Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 208, Task ID: 831

Task ID: 831
Risk Level: 6
Date Processed: 2016-04-28 13:10:10 (UTC)
Processing Time: 61.11 seconds
Virtual Environment: IntelliVM
Execution Arguments: "c:\windows\temp\7f17d7eabdc59686247c97d3324e12ad.exe"

Sample ID: 208
Type: basic
Owner: admin
Label: 7f17d7eabdc59686247c97d3324e12ad
Date Added: 2016-04-28 12:45:11 (UTC)
File Type: PE32:win32:gui
File Size: 784880 bytes
MD5: 7f17d7eabdc59686247c97d3324e12ad
SHA256: 6171b07e5cc0f7982bd107ef2144655a53239c4122516978201549e93425cc58
Description: None

Pattern Matching Results

5 Creates process in suspicious location
4 Reads process memory
5 PE: Contains compressed section
5 Adds autostart object
6 Modifies registry autorun entries
5 Possible injector
6 Creates executable in application data folder
3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]
3 Long sleep detected
6 Starts process from Application Data folder
6 Creates task in the task scheduler
3 Connects to local host
6 YARA score 6

Static Events

YARA rule hit: IE_PasswordSalt

Process/Thread Events

Creates process: C:\WINDOWS\Temp\7f17d7eabdc59686247c97d3324e12ad.exe ["c:\windows\temp\7f17d7eabdc59686247c97d3324e12ad.exe"]
Creates process: C:\Program Files\GUM1.tmp\GoogleUpdate.exe ["C:\Program Files\GUM1.tmp\GoogleUpdate.exe" /installsource taggedmi /install "appguid={8A69D345-D564-463C-AFF1-A69D9E530F96}&iid={713BE884-AA85-E703-D2DC-DB05F2B63B94}&lang=de&browser=4&usagestats=0&appname=Google%20Chrome&needsadmin=false&brand=CHMI&installdataindex=defaultbrowser"]
Creates process: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe ["C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe" /regserver]
Creates process: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe ["C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe" /ping
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48cmVxdWVzdCBwcm90b2NvbD0iMy4wIiB2ZXJzaW9uPSIxLjMuMjEuMTUzIiBzaGVsbF92ZXJzaW9uPSIxLjMuMjEuMTAzIiBpc21hY2hpbmU9IjAiIHNlc3Npb25pZD0ie0E3OTA1MDlGLUQyMjktNDNFNi1CODNELTZDQTA2MzlEQkZDMn0iIGluc3RhbGxzb3VyY2U9InRhZ2dlZG1pIiByZXF1ZXN0aWQ9IntCMUQwMkFFMS00QkRFLTQ3RjYtQTg5Qy0xMzVGQjQyQTVEREF9IiBkZWR1cD0iY3IiPjxvcyBwbGF0Zm9ybT0id2luIiB2ZXJzaW9uPSI1LjEiIHNwPSJTZXJ2aWNlIFBhY2sgMyIgYXJjaD0ieDg2Ii8-
PGFwcCBhcHBpZD0iezQzMEZENEQwLUI3MjktNEY2MS1BQTM0LTkxNTI2NDgxNzk5RH0iIHZlcnNpb249IiIgbmV4dHZlcnNpb249IjEuMy4yMS4xNTMiIGxhbmc9ImRlIiBicmFuZD0iQ0hNSSIgY2xpZW50PSIiIGlpZD0iezcxM0JFODg0LUFBODUtRTcwMy1EMkRDLURCMDVGMkI2M0I5NH0iPjxldmVudCBldmVudHR5cGU9IjIiIGV2ZW50cmVzdWx0PSIxIiBlcnJvcmNvZGU9IjAiIGV4dHJhY29kZTE9IjAiIGluc3RhbGxfdGltZV9tcz0iNDcxNyIvPjwvYXBwPjwvcmVxdWVzdD4]
Creates process: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe ["C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe" /handoff "appguid={8A69D345-D564-463C-AFF1-A69D9E530F96}&iid={713BE884-AA85-E703-D2DC-DB05F2B63B94}&lang=de&browser=4&usagestats=0&appname=Google%20Chrome&needsadmin=false&brand=CHMI&installdataindex=defaultbrowser" /installsource taggedmi /sessionid "{A790509F-D229-43E6-B83D-6CA0639DBFC2}"]
Creates process: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe ["C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe" -Embedding]
Reads from process: PID:1908 C:\WINDOWS\explorer.exe
Reads from process: PID:280 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Reads from process: PID:296 C:\WINDOWS\system32\ctfmon.exe
Reads from process: PID:736 C:\WINDOWS\system32\rundll32.exe
Reads from process: PID:836 C:\WINDOWS\Temp\7f17d7eabdc59686247c97d3324e12ad.exe
Terminates process: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.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\GS-1-5-21-1757981266-507921405-1957994488-1003{D19BAF17-7C87-467E-8D63-6C4B1C836373}
Creates mutex: \BaseNamedObjects\GS-1-5-21-1757981266-507921405-1957994488-1003{0E900C7B-04B0-47f9-81B0-F8D94F2DF01B}
Creates mutex: \BaseNamedObjects\GS-1-5-21-1757981266-507921405-1957994488-1003{A9A86B93-B54E-4570-BE89-42418507707B}
Creates mutex: \BaseNamedObjects\GS-1-5-21-1757981266-507921405-1957994488-1003{6885AE8E-C070-458d-9711-37B9BEAB65F6}
Creates mutex: \BaseNamedObjects\GS-1-5-21-1757981266-507921405-1957994488-1003{66CC0160-ABB3-4066-AE47-1CA6AD5065C8}
Creates mutex: \BaseNamedObjects\GS-1-5-21-1757981266-507921405-1957994488-1003{0A175FBE-AEEC-4fea-855A-2AA549A88846}
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.ELH
Creates event: \BaseNamedObjects\userenv: User Profile setup event
Creates event: \BaseNamedObjects\GS-1-5-21-1757981266-507921405-1957994488-1003{A0C1F415-D2CE-4ddc-9B48-14E56FD55162}
Creates event: \BaseNamedObjects\GS-1-5-21-1757981266-507921405-1957994488-1003{E8678EDB-A474-4D7D-866D-A3B14E92C99E}
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

