Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 26, Task ID: 102

Task ID:	102
Risk Level:	7
Date Processed:	2016-04-28 12:49:11 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe"
Sample ID:	26
Type:	basic
Owner:	admin
Label:	bdc27c485a35c61c7bf0bfedbf9b0b3f
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	994608 bytes
MD5:	bdc27c485a35c61c7bf0bfedbf9b0b3f
SHA256:	f89295cb1a70b1278e66a56acc10ee088a2ad2022664023d870c4698d0b4c7a1
Description:	None

Pattern Matching Results

3 Long sleep detected
6 Renames file on boot
2 PE: Nonstandard section
3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]
1 YARA score 1
7 Signed by adware producer [Adware, PUA]
5 Creates process in suspicious location
3 Connects to local host
4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable
Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\WINDOWS\Temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
["c:\windows\temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe"]

Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe
[C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe { "json_send_time" : "28/4/2016 14:49:54:686" ,
"product_id_version" : "" , "product_type" : "" , "product_id" : "" , "offer_id" : "77315" ,
"user_type" : "NULL" , "result" : "Success" , "user_operating_system_bits" : "" ,
"current_default_search" : "" , "current_homepage" : "" , "current_toolbars" : "" ,
"attempt_number" : "1" , "is_silent" : "" , "user_ms_dotnet_framework_ver" : "" ,
"user_acount_type" : "" , "user_ie_version" : "" , "user_default_browser_version" : "" ,
"user_default_browser" : "" , "user_service_pack" : "" , "user_operating_system" : "" ,
"revision_number" : "0" , "build_id" : "00000000" , "dm_version" : "1.3.7.9_NoStatic.130521.01" ,
"bundle_id" : "48dd2e32-2172-4f35-aac6-4a328190391d" , "machine_user_id" : "{6C411187-B302-4113-
B992-56B56F0A7EFC}" , "send_attempt" : "0" , "channel_id" : "" , "installation_session_id" :
"778F2147-88DC-4ED8-A85E-12949F8245E9" , "publisher_internal_id" : "1" , "publisher_id" :
"Brothersoft" , "publisher_account_id" : "Brothersoft" , "order" : "1.0" , "phase" : "Init" ,
"Is_Test" : "0" }]

Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe
[C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe { "user_ie_security_level" : "Unknown-0" ,
"json_send_time" : "28/4/2016 14:51:2:427" , "internal_error_description" : "HttpPost to CMS
result- try3: Error navigating (in GetNavigateError error code is -2146697211) to url:
http://cms.distributionengine.conduit-services.com//MainOffer/77256/?CurrentStep=1" ,
"internal_error_number" : "3" , "is_parallel" : "0" , "mrs_id" : "-1" , "vector_id" : "581222" ,
"rule_id" : "580630" , "product_id_version" : "" , "product_type" : "" , "product_id" : "" ,
"offer_id" : "77315" , "general_status_code" : "6" , "duration_details" : " InitPluginsDir:0
initializeParams:430 load_BITool:31 send_BI_Init:60 load_DownloadACC:70 retrieveUISource:10
unpack_webappfolder:0 unpack_icon:0 RetrieveMainOfferKey:0 unpack_OpenCandyDll:581
load_webapphost:0 unpack_ProxyInstaller:30 navigate_loadingUI:1241 navigateAsync_constMainOffer:0
BuildUserProfile:40 retrieve cid:10 callService1:62854 parse_ResponseXml:2184
init_external_offer:0 DiscoverUserAgent:210 " , "phase_duration" : "" , "error_details" : "55
Failed to communicate with CMS for main offer" , "result" : "Error" ,
"user_operating_system_bits" : "32" , "current_default_search" :
"http://search.live.com/results.aspx?q={searchTerms}&src=IE-SearchBox&Form=IE8SRC" ,
"current_homepage" : "about:blank" , "current_toolbars" : "" , "attempt_number" : "1" ,
"is_silent" : "0" , "user_ms_dotnet_framework_ver" : "3.5" , "user_acount_type" : "" ,
"user_ie_version" : "8.0.6001.18702" , "user_default_browser_version" : "8.0.6001.18702" ,
"user_default_browser" : "IEXPLORE.EXE" , "user_service_pack" : "3.0" , "user_operating_system" :
"Microsoft Windows XP" , "revision_number" : "0" , "build_id" : "00000000" , "dm_version" :
"1.3.7.9_NoStatic.130521.01" , "bundle_id" : "48dd2e32-2172-4f35-aac6-4a328190391d" ,
"machine_user_id" : "{6C411187-B302-4113-B992-56B56F0A7EFC}" , "send_attempt" : "0" ,
"channel_id" : "" , "installation_session_id" : "778F2147-88DC-4ED8-A85E-12949F8245E9" ,

