opens key: HKCU\software\microsoft\internet explorer\feeds
Opens key: HKLM\software\microsoft\internet explorer\feeds
Opens key: HKCU\software\classes\.url\persistenthandler
Opens key: HKCR\.url\persistenthandler
Opens key: HKLM\software\policies\microsoft\internet explorer\main\windowssearch
Opens key: HKLM\software\microsoft\windows search
Opens key: HKLM\software\policies\microsoft\internet explorer\toolbar\webbrowser
Opens key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser
Opens key: HKLM\software\microsoft\internet explorer\toolbar\webbrowser
Opens key: HKCU\software\microsoft\windows\currentversion\policies\ieak
Opens key: HKLM\software\microsoft\windows\currentversion\policies\ieak
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\policies\microsoft\internet explorer\commandbar
Opens key: HKCU\software\microsoft\internet explorer\commandbar
Opens key: HKLM\software\microsoft\internet explorer\commandbar
Opens key: HKLM\software\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\
Opens key: HKCU\control panel\desktop\windowmetrics
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\shell icons
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\offline files
Opens key: HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32
Opens key: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\apphelp.dll
Opens key: HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}
Opens key: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}
Opens key: HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\treatas
Opens key: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\treatas
Opens key: HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserverx86
Opens key: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\localserver32
Opens key: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\localserver32
Opens key: HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprochandler32
Opens key: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprochandler32
Opens key: HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprochandlerx86
Opens key: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-

080036587f03}\localserver
Opens key: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cscdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cscui.dll
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\treatas
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\treatas
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprocserver32
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprocserverx86
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\localserver32
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\localserver32
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprochandler32
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler32
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprochandlerx86
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\localserver
Opens key: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\localserver
Opens key: HKCU\software\classes\appid\{667524be-9ec0-4196-91c9-c6ed1f7a899d}
Opens key: HKCR\appid\{667524be-9ec0-4196-91c9-c6ed1f7a899d}
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\active accessibility\handlers
Opens key: HKCU\software\classes\typelib
Opens key: HKCR\typelib
Opens key: HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}
Opens key: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}
Opens key: HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1
Opens key: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1
Opens key: HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
00aa00389b71}\1.1\flags
Opens key: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\flags
Opens key: HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
00aa00389b71}\1.1\0
Opens key: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0
Opens key: HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
00aa00389b71}\1.1\0\win32
Opens key: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32
Opens key: HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
00aa00389b71}\1.1\helpdir
Opens key: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\helpdir
Opens key: HKCU\software\classes\interface
Opens key: HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}
Opens key: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}
Opens key: HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid
Opens key: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid
Opens key: HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
Opens key: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\typelib
Opens key: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib
Opens key: HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-00aa001a1953}
Opens key: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}
Opens key: HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-
00aa001a1953}\proxystubclsid
Opens key: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\proxystubclsid
Opens key: HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-
00aa001a1953}\proxystubclsid32
Opens key: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-
00aa001a1953}\typelib
Opens key: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\typelib
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: 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: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKLM\software\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKCU\software\microsoft\internet explorer\searchurl
Opens key: HKCU\software\microsoft\internet explorer\searchscopes
Opens key: HKLM\software\microsoft\internet explorer\searchscopes
Opens key: HKLM\software\policies\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
Opens key: HKCU\software\policies\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
Opens key: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
Opens key: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
Opens key: HKLM\software\policies\microsoft\internet explorer\searchscopes
Opens key: HKLM\software\policies\microsoft\internet explorer\toolbar
Opens key: HKCU\software\microsoft\internet explorer\toolbar
Opens key: HKCU\software\policies\microsoft\internet explorer\toolbars\restrictions
Opens key: HKLM\software\policies\microsoft\internet explorer\linksbar
Opens key: HKCU\software\microsoft\internet explorer\linksbar
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\xmllite.dll
Opens key: HKCU\software\microsoft\internet explorer\extensions
Opens key: HKLM\software\microsoft\internet explorer\extensions
Opens key: HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-4134-82b7-f2ba38496583}
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_addon_management
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_addon_management
Opens key: HKLM\software\microsoft\windows\currentversion\policies\ext\clsid
Opens key: HKCU\software\microsoft\windows\currentversion\policies\ext\clsid
Opens key: HKLM\software\microsoft\windows\currentversion\policies\ext
Opens key: HKCU\software\microsoft\windows\currentversion\policies\ext
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{e2e2dd38-d088-4134-82b7-f2ba38496583}
Opens key: HKLM\software\microsoft\windows\currentversion\ext\settings\{e2e2dd38-d088-4134-82b7-f2ba38496583}
Opens key: HKCU\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-4134-82b7-f2ba38496583}
Opens key: HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-4134-82b7-f2ba38496583}\lang0409
Opens key: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-11d2-bb9e-00c04f795683}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{fb5f1910-f110-11d2-bb9e-00c04f795683}
Opens key: HKLM\software\microsoft\windows\currentversion\ext\settings\{fb5f1910-f110-11d2-bb9e-00c04f795683}
Opens key: HKCU\software\microsoft\internet explorer\extensions\{fb5f1910-f110-11d2-bb9e-00c04f795683}
Opens key: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-11d2-bb9e-00c04f795683}\lang0409
Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions
Opens key: HKLM\software\policies\microsoft\internet explorer\iedevtools
Opens key: HKCU\software\microsoft\internet explorer\iedevtools
Opens key: HKLM\software\microsoft\internet explorer\iedevtools
Opens key: HKCU\software\microsoft\internet explorer\lowregistry\commandbar
Opens key: HKCU\software\microsoft\internet explorer\linksexplorer
Opens key: HKLM\software\microsoft\internet explorer\linksexplorer
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-