File System Events

Creates: C:\Program Files
Creates: C:\Program Files\GUM1.tmp
Creates: C:\Program Files\GUT2.tmp
Creates: C:\Program Files\GUM1.tmp\GoogleUpdate.exe
Creates: C:\Program Files\GUM1.tmp\GoogleCrashHandler.exe
Creates: C:\Program Files\GUM1.tmp\goopdate.dll
Creates: C:\Program Files\GUM1.tmp\npGoogleUpdate3.dll
Creates: C:\Program Files\GUM1.tmp\GoogleUpdateHelper.msi
Creates: C:\Program Files\GUM1.tmp\GoogleUpdateBroker.exe
Creates: C:\Program Files\GUM1.tmp\GoogleUpdateOnDemand.exe
Creates: C:\Program Files\GUM1.tmp\psmachine.dll
Creates: C:\Program Files\GUM1.tmp\psuser.dll
Creates: C:\Program Files\GUM1.tmp\GoogleCrashHandler64.exe
Creates: C:\Program Files\GUM1.tmp\goopdateres_am.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ar.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_bg.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_bn.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ca.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_cs.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_da.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_de.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_el.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_en.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_en-GB.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_es.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_es-419.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_et.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_fa.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_fi.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_fil.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_fr.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_gu.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_hi.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_hr.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_hu.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_id.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_is.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_it.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_iw.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ja.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_kn.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ko.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_lt.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_lv.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ml.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_mr.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ms.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_nl.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_no.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_pl.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_pt-BR.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_pt-PT.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ro.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ru.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_sk.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_sl.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_sr.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_sv.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_sw.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ta.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_te.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_th.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_tr.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_uk.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_ur.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_vi.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_zh-CN.dll
Creates: C:\Program Files\GUM1.tmp\goopdateres_zh-TW.dll
Creates: C:\Program Files\GUM1.tmp\GoogleUpdateSetup.exe
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\CrashReports
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdate.exe
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdate.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleCrashHandler.exe
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleCrashHandler64.exe
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_am.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ar.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_bg.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_bn.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ca.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_cs.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_da.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_de.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_el.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_en.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_en-GB.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_es.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_es-419.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_et.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_fa.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_fi.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_fil.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_fr.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_gu.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_hi.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_hr.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_hu.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_id.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_is.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_it.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_iw.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ja.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_kn.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ko.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_lt.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_lv.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ml.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_mr.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ms.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_nl.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_no.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_pl.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_pt-BR.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_pt-PT.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ro.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ru.dll

```
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sk.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sl.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sr.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sv.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sw.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ta.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_te.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_th.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_tr.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_uk.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ur.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_vi.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_zh-CN.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_zh-TW.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateHelper.msi
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\psuser.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\psmachine.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\GoogleUpdate.exe
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateSetup.exe
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\npGoogleUpdate3.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateBroker.exe
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateOnDemand.exe
  Creates:                C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-1757981266-507921405-
1957994488-1003Core.job
  Creates:                C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-1757981266-507921405-
1957994488-1003UA.job
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\Offline
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\Offline\{4CDEE892-655D-4B01-B68F-B20D1854BAAD}
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\Download
  Creates:                C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\Install
  Opens:                  C:\WINDOWS\Prefetch\7F17D7EABDC596B6247C97D3324E1-115C635E.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\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:\Program Files\GUNT.tmp
  Opens:                  C:\WINDOWS\Temp\66dd32a2-ae52-4539-9985-0f7347c7f538
  Opens:                  C:\Program Files\GUTZ.tmp
  Opens:                  C:\WINDOWS\Temp\7f17d7eabdc596b6247c97d3324e12ad.exe
  Opens:                  C:\Program Files\GUNT.tmp\GoogleUpdate.exe
  Opens:                  C:\WINDOWS\system32\apphelp.dll
  Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\Program Files
  Opens:                  C:\Program Files\GUNT.tmp\GoogleUpdate.exe.Manifest
  Opens:                  C:\Program Files\GUNT.tmp\GoogleUpdate.exe.Config
  Opens:                  C:\WINDOWS\Prefetch\GOOGLEUPDATE.EXE-1F78DA75.pf
  Opens:                  C:\Program Files\GUNT.tmp\goopdate.dll
  Opens:                  C:\WINDOWS\system32\iphlpapi.dll
  Opens:                  C:\WINDOWS\system32\ws2_32.dll
  Opens:                  C:\WINDOWS\system32\ws2help.dll
  Opens:                  C:\WINDOWS\system32\netapi32.dll
  Opens:                  C:\WINDOWS\system32\crypt32.dll
  Opens:                  C:\WINDOWS\system32\msasn1.dll
  Opens:                  C:\WINDOWS\system32\msi.dll
  Opens:                  C:\WINDOWS\system32\wintrust.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:\WINDOWS\system32\dbghelp.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_de.dll
  Opens:                  C:\WINDOWS\system32\clbcatq.dll
  Opens:                  C:\WINDOWS\system32\comres.dll
  Opens:                  C:\WINDOWS\Registration\R000000000007.clb
  Opens:                  C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                  C:\WINDOWS\system32\mscoree.dll
  Opens:                  C:\WINDOWS\system32\msvcr80.dll
  Opens:                  C:\WINDOWS\system32\msvcp80.dll
  Opens:                  C:\WINDOWS\system32\uxtheme.dll
  Opens:                  C:\WINDOWS\system32\WS2HELP.dll
  Opens:                  C:\WINDOWS\system32\psapi.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdate.exe
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdate.dll
  Opens:                  C:\Program Files\GUNT.tmp\GoogleCrashHandler.exe
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleCrashHandler.exe
  Opens:                  C:\Program Files\GUNT.tmp\GoogleCrashHandler64.exe
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleCrashHandler64.exe
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_am.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_am.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ar.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ar.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_bg.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_bg.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_bn.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_bn.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ca.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ca.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_cs.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_cs.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_da.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_da.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_de.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_el.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_el.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_en.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_en.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_en-GB.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_en-GB.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_es.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_es.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_es-419.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_es-419.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_et.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_et.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_fa.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_fa.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_fi.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_fi.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_fil.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_fil.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_fr.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_fr.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_gu.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_gu.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_hi.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_hi.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_hr.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_hr.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_hu.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_hu.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_id.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_id.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_is.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_is.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_it.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_it.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_iw.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_iw.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ja.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ja.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_kn.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_kn.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ko.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ko.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_lt.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_lt.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_lv.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_lv.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ml.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ml.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_mr.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_mr.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ms.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ms.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_nl.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_nl.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_no.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_no.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_pl.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_pl.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_pt-BR.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_pt-BR.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_pt-PT.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_pt-PT.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ro.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ro.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ru.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ru.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_sk.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sk.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_sl.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sl.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_sr.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sr.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_sv.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sv.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_sw.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sw.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ta.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ta.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_te.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_te.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_th.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_th.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_tr.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_tr.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_uk.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_uk.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_ur.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ur.dll
  Opens:                  C:\Program Files\GUNT.tmp\goopdateres_vi.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_vi.dll
```

```
Opens:                  C:\Program Files\GUNT.tmp\goopdateres_zh-CN.dll
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_zh-CN.dll
Opens:                  C:\Program Files\GUNT.tmp\goopdateres_zh-TW.dll
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_zh-TW.dll
Opens:                  C:\Program Files\GUNT.tmp\GoogleUpdateHelper.msi
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateHelper.msi
Opens:                  C:\Program Files\GUNT.tmp\psuser.dll
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\psuser.dll
Opens:                  C:\Program Files\GUNT.tmp\psmachine.dll
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\psmachine.dll
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\GoogleUpdate.exe
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateSetup.exe
Opens:                  C:\Program Files\GUNT.tmp\GoogleUpdateSetup.exe
Opens:                  C:\Program Files\GUNT.tmp\npGoogleUpdate3.dll
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\npGoogleUpdate3.dll
Opens:                  C:\Program Files\GUNT.tmp\GoogleUpdateBroker.exe
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateBroker.exe
Opens:                  C:\Program Files\GUNT.tmp\GoogleUpdateOnDemand.exe
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateOnDemand.exe
Opens:                  C:\WINDOWS\system32\mstask.dll
Opens:                  C:\WINDOWS\system32\mstask.dll.2.Manifest
Opens:                  C:\WINDOWS\system32\mstask.dll.2.Config
Opens:                  C:\WINDOWS\system32\ntdsapi.dll
Opens:                  C:\WINDOWS\system32\dnsapi.dll
Opens:                  C:\
Opens:                  C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-1757981266-507921405-
1957994488-1003Core.job
Opens:                  C:\WINDOWS\Tasks
Opens:                  C:\WINDOWS\system32\ntmarta.dll
Opens:                  C:\WINDOWS\system32\samlib.dll
Opens:                  C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-1757981266-507921405-
1957994488-1003UA.job
Opens:                  C:\Documents and Settings
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application Data
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application Data\Google
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\GoogleUpdate.exe.Manifest
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\GoogleUpdate.exe.Config
Opens:                  C:\WINDOWS\Prefetch\GOOGLEUPDATE.EXE-22383200.pf
Opens:                  C:\WINDOWS\Tasks\GoogleUpdateTaskMachine.job
Opens:                  C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-1757981266-507921405-
1957994488-1003.job
Opens:                  C:\WINDOWS\system32\wtsapi32.dll
Opens:                  C:\WINDOWS\system32\winsta.dll
Opens:                  C:\WINDOWS\system32\setupapi.dll
Opens:                  C:\Documents and Settings\AdminOby Documents\desktop.ini
Opens:                  C:\Documents and Settings\All Users
Opens:                  C:\Documents and Settings\All Users\Documents\desktop.ini
Opens:                  C:\WINDOWS\system32\winhttp.dll
Opens:                  C:\WINDOWS\system32\winlogon.exe
Opens:                  C:\WINDOWS\system32\xpsp2res.dll
Opens:                  C:\WINDOWS\system32
Opens:                  C:\WINDOWS\system32\rasapi32.dll
Opens:                  C:\WINDOWS\system32\rasman.dll
Opens:                  C:\WINDOWS\system32\tapi32.dll
Opens:                  C:\WINDOWS\system32\rtutils.dll
Opens:                  C:\WINDOWS\system32\winmm.dll
Opens:                  C:\WINDOWS\system32\TAPI32.dll.124.Manifest
Opens:                  C:\WINDOWS\system32\TAPI32.dll.124.Config
Opens:                  C:\WINDOWS\system32\mmsock.dll
Opens:                  C:\WINDOWS\system32\hnetcfg.dll
Opens:                  C:\WINDOWS\system32\wshtcpip.dll
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\Download
Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\Install
Opens:                  C:\WINDOWS\system32\winrnr.dll
Opens:                  C:\WINDOWS\system32\rasadhlp.dll
Opens:                  C:\WINDOWS\system32\dhcpcsvc.dll
Opens:                  C:\WINDOWS\system32\drivers\etc\hosts
Opens:                  C:\WINDOWS\system32\rsaenh.dll
Opens:                  C:\WINDOWS\system32\mprapi.dll
Opens:                  C:\WINDOWS\system32\activeds.dll
Opens:                  C:\WINDOWS\system32\adsldpc.dll
Opens:                  C:\WINDOWS\system32\atl.dll
Opens:                  C:\WINDOWS\system32\cmpbrpxy.dll
Opens:                  C:\WINDOWS\system32\bitsprx4.dll
Writes to:              C:\Program Files\GUT2.tmp
Writes to:              C:\Program Files\GUNT.tmp\GoogleUpdate.exe
Writes to:              C:\Program Files\GUNT.tmp\GoogleCrashHandler.exe
Writes to:              C:\Program Files\GUNT.tmp\goopdate.dll
Writes to:              C:\Program Files\GUNT.tmp\npGoogleUpdate3.dll
Writes to:              C:\Program Files\GUNT.tmp\GoogleUpdateHelper.msi
Writes to:              C:\Program Files\GUNT.tmp\GoogleUpdateBroker.exe
Writes to:              C:\Program Files\GUNT.tmp\GoogleUpdateOnDemand.exe
Writes to:              C:\Program Files\GUNT.tmp\psmachine.dll
Writes to:              C:\Program Files\GUNT.tmp\psuser.dll
Writes to:              C:\Program Files\GUNT.tmp\GoogleCrashHandler64.exe
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_am.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ar.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_bg.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_bn.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ca.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_cs.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_da.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_de.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_el.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_en.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_en-GB.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_es.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_es-419.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_et.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_fa.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_fi.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_fil.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_fr.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_gu.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_hi.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_hr.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_hu.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_id.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_is.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_it.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_iw.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ja.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_kn.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ko.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_lt.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_lv.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ml.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_mr.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ms.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_nl.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_no.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_pl.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_pt-BR.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_pt-PT.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ro.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ru.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_sk.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_sl.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_sr.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_sv.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_sw.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ta.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_te.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_th.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_tr.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_uk.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_ur.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_vi.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_zh-CN.dll
Writes to:              C:\Program Files\GUNT.tmp\goopdateres_zh-TW.dll
Writes to:              C:\Program Files\GUNT.tmp\GoogleUpdateSetup.exe
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdate.exe
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdate.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleCrashHandler.exe
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleCrashHandler64.exe
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_am.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ar.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_bg.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_bn.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ca.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_cs.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_da.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_de.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_el.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_en.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_en-GB.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_es.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_es-419.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_et.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_fa.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_fi.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_fil.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_fr.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_gu.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_hi.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_hr.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_hu.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_id.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_is.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_it.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_iw.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ja.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_kn.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ko.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_lt.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_lv.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ml.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_mr.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ms.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_nl.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_no.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_pl.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_pt-BR.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_pt-PT.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ro.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ru.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sk.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sl.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sr.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sv.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_sw.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ta.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_te.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_th.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_tr.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_uk.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_ur.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_vi.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_zh-CN.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\goopdateres_zh-TW.dll
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\GoogleUpdateHelper.msi
Writes to:              C:\Documents and Settings\Admin\Local Settings\Application
Data\Google\Update\1.3.21.153\psuser.dll
```

Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\psmachine.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdateSetup.exe
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\npGoogleUpdate3.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdateBroker.exe
Writes to: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdateOnDemand.exe
Writes to: C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-1757981266-507921405-1957994488-1003Core.job
Writes to: C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-1757981266-507921405-1957994488-1003UA.job
Reads from: C:\Program Files\QUIT2.tmp
Reads from: C:\WINDOWS\Temp\7f1767eabdc59686247c97d3324e12ad.exe
Reads from: C:\WINDOWS\Registration\R000000000007.clb
Reads from: C:\Program Files\GUNT.tmp\GoogleUpdate.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdate.exe
Reads from: C:\Program Files\GUNT.tmp\goopdate.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdate.dll
Reads from: C:\Program Files\GUNT.tmp\GoogleCrashHandler.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleCrashHandler.exe
Reads from: C:\Program Files\GUNT.tmp\GoogleCrashHandler64.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleCrashHandler64.exe
Reads from: C:\Program Files\GUNT.tmp\goopdateres_am.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_am.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ar.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ar.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_bg.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_bg.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_bn.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_bn.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ca.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ca.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_cs.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_cs.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_da.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_da.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_de.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_de.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_el.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_el.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_en.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_en.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_en-GB.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_en-GB.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_es.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_es.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_es-419.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_es-419.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_et.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_et.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_fa.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_fa.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_fi.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_fi.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_fil.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_fil.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_fr.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_fr.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_gu.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_gu.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_hi.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_hi.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_hr.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_hr.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_hu.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_hu.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_id.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_id.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_is.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_is.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_it.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_it.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_iw.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_iw.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ja.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ja.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_kn.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_kn.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ko.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ko.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_lt.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_lt.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_lv.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_lv.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ml.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ml.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_mr.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_mr.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ms.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ms.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_nl.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_nl.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_no.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_no.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_pl.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_pl.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_pt-BR.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_pt-BR.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_pt-PT.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_pt-PT.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ro.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ro.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ru.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ru.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_sk.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_sk.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_sl.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_sl.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_sr.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_sr.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_sv.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_sv.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_sw.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_sw.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ta.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ta.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_te.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_te.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_th.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_th.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_tr.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_tr.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_uk.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_uk.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_ur.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_ur.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_vi.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_vi.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_zh-CN.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_zh-CN.dll
Reads from: C:\Program Files\GUNT.tmp\goopdateres_zh-TW.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\goopdateres_zh-TW.dll
Reads from: C:\Program Files\GUNT.tmp\GoogleUpdateHelper.msi
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdateHelper.msi
Reads from: C:\Program Files\GUNT.tmp\psuser.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\psuser.dll
Reads from: C:\Program Files\GUNT.tmp\psmachine.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\psmachine.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\GoogleUpdate.exe
Reads from: C:\Program Files\GUNT.tmp\GoogleUpdateSetup.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdateSetup.exe
Reads from: C:\Program Files\GUNT.tmp\npGoogleUpdate3.dll
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\npGoogleUpdate3.dll
Reads from: C:\Program Files\GUNT.tmp\GoogleUpdateBroker.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdateBroker.exe
Reads from: C:\Program Files\GUNT.tmp\GoogleUpdateOnDemand.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\1.3.21.153\GoogleUpdateOnDemand.exe
Reads from: C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-1757981266-507921405-1957994488-1003UA.job
Reads from: C:\Documents and Settings\Admin\My Documents\desktop.ini
Reads from: C:\Documents and Settings\All Users\Documents\desktop.ini
Reads from: C:\WINDOWS\system32\drivers\etc\hosts
Reads from: C:\WINDOWS\system32\rsaenh.dll
Deletes: C:\Program Files\GUNT.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Application Data\Google\Update\Install

