Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3306, Task ID: 732

Task ID:	732
Risk Level:	10
Date Processed:	2016-05-18 10:31:27 (UTC)
Processing Time:	62.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe"
Sample ID:	3306
Type:	basic
Owner:	admin
Label:	35644f3d0029f81c3d478d3c2407fac3
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	597504 bytes
MD5:	35644f3d0029f81c3d478d3c2407fac3
SHA256:	05093ba493e460b909f4922656c72a340517b31d8d6ff569dd73a2c1c9fc04dd
Description:	None

Pattern Matching Results

6 Writes to system32 folder
2 PE: Nonstandard section
10 Creates malicious mutex: Expiro [Fileinfector]
6 Suspicious packer: VMProtect
5 Creates process in suspicious location
5 Validates shell extensions
3 Long sleep detected
4 Terminates process under Windows subfolder

Static Events

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\WINDOWS\Temp\35644f3d0029f81c3d478d3c2407fac3.exe ["c:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe"]
Creates process: C:\WINDOWS\system32\cisvc.exe [C:\WINDOWS\system32\cisvc.exe]
Creates process: C:\WINDOWS\system32\cidaemon.exe ["cidaemon.exe" DownLevelDaemon "c:\system volume information\catalog.wci" 1966721 16561]
Creates process: C:\WINDOWS\system32\verclsid.exe [/S /C {E4B29F9D-D390-480B-92FD-7DDB47101D71} /I {0000010B-0000-0000-C000-000000000046} /X 0x401]
Creates process: C:\WINDOWS\system32\verclsid.exe [/S /C {EB9B1153-3B57-4E68-959A-A3266BC3D7FE} /I {0000010B-0000-0000-C000-000000000046} /X 0x401]
Creates process: C:\WINDOWS\system32\verclsid.exe [/S /C {875CB1A1-0F29-45DE-A1AE-CFB4950D0B78} /I {0000010B-0000-0000-C000-000000000046} /X 0x401]
Creates process: C:\WINDOWS\system32\verclsid.exe [/S /C {FBF23B40-E3F0-101B-8488-00AA003E56F8} /I {0000010B-0000-0000-C000-000000000046} /X 0x401]
Loads service: CiSvc [C:\WINDOWS\system32\cisvc.exe]
Terminates process: C:\WINDOWS\Temp\35644f3d0029f81c3d478d3c2407fac3.exe
Terminates process: C:\WINDOWS\system32\verclsid.exe

Named Object Events

Creates mutex: \BaseNamedObjects__PDH_PLA_MUTEX__
Creates mutex: \BaseNamedObjects\kkq-vx_mtx1
Creates mutex: \BaseNamedObjects\kkq-vx_mtx28
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\SHIMLIB_LOG_MUTEX
Creates mutex: \BaseNamedObjects\gazavat-svc
Creates mutex: \BaseNamedObjects\gazavat-svc_28
Creates mutex: \BaseNamedObjects__CiPerfMonMutex
Creates mutex: \BaseNamedObjects\c::system volume information:catalog.wci__cimutexsem
Creates event: \BaseNamedObjects\DINPUTWINMM
Creates event: \BaseNamedObjects\userenv: User Profile setup event
Creates event: \BaseNamedObjects\crypt32LogoffEvent
Creates event: \BaseNamedObjects\c::system volume information__cievent3
Creates event: \BaseNamedObjects\c::system volume information:catalog.wci__cievent1