000000000046}\inprocserver32
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-
000000000046}\inprocserverx86
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-
000000000046}\localserver32
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandler32
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandlerx86
Opens key: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3af75140-f55e-11e5-ae32-08002719344d}
Opens key: HKCR\clsid\{3af75140-f55e-11e5-ae32-08002719344d}
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-
b1deb82c6e5e}\treatas
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\treatas
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-
b1deb82c6e5e}\inprocserver32
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprocserver32
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-
b1deb82c6e5e}\inprocserverx86
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-
b1deb82c6e5e}\localserver32
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\localserver32
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-
b1deb82c6e5e}\inprochandler32
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandler32
Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-
b1deb82c6e5e}\inprochandlerx86
Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprochandlerx86
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\system\currentcontrolset\control\lsa\sspicache\digest.dll
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
Opens key: HKCU\software\classes\htmlfile\shellex\{000214f9-0000-0000-c000-
000000000046}
Opens key: HKCR\htmlfile\shellex\{000214f9-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\.html\shellex\{000214f9-0000-0000-c000-
000000000046}
Opens key: HKCR\.html\shellex\{000214f9-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\systemfileassociations\text\shellex\{000214f9-
0000-0000-c000-000000000046}
Opens key: HKCR\systemfileassociations\text\shellex\{000214f9-0000-0000-c000-
000000000046}
Opens key: HKCU\software\classes*
Opens key: HKCR*
Opens key: HKCU\software\classes*\shellex\{000214f9-0000-0000-c000-000000000046}
Opens key: HKCR*\shellex\{000214f9-0000-0000-c000-000000000046}
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\url
history
Opens key: HKCU\software\classes\interface\{8a7476f4-d264-4e13-ae72-20cd9831d98c}
Opens key: HKCR\interface\{8a7476f4-d264-4e13-ae72-20cd9831d98c}
Opens key: HKCU\software\classes\interface\{8a7476f4-d264-4e13-ae72-
20cd9831d98c}\proxystubclsid32
Opens key: HKCR\interface\{8a7476f4-d264-4e13-ae72-20cd9831d98c}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}
Opens key: HKCR\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}
Opens key: HKCU\software\classes\interface\{b40c43f1-f039-44d2-aeb7-
87f5af8abc3d}\proxystubclsid32
Opens key: HKCR\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}
Opens key: HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}
Opens key: HKCU\software\classes\interface\{d358f4e1-0465-4965-9dd5-
cae303d2c345}\proxystubclsid32
Opens key: HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14}

Opens key: HKCR\interface\{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14}
Opens key: HKCU\software\classes\interface\{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14}\proxystubclsid32
Opens key: HKCR\interface\{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14}\proxystubclsid32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mlang.dll
Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserverx86
Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\localserver32
Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\localserver32
Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandler32
Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandler32
Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandlerx86
Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\localserver
Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\localserver
Opens key: HKCU\software\classes\appid\{77ab4812-5411-4ea9-8437-77ad0f230302}
Opens key: HKCR\appid\{77ab4812-5411-4ea9-8437-77ad0f230302}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcr80.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcp80.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\acroiehelpershim.dll
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserver32
Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\acroiehelper.dll
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}
Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\treatas
Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\treatas
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserverx86
Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\localserver32
Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\localserver32
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler32
Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler32
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandlerx86
Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\localserver
Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\localserver
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserverx86
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\localserver32
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\localserver32
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler32
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandler32
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandlerx86
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\localserver
Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcr100.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\jp2ssv.dll
Opens key: HKLM\software\javasoft
Opens key: HKLM\software\javasoft\java plug-in
Opens key: HKLM\software\javasoft\java plug-in\10.2.0
Opens key: HKLM\software\javasoft\java plug-in\1.7.0_02
Opens key: HKLM\software\javasoft\java runtime environment
Opens key: HKLM\software\javasoft\java runtime environment\1.7.0_02
Opens key: HKCU\software\classes
Opens key: HKCU\software\classes\clsid

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}
Opens key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}\inprocserver32
Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas
Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas
Opens key: HKCU\software\classes\javaplugin.1020
Opens key: HKCU\software\classes\javaplugin.1020\clsid
Opens key: HKLM\software\mozilla
Opens key: HKLM\software\mozilla\mozilla firefox
Opens key: HKLM\software\mozilla.org
Opens key: HKCU\software\classes\htmlfile\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCR\htmlfile\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCU\software\classes\.html\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCR\.html\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCU\software\classes\systemfileassociations\text\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCR\systemfileassociations\text\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCU\software\classes*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCR*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
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\sxs.dll
Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}
Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}
Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0
Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0
Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0
Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0
Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0\win32
Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0\win32
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: HKCU\software\classes\htmlfile\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKCR\htmlfile\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\.html\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKCR\.html\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\systemfileassociations\text\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKCR\systemfileassociations\text\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes*\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKCR*\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKLM\software\policies\microsoft\internet explorer\browseremulation
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandler32
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandlerx86
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-
00c04fb6bfc4}\localserver
Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\localserver
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\4
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: 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\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\protocols\name-space handler\about\
Opens key: HKCR\protocols\name-space handler\about
Opens key: HKCU\software\classes\protocols\name-space handler*\
Opens key: HKCR\protocols\name-space handler*
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: 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\windows nt\currentversion\windows
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\microsoft\internet explorer\domstorage
Opens key: HKLM\software\microsoft\internet explorer\domstorage
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\classes\protocols\name-space handler\file\
Opens key: HKCR\protocols\name-space handler\file
Opens key: HKCU\software\classes\protocols\filter\text/html
Opens key: HKCR\protocols\filter\text/html
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_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\psapi.dll
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\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}
Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\treatas
Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\treatas
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32
Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserverx86
Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\localserver32
Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\localserver32
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandler32
Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandlerx86
Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\localserver
Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\localserver
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: 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\policies\microsoft\internet explorer\zoom
Opens key: HKCU\software\microsoft\internet explorer\zoom
Opens key: HKLM\software\microsoft\internet explorer\zoom
Opens key: HKLM\software\policies\microsoft\internet explorer\phishingfilter
Opens key: HKCU\software\microsoft\internet explorer\phishingfilter
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
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: HKCU\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKCU\software\classes\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}
Opens key: HKCR\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}
Opens key: HKCU\software\classes\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}\proxystubclsid32
Opens key: HKCR\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}\proxystubclsid32
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\internet explorer\browseremulation
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\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\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\treatas
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserverx86
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\localserver32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\localserver32
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandlerx86
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\localserver
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\localserver
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\treatas
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserverx86
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\localserver32
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver32
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler32