"publisher_internal_id" : "1" , "publisher_id" : "Brothersoft" , "publisher_account_id" : "Brothersoft" , "order" : "2.0" , "phase" : "InitComplete" , "Is_Test" : "0" }]
Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Terminates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\oleacc-msaa-loaded
Creates mutex: \BaseNamedObjects\ActiveSetupMutexId
Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local settings!temporary internet files!content.ie5!
Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!cookies!
Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local settings!history!history.ie5!
Creates mutex: \BaseNamedObjects\WininetConnectionMutex
Creates mutex: \BaseNamedObjects\!PrivacIE!SharedMemory!Mutex
Creates mutex: \BaseNamedObjects\ZonesCounterMutex
Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex: \BaseNamedObjects\MSIMGSIZECacheMutex
Creates mutex: \BaseNamedObjects_!SHMSFTHISTORY!_
Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!local settings!history!history.ie5!mshist012016042820160429!
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.IDH
Creates event: \BaseNamedObjects\userenv: User Profile setup event
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore: \BaseNamedObjects\OleDfRoot000024B99

File System Events

Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsa2.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp
Creates: C:\DOCUME~1
Creates: C:\DOCUME~1\Admin
Creates: C:\DOCUME~1\Admin\LOCALS~1
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\System.dll
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\System.dll
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\webapphost.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\BI.exe
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\DM_loader.gif
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\DownloadACC.exe
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\Failed.htm
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\icon.png
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\OCSetupHlp.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsv4.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nst5.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn6.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\inetc.dll
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\webapphost.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\a.txt
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\ProxyInstaller.exe
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\~DF4B9C.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\inetc.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\offer.xml
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\navcancl[1]
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn6.tmp\inetc.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\navcancl[1]

Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\background_gradient[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\info_48[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\info_48[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\bullet[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\background_gradient[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\info_48[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\bullet[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\bullet[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\dnserrordiagoff_webOC[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\dnserrordiagoff_webOC[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\down[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\background_gradient[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\down[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\dnserrordiagoff_webOC[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\info_48[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\bullet[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\xml.dll
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\xml.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\nsArray.dll
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\nsArray.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\down[2]
Creates: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\errorPageStrings[1]
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsy7.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nss8.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm9.tmp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\inetc.dll
Creates: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012016042820160429
Creates: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012016042820160429\index.dat
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\a.txt
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm9.tmp\inetc.dll
Opens: C:\WINDOWS\Prefetch\BDC27C485A35C61C7BF0BFEDBF9B0-17324D5A.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config

Opens: C:\WINDOWS\Temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
Opens: C:\windows\temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe.124.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Config
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\shfolder.dll
Opens: C:\WINDOWS\system32\setupapi.dll
Opens: C:\
Opens: C:\Documents and Settings
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp
Opens: C:\WINDOWS\Temp\42f86ce3-3213-45b1-8684-b119ee2cb467
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\System.dll
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\webapphost.dll
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\webapphost.dll.2.Manifest
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\webapphost.dll.2.Config
Opens: C:\WINDOWS\system32\winspool.drv
Opens: C:\WINDOWS\system32\oledlg.dll
Opens: C:\WINDOWS\system32\crypt32.dll
Opens: C:\WINDOWS\system32\msasn1.dll
Opens: C:\WINDOWS\system32\oleacc.dll
Opens: C:\WINDOWS\system32\msvcp60.dll
Opens: C:\WINDOWS\system32\oleaccrc.dll
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\WINDOWS\system32\WININET.dll.123.Manifest
Opens: C:\WINDOWS\system32\WININET.dll.123.Config
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\webapphost.dll.1000.Manifest
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\BI.exe
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\systest.sdb
Opens: C:\Documents and Settings\Admin\Local Settings
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe.Manifest
Opens: C:\WINDOWS\Prefetch\BI.EXE-35A91DD2.pf
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nse3.tmp\BI.exe.124.Manifest
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsv4.tmp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\inetc.dll
Opens: C:\WINDOWS\Fonts\sserife.fon
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\system32\MSIMTF.dll
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\History
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
Opens: C:\Documents and Settings\Admin\Cookies
Opens: C:\Documents and Settings\Admin\Cookies\index.dat
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.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\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\sensapi.dll
Opens: C:\WINDOWS\system32\mswsock.dll
Opens: C:\WINDOWS\system32\rasadhlp.dll
Opens: C:\WINDOWS\system32\dnsapi.dll
Opens: C:\WINDOWS\system32\iphlpapi.dll
Opens: C:\WINDOWS\system32\drivers\etc\hosts
Opens: C:\WINDOWS\system32\rsaenh.dll
Opens: C:\WINDOWS\system32\asycfilt.dll
Opens: C:\WINDOWS\system32\msv1_0.dll
Opens: C:\WINDOWS\system32\clbcatq.dll