Creates event: \BaseNamedObjects\c::system volume information:catalog.wci__cievent2
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore: \BaseNamedObjects\OleDfRoot00002550B
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Creates: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
Creates: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe
Creates: C:\WINDOWS\system32\cisvc.vir
Creates: C:\WINDOWS\system32\cisvc.exe
Creates: C:\WINDOWS\system32\clipsrv.vir
Creates: C:\WINDOWS\system32\clipsrv.exe
Creates: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
Creates: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
Creates: C:\System Volume Information
Creates: C:\System Volume Information\catalog.wci
Creates: C:\WINDOWS\system32\dmadmin.vir
Creates: C:\System Volume Information\catalog.wci\CiSP0000.000
Creates: C:\System Volume Information\catalog.wci\CiSP0000.001
Creates: C:\System Volume Information\catalog.wci\CiSP0000.002
Creates: C:\WINDOWS\system32\dmadmin.exe
Creates: C:\System Volume Information\catalog.wci\INDEX.000
Creates: C:\System Volume Information\catalog.wci\INDEX.001
Creates: C:\System Volume Information\catalog.wci\INDEX.002
Creates: C:\System Volume Information\catalog.wci\CiFLfffd.000
Creates: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.vir
Creates: C:\System Volume Information\catalog.wci\CiFLfffd.001
Creates: C:\System Volume Information\catalog.wci\CiFLfffd.002
Creates: C:\System Volume Information\catalog.wci\CiCL0001.000
Creates: C:\System Volume Information\catalog.wci\CiCL0001.001
Creates: C:\System Volume Information\catalog.wci\CiCL0001.002
Creates: C:\System Volume Information\catalog.wci\CiSL0001.000
Creates: C:\System Volume Information\catalog.wci\CiSL0001.001
Creates: C:\System Volume Information\catalog.wci\CiSL0001.002
Creates: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.exe
Creates: C:\System Volume Information\catalog.wci\CiP10000.000
Creates: C:\System Volume Information\catalog.wci\CiP10000.001
Creates: C:\System Volume Information\catalog.wci\CiP10000.002
Creates: C:\System Volume Information\catalog.wci\CiP20000.000
Creates: C:\System Volume Information\catalog.wci\CiP20000.001
Creates: C:\System Volume Information\catalog.wci\CiP20000.002
Creates: C:\System Volume Information\catalog.wci\CiPT0000.000
Creates: C:\System Volume Information\catalog.wci\CiPT0000.001
Creates: C:\System Volume Information\catalog.wci\CiPT0000.002
Creates: C:\System Volume Information\catalog.wci\CiST0000.000
Creates: C:\System Volume Information\catalog.wci\CiST0000.001
Creates: C:\System Volume Information\catalog.wci\CiST0000.002
Creates: C:\System Volume Information\catalog.wci\00000001.ps1
Creates: C:\System Volume Information\catalog.wci\propstor.bk1
Creates: C:\System Volume Information\catalog.wci\00000001.ps2
Creates: C:\System Volume Information\catalog.wci\propstor.bk2
Creates: C:\System Volume Information\catalog.wci\cicat.hsh
Creates: C:\System Volume Information\catalog.wci\CiVP0000.000
Creates: C:\System Volume Information\catalog.wci\CiVP0000.001
Creates: C:\System Volume Information\catalog.wci\CiVP0000.002
Creates: C:\System Volume Information\catalog.wci\cicat.fid
Creates: C:\WINDOWS\system32\imapi.vir
Creates: C:\WINDOWS\system32\imapi.exe
Creates: C:\System Volume Information\catalog.wci\00000002.ps1
Creates: C:\System Volume Information\catalog.wci\00000002.ps2
Creates: C:\WINDOWS\system32\mnmsrvc.vir
Creates: C:\WINDOWS\system32\mnmsrvc.exe
Creates: C:\WINDOWS\system32\msiexec.vir
Creates: C:\WINDOWS\system32\msiexec.exe
Creates: C:\WINDOWS\system32\netdde.vir
Creates: C:\WINDOWS\system32\netdde.exe
Creates: C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
Creates: C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
Creates: C:\WINDOWS\system32\sessmgr.vir
Creates: C:\WINDOWS\system32\sessmgr.exe
Creates: C:\WINDOWS\system32\locator.vir
Creates: C:\WINDOWS\system32\locator.exe
Creates: C:\WINDOWS\system32\scardsvr.vir
Creates: C:\WINDOWS\system32\scardsvr.exe
Creates: C:\WINDOWS\system32\smlogsvc.vir
Creates: C:\windows\system32\smlogsvc.exe
Creates: C:\WINDOWS\system32\vssvc.vir
Creates: C:\WINDOWS\system32\vssvc.exe
Creates: C:\WINDOWS\system32\wbem\wmiapsrv.vir

```
  Creates:                C:\WINDOWS\system32\wbem\wmiapsrv.exe
  Creates:                C:\Program Files\Internet Explorer\iexplore.vir
  Creates:                C:\Program Files\Internet Explorer\iexplore.exe
  Creates:                C:\System Volume Information\catalog.wci\00010001.ci
  Creates:                C:\System Volume Information\catalog.wci\00010001.dir
  Creates:                C:\System Volume Information\catalog.wci\CiFLfffc.000
  Creates:                C:\System Volume Information\catalog.wci\CiFLfffc.001
  Creates:                C:\System Volume Information\catalog.wci\CiFLfffc.002