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandlerx86
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver
Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver
Opens key: HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}
Opens key: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}
Opens key: HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\proxystubclsid32
Opens key: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}\inprocserverx86
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}\localserver32
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\localserver32
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}\inprochandlerx86
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}\localserver
Opens key: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\localserver
Opens key: HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\forward
Opens key: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\forward
Opens key: HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\typelib
Opens key: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\typelib
Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
Opens key: HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
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: HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
Opens key: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
Opens key: HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32
Opens key: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}
Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}
Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\treatas
Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\treatas
Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32
Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32
Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserverx86
Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver32
Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver32
Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandler32
Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandler32
Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\inprochandlerx86
Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver
Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\actxprxy.dll
Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
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\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: HKCU\software\classes\interface\{9d973e3b-f610-4f03-83d3-aed90c3237ac}
Opens key: HKCR\interface\{9d973e3b-f610-4f03-83d3-aed90c3237ac}
Opens key: HKCU\software\classes\interface\{9d973e3b-f610-4f03-83d3-aed90c3237ac}\synchronousinterface
Opens key: HKCR\interface\{9d973e3b-f610-4f03-83d3-aed90c3237ac}\synchronousinterface
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_status_bar_throttling
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_status_bar_throttling
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\policies\microsoft\internet explorer\control panel
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\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105
Opens key: HKLM\software\microsoft\internet explorer\activex compatibility
Opens key: HKLM\software\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKLM\software\microsoft\windows\currentversion\ext\settings\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_alloweddomainlist
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_alloweddomainlist
Opens key: HKLM\software\microsoft\internet explorer\extension compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_activexinstall
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_activexinstall
Opens key: HKCU\software\classes\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
Opens key: HKCR\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333}
Opens key: HKCU\software\microsoft\code store database\distribution units
Opens key: HKLM\software\microsoft\code store database\distribution units
Opens key: HKLM\software\microsoft\code store database\distribution units\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\availableversion
Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\availableversion
Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\installedversion
Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\installedversion

Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\appid
Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\appid
Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\inprocserver32
Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\inprocserver32
Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\localserver32
Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\localserver32
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\treatas
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\treatas
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserverx86
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\localserver32
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\localserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprochandler32
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprochandler32
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprochandlerx86
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\localserver
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\localserver
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\jp2iexp.dll
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_activex_repurposedetection
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\windows nt\currentversion\image file execution options\wsock32.dll
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: HKLM\software\microsoft\windows nt\currentversion\image file execution options\jvm.dll
Opens key: HKCU\software\classes\htmlfile\shell
Opens key: HKCR\htmlfile\shell
Opens key: HKCU\software\classes\htmlfile\shell\opennew
Opens key: HKCR\htmlfile\shell\opennew
Opens key: HKCU\software\classes\htmlfile\shell\edit
Opens key: HKCR\htmlfile\shell\edit
Opens key: HKCU\software\classes\htmlfile\shell\edit\command
Opens key: HKCR\htmlfile\shell\edit\command
Opens key: HKLM\software\microsoft\internet explorer\default html editor
Opens key: HKCU\software\classes\.html\openwithlist
Opens key: HKCR\.html\openwithlist
Opens key: HKCU\software\microsoft\internet explorer\default html editor
Opens key: HKLM\software\microsoft\internet explorer\default html editor\
Opens key: HKLM\software\microsoft\internet explorer\default html editor\shell\edit
Opens key: HKLM\software\microsoft\internet explorer\default html editor\shell\edit\command
Opens key: HKCU\software\microsoft\internet explorer\default mhtml editor
Opens key: HKLM\software\microsoft\internet explorer\default mhtml editor
Opens key: HKLM\software\microsoft\internet explorer\default mhtml editor\shell\edit\command
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm
Opens key: HKCU\software\classes\.htm
Opens key: HKCR\.htm
Opens key: HKCU\software\classes\.htm\openwithlist
Opens key: HKCR\.htm\openwithlist
Opens key: HKCU\software\classes\applications\notepad.exe
Opens key: HKCR\applications\notepad.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\verify.dll
Opens key: HKCR\applications\notepad.exe\
Opens key: HKCU\software\classes\applications\notepad.exe\shell\edit
Opens key: HKCR\applications\notepad.exe\shell\edit
Opens key: HKCU\software\classes\applications\notepad.exe\shell\edit\command

Opens key: HKCR\applications\notepad.exe\shell\edit\command
Opens key: HKLM\software\policies\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\java.dll
Opens key: HKCU\software\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\microsoft\internet explorer\feed discovery\
Opens key: HKCU\software\microsoft\internet explorer\feed discovery\
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\microsoft\windows nt\currentversion\image file execution options\zip.dll
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shell
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shell
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellex\iconhandler
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shellex\iconhandler
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\clsid
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\clsid
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserverx86
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver32
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver32
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandlerx86
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver
Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ff393560-c2a7-11cf-bff4-444553540000}
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016032920160330
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\
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: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore
Opens key: HKLM\software\policies\microsoft\internet explorer\caretbrowsing
Opens key: HKCU\software\microsoft\internet explorer\caretbrowsing
Opens key: HKLM\software\microsoft\internet explorer\caretbrowsing
Opens key: HKLM\software\microsoft\internet explorer\migration
Opens key: HKCU\software\classes\http
Opens key: HKCR\http
Opens key: HKCU\software\classes\http\shell\open\ddeexec\ifexec
Opens key: HKCR\http\shell\open\ddeexec\ifexec
Opens key: HKCU\software\classes\https
Opens key: HKCR\https