Opens: C:\WINDOWS\system32\comres.dll
Opens: C:\WINDOWS\Registration\R000000000007.clb
Opens: C:\WINDOWS\system32\ieframe.dll
Opens: C:\Program Files\Internet Explorer\iexplore.exe
Opens: C:\WINDOWS\system32\ieframe.dll.123.Manifest
Opens: C:\WINDOWS\system32\ieframe.dll.123.Config
Opens: C:\WINDOWS\system32\en-US\ieframe.dll.mui
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\inetc.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\icon.png
Opens: C:\WINDOWS\system32\mshtml.dll
Opens: C:\WINDOWS\system32\msls31.dll
Opens: C:\WINDOWS\system32\hnetcfg.dll
Opens: C:\WINDOWS\system32\wshtcpip.dll
Opens: C:\WINDOWS
Opens: C:\WINDOWS\system32
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\navcancl[2]
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\a.txt
Opens: C:\WINDOWS\system32\psapi.dll
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsn6.tmp\
Opens: C:\WINDOWS\system32\mlang.dll
Opens: C:\WINDOWS\system32\MLANG.dll.123.Manifest
Opens: C:\WINDOWS\system32\MLANG.dll.123.Config
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\navcancl[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\navcancl[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
Opens: C:\WINDOWS\system32\iepeers.dll
Opens: C:\WINDOWS\system32\iepeers.dll.123.Manifest
Opens: C:\WINDOWS\system32\iepeers.dll.123.Config
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
Opens: C:\WINDOWS\system32\jscript.dll
Opens: C:\WINDOWS\system32\winlogon.exe
Opens: C:\WINDOWS\system32\xpsp2res.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\background_gradient[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\info_48[1]
Opens: C:\WINDOWS\system32\imgutil.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\bullet[1]
Opens: C:\WINDOWS\system32\pngfilt.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\background_gradient[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\info_48[2]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\bullet[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\info_48[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\bullet[2]
Opens: C:\WINDOWS\Fonts\SEGOEUI.TTF
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\dnserrordiagoff_webOC[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\down[1]
Opens: C:\WINDOWS\Fonts\wingding.ttf
Opens: C:\WINDOWS\system32\en-US\mshtml.dll.mui
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5\CXCXW1MR\dnserrordiagoff_webOC[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X\dnserrordiagoff_webOC[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\background_gradient[2]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\down[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\info_48[2]
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\xml.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\offer.xml
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\nsArray.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\bullet[2]
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\down[2]
Opens: C:
Opens: C:\WINDOWS\system32\config
Opens: C:\WINDOWS\system32\drivers
Opens: C:\WINDOWS\system32\drivers\etc
Opens: C:\WINDOWS\Temp
Opens: C:\WINDOWS\WinSxS
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:\WINDOWS\system32\user32.dll
Opens: C:\WINDOWS\system32\gdi32.dll
Opens: C:\WINDOWS\system32\advapi32.dll
Opens: C:\WINDOWS\system32\rpcrt4.dll
Opens: C:\WINDOWS\system32\secur32.dll
Opens: C:\WINDOWS\system32\msvcrt.dll
Opens: C:\WINDOWS\system32\shlwapi.dll
Opens: C:\WINDOWS\system32\ole32.dll
Opens: C:\WINDOWS\system32\version.dll
Opens: C:\WINDOWS\system32\ctype.nls
Opens: C:\WINDOWS\system32\sortkey.nls
Opens: C:\WINDOWS\system32\wininet.dll
Opens: C:\WINDOWS\system32\normaliz.dll
Opens: C:\WINDOWS\system32\urlmon.dll
Opens: C:\WINDOWS\system32\oleaut32.dll
Opens: C:\WINDOWS\system32\iertutil.dll
Opens: C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM
Opens: C:\WINDOWS\system32\userenv.dll
Opens: C:\WINDOWS\Temp\42f86ce3-3213-45b1-8684-b119ee2cb467\969_inetc.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\Failed.htm
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\WINDOWS\Fonts\arialbd.ttf
Opens: C:\WINDOWS\Fonts\verdana.ttf
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsy7.tmp
Opens: C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp
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:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\inetc.dll
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\MSHist012016042820160429
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012016042820160429\index.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\a.txt
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsm9.tmp\
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nsa2.tmp
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\System.dll
Writes to: C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\webapphost.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\BI.exe
Writes to: C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\DM_loader.gif
Writes to: C:\Documents and Settings\Admin\Local
Settings\Temp\nse3.tmp\DownloadACC.exe
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\Failed.htm
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\icon.png

Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nst5.tmp
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\inetc.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\OCSetupHlp.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\ProxyInstaller.exe
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\inetc.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\navcancl[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\navcancl[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\background_gradient[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\info_48[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\bullet[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\background_gradient[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\info_48[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\bullet[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\info_48[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\bullet[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\dnserrordiagoff_webOC[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\dnserrordiagoff_webOC[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\down[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\background_gradient[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\down[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\dnserrordiagoff_webOC[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\info_48[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\bullet[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\offer.xml
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\xml.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\nsArray.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\down[2]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\errorPageStrings[1]
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nss8.tmp
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\inetc.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012016042820160429\index.dat
Reads from: C:\WINDOWS\Temp\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\nsa2.tmp
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\BI.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\nst5.tmp
Reads from: C:\AUTOEXEC.BAT
Reads from: C:\WINDOWS\system32\drivers\etc\hosts
Reads from: C:\WINDOWS\system32\rsaenh.dll
Reads from: C:\WINDOWS\Registration\R000000000007.clb
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\offer.xml

Reads from: C:\WINDOWS\Prefetch\BI.EXE-35A91DD2.pf
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp\Failed.htm
Reads from: C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\nss8.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsm1.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nse3.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsv4.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\navcancl[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\a.txt
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsn6.tmp\inetc.dll
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\navcancl[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\navcancl[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\ErrorPageTemplate[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\errorPageStrings[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\errorPageStrings[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\background_gradient[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\info_48[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\bullet[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\ErrorPageTemplate[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\errorPageStrings[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\httpErrorPagesScripts[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\background_gradient[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\info_48[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\bullet[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\info_48[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\bullet[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\dnserrordiagoff_webOC[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\httpErrorPagesScripts[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\down[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\dnserrordiagoff_webOC[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\UH4D6D6X\dnserrordiagoff_webOC[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\background_gradient[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\down[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\info_48[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\bullet[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ErrorPageTemplate[1]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNQBKF\down[2]
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsy7.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp
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:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\a.txt
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsm9.tmp\inetc.dll

Network Events

DNS query: ude.conduit-data.com
DNS query: offering.service.distributionengine.conduit-services.com
DNS query: cms.distributionengine.conduit-services.com
DNS response: offering.service.distributionengine.ams.conduit-services.com ⇒ 195.78.120.173
Connects to: 195.78.120.173:80
Connects to: 127.0.0.1:1053
Sends data to: 8.8.8.8:53
Sends data to: offering.service.distributionengine.ams.conduit-services.com:80 (195.78.120.173)
Receives data from: 0.0.0.0:0
Receives data from: offering.service.distributionengine.ams.conduit-services.com:80 (195.78.120.173)

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Creates key: HKCU\software\appdatalow\software\smartbar
Creates key: HKCU\software
Creates key: HKCU\software\appdatalow
Creates key: HKCU\software\appdatalow\software
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: 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\windows\currentversion\internet settings\connections
Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location awareness
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
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: HKLM\system\currentcontrolset\control\session manager
Creates key: HKCU\software\conduit\distributionengine\1\offerhistory\755131
Creates key: HKCU\software\conduit
Creates key: HKCU\software\conduit\distributionengine
Creates key: HKCU\software\conduit\distributionengine\1
Creates key: HKCU\software\conduit\distributionengine\1\offerhistory
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429
Creates key: HKCU\software\microsoft\internet explorer\main\windowssearch
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\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
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\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\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\comctl32.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\version.dll
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\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: 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\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shfolder.dll
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\
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
Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\software\microsoft\rpc\pagedbuffers
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Opens key: HKCU\software\classes\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: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.dll
Opens key: HKCU\software\appdatalow\software\smartbar
Opens key: HKCU\software\clients\startmenuinternet
Opens key: HKLM\software\clients\startmenuinternet
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\winspool.drv
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oledlg.dll
Opens key: HKCU\software\classes\clsid
Opens key: HKCR\clsid
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
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\msvcp60.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleacc.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.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\urlmon.dll
Opens key: HKCU\software\classes\protocols\name-space handler\
Opens key: HKCR\protocols\name-space handler
Opens key: HKCU\software\classes\protocols\name-space handler
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\webapphost.dll
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\apphelp.dll
Opens key: HKLM\system\wpa\tabletpc
Opens key: HKLM\system\wpa\mediacenter
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\bi.exe
Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\bi.exe
Opens key: HKLM\software\microsoft\ctf\compatibility\bi.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\bi.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\inetc.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
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: 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
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: 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: 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\windows\currentversion\internet settings\http
filters\rpa
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\software\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: HKU\
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\image file execution options\mswsock.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasadhlp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\microsoft\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\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
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\msv1_0.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\asycfilt.dll
Opens key: HKCU\software\microsoft\internet explorer\main
Opens key: HKCU\software\microsoft\internet explorer\searchscopes
Opens key: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
Opens key: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comres.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\clbcatq.dll
Opens key: HKLM\software\microsoft\com3\debug
Opens key: HKLM\software\microsoft\internet explorer\toolbar
Opens key: HKLM\software\microsoft\net framework setup\ndp
Opens key: HKLM\software\microsoft\net framework setup\ndp\v2.0.50727
Opens key: HKLM\software\classes
Opens key: HKLM\software\microsoft\net framework setup\ndp\v3.0