Network Events

DNS query:	wpad
DNS query:	tools.google.com
DNS response:	tools.l.google.com ⇒ 216.58.200.110
DNS response:	tools.l.google.com ⇒ 74.125.200.101
DNS response:	tools.l.google.com ⇒ 74.125.200.100
DNS response:	tools.l.google.com ⇒ 74.125.200.139
DNS response:	tools.l.google.com ⇒ 74.125.200.138
DNS response:	tools.l.google.com ⇒ 74.125.200.113
DNS response:	tools.l.google.com ⇒ 74.125.200.102
Connects to:	127.0.0.1:1046
Connects to:	127.0.0.1:1048
Connects to:	216.58.200.110:80
Connects to:	74.125.200.101:80
Sends data to:	8.8.8.8:53
Sends data to:	127.0.0.1:1048
Sends data to:	tools.l.google.com:80 (216.58.200.110)
Sends data to:	127.0.0.1:1046
Sends data to:	tools.l.google.com:80 (74.125.200.101)
Receives data from:	0.0.0.0:0
Receives data from:	tools.l.google.com:80 (216.58.200.110)
Receives data from:	tools.l.google.com:80 (74.125.200.101)

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key:	HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-a69d9e530f96}
Creates key:	HKCU\software
Creates key:	HKCU\software\google
Creates key:	HKCU\software\google\update
Creates key:	HKCU\software\google\update\clientstate
Creates key:	HKCU\software\google\update\network
Creates key:	HKCU\software\google\update\network\secure
Creates key:	HKCU\software\google\
Creates key:	HKCU\software\google\update\
Creates key:	HKCU\software\google\update\clientstate\
Creates key:	HKCU\software\google\update\clients\
Creates key:	HKCU\software\google\update\clients\{430fd4d0-b729-4f61-aa34-91526481799d}
Creates key:	HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-91526481799d}
Creates key:	HKCU\software\microsoft\windows\currentversion\run
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters\
Creates key:	HKCU\software\microsoft\windows nt\currentversion\time zones
Creates key:	HKCU\software\classes\clsid\{e4801c24-04d0-4f28-8cf0-adace2bd839c}
Creates key:	HKCU\software\classes\clsid\{e4801c24-04d0-4f28-8cf0-

adace2bd839c}\inprochandler32
  Creates key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}
  Creates key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprocserver32
  Creates key: HKCU\software\classes\clsid
  Creates key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-60d9cdcd84c5}
  Creates key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-60d9cdcd84c5}\inprocserver32
  Creates key: HKCU\software\classes\interface
  Creates key: HKCU\software\classes\interface\{2e629606-312a-482f-9b12-2c4abf6f0b6d}
  Creates key: HKCU\software\classes\interface\{2e629606-312a-482f-9b12-2c4abf6f0b6d}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{2e629606-312a-482f-9b12-2c4abf6f0b6d}\typelib
  Creates key: HKCU\software\classes\interface\{31ac3f11-e5ea-4a85-8a3d-8e095a39c27b}
  Creates key: HKCU\software\classes\interface\{31ac3f11-e5ea-4a85-8a3d-8e095a39c27b}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{31ac3f11-e5ea-4a85-8a3d-8e095a39c27b}\typelib
  Creates key: HKCU\software\classes\interface\{8476ce12-ae1f-4198-805c-ba0f9b783f57}
  Creates key: HKCU\software\classes\interface\{8476ce12-ae1f-4198-805c-ba0f9b783f57}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{8476ce12-ae1f-4198-805c-ba0f9b783f57}\typelib
  Creates key: HKCU\software\classes\interface\{0cd01d1e-4a1c-489d-93b9-9b6672877c57}
  Creates key: HKCU\software\classes\interface\{0cd01d1e-4a1c-489d-93b9-9b6672877c57}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{0cd01d1e-4a1c-489d-93b9-9b6672877c57}\typelib
  Creates key: HKCU\software\classes\interface\{4e223325-c16b-4eeb-aedc-19ae99e237fa}
  Creates key: HKCU\software\classes\interface\{4e223325-c16b-4eeb-aedc-19ae99e237fa}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{4e223325-c16b-4eeb-aedc-19ae99e237fa}\typelib
  Creates key: HKCU\software\classes\interface\{bcdcb538-01c0-46d1-a6a7-52f4d021c272}
  Creates key: HKCU\software\classes\interface\{bcdcb538-01c0-46d1-a6a7-52f4d021c272}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{bcdcb538-01c0-46d1-a6a7-52f4d021c272}\typelib
  Creates key: HKCU\software\classes\interface\{49d7563b-2ddb-4831-88c8-768a53833837}
  Creates key: HKCU\software\classes\interface\{49d7563b-2ddb-4831-88c8-768a53833837}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{49d7563b-2ddb-4831-88c8-768a53833837}\typelib
  Creates key: HKCU\software\classes\interface\{dab1d343-1b2a-47f9-b445-93dc50704bfe}
  Creates key: HKCU\software\classes\interface\{dab1d343-1b2a-47f9-b445-93dc50704bfe}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{dab1d343-1b2a-47f9-b445-93dc50704bfe}\typelib
  Creates key: HKCU\software\classes\interface\{3d05f64f-71e3-48a5-bf6b-83315bc8ae1f}
  Creates key: HKCU\software\classes\interface\{3d05f64f-71e3-48a5-bf6b-83315bc8ae1f}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{3d05f64f-71e3-48a5-bf6b-83315bc8ae1f}\typelib
  Creates key: HKCU\software\classes\interface\{6db17455-4e85-46e7-9d23-e555e4b005af}
  Creates key: HKCU\software\classes\interface\{6db17455-4e85-46e7-9d23-e555e4b005af}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{6db17455-4e85-46e7-9d23-e555e4b005af}\typelib
  Creates key: HKCU\software\classes\interface\{dd424756-6d46-496a-924e-bd5630b4cbba}
  Creates key: HKCU\software\classes\interface\{dd424756-6d46-496a-924e-bd5630b4cbba}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{dd424756-6d46-496a-924e-bd5630b4cbba}\typelib
  Creates key: HKCU\software\classes\interface\{d106ab5f-a70e-400e-a21b-96208c1d8dbb}
  Creates key: HKCU\software\classes\interface\{d106ab5f-a70e-400e-a21b-96208c1d8dbb}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{d106ab5f-a70e-400e-a21b-96208c1d8dbb}\typelib
  Creates key: HKCU\software\classes\interface\{b3a47570-0a85-4aea-8270-529d47899603}
  Creates key: HKCU\software\classes\interface\{b3a47570-0a85-4aea-8270-529d47899603}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{b3a47570-0a85-4aea-8270-529d47899603}\typelib
  Creates key: HKCU\software\classes\interface\{18d0f672-18b4-48e6-ad36-6e6bf01dbbc4}
  Creates key: HKCU\software\classes\interface\{18d0f672-18b4-48e6-ad36-6e6bf01dbbc4}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{18d0f672-18b4-48e6-ad36-6e6bf01dbbc4}\typelib
  Creates key: HKCU\software\classes\interface\{2d363682-561d-4c3a-81c6-f2f82107562a}
  Creates key: HKCU\software\classes\interface\{2d363682-561d-4c3a-81c6-f2f82107562a}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{2d363682-561d-4c3a-81c6-f2f82107562a}\typelib
  Creates key: HKCU\software\classes\interface\{dca88386-6f03-4dbd-a366-d90bc9f68de6}
  Creates key: HKCU\software\classes\interface\{dca88386-6f03-4dbd-a366-d90bc9f68de6}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{dca88386-6f03-4dbd-a366-d90bc9f68de6}\typelib
  Creates key: HKCU\software\classes\interface\{76f7b787-a67c-4c73-82c7-31f5e3aabc5c}
  Creates key: HKCU\software\classes\interface\{76f7b787-a67c-4c73-82c7-31f5e3aabc5c}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{76f7b787-a67c-4c73-82c7-31f5e3aabc5c}\typelib
  Creates key: HKCU\software\classes\interface\{128c2da6-2bc0-44c0-b3f6-4ec22e647964}
  Creates key: HKCU\software\classes\interface\{128c2da6-2bc0-44c0-b3f6-4ec22e647964}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{128c2da6-2bc0-44c0-b3f6-4ec22e647964}\typelib
  Creates key: HKCU\software\classes\interface\{084d78a8-b084-4e14-a629-a2c419b0e3d9}
  Creates key: HKCU\software\classes\interface\{084d78a8-b084-4e14-a629-a2c419b0e3d9}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{084d78a8-b084-4e14-a629-a2c419b0e3d9}\typelib
  Creates key: HKCU\software\classes\interface\{909489c2-85a6-4322-aa56-d2527864 9d67}
  Creates key: HKCU\software\classes\interface\{909489c2-85a6-4322-aa56-d2527864 9d67}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{909489c2-85a6-4322-aa56-d2527864 9d67}\typelib
  Creates key: HKCU\software\classes\interface\{494b20cf-282e-4bdd-9f5d-b70cb09d351e}
  Creates key: HKCU\software\classes\interface\{494b20cf-282e-4bdd-9f5d-b70cb09d351e}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{494b20cf-282e-4bdd-9f5d-b70cb09d351e}\typelib
  Creates key: HKCU\software\classes\interface\{5b25a8dc-178 0-4178-a629-6be8b8defaa2}
  Creates key: HKCU\software\classes\interface\{5b25a8dc-178 0-4178-a629-6be8b8defaa2}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{5b25a8dc-178 0-4178-a629-6be8b8defaa2}\typelib
  Creates key: HKCU\software\classes\interface\{fe908cdd-22bb-472a-9870-1a0390e42f36}
  Creates key: HKCU\software\classes\interface\{fe908cdd-22bb-472a-9870-1a0390e42f36}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{fe908cdd-22bb-472a-9870-1a0390e42f36}\typelib
  Creates key: HKCU\software\classes\interface\{1c542ced-ca3b-4013-a9df-ca6ce5ff6503}
  Creates key: HKCU\software\classes\interface\{1c542ced-ca3b-4013-a9df-ca6ce5ff6503}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{1c542ced-ca3b-4013-a9df-ca6ce5ff6503}\typelib
  Creates key: HKCU\software\classes\interface\{5ccc b0ef-7073-4516-8028-4c628d0c8aab}
  Creates key: HKCU\software\classes\interface\{5ccc b0ef-7073-4516-8028-4c628d0c8aab}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{5ccc b0ef-7073-4516-8028-4c628d0c8aab}\typelib
  Creates key: HKCU\software\classes\interface\{247954f9-9edc-4e68-8cc3-150c2b89eadf}
  Creates key: HKCU\software\classes\interface\{247954f9-9edc-4e68-8cc3-150c2b89eadf}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{247954f9-9edc-4e68-8cc3-150c2b89eadf}\typelib
  Creates key: HKCU\software\classes\interface\{4de778fe-f195-4ee3-9dab-fe446c239221}
  Creates key: HKCU\software\classes\interface\{4de778fe-f195-4ee3-9dab-fe446c239221}\proxystubclsid32
  Creates key: HKCU\software\classes\interface\{4de778fe-f195-4ee3-9dab-fe446c239221}\typelib
  Creates key: HKCU\software\classes\googleupdate.update3comclassuser.1.0
  Creates key: HKCU\software\classes\googleupdate.update3comclassuser.1.0\clsid
  Creates key: HKCU\software\classes\googleupdate.update3comclassuser
  Creates key: HKCU\software\classes\googleupdate.update3comclassuser\clsid
  Creates key: HKCU\software\classes\googleupdate.update3comclassuser\curver
  Creates key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}
  Creates key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\progid
  Creates key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\versionindependentprogid
  Creates key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\localserver32
  Creates key: HKCU\software\classes\googleupdate.update3webuser.1.0
  Creates key: HKCU\software\classes\googleupdate.update3webuser.1.0\clsid
  Creates key: HKCU\software\classes\googleupdate.update3webuser
  Creates key: HKCU\software\classes\googleupdate.update3webuser\clsid
  Creates key: HKCU\software\classes\googleupdate.update3webuser\curver
  Creates key: HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}
  Creates key: HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}\progid
  Creates key: HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}\versionindependentprogid
  Creates key: HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}\localserver32
  Creates key: HKCU\software\classes\googleupdate.ondemandcomclassuser.1.0
  Creates key: HKCU\software\classes\googleupdate.ondemandcomclassuser.1.0\clsid
  Creates key: HKCU\software\classes\googleupdate.ondemandcomclassuser
  Creates key: HKCU\software\classes\googleupdate.ondemandcomclassuser\clsid
  Creates key: HKCU\software\classes\googleupdate.ondemandcomclassuser\curver
  Creates key: HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}
  Creates key: HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}\progid
  Creates key: HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}\versionindependentprogid
  Creates key: HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}\localserver32
  Creates key: HKCU\software\classes\google.oneclickprocesslauncheruser.1.0
  Creates key: HKCU\software\classes\google.oneclickprocesslauncheruser.1.0\clsid
  Creates key: HKCU\software\classes\google.oneclickprocesslauncheruser
  Creates key: HKCU\software\classes\google.oneclickprocesslauncheruser\clsid
  Creates key: HKCU\software\classes\google.oneclickprocesslauncheruser\curver
  Creates key: HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}
  Creates key: HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}\progid
  Creates key: HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}\versionindependentprogid
  Creates key: HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}\localserver32
  Creates key: HKCU\software\microsoft\internet explorer\low rights
  Creates key: HKCU\software\microsoft\internet explorer\low rights\elevationpolicy
  Creates key: HKCU\software\microsoft\internet explorer\low rights\elevationpolicy\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}
  Creates key: HKCU\software\mozillaplugins
  Creates key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=9
  Creates key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=9\mimetypes
  Creates key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=9\mimetypes\application/x-vnd.google.oneclickctrl.9
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\preapproved
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\preapproved\{c442ac41-9200-4770-8cc0-7cdb4f245c55}
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c442ac41-9200-4770-8cc0-7cdb4f245c55}
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\iexplore
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\iexplore\alloweddomains
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\iexplore\alloweddomains*
  Creates key: HKCU\software\microsoft\internet explorer\low rights\elevationpolicy\{c442ac41-9200-4770-8cc0-7cdb4f245c55}
  Creates key: HKCU\software\classes\google.oneclickctrl.9
  Creates key: HKCU\software\classes\google.oneclickctrl.9\clsid
  Creates key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}
  Creates key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\progid
  Creates key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\inprocserver32
  Creates key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\implemented categories
  Creates key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\implemented categories\{59fb2056-d625-48d0-a944-1a85b5ab2640}
  Creates key: HKCU\software\classes\mime
  Creates key: HKCU\software\classes\mime\database
  Creates key: HKCU\software\classes\mime\database\content type
  Creates key: HKCU\software\classes\mime\database\content type\application/x-vnd.google.oneclickctrl.9
  Creates key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=3
  Creates key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=3\mimetypes
  Creates key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=3\mimetypes\application/x-vnd.google.update3webcontrol.3
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\preapproved\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\iexplore
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\iexplore\alloweddomains
  Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\iexplore\alloweddomains*
  Creates key: HKCU\software\microsoft\internet explorer\low rights\elevationpolicy\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}
  Creates key: HKCU\software\classes\google.update3webcontrol.3
  Creates key: HKCU\software\classes\google.update3webcontrol.3\clsid
  Creates key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}
  Creates key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\progid
  Creates key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\inprocserver32
  Creates key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\implemented categories
  Creates key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\implemented categories\{59fb2056-d625-48d0-a944-1a85b5ab2640}
  Creates key: HKCU\software\classes\mime\database\content type\application/x-vnd.google.update3webcontrol.3
  Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\

Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKLM\software\microsoft\tracing
Creates key: HKCU\software\google\update\proxy
Deletes value: HKCU\software\google\update[eulaaccepted]
Deletes value: HKCU\software\google\update[uid]
Deletes value: HKCU\software\google\update[old-uid]
Deletes value: HKCU\software\google\update[ui]
Deletes value: HKCU\software\google\update[lastchecked]
Deletes value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-91526481799d}[updateavailablecount]
Deletes value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-91526481799d}[updateavailablesince]
Deletes value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-a69d9e530f96}[iid]
Deletes value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-a69d9e530f96}[ttokken]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\7f17d7eabdc59682d47c97d3324e12ad.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
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\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\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\gdi32.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\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\system\setup
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\7f17d7eabdc59682d47c97d3324e12ad.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\currentversion
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\googleupdate.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\googleupdate.exe
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\software\microsoft\windows nt\currentversion\image file execution options\iphlpapi.dll
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netapi32.dll
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\cmgrhlp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll
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\iertutil.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\protocols\name-space handler\
Opens key: HKCR\protocols\name-space handler
Opens key: HKCU\software\classes\protocols\name-space handler
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\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\wintrust.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\googledate.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
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\googleupdate.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\software\google\updatedev\
Opens key: HKCU\software\google\update\clientstate\
Opens key: HKCU\software\google\update\
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dbghelp.dll
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\s-1-5-21-1757981266-507921405-1957994488-1003
Opens key: HKU\
Opens key: HKCU\software\google\update\clients\{430fd4d0-b729-4f61-aa34-91526481799d}
Opens key: HKLM\software\microsoft\ccm3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cscres.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\clbcatq.dll
Opens key: HKLM\software\microsoft\ccm3\debug
Opens key: HKLM\software\microsoft\ctf\compatibility\googleupdate.exe
Opens key: HKLM\software\classes
Opens key: HKCR\clsid
Opens key: HKCU\software\classes\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}

Opens key: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}
Opens key: HKCU\software\classes\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\treatas
Opens key: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\treatas
Opens key: HKCU\software\classes\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprocserver32
Opens key: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprocserver32
Opens key: HKCU\software\classes\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprocserverx86
Opens key: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\localserver32
Opens key: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\localserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime
Opens key: HKCU\software\classes\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprochandler32
Opens key: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprochandler32
Opens key: HKCU\software\classes\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprochandlerx86
Opens key: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\localserver
Opens key: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msxml3.dll
Opens key: HKLM\software\microsoft\msxml30
Opens key: HKCU\software\microsoft\ctf
Opens key: HKLM\software\microsoft\ctf\systemshared
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\uxtheme.dll
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\psapi.dll
Opens key: HKCU\software\classes\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}
Opens key: HKCR\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}
Opens key: HKCU\software\classes\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\treatas
Opens key: HKCR\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\treatas
Opens key: HKCU\software\classes\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\inprocserver32
Opens key: HKCR\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\inprocserver32
Opens key: HKCU\software\classes\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\inprocserverx86
Opens key: HKCR\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\localserver32
Opens key: HKCR\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\localserver32
Opens key: HKCU\software\classes\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\inprochandler32
Opens key: HKCR\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\inprochandler32
Opens key: HKCU\software\classes\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\inprochandlerx86
Opens key: HKCR\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\localserver
Opens key: HKCR\clsid\{148bd52e-a2ab-11ce-b11f-00aa00530503}\localserver
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\mpr.dll
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
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\winldap32.dll
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdsapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mstask.dll
Opens key: HKLM\software\microsoft\schedulingagent
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\pacific standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\afghanistan standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\alaskan standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\arab standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\arabian standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\arabic standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\atlantic standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\aus central standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\aus eastern standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\azores standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\canada central standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\cape verde standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\caucasus standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\cen. australia standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\central america standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\central asia standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\central europe standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\central european standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\central pacific standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\central standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\china standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\dateline standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\e. africa standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\e. australia standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\e. europe standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\e. south america standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\eastern standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\egypt standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\ekaterinburg standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\fiji standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\fle standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\gmt standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\greenland standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\greenwich standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\gtb standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\hawaiian standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\india standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\iran standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\israel standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\korea standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\mexico standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\mexico standard time 2
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\mid-atlantic standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\mountain standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\myanmar standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\n. central asia standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\nepal standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\new zealand standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\newfoundland standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\north asia east standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\north asia standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\pacific sa standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\romance standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\russian standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\sa eastern standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\sa pacific standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\sa western standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\samoa standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\se asia standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\singapore standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\south africa standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\sri lanka standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\taipei standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\tasmania standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\tokyo standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\tonga standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\us eastern standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\us mountain standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\vladivostok standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\w. australia standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\w. central africa standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\w. europe standard time
Opens key: HKLM\software\microsoft\windows nt\currentversion\time zones\w. europe standard time\dynamic dst
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\googleupdate.exe
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
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: HKLM\software\microsoft\windows nt\currentversion\image file execution options\samlib.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntmarta.dll
Opens key: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-9152648179bd}
Opens key: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-a69d9e530f96}
Opens key: HKCU\software\google\update\uid
Opens key: HKCU\software\classes
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\psuser.dll
Opens key: HKCU\software
Opens key: HKCU\software\classes\clsid
Opens key: HKCU\software\classes\clsid\{a4801c24-04d0-4f28-8cf0-adace2bd839c}
Opens key: HKCU\software\classes\clsid\{a4801c24-04d0-4f28-8cf0-adace2bd839c}\inprochandler32
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprocserver32
Opens key: HKCU\software\classes\googleupdate.update3comclassuser.1.0
Opens key: HKCU\software\classes\googleupdate.update3comclassuser.1.0\clsid
Opens key: HKCU\software\classes\googleupdate.update3comclassuser
Opens key: HKCU\software\classes\googleupdate.update3comclassuser\clsid
Opens key: HKCU\software\classes\googleupdate.update3comclassuser\curver
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\progid
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\versionindependentprogid
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\localserver32
Opens key: HKCU\software\classes\googleupdate.update3webuser.1.0
Opens key: HKCU\software\classes\googleupdate.update3webuser.1.0\clsid
Opens key: HKCU\software\classes\googleupdate.update3webuser
Opens key: HKCU\software\classes\googleupdate.update3webuser\clsid
Opens key: HKCU\software\classes\googleupdate.update3webuser\curver
Opens key: HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}