Opens key: HKCU\software\classes\https\shell\open\ddeexec\ifexec
Opens key: HKCR\https\shell\open\ddeexec\ifexec
Opens key: HKCU\software\classes\ftp
Opens key: HKCR\ftp
Opens key: HKCU\software\classes\internetshortcut
Opens key: HKCR\internetshortcut
Opens key: HKCU\software\classes\internetshortcut\defaulticon
Opens key: HKCR\internetshortcut\defaulticon
Opens key: HKCU\software\classes\http\shell\open\command
Opens key: HKCR\http\shell\open\command
Opens key: HKCU\software\classes\http\shell\open\ddeexec
Opens key: HKCR\http\shell\open\ddeexec
Opens key: HKCU\software\classes\http\shell\open\ddeexec\application
Opens key: HKCR\http\shell\open\ddeexec\application
Opens key: HKCU\software\classes\http\shell\open\ddeexec\topic
Opens key: HKCR\http\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\https\shell\open\command
Opens key: HKCR\https\shell\open\command
Opens key: HKCU\software\classes\https\shell\open\ddeexec
Opens key: HKCR\https\shell\open\ddeexec
Opens key: HKCU\software\classes\https\shell\open\ddeexec\application
Opens key: HKCR\https\shell\open\ddeexec\application
Opens key: HKCU\software\classes\https\shell\open\ddeexec\topic
Opens key: HKCR\https\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\ftp\shell\open\command
Opens key: HKCR\ftp\shell\open\command
Opens key: HKCU\software\classes\ftp\shell\open\ddeexec
Opens key: HKCR\ftp\shell\open\ddeexec
Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\ifexec
Opens key: HKCR\ftp\shell\open\ddeexec\ifexec
Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\application
Opens key: HKCR\ftp\shell\open\ddeexec\application
Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\topic
Opens key: HKCR\ftp\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\htmlfile\shell\open
Opens key: HKCR\htmlfile\shell\open
Opens key: HKCU\software\classes\htmlfile\shell\open\command
Opens key: HKCR\htmlfile\shell\open\command
Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec
Opens key: HKCR\htmlfile\shell\open\ddeexec
Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec\application
Opens key: HKCR\htmlfile\shell\open\ddeexec\application
Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec\topic
Opens key: HKCR\htmlfile\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\mhtmlfile\shell
Opens key: HKCR\mhtmlfile\shell
Opens key: HKCU\software\classes\htmlfile\shell\opennew\command
Opens key: HKCR\htmlfile\shell\opennew\command
Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec
Opens key: HKCR\htmlfile\shell\opennew\ddeexec
Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec\ifexec
Opens key: HKCR\htmlfile\shell\opennew\ddeexec\ifexec
Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec\application
Opens key: HKCR\htmlfile\shell\opennew\ddeexec\application
Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec\topic
Opens key: HKCR\htmlfile\shell\opennew\ddeexec\topic
Opens key: HKCU\software\classes\.mht
Opens key: HKCR\.mht
Opens key: HKCU\software\classes\.mhtml
Opens key: HKCR\.mhtml
Opens key: HKCU\software\classes\mhtmlfile\shell\open
Opens key: HKCR\mhtmlfile\shell\open
Opens key: HKCU\software\classes\mhtmlfile\shell\open\command
Opens key: HKCR\mhtmlfile\shell\open\command
Opens key: HKCU\software\classes\mhtmlfile\shell\open\ddeexec
Opens key: HKCR\mhtmlfile\shell\open\ddeexec
Opens key: HKCU\software\classes\mhtmlfile\shell\open\ddeexec\application
Opens key: HKCR\mhtmlfile\shell\open\ddeexec\application
Opens key: HKCU\software\classes\mhtmlfile\shell\open\ddeexec\topic
Opens key: HKCR\mhtmlfile\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew
Opens key: HKCR\mhtmlfile\shell\opennew
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\command
Opens key: HKCR\mhtmlfile\shell\opennew\command
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec
Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec\ifexec
Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\ifexec
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec\application
Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\application
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec\topic
Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\topic
Opens key: HKCU\software\classes\.url

Opens key: HKCR\.url
Opens key: HKCU\software\classes\internetshortcut\clsid
Opens key: HKCR\internetshortcut\clsid
Opens key: HKCU\software\classes\internetshortcut\shell\open
Opens key: HKCR\internetshortcut\shell\open
Opens key: HKCU\software\classes\internetshortcut\shell\open\command
Opens key: HKCR\internetshortcut\shell\open\command
Opens key: HKCU\software\classes\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}
Opens key: HKCR\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}
Opens key: HKCU\software\classes\applications\iexplore.exe\shell\open\command
Opens key: HKCR\applications\iexplore.exe\shell\open\command
Opens key: HKCU\software\microsoft\cryptography\providers\type 001
Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 001
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\user preferences
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\deploy.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jp2native.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\net.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\nio.dll
Opens key: HKLM\software\oracle\javafx
Opens key: HKLM\software\javasoft\java runtime environment\1.7
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\java.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\java.exe
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\awt.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\java.exe
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\d3d8thk.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\d3d9.dll
Opens key: HKLM\software\microsoft\direct3d
Opens key: HKLM\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-
9b1f4867732a}\0000
Opens key: HKLM\system\currentcontrolset\control\watchdog\display
Opens key: HKLM\software\microsoft\directdraw\gammacalibrator
Opens key: HKLM\software\microsoft\direct3d\drivers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\java.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\javasoft\java update\policy
Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32
Opens key:
HKCU\software\microsoft\windows\currentversion\policies\comdlg32\placesbar
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\fontmanager.dll
Opens key: HKCU\eudc\1252
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\t2k.dll
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}