Opens key: HKLM\software\microsoft\net framework setup\ndp\v3.5
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
Opens key: HKCU\software\conduit\distributionengine\1\offerhistory
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver
Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ieframe.dll
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
Opens key: HKLM\software\microsoft\internet explorer\setup
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll
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: 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\microsoft\internet explorer\main
Opens key: HKCU\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_protocol

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_protocol
Opens key: HKLM\software\policies\microsoft\internet explorer\browseremulation
Opens key: HKCU\software\policies\microsoft\internet explorer\browseremulation
Opens key: HKCU\software\classes\protocols\name-space handler\res\
Opens key: HKCR\protocols\name-space handler\res
Opens key: HKCU\software\classes\protocols\name-space handler*\
Opens key: HKCR\protocols\name-space handler*
Opens key: HKCU\software\classes\protocols\handler\res
Opens key: HKCR\protocols\handler\res
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msls31.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mshtml.dll
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_aria_support
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_aria_support
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_private_font_setting
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_private_font_setting
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_css_show_hide_events
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_css_show_hide_events
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_display_node_advise_kb833311
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_display_node_advise_kb833311
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_allow_expanduri_bypass
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_allow_expanduri_bypass
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_databinding_support
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_databinding_support
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enforce_bstr
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enforce_bstr
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enable_dynamic_object_caching

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_dynamic_object_caching
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_object_caching
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_object_caching
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
Opens key: HKCU\software\microsoft\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\policies\microsoft\internet explorer\domstorage
Opens key: HKCU\software\microsoft\internet explorer\domstorage
Opens key: HKLM\software\microsoft\internet explorer\domstorage
Opens key: HKLM\software\policies\microsoft\internet explorer\safety\privacie
Opens key: HKCU\software\policies\microsoft\internet explorer\safety\privacie
Opens key: HKCU\software\microsoft\internet explorer\safety\privacie
Opens key: HKLM\software\microsoft\internet explorer\safety\privacie
Opens key: HKLM\software\policies\microsoft\cryptography
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: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
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\windows\currentversion\internet settings\zonemap\
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\hnetcfg.dll
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: 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: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wshtcpip.dll
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\policies\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key: HKCU\software\microsoft\internet explorer
Opens key: HKLM\software\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_load_shdoclc_resources
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_load_shdoclc_resources
Opens key: HKCU\software\classes\.htm
Opens key: HKCR\.htm
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: 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\classes\protocols\name-space handler\about\
Opens key: HKCR\protocols\name-space handler\about
Opens key: HKCU\software\classes\protocols\handler\about
Opens key: HKCR\protocols\handler\about
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_document_compatible_mode
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_document_compatible_mode
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\policies\microsoft\internet explorer\zoom
Opens key: HKCU\software\policies\microsoft\internet explorer\zoom
Opens key: HKCU\software\microsoft\internet explorer\zoom
Opens key: HKLM\software\microsoft\internet explorer\zoom
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_weboc_document_zoom
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_weboc_document_zoom
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_enable_compat_logging