Opens key: HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}\progid
Opens key: HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}\versionindependentprogid
Opens key: HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}\localserver32
Opens key: HKCU\software\classes\googleupdate.ondemandcomclassfactory.1.0
Opens key: HKCU\software\classes\googleupdate.ondemandcomclassfactory.1.0\clsid
Opens key: HKCU\software\classes\googleupdate.ondemandcomclassfactory
Opens key: HKCU\software\classes\googleupdate.ondemandcomclassfactory\clsid
Opens key: HKCU\software\classes\googleupdate.ondemandcomclassfactory\curver
Opens key: HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}
Opens key: HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}\progid
Opens key: HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}\versionindependentprogid
Opens key: HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}\localserver32
Opens key: HKCU\software\classes\googleupdate.credentialdialoguser.1.0
Opens key: HKCU\software\classes\googleupdate.credentialdialoguser.1.0\clsid
Opens key: HKCU\software\classes\googleupdate.credentialdialoguser
Opens key: HKCU\software\classes\googleupdate.credentialdialoguser\clsid
Opens key: HKCU\software\classes\googleupdate.credentialdialoguser\curver
Opens key: HKCU\software\classes\clsid\{e67be843-bbbe-4484-95fb-05271ae86750}
Opens key: HKCU\software\classes\clsid\{e67be843-bbbe-4484-95fb-05271ae86750}\progid
Opens key: HKCU\software\classes\clsid\{e67be843-bbbe-4484-95fb-05271ae86750}\versionindependentprogid
Opens key: HKCU\software\classes\clsid\{e67be843-bbbe-4484-95fb-05271ae86750}\localserver32
Opens key: HKCU\software\classes\google.oneclickprocesslauncheruser.1.0
Opens key: HKCU\software\classes\google.oneclickprocesslauncheruser.1.0\clsid
Opens key: HKCU\software\classes\google.oneclickprocesslauncheruser
Opens key: HKCU\software\classes\google.oneclickprocesslauncheruser\clsid
Opens key: HKCU\software\classes\google.oneclickprocesslauncheruser\curver
Opens key: HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}
Opens key: HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}\progid
Opens key: HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}\versionindependentprogid
Opens key: HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}\localserver32
Opens key: HKCU\software\microsoft
Opens key: HKCU\software\microsoft\internet explorer
Opens key: HKCU\software\microsoft\internet explorer\low rights
Opens key: HKCU\software\microsoft\internet explorer\low rights\elevationpolicy
Opens key: HKCU\software\microsoft\internet explorer\low rights\elevationpolicy\{51f9e8ef-59d7-475b-a106-c7ea6f30c119}
Opens key: HKCU\software\classes\clsid\{0f873691-a4e5-4cfc-bd3e-73e6154572dd}
Opens key: HKCR\clsid\{0f873691-a4e5-4cfc-bd3e-73e6154572dd}
Opens key: HKCU\software\policies\microsoft\windows\app management
Opens key: HKLM\software\policies\microsoft\windows\app management
Opens key: HKLM\software\google\update\
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winsta.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\npgoogleupdate3.dll
Opens key: HKCU\software\mozillaplugins
Opens key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=9
Opens key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=9\mimetypes
Opens key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=9\mimetypes\application/x-vnd.google.oneclickctrl.9
Opens key: HKCU\software\microsoft\windows
Opens key: HKCU\software\microsoft\windows\currentversion
Opens key: HKCU\software\microsoft\windows\currentversion\ext
Opens key: HKCU\software\microsoft\windows\currentversion\ext\preapproved
Opens key: HKCU\software\microsoft\windows\currentversion\ext\preapproved\{c442ac41-9200-4770-8cc0-7cdb4f245c55}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c442ac41-9200-4770-8cc0-7cdb4f245c55}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\iexplore
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\iexplore\alloweddomains
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\iexplore\alloweddomains*
Opens key: HKCU\software\microsoft\internet explorer\low rights\elevationpolicy\{c442ac41-9200-4770-8cc0-7cdb4f245c55}
Opens key: HKCU\software\classes\google.oneclickctrl.9
Opens key: HKCU\software\classes\google.oneclickctrl.9\clsid
Opens key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}
Opens key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\progid
Opens key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\inprocserver32
Opens key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\implemented categories
Opens key: HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}\implemented categories\{59fb2056-d625-48d0-a944-1a85b5ab2640}
Opens key: HKCU\software\classes\mime
Opens key: HKCU\software\classes\mime\database
Opens key: HKCU\software\classes\mime\database\content type
Opens key: HKCU\software\classes\mime\database\content type\application/x-vnd.google.oneclickctrl.9
Opens key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=3
Opens key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=3\mimetypes
Opens key: HKCU\software\mozillaplugins\@tools.google.com/google update;version=3\mimetypes\application/x-vnd.google.update3webcontrol.3
Opens key: HKCU\software\microsoft\windows\currentversion\ext\preapproved\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\iexplore
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\iexplore\alloweddomains
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\iexplore\alloweddomains*
Opens key: HKCU\software\microsoft\internet explorer\low rights\elevationpolicy\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}
Opens key: HKCU\software\classes\google.update3webcontrol.3
Opens key: HKCU\software\classes\google.update3webcontrol.3\clsid
Opens key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}
Opens key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\progid
Opens key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\inprocserver32
Opens key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\implemented categories
Opens key: HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}\implemented categories\{59fb2056-d625-48d0-a944-1a85b5ab2640}
Opens key: HKCU\software\classes\mime\database\content type\application/x-vnd.google.update3webcontrol.3
Opens key: HKLM\software\policies\google\update\
Opens key: HKLM\software\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\filesets
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\filesets\.exe
Opens key: HKCU\software\classes\.exe
Opens key: HKCR\.exe
Opens key: HKCU\software\classes\exefile
Opens key: HKCR\exefile
Opens key: HKCU\software\classes\exefile\curver
Opens key: HKCR\exefile\curver
Opens key: HKCR\exefile\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\
Opens key: HKCU\software\microsoft\windows\currentversion\policies\system
Opens key: HKCU\software\classes\exefile\shellex\iconhandler
Opens key: HKCR\exefile\shellex\iconhandler
Opens key: HKCU\software\classes\systemfileassociations\.exe
Opens key: HKCR\systemfileassociations\.exe
Opens key: HKCU\software\classes\systemfileassociations\application
Opens key: HKCR\systemfileassociations\application
Opens key: HKCU\software\classes\exefile\clsid
Opens key: HKCR\exefile\clsid
Opens key: HKCU\software\classes*
Opens key: HKCR*
Opens key: HKCU\software\classes*\clsid
Opens key: HKCR*\clsid
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi.dll
Opens key: HKLM\system\currentcontrolset\control\minint
Opens key: HKLM\system\wpa\pnp
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Opens key: HKCU\software\classes\directory
Opens key: HKCR\directory
Opens key: HKCU\software\classes\directory\curver
Opens key: HKCR\directory\curver
Opens key: HKCR\directory\
Opens key: HKCU\software\classes\directory\shellex\iconhandler
Opens key: HKCR\directory\shellex\iconhandler
Opens key: HKCU\software\classes\directory\clsid
Opens key: HKCR\directory\clsid
Opens key: HKCU\software\classes\folder
Opens key: HKCR\folder
Opens key: HKCU\software\classes\folder\clsid
Opens key: HKCR\folder\clsid
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks
Opens key: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
Opens key: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
Opens key: HKCU\software\classes\exefile\shell\open
Opens key: HKCR\exefile\shell\open
Opens key: HKCU\software\classes\exefile\shell\open\command
Opens key: HKCR\exefile\shell\open\command
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\googleupdate.exe
Opens key: HKCU\software\classes\exefile\shell\open\ddeexec
Opens key: HKCR\exefile\shell\open\ddeexec
Opens key: HKCU\software\classes\applications\googleupdate.exe
Opens key: HKCR\applications\googleupdate.exe
Opens key: HKCU\software\microsoft\windows\shellnoroam
Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache
Opens key: HKLM\software\microsoft\windows\shellnoroam\muicache\
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winhttp.dll
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\winhttp\tracing
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\app2res.dll
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\treatas
Opens key: HKCR\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\treatas
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprocserver32
Opens key: HKCR\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprocserver32
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprocserverx86
Opens key: HKCR\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprocserverx86
Opens key: HKCR\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\localserver32
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprochandler32
Opens key: HKCR\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprochandler32
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprochandlerx86
Opens key: HKCR\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprochandler
Opens key: HKCR\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}\inprochandler
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\connections
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\winhttp\unsafesslapps
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\clients\startmenuinternet
Opens key: HKLM\software\clients\startmenuinternet
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: HKCU\software\microsoft\windows\currentversion\internet settings\connections
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\hnetcfg.dll
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wshtcpip.dll
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7649d7cec8c}
Opens key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}
Opens key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\treatas
Opens key: HKCR\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\treatas
Opens key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\inprocserver32
Opens key: HKCR\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\inprocserver32
Opens key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\inprocserver86
Opens key: HKCR\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\inprocserver86
Opens key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\localserver32
Opens key: HKCR\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\localserver32
Opens key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\inprochandler32
Opens key: HKCR\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\inprochandler32
Opens key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\inprochandler86
Opens key: HKCR\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\inprochandler86
Opens key: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\localserver
Opens key: HKCR\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}\localserver
Opens key: HKCR\clsid\{6d7374de-63aa-473c-8c02-80d9cdcd84c5}
Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver86
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver86
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\localserver32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\localserver32
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler86
Opens key: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler86
Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\localserver
Opens key: HKCU\software\classes\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}
Opens key: HKCR\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}
Opens key: HKCU\software\classes\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\treatas
Opens key: HKCR\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\treatas
Opens key: HKCU\software\classes\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\inprocserver32
Opens key: HKCR\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\inprocserver86
Opens key: HKCR\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\inprocserver86
Opens key: HKCU\software\classes\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\localserver32
Opens key: HKCR\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\localserver32
Opens key: HKCU\software\classes\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\inprochandler32
Opens key: HKCR\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\localserver
Opens key: HKCR\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}\localserver
Opens key: HKCR\clsid\{a480c024-04d0-4f28-8cf0-adace2bd839c}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntsnnr.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\dhcpcsvc.dll
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\transient
Opens key: HKCU\software\google\update\clients\
Opens key: HKCU\software\google\update\clients\{8a69d345-d564-463c-aff1-a69d9e530f96}
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}
Opens key: HKCR\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\treatas
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprocserver32
Opens key: HKCR\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprocserver32
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprocserver86
Opens key: HKCR\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprocserver86
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\localserver32
Opens key: HKCR\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\localserver32
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprochandler32
Opens key: HKCR\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprochandler32
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprochandler86
Opens key: HKCR\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\inprochandler86
Opens key: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\localserver
Opens key: HKCR\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}\localserver
Opens key: HKCR\clsid\{e8cf3e55-f919-49d9-abc0-948e6cb34b9f}
Opens key: HKCU\software\microsoft\ctf\langbardd\n
Opens key: HKLM\software\microsoft\ctf\langbardd\n
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKLM\system\currentcontrolset\services\netbt\linkage
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\adsldpc.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\atl.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\activeds.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mprapi.dll
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\treatas
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\treatas
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprocserver32
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprocserver32
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprocserver86
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprocserver86
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\localserver32
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\localserver32
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprochandler32
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprochandler32
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprochandler86
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprochandler86
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\localserver
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\localserver
Opens key: HKCU\software\classes\appid\{69ad4aee-51be-439b-a92c-86ae490e8b30}
Opens key: HKCR\appid\{69ad4aee-51be-439b-a92c-86ae490e8b30}
Opens key: HKCU\software\classes\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprochandler
Opens key: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}\inprochandler
Opens key: HKCU\software\classes\interface\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}
Opens key: HKCR\interface\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}
Opens key: HKCU\software\classes\interface\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\proxystubclsid32
Opens key: HKCR\interface\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}
Opens key: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}
Opens key: HKCU\software\classes\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\treatas
Opens key: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\treatas
Opens key: HKCU\software\classes\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprocserver32
Opens key: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprocserver32
Opens key: HKCU\software\classes\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprocserver86
Opens key: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprocserver86
Opens key: HKCU\software\classes\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\localserver32
Opens key: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\localserver32
Opens key: HKCU\software\classes\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprochandler32
Opens key: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprochandler32
Opens key: HKCU\software\classes\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprochandler86
Opens key: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprochandler86
Opens key: HKCU\software\classes\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\localserver
Opens key: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\qmgrprxy.dll
Opens key: HKCU\software\classes\interface\{1af4f612-3b71-466f-8f58-7b6f73ac57ad}
Opens key: HKCR\interface\{1af4f612-3b71-466f-8f58-7b6f73ac57ad}
Opens key: HKCU\software\classes\interface\{1af4f612-3b71-466f-8f58-7b6f73ac57ad}\proxystubclsid32
Opens key: HKCR\interface\{1af4f612-3b71-466f-8f58-7b6f73ac57ad}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{37668d37-507e-4160-9316-26306d150b12}
Opens key: HKCR\interface\{37668d37-507e-4160-9316-26306d150b12}
Opens key: HKCU\software\classes\interface\{37668d37-507e-4160-9316-26306d150b12}\proxystubclsid32
Opens key: HKCR\interface\{37668d37-507e-4160-9316-26306d150b12}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{f1bd1079-9f01-4bdc-8036-f09b70095066}
Opens key: HKCR\interface\{f1bd1079-9f01-4bdc-8036-f09b70095066}
Opens key: HKCU\software\classes\interface\{f1bd1079-9f01-4bdc-8036-f09b70095066}\proxystubclsid32
Opens key: HKCR\interface\{f1bd1079-9f01-4bdc-8036-f09b70095066}\proxystubclsid32
Opens key: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}
Opens key: HKCU\software\classes\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}
Opens key: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\treatas
Opens key: HKCU\software\classes\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\treatas
Opens key: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprocserver32
Opens key: HKCU\software\classes\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprocserver32
Opens key: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprocserver86
Opens key: HKCU\software\classes\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprocserver86
Opens key: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\localserver32
Opens key: HKCU\software\classes\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\localserver32
Opens key: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprochandler32
Opens key: HKCU\software\classes\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprochandler32
Opens key: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprochandler86
Opens key: HKCU\software\classes\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprochandler86
Opens key: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\localserver
Opens key: HKCU\software\classes\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\bitsprx4.dll
Opens key: HKCU\software\classes\interface\{97ea99c7-0186-4ad4-8df9-c5b4e0ed6b22}
Opens key: HKCR\interface\{97ea99c7-0186-4ad4-8df9-c5b4e0ed6b22}
Opens key: HKCU\software\classes\interface\{97ea99c7-0186-4ad4-8df9-c5b4e0ed6b22}\proxystubclsid32
Opens key: HKCR\interface\{97ea99c7-0186-4ad4-8df9-c5b4e0ed6b22}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{ca51e165-c365-424c-8d41-24aaa4ff3c40}
Opens key: HKCR\interface\{ca51e165-c365-424c-8d41-24aaa4ff3c40}
Opens key: HKCU\software\classes\interface\{ca51e165-c365-424c-8d41-24aaa4ff3c40}\proxystubclsid32
Opens key: HKCR\interface\{ca51e165-c365-424c-8d41-24aaa4ff3c40}\proxystubclsid32
Opens key: HKCU\software\classes\interface\{01b7bd23-fb88-4a77-8490-5891d3e4653a}
Opens key: HKCR\interface\{01b7bd23-fb88-4a77-8490-5891d3e4653a}
Opens key: HKCU\software\classes\interface\{01b7bd23-fb88-4a77-8490-5891d3e4653a}\proxystubclsid32
Opens key: HKCR\interface\{01b7bd23-fb88-4a77-8490-5891d3e4653a}\proxystubclsid32
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[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[7f17d7eabdc59688247c97d3324e12ad]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[7f17d7eabdc59688247c97d3324e12ad]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[relockresourcetimeout]
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\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\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
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\{ddaf1f24-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{ddaf1f24-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[googleupdate]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[googleupdate]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[googleupdate.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKLM\system\currentcontrolset\control\vmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
Queries value: HKLM\system\currentcontrolset\control\vmi\security[00000000-0000-0000-
0000-000000000000]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
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:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKCU\software\google\update[eulaaccepted]
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\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[profileimagepath]
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: HKLM\software\microsoft\ccm3[ccm<enabled]
Queries value: HKLM\software\microsoft\ole[minimumfreememorytargetcreateprocess]
Queries value: HKLM\software\microsoft\ole[minimumfreememorytargetcreatedobject]
Queries value: HKLM\software\microsoft\ccm3[regdbversion]
Queries value: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}\inprocserver32[]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-00c04f990bb4}[appid]
Queries value: HKCR\clsid\{f6d90f11-9c73-11d3-b32e-
00c04f990bb4}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Queries value: HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
Queries value: HKCU\software\google\update[gupdate_task_name_c]
Queries value: HKCR\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserver32[]
Queries value: HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}[appid]
Queries value: HKCR\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\inprocserver32[threadingmodel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[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[waitforonameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usewedns]
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\ldap[ldapclientintegrity]
Queries value: HKLM\software\microsoft\schedulingagent[tasksfolder]
Queries value: HKLM\software\microsoft\schedulingagent[notifyontaskmiss]
Queries value: HKLM\software\microsoft\schedulingagent[viewhiddentasks]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKCU\software\microsoft\windows nt\currentversion\time
zones[timezonekeyname]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\pacific
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\pacific
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\pacific
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\afghanistan
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\afghanistan
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\afghanistan
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\alaskan
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\alaskan
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\alaskan
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arab
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arab

standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arab
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arabian
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arabian
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arabian
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arabic
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arabic
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\arabic
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\atlantic
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\atlantic
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\atlantic
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\aus central
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\aus central
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\aus central
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\aus eastern
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\aus eastern
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\aus eastern
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\azores
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\azores
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\azores
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\canada
central standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\canada
central standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\canada
central standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\cape verde
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\cape verde
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\cape verde
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\caucasus
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\caucasus
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\caucasus
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\cen.
australia standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\cen.
australia standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\cen.
australia standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
america standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
america standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
america standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
asia standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
asia standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
asia standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
europe standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
europe standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
europe standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
european standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
european standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
european standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
pacific standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
pacific standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
pacific standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\central
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\china
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\china
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\china
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\dateline
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\dateline
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\dateline
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. africa
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. africa
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. africa
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e.
australia standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e.
australia standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e.
australia standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. europe
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. europe
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. europe
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. south
america standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. south
america standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\e. south
america standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\eastern
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\eastern
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\eastern
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\egypt
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\egypt
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\egypt
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time
zones\ekaterinburg standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time
zones\ekaterinburg standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time
zones\ekaterinburg standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\fiji
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\fiji
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\fiji
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\fle
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\fle
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\fle
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\gmt
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\gmt
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\gmt
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\greenland
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\greenland
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\greenland
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\greenwich
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\greenwich
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\greenwich
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\gtb
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\gtb
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\gtb
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\hawaiian
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\hawaiian
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\hawaiian
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\india
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\india
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\india
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\iran
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\iran
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\iran
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\israel
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\israel
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\israel
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\korea
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\korea
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\korea
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mexico
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mexico
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mexico
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mexico
standard time 2[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mexico
standard time 2[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mexico
standard time 2[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mid-
atlantic standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mid-
atlantic standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mid-
atlantic standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mountain
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mountain
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\mountain
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\myanmar
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\myanmar
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\myanmar
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\n. central
asia standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\n. central
asia standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\n. central
asia standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\nepal
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\nepal
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\nepal
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\new zealand
standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\new zealand
standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\new zealand
standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time
zones\newfoundland standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time
zones\newfoundland standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time
zones\newfoundland standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\north asia
east standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\north asia
east standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\north asia
east standard time[tzi]

Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\north asia standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\north asia standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\north asia standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\pacific sa standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\pacific sa standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\pacific sa standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\romance standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\romance standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\romance standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\russian standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\russian standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\russian standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa eastern standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa eastern standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa eastern standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa pacific standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa pacific standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa pacific standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa western standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa western standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sa western standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\samoa standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\samoa standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\samoa standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\se asia standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\se asia standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\se asia standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\singapore standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\singapore standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\singapore standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\south africa standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\south africa standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\south africa standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sri lanka standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sri lanka standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\sri lanka standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\taipei standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\taipei standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\taipei standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tasmania standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tasmania standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tasmania standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tokyo standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tokyo standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tokyo standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tonga standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tonga standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\tonga standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\us eastern standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\us eastern standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\us eastern standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\us mountain standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\us mountain standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\us mountain standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\vladivostok standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\vladivostok standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\vladivostok standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. australia standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. australia standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. australia standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. central africa standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. central africa standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. central africa standard time[tzi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. europe standard time[std]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. europe standard time[dlt]
Queries value: HKLM\software\microsoft\windows nt\currentversion\time zones\w. europe standard time[tzi]
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: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfilesclsidjunctions]
Queries value: HKCU\software\google\update[gupdate_task_name_ua]
Queries value: HKCU\software\google\update\clients\{430fd4d0-b729-4f61-aa34-9152648179965}[pv]
Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-9152648179965}[usagestats]
Queries value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-a69d9e530f96}[usagestats]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-9152648179965}[brand]
Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-9152648179965}[installtime]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
Queries value: HKCR\.exe[]
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[hosimplestartmenu]
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\exefile[docobject]
Queries value: HKCR\exefile[browseinplace]
Queries value: HKCR\exefile[isshortcut]
Queries value: HKCR\exefile[alwaysshowext]
Queries value: HKCR\exefile[nevershowext]
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:
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\directory[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common documents]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[desktop]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common desktop]
Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[loadwithoutcom]
Queries value: HKCR\exefile\shell\open\command[]
Queries value: HKCR\exefile\shell\open\command[command]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and settings\admin\local settings\application data\google\update\googleupdate.exe]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[sharecredswithwinhttp]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3306ddf0975}\localserver32[]
Queries value: HKLM\software\classes\clsid\{022105bd-948a-40c9-ab42-a3306ddf0975}\localserver32[]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\connections[winhttpsettings]
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: HKLM\software\clients\startmenuinternet[]
  Queries value: HKCU\software\google\update[old-uid]
  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: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value: HKCU\software\google\update\proxy[source]
  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: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[leaseobtainedtime]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[leaseterminatestime]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[dhcpserver]
  Queries value: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-
60d9cdc884c5}\inprocserver32[inprocserver32]
  Queries value: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-
60d9cdc884c5}\inprocserver32[]
  Queries value: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-
60d9cdc884c5}[appid]
  Queries value: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-
60d9cdc884c5}\inprocserver32[threadingmodel]
  Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value: HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[dhcpdomain]
  Queries value: HKCR\clsid\{00020420-0000-0000-c000-000000000046}[appid]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[ipautoconfigurationenabled]
  Queries value: HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[addresstype]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7649d7cec6c}[dhcpnameserver]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
  Queries value: HKCU\software\classes\clsid\{e4805c24-04d0-4f28-8cf0-
adace2bd839c}\inprochandler32[]
  Queries value: HKCU\software\classes\clsid\{e4805c24-04d0-4f28-8cf0-
adace2bd839c}[appid]
  Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[nameserver]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\{dhcpnameserver}
  Queries value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-
a69d9e530f96}[pv]
  Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-
91526481799d}[eulaaccepted]
  Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-
91526481799d}[oeminstall]
  Queries value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-
a69d9e530f96}[eulaaccepted]
  Queries value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-
a69d9e530f96}[oeminstall]
  Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-
91526481799d}[lang]
  Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-
91526481799d}[client]
  Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-
91526481799d}[iid]
  Queries value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-
91526481799d}[experiment_labels]
  Queries value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-
a69d9e530f96}[experiment_labels]
  Queries value: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-
948e6cb348d9}\inprocserver32[inprocserver32]
  Queries value: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-
948e6cb348d9}\inprocserver32[]
  Queries value: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-
948e6cb348d9}[appid]
  Queries value: HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-
948e6cb348d9}\inprocserver32[threadingmodel]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\{dhcpdomain}
  Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value: HKLM\software\microsoft\cryptography[machineguid]
  Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]
  Queries value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-
a69d9e530f96}[dr]
  Queries value: HKCR\clsid\{4991d34b-80a1-4291-83b6-3328366b9097}[appid]
  Queries value: HKCR\appid\{69ad4aee-51be-439b-a92c-86ae490e8b30}[dllsurrogate]
  Queries value: HKCR\appid\{69ad4aee-51be-439b-a92c-86ae490e8b30}[localservice]
  Queries value: HKCR\interface\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\proxystubclsid32[]
  Queries value: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-
daa1b78cee7c}\inprocserver32[inprocserver32]
  Queries value: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}\inprocserver32[]
  Queries value: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-daa1b78cee7c}[appid]
  Queries value: HKCR\clsid\{5ce34c0d-0dc9-4c1f-897c-
daa1b78cee7c}\inprocserver32[threadingmodel]
  Queries value: HKCR\interface\{1af4f612-3b71-466f-8f58-7b6f73ac57ad}\proxystubclsid32[]
  Queries value: HKCR\interface\{17668d37-507e-4160-9316-26306d150b12}\proxystubclsid32[]
  Queries value: HKCR\interface\{f1bd1079-9f01-4bdc-8036-f09b70095066}\proxystubclsid32[]
  Queries value: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-
f09b70095066}\inprocserver32[inprocserver32]
  Queries value: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}\inprocserver32[]
  Queries value: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-f09b70095066}[appid]
  Queries value: HKCR\clsid\{f1bd1079-9f01-4bdc-8036-
f09b70095066}\inprocserver32[threadingmodel]
  Queries value: HKCR\interface\{97ea99c7-0186-4ad4-8df9-c5b4e0ed6b22}\proxystubclsid32[]
  Queries value: HKCR\interface\{ca51e165-c365-424c-8d41-24aaa4ff5b40}\proxystubclsid32[]
  Queries value: HKCR\interface\{01b7bd23-fb88-4a77-8490-5891d3e4653a}\proxystubclsid32[]
  Sets/Creates value: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-
a69d9e530f96}[usagestats]

```
  Sets/Creates value:       HKCU\software\google\update[path]
  Sets/Creates value:       HKCU\software\google\update[uninstallcmdline]
  Sets/Creates value:       HKCU\software\google\update\clients\{430fd4d0-b729-4f61-aa34-
91526481799d}[pv]
  Sets/Creates value:       HKCU\software\google\update\clients\{430fd4d0-b729-4f61-aa34-
91526481799d}[name]
  Sets/Creates value:       HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-
91526481799d}[pv]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\run[google update]
  Sets/Creates value:       HKCU\software\google\update[ismachineregistered]
  Sets/Creates value:       HKCU\software\classes\clsid\{a4801c24-04d0-4f28-8cf0-
adace2bd839c}\inprochandler32[]
  Sets/Creates value:       HKCU\software\classes\clsid\{a4801c24-04d0-4f28-8cf0-
adace2bd839c}\inprochandler32[threadingmodel]
  Sets/Creates value:       HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-
94be6cb3469f}\inprocserver32[]
  Sets/Creates value:       HKCU\software\classes\clsid\{e8cf3e55-f919-49d9-abc0-
94be6cb3469f}\inprocserver32[threadingmodel]
  Sets/Creates value:       HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-
60d9cdcd84c5}\inprocserver32[]
  Sets/Creates value:       HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-
60d9cdcd84c5}\inprocserver32[threadingmodel]
  Sets/Creates value:       HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-60d9cdcd84c5}[]
  Sets/Creates value:       HKCU\software\classes\interface\{2e629606-312a-482f-9b12-
2c4abf6f0b6d}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{2e629606-312a-482f-9b12-2c4abf6f0b6d}[]
  Sets/Creates value:       HKCU\software\classes\interface\{2e629606-312a-482f-9b12-
2c4abf6f0b6d}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{31acf3f1-e5ea-4a85-8a3d-
8e095a39c27b}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{31acf3f1-e5ea-4a85-8a3d-8e095a39c27b}[]
  Sets/Creates value:       HKCU\software\classes\interface\{31acf3f1-e5ea-4a85-8a3d-
8e095a39c27b}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{8476ce12-ae1f-4198-805c-
ba0f9b783f57}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{8476ce12-ae1f-4198-805c-ba0f9b783f57}[]
  Sets/Creates value:       HKCU\software\classes\interface\{8476ce12-ae1f-4198-805c-
ba0f9b783f57}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{0cd01d1e-4a1c-489d-93b9-
9b6672877c57}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{0cd01d1e-4a1c-489d-93b9-9b6672877c57}[]
  Sets/Creates value:       HKCU\software\classes\interface\{0cd01d1e-4a1c-489d-93b9-
9b6672877c57}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{4e223225-c16b-4eeb-aedc-
19ae99e237fa}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{4e223225-c16b-4eeb-aedc-19ae99e237fa}[]
  Sets/Creates value:       HKCU\software\classes\interface\{4e223225-c16b-4eeb-aedc-
19ae99e237fa}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{bcdcb538-01c0-46d1-a6a7-
52f4d021c272}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{bcdcb538-01c0-46d1-a6a7-52f4d021c272}[]
  Sets/Creates value:       HKCU\software\classes\interface\{bcdcb538-01c0-46d1-a6a7-
52f4d021c272}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{49d7563b-2ddb-4831-88c8-
768a53833837}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{49d7563b-2ddb-4831-88c8-768a53833837}[]
  Sets/Creates value:       HKCU\software\classes\interface\{49d7563b-2ddb-4831-88c8-
768a53833837}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{dab1d343-1b2a-47f9-b445-
93dc50704bfe}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{dab1d343-1b2a-47f9-b445-93dc50704bfe}[]
  Sets/Creates value:       HKCU\software\classes\interface\{dab1d343-1b2a-47f9-b445-
93dc50704bfe}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{3d05f64f-71e3-48a5-bf6b-
83315bc8ae1f}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{3d05f64f-71e3-48a5-bf6b-83315bc8ae1f}[]
  Sets/Creates value:       HKCU\software\classes\interface\{3d05f64f-71e3-48a5-bf6b-
83315bc8ae1f}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{6db17455-4e85-46e7-9d23-
e555e4b005af}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{6db17455-4e85-46e7-9d23-e555e4b005af}[]
  Sets/Creates value:       HKCU\software\classes\interface\{6db17455-4e85-46e7-9d23-
e555e4b005af}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{dd42475d-6d46-496a-924e-
bd5630b4cbba}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{dd42475d-6d46-496a-924e-bd5630b4cbba}[]
  Sets/Creates value:       HKCU\software\classes\interface\{dd42475d-6d46-496a-924e-
bd5630b4cbba}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{d106ab5f-a70e-400e-a21b-
96208c1d8dbb}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{d106ab5f-a70e-400e-a21b-96208c1d8dbb}[]
  Sets/Creates value:       HKCU\software\classes\interface\{d106ab5f-a70e-400e-a21b-
96208c1d8dbb}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{b3a47570-0a85-4aea-8270-
529d47899603}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{b3a47570-0a85-4aea-8270-529d47899603}[]
  Sets/Creates value:       HKCU\software\classes\interface\{b3a47570-0a85-4aea-8270-
529d47899603}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{18d0f672-18b4-48e6-ad36-
6e6bf01dbbc4}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{18d0f672-18b4-48e6-ad36-6e6bf01dbbc4}[]
  Sets/Creates value:       HKCU\software\classes\interface\{18d0f672-18b4-48e6-ad36-
6e6bf01dbbc4}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{2d363682-561d-4c3a-81c6-
f2f82107562a}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{2d363682-561d-4c3a-81c6-f2f82107562a}[]
  Sets/Creates value:       HKCU\software\classes\interface\{2d363682-561d-4c3a-81c6-
f2f82107562a}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{dca88386-4f03-4dbd-a366-
d90bc9f68de6}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{dca88386-4f03-4dbd-a366-d90bc9f68de6}[]
  Sets/Creates value:       HKCU\software\classes\interface\{dca88386-4f03-4dbd-a366-
d90bc9f68de6}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{76f7b787-a67c-4c73-82c7-
31f5e3aabc5c}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{76f7b787-a67c-4c73-82c7-31f5e3aabc5c}[]
  Sets/Creates value:       HKCU\software\classes\interface\{76f7b787-a67c-4c73-82c7-
31f5e3aabc5c}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{128c2da6-2bc0-44c0-b3f6-
4ec22e647964}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{128c2da6-2bc0-44c0-b3f6-4ec22e647964}[]
  Sets/Creates value:       HKCU\software\classes\interface\{128c2da6-2bc0-44c0-b3f6-
4ec22e647964}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{084d78a8-b084-4e14-a629-
a2c419b0e3d9}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{084d78a8-b084-4e14-a629-a2c419b0e3d9}[]
  Sets/Creates value:       HKCU\software\classes\interface\{084d78a8-b084-4e14-a629-
a2c419b0e3d9}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{909489c2-85a6-4322-aa56-
d25278649d67}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{909489c2-85a6-4322-aa56-d25278649d67}[]
  Sets/Creates value:       HKCU\software\classes\interface\{909489c2-85a6-4322-aa56-
d25278649d67}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{494b20cf-282e-4bdd-9f5d-
b70cb09d351e}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{494b20cf-282e-4bdd-9f5d-b70cb09d351e}[]
  Sets/Creates value:       HKCU\software\classes\interface\{494b20cf-282e-4bdd-9f5d-
b70cb09d351e}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{5b25a8dc-178d-4178-a629-
6be8b8defaa2}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{5b25a8dc-178d-4178-a629-6be8b8defaa2}[]
  Sets/Creates value:       HKCU\software\classes\interface\{5b25a8dc-178d-4178-a629-
6be8b8defaa2}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{fe908cdd-22bb-472a-9870-
1a0390e42f36}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{fe908cdd-22bb-472a-9870-1a0390e42f36}[]
  Sets/Creates value:       HKCU\software\classes\interface\{fe908cdd-22bb-472a-9870-
1a0390e42f36}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{1c642ced-ca3b-4013-a9df-
ca6ce5ff6503}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{1c642ced-ca3b-4013-a9df-ca6ce5ff6503}[]
  Sets/Creates value:       HKCU\software\classes\interface\{1c642ced-ca3b-4013-a9df-
ca6ce5ff6503}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\clsid\{5cccb0ef-7073-4516-8028-
4c628d0c8aab}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\clsid\{5cccb0ef-7073-4516-8028-4c628d0c8aab}[]
  Sets/Creates value:       HKCU\software\classes\clsid\{5cccb0ef-7073-4516-8028-
4c628d0c8aab}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{247954f9-9edc-4e68-8cc3-
150c2b89eadf}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{247954f9-9edc-4e68-8cc3-150c2b89eadf}[]
  Sets/Creates value:       HKCU\software\classes\interface\{247954f9-9edc-4e68-8cc3-
150c2b89eadf}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\interface\{4de778fe-f195-4ee3-9dab-
fe446c239221}\proxystubclsid32[]
  Sets/Creates value:       HKCU\software\classes\interface\{4de778fe-f195-4ee3-9dab-fe446c239221}[]
  Sets/Creates value:       HKCU\software\classes\interface\{4de778fe-f195-4ee3-9dab-
fe446c239221}\nummethods[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3comclassuser.1.0[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3comclassuser.1.0\clsid[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3comclassuser[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3comclassuser\clsid[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3comclassuser\curver[]
  Sets/Creates value:       HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-a3300ddf097f}[]
  Sets/Creates value:       HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-
a3300ddf097f}\progid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-
a3300ddf097f}\versionindependentprogid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{022105bd-948a-40c9-ab42-
a3300ddf097f}\localserver32[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3webuser.1.0[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3webuser.1.0\clsid[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3webuser[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3webuser\clsid[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.update3webuser\curver[]
  Sets/Creates value:       HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-e5cbfc70cc43}[]
  Sets/Creates value:       HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-
e5cbfc70cc43}\progid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-
e5cbfc70cc43}\versionindependentprogid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{22181302-a8a6-4f84-a541-
e5cbfc70cc43}\localserver32[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.ondemandcomclassuser.1.0[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.ondemandcomclassuser.1.0\clsid[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.ondemandcomclassuser[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.ondemandcomclassuser\clsid[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.ondemandcomclassuser\curver[]
  Sets/Creates value:       HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-114a56e93598}[]
  Sets/Creates value:       HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-
114a56e93598}\progid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-
114a56e93598}\versionindependentprogid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{2f0e2680-9ff5-43c0-b76e-
114a56e93598}\localserver32[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.credentialdialoguser.1.0[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.credentialdialoguser.1.0\clsid[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.credentialdialoguser[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.credentialdialoguser\clsid[]
  Sets/Creates value:       HKCU\software\classes\googleupdate.credentialdialoguser\curver[]
  Sets/Creates value:       HKCU\software\classes\clsid\{e67be843-bbbe-4484-95fb-05271ae80750}[]
  Sets/Creates value:       HKCU\software\classes\clsid\{e67be843-bbbe-4484-95fb-
05271ae80750}\progid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{e67be843-bbbe-4484-95fb-
05271ae80750}\versionindependentprogid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{e67be843-bbbe-4484-95fb-
05271ae80750}\localserver32[]
  Sets/Creates value:       HKCU\software\classes\google.oneclickprocesslauncheruser.1.0[]
  Sets/Creates value:       HKCU\software\classes\google.oneclickprocesslauncheruser.1.0\clsid[]
  Sets/Creates value:       HKCU\software\classes\google.oneclickprocesslauncheruser[]
  Sets/Creates value:       HKCU\software\classes\google.oneclickprocesslauncheruser\clsid[]
  Sets/Creates value:       HKCU\software\classes\google.oneclickprocesslauncheruser\curver[]
  Sets/Creates value:       HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-c7ead5f30c119}[]
  Sets/Creates value:       HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-
c7ead5f30c119}\progid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-
c7ead5f30c119}\versionindependentprogid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{51f9e8ef-59d7-475b-a106-
c7ead5f30c119}\localserver32[]
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\low
rights\elevationpolicy\{51f9e8ef-59d7-475b-a106-c7ead5f30c119}[clsid]
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\low
rights\elevationpolicy\{51f9e8ef-59d7-475b-a106-c7ead5f30c119}[policy]
  Sets/Creates value:       HKCU\software\google\update[lastsuccessfulversion]
  Sets/Creates value:       HKCU\software\google\update[version]
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${path}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${path}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${description}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${description}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${productname}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${productname}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${vendor}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${vendor}
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\low
rights\elevationpolicy\{c442ac41-9200-4770-8cc0-7cdb4f245c55}[appname]
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\low
rights\elevationpolicy\{c442ac41-9200-4770-8cc0-7cdb4f245c55}[apppath]
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\low
rights\elevationpolicy\{c442ac41-9200-4770-8cc0-7cdb4f245c55}[policy]
  Sets/Creates value:       HKCU\software\classes\google.oneclickctrl.9[]
  Sets/Creates value:       HKCU\software\classes\google.oneclickctrl.9\clsid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-7cdb4f245c55}[]
  Sets/Creates value:       HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-
7cdb4f245c55}\progid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-
7cdb4f245c55}\inprocserver32[]
  Sets/Creates value:       HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-
7cdb4f245c55}\inprocserver32[threadingmodel]
  Sets/Creates value:       HKCU\software\classes\clsid\{c442ac41-9200-4770-8cc0-
7cdb4f245c55}\implemented categories\{59fb2056-d625-48d0-a944-1a85b5ab2640}[]
  Sets/Creates value:       HKCU\software\classes\mime\database\content type\application/x-
vnd.google.oneclickctrl.9[clsid]
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${path}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${description}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${productname}
  Sets/Creates value:       HKCU\software\mozillaplugins\@tools.google.com/google
update;version=${vendor}
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\low
rights\elevationpolicy\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}[appname]
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\low
rights\elevationpolicy\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}[apppath]
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\low
rights\elevationpolicy\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}[policy]
  Sets/Creates value:       HKCU\software\classes\google.updatewebcontrol.3[]
  Sets/Creates value:       HKCU\software\classes\google.updatewebcontrol.3\clsid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-41ffc1a3c19d}[]
  Sets/Creates value:       HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-
41ffc1a3c19d}\progid[]
  Sets/Creates value:       HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-
41ffc1a3c19d}\inprocserver32[]
  Sets/Creates value:       HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-
41ffc1a3c19d}\inprocserver32[threadingmodel]
  Sets/Creates value:       HKCU\software\classes\clsid\{c3101a8b-0ee1-4612-bfe9-
```