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[iexplore]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[iexplore]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\setup[systemsetupinprogress]
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\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\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[iexplore.exe]
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: HKLM\software\microsoft\internet explorer\main[depoff]
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: 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\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: 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\explorer\user shell
folders[cache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
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: 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: 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: 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[iexplore.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\internet settings[migrateproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Queries value: HKCU\software\microsoft\internet explorer\main[start page]
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: HKCU\software\microsoft\internet explorer\main[secondary start pages]
Queries value: HKLM\software\microsoft\internet explorer\main[secondary start pages]
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: HKCU\software\microsoft\internet explorer\main[hangresistantframe]
Queries value: HKLM\software\microsoft\internet explorer\main[hangresistantframe]
Queries value: HKCU\software\microsoft\internet explorer\main[compatibilityflags]
Queries value: HKCU\software\microsoft\internet explorer\new windows[detourdialogs]
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\ole[maximumallowedallocationsize]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKCU\software\microsoft\internet explorer\sqm[serverfreezeonupload]
Queries value: HKLM\software\microsoft\internet explorer\sqm[serverfreezeonupload]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKCU\software\microsoft\internet explorer\sqm[disablecustomerimprovementprogram]
Queries value: HKLM\software\microsoft\internet explorer\sqm[disablecustomerimprovementprogram]
Queries value: HKCU\software\microsoft\internet explorer\sqm[sqmoptinforie8]
Queries value: HKLM\software\microsoft\internet explorer\sqm[sqmoptinforie8]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[unattendloaded]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[tldupdates]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[desktop]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[flags]
Queries value: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32[]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[vercache]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}[flags]
Queries value: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32[]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}[vercache]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[favorites]
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[iexplore.exe]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablefixsecuritysettings]
Queries value: HKCU\software\microsoft\internet explorer\security[disablefixsecuritysettings]
Queries value: HKLM\software\microsoft\internet explorer\security[disablefixsecuritysettings]
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\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
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: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask]
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\policies\explorer[allowfileclsidjunctions]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[recent]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[progid]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[application]
Queries value: HKCR\.html[]
Queries value: HKCR\htmlfile\shellex\iconhandler[]
Queries value: HKCR\htmlfile[docobject]
Queries value: HKCR\.html[perceivedtype]
Queries value: HKCR\systemfileassociations\text[docobject]
Queries value: HKCR\htmlfile[browseinplace]
Queries value: HKCR\systemfileassociations\text[browseinplace]
Queries value: HKCR\htmlfile\clsid[]
Queries value: HKCR\htmlfile[isshortcut]
Queries value: HKCR\systemfileassociations\text[isshortcut]
Queries value: HKCR\htmlfile[alwaysshowext]
Queries value: HKCR\systemfileassociations\text[alwaysshowext]
Queries value: HKCR\htmlfile[nevershowext]
Queries value: HKCR\systemfileassociations\text[nevershowext]
Queries value: HKLM\system\currentcontrolset\control\session manager\appcompatibility[disableappcompat]
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 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:
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: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common appdata]

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: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal]
Queries value: HKCU\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: HKLM\software\microsoft\windows nt\currentversion\profilelist[profilesdirectory]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[allusersprofile]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[defaultuserprofile]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileimagepath]
Queries value: HKCU\software\microsoft\windows nt\currentversion\winlogon[parseautoexec]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKCU\software\microsoft\internet explorer\main[window_min_width]
Queries value: HKCU\software\microsoft\internet explorer\main[window_min_height]
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\internet explorer\recovery[enabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
Queries value: HKLM\software\microsoft\com3[gipactivitybypass]
Queries value: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32[]
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\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[appid]
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[groups]
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: HKCU\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: HKLM\software\policies\microsoft\internet explorer\main[tabshutdowndelay]
Queries value: HKCU\software\microsoft\internet explorer\main[tabshutdowndelay]
Queries value: HKLM\software\microsoft\internet explorer\main[tabshutdowndelay]
Queries value: HKCU\software\microsoft\internet explorer\main\windowssearch[enabledscopes]
Queries value: HKCR\.url\persistenthandler[]
Queries value: HKLM\software\microsoft\windows search[currentversion]
Queries value: HKCU\software\microsoft\internet explorer\main[window_placement]
Queries value: HKCU\software\microsoft\internet explorer\toolbar\webbrowser[itbar7position]

Queries value: HKCU\software\microsoft\internet explorer\main[fullscreen]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer[max cached icons]
Queries value: HKCU\control panel\desktop\windowmetrics[shell icon size]
Queries value: HKCU\control panel\desktop\windowmetrics[shell small icon size]
Queries value: HKCU\control panel\desktop\windowmetrics[shell icon bpp]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\offline files[suppressionpolicy]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\offline files[]
Queries value: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32[]
Queries value: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32[loadwithoutcom]
Queries value: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}[appid]
Queries value: HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32[]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
Queries value: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}[appid]
Queries value: HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32[threadingmodel]
Queries value: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1[]
Queries value: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\flags[]
Queries value: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32[]
Queries value: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}[]
Queries value: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid[]
Queries value: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32[]
Queries value: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib[]
Queries value: HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib[version]
Queries value: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}[]
Queries value: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\proxystubclsid[]
Queries value: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\proxystubclsid32[]
Queries value: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\typelib[]
Queries value: HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\typelib[version]
Queries value: HKCU\software\microsoft\internet explorer\main[useie7autocomplete]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tahoma]
Queries value: HKCU\software\microsoft\internet explorer\main[searchcontrolwidth]
Queries value: HKCU\software\microsoft\internet explorer\main[searchmigrated]
Queries value: HKCU\software\microsoft\internet explorer\main[searchmigratedinstalled]
Queries value: HKCU\software\microsoft\internet explorer\main[searchmigrateddefaultname]
Queries value: HKCU\software\microsoft\internet explorer\main[searchmigrateddefaulturl]
Queries value: HKCU\software\microsoft\internet explorer\searchurl[provider]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[defaultscope]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[deleted]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[url]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[displayname]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[displayname]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[showsearchsuggestions]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[showsearchsuggestions]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[showsearchsuggestionsglobal]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes[showsearchsuggestionsglobal]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl_json]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl_json]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl_jsonfallback]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl_jsonfallback]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}[suggestionsurl]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-