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_enable_compat_logging
Opens key: HKCU\software\policies\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer\international
Opens key: HKLM\software\policies\microsoft\internet explorer\international\scripts
Opens key: HKCU\software\microsoft\internet explorer\international\scripts
Opens key: HKLM\software\microsoft\internet explorer\international\scripts
Opens key: HKLM\software\policies\microsoft\internet explorer\settings
Opens key: HKCU\software\microsoft\internet explorer\settings
Opens key: HKLM\software\microsoft\internet explorer\settings
Opens key: HKCU\software\microsoft\internet explorer\styles
Opens key: HKCU\software\microsoft\windows\currentversion\policies\activedesktop
Opens key: HKCU\software\microsoft\windows\currentversion\policies
Opens key: HKCU\software\microsoft\internet explorer\pagesetup
Opens key: HKCU\software\microsoft\internet explorer\menuext
Opens key: HKCU\software\microsoft\internet explorer\menuext\%s
Opens key: HKLM\system\currentcontrolset\control\nls\codepage
Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mlang.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKLM\software\microsoft\internet explorer\version vector
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_sslux
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_sslux
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_shim_mshelp_combine
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_shim_mshelp_combine
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown
Opens key: HKCU\software\classes\.css
Opens key: HKCR\.css
Opens key: HKCU\software\classes\protocols\filter\text/css
Opens key: HKCR\protocols\filter\text/css
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors
Opens key: HKLM\software\microsoft\internet explorer\default behaviors
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iepeers.dll
Opens key: HKCU\software\policies\microsoft\internet explorer\persistence
Opens key: HKLM\software\policies\microsoft\internet explorer\persistence
Opens key: HKCU\software\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\policies\microsoft\internet explorer\dxtrans
Opens key: HKCU\software\microsoft\internet explorer\dxtrans
Opens key: HKLM\software\microsoft\internet explorer\dxtrans
Opens key: HKCU\software\classes\.js
Opens key: HKCR\.js
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_feeds
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_feeds
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_script
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_script
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\
Opens key: HKLM\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\restrictions
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver
Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msimtf.dll
Opens key: HKLM\software\microsoft\ctf\tip
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile
Opens key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\localserver32
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandler32
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandlerx86
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\localserver
Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\treatas
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserverx86
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\localserver32
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandler32
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandlerx86
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\localserver
Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
Opens key: HKLM\software\microsoft\ctf\tip\
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
Opens key: HKCU\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
0f816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
Opens key: HKCU\software\policies\microsoft\internet explorer\control panel
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\url
history
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32

Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserverx86
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver
Opens key: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\jscript.dll
Opens key: HKLM\software\microsoft\windows script\features
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
Opens key: HKLM\software\microsoft\internet explorer\activex compatibility
Opens key: HKLM\software\microsoft\internet explorer\activex compatibility\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKCU\software\classes\appid\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
Opens key: HKCR\appid\bdc27c485a35c61c7bf0bfedbf9b0b3f.exe
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation
Opens key: HKCU\software\classes\.jpg
Opens key: HKCR\.jpg
Opens key: HKCU\software\classes\protocols\filter\image/jpeg
Opens key: HKCR\protocols\filter\image/jpeg
Opens key: HKCU\software\classes\.png
Opens key: HKCR\.png
Opens key: HKCU\software\classes\protocols\filter\image/png
Opens key: HKCR\protocols\filter\image/png
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_img
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_block_lmz_img
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imgutil.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\xpsp2res.dll
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32

Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandlerx86
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
Opens key: HKCU\software\classes\mime\database\content type
Opens key: HKCR\mime\database\content type
Opens key: HKCU\software\classes\mime\database\content type\image/bmp\bits
Opens key: HKCR\mime\database\content type\image/bmp\bits
Opens key: HKCU\software\classes\mime\database\content type\image/gif\bits
Opens key: HKCR\mime\database\content type\image/gif\bits
Opens key: HKCU\software\classes\mime\database\content type\image/jpeg\bits
Opens key: HKCR\mime\database\content type\image/jpeg\bits
Opens key: HKCU\software\classes\mime\database\content type\image/pjpeg\bits
Opens key: HKCR\mime\database\content type\image/pjpeg\bits
Opens key: HKCU\software\classes\mime\database\content type\image/png\bits
Opens key: HKCR\mime\database\content type\image/png\bits
Opens key: HKCU\software\classes\mime\database\content type\image/tiff\bits
Opens key: HKCR\mime\database\content type\image/tiff\bits
Opens key: HKCU\software\classes\mime\database\content type\image/x-icon\bits
Opens key: HKCR\mime\database\content type\image/x-icon\bits
Opens key: HKCU\software\classes\mime\database\content type\image/x-jg\bits
Opens key: HKCR\mime\database\content type\image/x-jg\bits
Opens key: HKCU\software\classes\mime\database\content type\image/x-png\bits
Opens key: HKCR\mime\database\content type\image/x-png\bits
Opens key: HKCU\software\classes\mime\database\content type\image/x-wmf\bits
Opens key: HKCR\mime\database\content type\image/x-wmf\bits
Opens key: HKCU\software\classes\mime\database\content type\image/x-png
Opens key: HKCR\mime\database\content type\image/x-png
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver
Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\pngfilt.dll
Opens key: HKLM\software\policies\microsoft\internet explorer\recovery
Opens key: HKCU\software\microsoft\internet explorer\recovery
Opens key: HKLM\software\microsoft\internet explorer\recovery
Opens key: HKCU\software\microsoft\ftp
Opens key: HKLM\software\policies\microsoft\internet explorer\services
Opens key: HKCU\software\microsoft\internet explorer\services
Opens key: HKLM\software\microsoft\internet explorer\services
Opens key: HKLM\software\policies\microsoft\internet explorer\activities
Opens key: HKCU\software\microsoft\internet explorer\activities
Opens key: HKLM\software\microsoft\internet explorer\activities
Opens key: HKLM\software\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKCU\software\policies\microsoft\internet explorer\infodelivery\restrictions
Opens key: HKLM\software\policies\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\microsoft\internet explorer\suggested sites
Opens key: HKCU\software\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\microsoft\internet explorer\feed discovery
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_isolate_named_windows
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_isolate_named_windows
Opens key: HKCU\software\classes\protocols\name-space handler\http\
Opens key: HKCR\protocols\name-space handler\http
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_maxconnectionsperserver
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
Opens key: HKCU\software\microsoft\windows\currentversion\urlmon settings
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\treatas
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\treatas
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserverx86
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\localserver32
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver32
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandler32
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandler32
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprochandlerx86
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\localserver
Opens key: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_navigation_sounds
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_navigation_sounds
Opens key: HKCU\appevents\schemes\apps\explorer\activatingdocument\.current
Opens key: HKCU\software\microsoft\internet explorer\searchproviders\
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: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xml.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\nsarray.dll
Opens key: HKLM\system\currentcontrolset\control\windows
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm
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\.htm
Opens key: HKCR\systemfileassociations\.htm
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: HKCU\appevents\schemes\apps\explorer\navigating\.current
Opens key: HKCU\software\microsoft\multimedia\sound mapper
Opens key: HKCU\software\microsoft\windows\currentversion\multimedia\midimap
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\.htm\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCR\.htm\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*
Opens key: HKCR*
Opens key: HKCU\software\classes*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCR*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
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\.htm\shellex\{000214e6-0000-0000-c000-000000000046}
Opens key: HKCR\.htm\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: HKCU\software\classes\protocols\name-space handler\file\
Opens key: HKCR\protocols\name-space handler\file
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: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_crossdomain_fix_kb867801
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_crossdomain_fix_kb867801
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\uxtheme.dll
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}
Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas
Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32
Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32
Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserverx86
Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver32
Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver32
Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler32
Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler32
Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandlerx86
Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver
Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\localserver

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\mshist012016042820160429
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: 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: 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\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[bdc27c485a35c61c7bf0bfedbf9b0b3f]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[bdc27c485a35c61c7bf0bfedbf9b0b3f]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
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\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:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
Queries value: HKLM\system\wpa\pnp[seed]
Queries value: HKLM\system\setup[osloaderpath]
Queries value: HKLM\system\setup[systempartition]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[generation]
Queries value: 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: HKLM\software\clients\startmenuinternet[]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
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\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[bi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[bi]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[bi.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKCU\software\microsoft\windows\currentversion\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: 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[bi.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: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[bi.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
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[programfilesdir]
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\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: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]

Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseobtainedtime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseterminatestime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpserver]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipautoconfigurationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
Queries value: HKLM\software\microsoft\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: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local appdata]
Queries value: HKCU\software\microsoft\internet explorer\main[start page]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes[defaultscope]
Queries value: HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[url]
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\system\currentcontrolset\control\session
manager\environment[processor_architecture]
Queries value: HKLM\software\microsoft\net framework setup\ndp\v2.0.50727[install]
Queries value: HKLM\software\microsoft\net framework setup\ndp\v2.0.50727[sp]
Queries value: HKLM\software\microsoft\net framework setup\ndp\v3.0[install]
Queries value: HKLM\software\microsoft\net framework setup\ndp\v3.0[sp]
Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKLM\software\microsoft\net framework setup\ndp\v3.5[install]
Queries value: HKLM\software\microsoft\net framework setup\ndp\v3.5[sp]
Queries value: HKLM\software\microsoft\windows\currentversion[currentversion]
Queries value: HKLM\software\microsoft\windows nt\currentversion[currentversion]
Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
Queries value: HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
Queries value: HKCR\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[createuricachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value: HKLM\software\microsoft\internet explorer\main[navigationdelay]
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: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
Queries value: HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046} 0x401]
Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046} 0x401]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
Queries value: HKCR\protocols\handler\res[clsid]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[appid]
Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams[bdc27c485a35c61c7bf0bfedbf9b0b3f.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[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_object_caching[*]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
Queries value: HKLM\software\microsoft\internet explorer\application compatibility[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit]
Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[urlencoding]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
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[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize]
Queries value: HKCU\software\microsoft\internet explorer[no3dborder]
Queries value: HKLM\software\microsoft\internet explorer[no3dborder]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKCR\.htm[content type]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing[*]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[istextplainhonored]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_safe_bindtoobject[*]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragscrollinset]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragscrolldelay]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragscrollinterval]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[*]
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\system\currentcontrolset\control\session manager[pendingfilerenameoperations2]
Queries value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2106]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\3[2106]
Queries value: HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
Queries value: HKLM\software\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: 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[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[2700]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[2700]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones[securitysafe]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nofileurl]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[2106]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[2106]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_subdownload_lockdown[*]
Queries value: HKCR\.css[content type]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_behaviors[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[2000]
Queries value: HKLM\software\microsoft\internet explorer\default behaviors[discovery]
Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]
Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid]
Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1400]
Queries value: HKCR\.js[content type]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]
Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]
Queries value: HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1201]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKCR\.jpg[content type]
Queries value: HKCR\.png[content type]
Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid]
Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
Queries value: HKCR\mime\database\content type\image/bmp\bits[0]
Queries value: HKCR\mime\database\content type\image/gif\bits[0]
Queries value: HKCR\mime\database\content type\image/jpeg\bits[0]
Queries value: HKCR\mime\database\content type\image/pjpeg\bits[0]
Queries value: HKCR\mime\database\content type\image/png\bits[0]
Queries value: HKCR\mime\database\content type\image/x-png\bits[0]
Queries value: HKCR\mime\database\content type\image/x-wmf\bits[0]
Queries value: HKCR\mime\database\content type\image/x-png[image filter clsid]
Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]

Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\internet explorer\recovery[autorecover]
Queries value: HKCU\software\microsoft\ftp[use web based ftp]
Queries value: HKCU\software\microsoft\internet explorer\services[selectionactivitybuttondisable]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]
Queries value: HKLM\software\microsoft\internet explorer\feed discovery[sound]
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: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user agent]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_0server[bdc27c485a35c61c7bf0bfedbf9b0b3f.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
Queries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[]
Queries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[appid]
Queries value: HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1a10]
Queries value: HKCU\software\microsoft\internet explorer\main[autosearch]
Queries value: HKCU\software\microsoft\internet explorer\main[friendly http errors]
Queries value: HKLM\software\microsoft\internet explorer[version]
Queries value: HKLM\software\microsoft\windows\currentversion[productname]
Queries value: HKLM\software\microsoft\windows nt\currentversion[productname]
Queries value: HKLM\system\currentcontrolset\control\windows[csdversion]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[currentlevel]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
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\htmlfile\shellex\iconhandler[]
Queries value: HKCR\htmlfile[docobject]
Queries value: HKCR\.htm[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: HKCU\appevents\schemes\apps\explorer\navigating\.current[]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[recent]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Queries value: HKCR\clsid\{275c23e2-3747-11d0-9fea-

00aa003f8646}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32[]
Queries value: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[appid]
Queries value: HKCR\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1250]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1251]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1253]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1254]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1255]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1256]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1257]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1258]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[874]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[1361]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
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: 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\mshist012016042820160429[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016042820160429[cacheoptions]
Queries value: HKCU\software\microsoft\internet
explorer\main\windowssearch[enabledscopes]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
Queries value: HKCR\.url\persistenthandler[]
Queries value: HKLM\software\microsoft\windows search[currentversion]
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: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[flags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[state]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[userpreference]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[centralprofile]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimelow]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileloadtimehigh]
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]
Sets/Creates value: HKCU\software\appdatalow\software\smartbar[globaluserid]
Sets/Creates value: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations]
Sets/Creates value: HKCU\software\conduit\distributionengine\1\offerhistory\755131[offerid]
Sets/Creates value: HKCU\software\conduit\distributionengine\1\offerhistory\755131[offerurl]
Sets/Creates value: HKCU\software\conduit\distributionengine\1\offerhistory\755131[homapage]
Sets/Creates value: HKCU\software\conduit\distributionengine\1\offerhistory\755131[defaultsearch]
Sets/Creates value: HKCU\software\conduit\distributionengine\1\offerhistory\755131[offerdescription]
Sets/Creates value: HKCU\software\conduit\distributionengine\1\offerhistory\755131[ruleid]
Sets/Creates value: HKCU\software\conduit\distributionengine\1\offerhistory\755131[rootofferid]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cacheprefix]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cachelimit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cacheoptions]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cacherepair]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[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: 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\internet settings\zonemap[proxybypass]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[uncasintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[local appdata]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042820160429[cachepath]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[favorites]
Value changes: HKCU\software\microsoft\internet explorer\main\windowssearch[version]
Value changes: HKLM\system\currentcontrolset\control\session manager[pendingfilerenameoperations]