41ffc1a3c19d}\implemented categories\{59fb2056-d625-48d0-a944-1a85b5ab2640}[]
  Sets/Creates value: HKCU\software\classes\mime\database\content type\application/x-vnd.google.update3webcontrol.3[clsid]
  Sets/Creates value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-9152648179fb}[iid]
  Sets/Creates value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-9152648179fb}[brand]
  Sets/Creates value: HKCU\software\google\update\clientstate\{430fd4d0-b729-4f61-aa34-9152648179fb}[installtime]
  Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and settings\admin\local settings\application data\google\update\googleupdate.exe]
  Sets/Creates value: HKCU\software\google\update\proxy[source]
  Value changes: HKLM\software\microsoft\cryptography\rng[seed]
  Value changes: HKCU\software\microsoft\windows nt\currentversion\time zones[timezonekeyname]
  Value changes: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-60d9cdcd84c5}\inprocserver32[]
  Value changes: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-60d9cdcd84c5}\inprocserver32[threadingmodel]
  Value changes: HKCU\software\classes\clsid\{6d7374de-63aa-473c-8c02-60d9cdcd84c5}[]
  Value changes: HKCU\software\classes\interface\{2e629606-312a-482f-9b12-2c4abf6f0b6d}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{2e629606-312a-482f-9b12-2c4abf6f0b6d}\nummethods[]
  Value changes: HKCU\software\classes\interface\{31ac3f11-e5ea-4a85-8a3d-8e095a39c27b}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{31ac3f11-e5ea-4a85-8a3d-8e095a39c27b}\nummethods[]
  Value changes: HKCU\software\classes\interface\{8476ce12-ae1f-4198-805c-ba0f9b783f57}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{8476ce12-ae1f-4198-805c-ba0f9b783f57}\nummethods[]
  Value changes: HKCU\software\classes\interface\{0cd01d1e-4a1c-489d-93b9-9b6672877c57}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{0cd01d1e-4a1c-489d-93b9-9b6672877c57}\nummethods[]
  Value changes: HKCU\software\classes\interface\{4e223325-c16b-4eeb-aedc-19ae99a237fa}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{4e223325-c16b-4eeb-aedc-19ae99a237fa}\nummethods[]
  Value changes: HKCU\software\classes\interface\{bcdcb538-01c0-46d1-a6a7-52f4d021c272}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{bcdcb538-01c0-46d1-a6a7-52f4d021c272}\nummethods[]
  Value changes: HKCU\software\classes\interface\{49d7563b-2ddb-4831-88c8-768a53833837}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{49d7563b-2ddb-4831-88c8-768a53833837}\nummethods[]
  Value changes: HKCU\software\classes\interface\{dab1d343-1b2a-47f9-b445-93dc50704bfe}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{dab1d343-1b2a-47f9-b445-93dc50704bfe}\nummethods[]
  Value changes: HKCU\software\classes\interface\{3d05f64f-71e3-48a5-bf6b-83315bc8ae1f}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{3d05f64f-71e3-48a5-bf6b-83315bc8ae1f}\nummethods[]
  Value changes: HKCU\software\classes\interface\{6db17455-4e85-46e7-9d23-e555e4b005af}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{6db17455-4e85-46e7-9d23-e555e4b005af}\nummethods[]
  Value changes: HKCU\software\classes\interface\{dd42475d-6d46-496a-924e-bd5630b4cbba}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{dd42475d-6d46-496a-924e-bd5630b4cbba}\nummethods[]
  Value changes: HKCU\software\classes\interface\{d106ab5f-a70e-400e-a21b-96208c1d8dbb}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{d106ab5f-a70e-400e-a21b-96208c1d8dbb}\nummethods[]
  Value changes: HKCU\software\classes\interface\{b3a47570-0a85-4eea-8270-529d47899603}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{b3a47570-0a85-4eea-8270-529d47899603}\nummethods[]
  Value changes: HKCU\software\classes\interface\{18d0f672-18b4-48e6-ad36-6e6bf01dbbc4}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{18d0f672-18b4-48e6-ad36-6e6bf01dbbc4}\nummethods[]
  Value changes: HKCU\software\classes\interface\{2d363682-561d-4c3a-81c6-f2f82107562a}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{2d363682-561d-4c3a-81c6-f2f82107562a}\nummethods[]
  Value changes: HKCU\software\classes\interface\{dcab8386-4f03-4dbd-a366-d90bc9f68de6}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{dcab8386-4f03-4dbd-a366-d90bc9f68de6}\nummethods[]
  Value changes: HKCU\software\classes\interface\{76f7b787-a67c-4c73-82c7-31f5e3aabc5c}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{76f7b787-a67c-4c73-82c7-31f5e3aabc5c}\nummethods[]
  Value changes: HKCU\software\classes\interface\{128c2da6-2bc0-44c0-b3f6-4ec22e647964}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{128c2da6-2bc0-44c0-b3f6-4ec22e647964}\nummethods[]
  Value changes: HKCU\software\classes\interface\{0844f8a8-b084-4e14-a629-a2c419b0e3d9}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{0844f8a8-b084-4e14-a629-a2c419b0e3d9}\nummethods[]
  Value changes: HKCU\software\classes\interface\{909489c2-85a6-4322-aa56-d252786949d7}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{909489c2-85a6-4322-aa56-d252786949d7}\nummethods[]
  Value changes: HKCU\software\classes\interface\{494b20cf-282e-4bdd-9f5d-b70cb09d351e}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{494b20cf-282e-4bdd-9f5d-b70cb09d351e}\nummethods[]
  Value changes: HKCU\software\classes\interface\{5b25a8dc-1780-4178-a629-6be8b8defaa2}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{5b25a8dc-1780-4178-a629-6be8b8defaa2}\nummethods[]
  Value changes: HKCU\software\classes\interface\{fe908cdd-22bb-472a-9870-1a0390e42f36}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{fe908cdd-22bb-472a-9870-1a0390e42f36}\nummethods[]
  Value changes: HKCU\software\classes\interface\{1c642ced-ca3b-4013-a9df-ca6ce5ff6503}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{1c642ced-ca3b-4013-a9df-ca6ce5ff6503}\nummethods[]
  Value changes: HKCU\software\classes\interface\{5cccb0ef-7073-4516-8028-4c628d0c8aab}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{5cccb0ef-7073-4516-8028-4c628d0c8aab}\nummethods[]
  Value changes: HKCU\software\classes\interface\{247954f9-9edc-4e68-8cc3-150c2b89eadf}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{247954f9-9edc-4e68-8cc3-150c2b89eadf}\nummethods[]
  Value changes: HKCU\software\classes\interface\{4de778fe-f195-4ea3-9dab-fe446c239221}\proxystubclsid32[]
  Value changes: HKCU\software\classes\interface\{4de778fe-f195-4ea3-9dab-fe446c239221}\nummethods[]
  Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[personal]
  Value changes: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\baseclass]
  Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common documents]
  Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[desktop]
  Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common desktop]
  Value changes: HKCU\software\google\update\clientstate\{8a69d345-d564-463c-aff1-a69d9e530f96}[usagestats]
  Value changes: HKCU\software\google\update\proxy[source]