472f-a0ff-e1416b8b2e3a}[suggestionsurl]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[suggestionsurlfallback]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[previewurl]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[previewurl]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[previewurlfallback]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[previewurlfallback]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[faviconurl]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[faviconurl]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[faviconurlfallback]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[faviconpath]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[codepage]
Queries value: HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[codepage]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[sortindex]
Queries value: HKCU\software\microsoft\internet explorer\tabbedbrowsing[enabled]
Queries value: HKCU\software\microsoft\internet explorer\toolbar[locked]
Queries value: HKCU\software\microsoft\internet explorer\linksbar[enabled]
Queries value: HKCU\software\microsoft\internet
explorer\tabbedbrowsing[activitymetertimerinterval]
Queries value: HKCU\software\microsoft\internet
explorer\tabbedbrowsing[activitymeterdisable]
Queries value: HKCU\software\microsoft\internet
explorer\tabbedbrowsing[quicktabsthreshold]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}[clsid]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-
4134-82b7-f2ba38496583}\iexplore[count]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}[buttontext]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}[menutext]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}[menucustomize]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}[menustatusbar]
Queries value: HKCU\software\microsoft\internet
explorer\lowregistry\extensions\cmdmapping[{e2e2dd38-d088-4134-82b7-f2ba38496583}]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[clsid]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-
11d2-bb9e-00c04f795683}\iexplore[count]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[buttontext]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[menutext]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[menucustomize]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[menustatusbar]
Queries value: HKCU\software\microsoft\internet
explorer\lowregistry\extensions\cmdmapping[{fb5f1910-f110-11d2-bb9e-00c04f795683}]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[default visible]
Queries value: HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[icon]
Queries value: HKCU\software\microsoft\internet
explorer\tabbedbrowsing[thumbnailbehavior]
Queries value: HKCU\software\microsoft\internet
explorer\toolbar\webbrowser[itbar7height]
Queries value: HKCR\clsid\{0002df01-0000-0000-c000-
000000000046}\localserver32[localserver32]
Queries value: HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32[]
Queries value: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-
b1deb82c6e5e}\localserver32[localserver32]
Queries value: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\localserver32[]
Queries value: HKLM\software\microsoft\rpc\securityservice[10]
Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
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\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\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\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\rpc\securityservice[defaultauthlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
Queries value: HKCR\interface\{8a7476f4-d264-4e13-ae72-20cd9831d98c}\proxystubclsid32[]
Queries value: HKCR\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}\proxystubclsid32[]
Queries value: HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32[]
Queries value: HKCR\interface\{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14}\proxystubclsid32[]
Queries value: HKCU\software\microsoft\internet explorer\main[enableprebinding]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
Queries value: HKCU\software\microsoft\internet explorer\main[window title]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[statusbarweb]
Queries value: HKCU\software\microsoft\internet explorer\main[statusbarweb]
Queries value: HKLM\software\microsoft\internet explorer\main[statusbarweb]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[enable browser
extensions]
Queries value: HKCU\software\microsoft\internet explorer\main[enable browser
extensions]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[alwaysshowmenus]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nobandcustomize]
Queries value: HKCU\software\microsoft\internet
explorer\toolbar\webbrowser[itbar7layout]
Queries value: HKCU\software\microsoft\internet explorer\main[alwaysshowmenus]
Queries value: HKLM\software\microsoft\internet explorer\main[alwaysshowmenus]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore[count]
Queries value: HKCR\clsid\{18df081c-e8ad-4283-a596-
fa578c2ebdc3}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[appid]
Queries value: HKCR\appid\{77ab4812-5411-4ea9-8437-77ad0f230302}[dllsurrogate]
Queries value: HKCR\appid\{77ab4812-5411-4ea9-8437-77ad0f230302}[localservice]
Queries value: HKCR\clsid\{18df081c-e8ad-4283-a596-
fa578c2ebdc3}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserver32[]
Queries value: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-
784b7d6be0b3}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}[appid]
Queries value: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-
784b7d6be0b3}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore[loadtimecount]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
4283-a596-fa578c2ebdc3}\iexplore[loadtime]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
435b-bc74-9c25c1c588a9}\iexplore[count]
Queries value: HKCR\clsid\{dbc80044-a445-435b-bc74-
9c25c1c588a9}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}[appid]
Queries value: HKCR\clsid\{dbc80044-a445-435b-bc74-
9c25c1c588a9}\inprocserver32[threadingmodel]
Queries value: HKLM\software\javasoft\java plug-in\10.2.0[usenewjavaplugin]
Queries value: HKLM\software\javasoft\java runtime environment\1.7.0_02[javahome]
Queries value: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas[]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]
Queries value: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0\win32[]
Queries value: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
Queries value: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}[appid]
Queries value: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[icon]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[minlevel]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[icon]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\1[minlevel]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\1[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[icon]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\2[minlevel]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\2[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[icon]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3[minlevel]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[icon]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\4[minlevel]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\4[recommendedlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[currentlevel]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[urlencoding]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize]
Queries value: HKCR\protocols\handler\about[clsid]
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\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams[iexplore.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[iexplore.exe]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
Queries value: HKLM\software\microsoft\internet explorer\application compatibility[iexplore.exe]
Queries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit]
Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
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[iexplore.exe]
Queries value: HKCR\.html[content type]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing[iexplore.exe]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2100]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[istextplainhonored]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject[iexplore.exe]
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: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[iexplore.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
Queries value: HKCR\clsid\{a6b222ab-a5ea-4899-b230-
084657eddc7d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32[]
Queries value: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}[appid]
Queries value: HKCR\clsid\{a6b222ab-a5ea-4899-b230-
084657eddc7d}\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: HKCU\software\microsoft\internet explorer\zoom[resettextsizeonstartup]
Queries value: HKCU\software\microsoft\internet explorer\zoom[resettextsizeonzoom]
Queries value: HKCU\software\microsoft\internet explorer\zoom[resetzoomonstartup2]
Queries value: HKCU\software\microsoft\internet explorer\zoom[zoomfactor]
Queries value: HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
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\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: HKCR\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}\proxystubclsid32[]
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[iexplore.exe]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[allsitescompatibilitymode]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[intranetcompatibilitymode]
Queries value: HKCU\software\microsoft\internet explorer\browseremulation[localmachinecompatibilitymode]
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\currentversion\internet settings\zones\3[2700]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3[2700]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[iexplore.exe]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones[securitysafe]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}[appid]
Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32[]
Queries value: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[appid]
Queries value: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\proxystubclsid32[]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-000000000046}[appid]
Queries value: HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\typelib[]
Queries value: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\typelib[version]
Queries value: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
Queries value: HKLM\software\microsoft\rpc[udtalignmentpolicy]
Queries value: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[]
Queries value: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32[]
Queries value: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}[appid]
Queries value: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
Queries value: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[]
Queries value: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version]
Queries value: HKCU\software\microsoft\internet explorer\toolbar[menuuserexpanded]
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\interface\{9d973e3b-f610-4f03-83d3-aed90c3237ac}\synchronousinterface[]
Queries value: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1c00]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1207]
Queries value: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[appid]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]
Queries value: HKLM\software\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[compatibility flags]
Queries value: HKLM\software\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[miscstatus flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[120b]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1208]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2201]
Queries value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32[inprocserver32]
Queries value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32[]
Queries value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}[appid]
Queries value: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}[appid]
Queries value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32[threadingmodel]
Queries value: HKLM\software\javasoft\java runtime environment\1.7.0_02[eula]
Queries value: HKLM\software\javasoft\java plug-in\10.2.0[usejava2iexplorer]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore[count]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1201]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\jvm.dll[checkapphelp]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2000]
Queries value: HKCR\htmlfile\shell[]
Queries value: HKCR\htmlfile\shell\edit\command[]
Queries value: HKLM\software\microsoft\internet explorer\default html editor[stubs]
Queries value: HKLM\software\microsoft\internet explorer\default html editor[description]
Queries value: HKLM\software\microsoft\internet explorer\default html

editor\shell\edit[friendlyappname]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm[progid]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm[application]
Queries value: HKCR\.htm[]
Queries value: HKCR\applications\notepad.exe\shell\edit\command[]
Queries value: HKCU\software\microsoft\internet explorer\main[checkdocumentforprogid]
Queries value: HKLM\software\microsoft\internet explorer\main[checkdocumentforprogid]
Queries value: HKLM\software\microsoft\internet explorer\feed discovery[enabled]
Queries value: HKCU\software\microsoft\ftp[use web based ftp]
Queries value: HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowclsidprogidmapping]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[docobject]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[browseinplace]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[isshortcut]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[alwaysshowext]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[nevershowext]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x401]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x401]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[appid]
Queries value: HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cacheoptions]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll,-9216]
Queries value: HKLM\software\microsoft\internet explorer\main[maxrenderline]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[use formsuggest]
Queries value: HKCU\software\microsoft\internet explorer\main[use formsuggest]
Queries value: HKLM\software\microsoft\internet explorer\main[use formsuggest]
Queries value: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-
11cf-aaa5-00401c608501}\iexplore[type]
Queries value: HKCU\software\microsoft\internet explorer\caretbrowsing[enableonstartup]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[migrationtime]
Queries value: HKLM\software\microsoft\internet explorer\migration[ie installed date]
Queries value: HKCU\software\microsoft\internet
explorer\main[ie8runonceperinstallcompleted]
Queries value: HKCU\software\microsoft\internet explorer\main[ie8runoncecompletiontime]
Queries value: HKCU\software\microsoft\internet explorer\main[check_associations]
Queries value: HKLM\software\microsoft\internet explorer\main[check_associations]
Queries value: HKCR\http[editflags]
Queries value: HKCR\http[url protocol]
Queries value: HKCR\http[webnavigableclsid]
Queries value: HKCR\https[editflags]

Queries value: HKCR\https[url protocol]
Queries value: HKCR\ftp[editflags]
Queries value: HKCR\ftp[url protocol]
Queries value: HKCR\internetshortcut[editflags]
Queries value: HKCR\internetshortcut\defaulticon[]
Queries value: HKCR\.htm[content type]
Queries value: HKCR\http\shell\open\command[]
Queries value: HKCR\http\shell\open\ddeexec[]
Queries value: HKCR\http\shell\open\ddeexec[noactivatehandler]
Queries value: HKCR\http\shell\open\ddeexec\application[]
Queries value: HKCR\http\shell\open\ddeexec\topic[]
Queries value: HKCR\https\shell\open\command[]
Queries value: HKCR\https\shell\open\ddeexec[]
Queries value: HKCR\https\shell\open\ddeexec[noactivatehandler]
Queries value: HKCR\https\shell\open\ddeexec\application[]
Queries value: HKCR\https\shell\open\ddeexec\topic[]
Queries value: HKCR\ftp\shell\open\command[]
Queries value: HKCR\ftp\shell\open\ddeexec[]
Queries value: HKCR\ftp\shell\open\ddeexec\ifexec[]
Queries value: HKCR\ftp\shell\open\ddeexec[noactivatehandler]
Queries value: HKCR\ftp\shell\open\ddeexec\application[]
Queries value: HKCR\ftp\shell\open\ddeexec\topic[]
Queries value: HKCR\htmlfile\shell\open[]
Queries value: HKCR\htmlfile\shell\open[muiverb]
Queries value: HKCR\htmlfile\shell\open\command[]
Queries value: HKCR\htmlfile\shell\open\ddeexec[]
Queries value: HKCR\htmlfile\shell\open\ddeexec[noactivatehandler]
Queries value: HKCR\htmlfile\shell\open\ddeexec\application[]
Queries value: HKCR\htmlfile\shell\open\ddeexec\topic[]
Queries value: HKCR\mhtmlfile\shell[]
Queries value: HKCR\htmlfile\shell\opennew[]
Queries value: HKCR\htmlfile\shell\opennew[muiverb]
Queries value: HKCR\htmlfile\shell\opennew\command[]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec[]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec\ifexec[]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec[noactivatehandler]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec\application[]
Queries value: HKCR\htmlfile\shell\opennew\ddeexec\topic[]
Queries value: HKCR\.mht[]
Queries value: HKCR\.mht[content type]
Queries value: HKCR\.mhtml[]
Queries value: HKCR\.mhtml[content type]
Queries value: HKCR\mhtmlfile\shell\open[]
Queries value: HKCR\mhtmlfile\shell\open[muiverb]
Queries value: HKCR\mhtmlfile\shell\open\command[]
Queries value: HKCR\mhtmlfile\shell\open\ddeexec[]
Queries value: HKCR\mhtmlfile\shell\open\ddeexec\application[]
Queries value: HKCR\mhtmlfile\shell\open\ddeexec\topic[]
Queries value: HKCR\mhtmlfile\shell\opennew[]
Queries value: HKCR\mhtmlfile\shell\opennew[muiverb]
Queries value: HKCR\mhtmlfile\shell\opennew\command[]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec[]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec\ifexec[]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec[noactivatehandler]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec\application[]
Queries value: HKCR\mhtmlfile\shell\opennew\ddeexec\topic[]
Queries value: HKCR\.url[]
Queries value: HKCR\internetshortcut\clsid[]
Queries value: HKCR\internetshortcut\shell\open[clsid]
Queries value: HKCR\internetshortcut\shell\open[legacydisable]
Queries value: HKCR\internetshortcut\shell\open\command[]
Queries value: HKCR\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}[]
Queries value: HKCR\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}[friendlytypename]
Queries value: HKCR\applications\iexplore.exe\shell\open\command[]
Queries value: HKCU\software\microsoft\internet explorer\suggested
sites[objectscreated]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[slicepath]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[version]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[upgradetime]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
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: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCU\software\microsoft\internet explorer\user
preferences[2d53cffc5c1a3dd2e97b7979ac2a92bd59bc839e81]
Queries value: HKCU\software\microsoft\internet explorer\user
preferences[88d7d0879dab32e14de5b3a805a34f98aff34f5977]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[local appdata]
Queries value: HKLM\software\javasoft\java runtime environment\1.7[javahome]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[java]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[java]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[gdiprocesshandlequota]
Queries value: HKCU\software\microsoft\internet
explorer\tabbedbrowsing[quicktabslastused]
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\direct3d[geometrydriver]
Queries value: HKLM\software\microsoft\direct3d[loaddebugruntime]
Queries value: HKLM\software\microsoft\direct3d[forcedriverflagsoff]
Queries value: HKLM\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-
9b1f4867732a}\0000[installeddisplaydrivers]
Queries value: HKLM\system\currentcontrolset\control\watchdog\display[earecovery]
Queries value: HKLM\system\currentcontrolset\control\watchdog\display[fullrecovery]
Queries value: HKLM\software\microsoft\direct3d\drivers[softwareonly]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[java.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKLM\software\javasoft\java update\policy[promptautoupdatecheck]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[java.exe]
Queries value: HKCU\control panel\desktop[fontsmoothingorientation]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[themeactive]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[dllname]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[sizename]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[colorname]
Sets/Creates value: HKCU\software\microsoft\internet explorer\recovery\active[{3af75143-
f55e-11e5-ae32-08002719344d}]
Sets/Creates value: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}[]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32[]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}[]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32[]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}[]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}\inprocserver32[]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}[]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}\inprocserver32[]
Sets/Creates value: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}[]
Sets/Creates value: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32[]
Sets/Creates value: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\javaplugin.1020\clsid[]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cachepath]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cacheprefix]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cachelimit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cacheoptions]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cacherepair]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
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[history]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[desktop]
Value changes: HKCU\software\microsoft\internet explorer\main[compatibilityflags]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[favorites]
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\internet settings\zones[securitysafe]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]
Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common appdata]
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]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[local appdata]
Value changes: HKCU\software\microsoft\internet explorer\main\windowssearch[version]
Value changes: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32[]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-4134-82b7-f2ba38496583}\iexplore[type]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-4134-82b7-f2ba38496583}\iexplore[count]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-4134-82b7-f2ba38496583}\iexplore[time]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-11d2-bb9e-00c04f795683}\iexplore[type]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-11d2-bb9e-00c04f795683}\iexplore[count]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-11d2-bb9e-00c04f795683}\iexplore[time]
Value changes: HKCU\software\microsoft\internet explorer\main[fullscreen]
Value changes: HKCU\software\microsoft\internet explorer\main[window_placement]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore[type]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore[count]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore[time]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore[loadtime]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\iexplore[loadtimecount]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}\iexplore[type]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}\iexplore[count]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}\iexplore[time]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore[type]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore[count]
Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\iexplore[time]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016032920160330[cachepath]
Value changes: HKCU\software\microsoft\direct3d\mostrecentapplication[name]