  Opens:                  C:\WINDOWS\Prefetch\35644F3D0029F81C3D478D3C2407F-06C959F7.pf
  Opens:                  C:\Documents and Settings\Admin
  Opens:                  C:\WINDOWS\system32\netapi32.dll
  Opens:                  C:\WINDOWS\system32\pdh.dll
  Opens:                  C:\WINDOWS\system32\crypt32.dll
  Opens:                  C:\WINDOWS\system32\msasn1.dll
  Opens:                  C:\WINDOWS\system32\odbc32.dll
  Opens:                  C:\WINDOWS\system32\odbcbcp.dll
  Opens:                  C:\WINDOWS\system32\imm32.dll
  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\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\odbcint.dll
  Opens:                  C:\WINDOWS\system32\sfc_os.dll
  Opens:                  C:\WINDOWS\system32\wintrust.dll
  Opens:                  C:\WINDOWS\system32\pstorec.dll
  Opens:                  C:\WINDOWS\system32\atl.dll
  Opens:                  C:\WINDOWS\system32\crtdll.dll
  Opens:                  C:\WINDOWS\system32\sfc.dll
  Opens:                  C:\WINDOWS\system32\MSCTF.dll
  Opens:                  C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                  C:\windows\SysWOW64\svchost.exe
  Opens:                  C:\windows\system32\svchost.exe
  Opens:                  C:\WINDOWS\system32\svchost.exe
  Opens:                  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe
  Opens:                  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
  Opens:                  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
  Opens:                  C:\WINDOWS\Temp\27db9baa-dc60-425c-8aca-ef0ca60d7b54
  Opens:                  C:\windows\SysWOW64\cisvc.exe
  Opens:                  C:\WINDOWS\system32\cisvc.exe
  Opens:                  C:\WINDOWS\system32
  Opens:                  C:\WINDOWS\system32\cisvc.vir
  Opens:                  C:\WINDOWS\Prefetch\CISVC.EXE-21F69875.pf
  Opens:                  C:\WINDOWS\system32\query.dll
  Opens:                  C:\WINDOWS\system32\shimeng.dll
  Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\WINDOWS\AppPatch\AcGenral.dll
  Opens:                  C:\WINDOWS\system32\winmm.dll
  Opens:                  C:\WINDOWS\system32\msacm32.dll
  Opens:                  C:\WINDOWS\system32\uxtheme.dll
  Opens:                  C:\WINDOWS\system32\comctl32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\comctl32.dll.124.Config
  Opens:                  C:
  Opens:                  C:\WINDOWS\system32\setupapi.dll
  Opens:                  C:\WINDOWS\system32\rpcss.dll
  Opens:                  C:\WINDOWS\system32\clbcatq.dll
  Opens:                  C:\WINDOWS\system32\comres.dll
  Opens:                  C:\WINDOWS\Registration\R000000000007.clb
  Opens:                  C:\WINDOWS\system32\ciadmin.dll
  Opens:                  C:\WINDOWS\system32\ciadmin.dll.2.Manifest
  Opens:                  C:\WINDOWS\system32\ciadmin.dll.2.Config
  Opens:                  C:\WINDOWS\system32\ixsso.dll
  Opens:                  C:\WINDOWS\system32\nlhtml.dll
  Opens:                  C:\windows\SysWOW64\clipsrv.exe
  Opens:                  C:\WINDOWS\system32\clipsrv.exe
  Opens:                  C:\WINDOWS\system32\offfilt.dll
  Opens:                  C:\WINDOWS\system32\clipsrv.vir
  Opens:                  C:\WINDOWS\system32\ciodm.dll
  Opens:                  C:\WINDOWS\system32\infosoft.dll
  Opens:                  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
  Opens:                  C:\WINDOWS\system32\mimefilt.dll
  Opens:                  C:\WINDOWS\system32\langwrbk.dll
  Opens:                  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
  Opens:                  C:\windows\SysWOW64\dllhost.exe
  Opens:                  C:\WINDOWS\system32\dllhost.exe
```

Opens: C:\System Volume Information\catalog.wci
Opens: C:\
Opens: C:\windows\SysWOW64\dmadmin.exe
Opens: C:\WINDOWS\system32\dmadmin.exe
Opens: C:\WINDOWS\system32\dmadmin.vir
Opens: C:\WINDOWS\system32\ntmarta.dll
Opens: C:\WINDOWS\system32\samlib.dll
Opens: C:\WINDOWS\Microsoft.NET\Framework\v3.0\WPF\PresentationFontCache.exe
Opens: C:\System Volume Information\catalog.wci\INDEX.001
Opens: C:\System Volume Information\catalog.wci\INDEX.002
Opens: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.exe
Opens: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation
Opens: C:\System Volume Information\catalog.wci\CiCL0001.000
Opens: C:\System Volume Information\catalog.wci\CiCL0001.001
Opens: C:\System Volume Information\catalog.wci\CiCL0001.002
Opens: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.vir
Opens: C:\System Volume Information\catalog.wci\CiFLfffd.000
Opens: C:\System Volume Information\catalog.wci\CiFLfffd.001
Opens: C:\System Volume Information\catalog.wci\CiFLfffd.002
Opens: C:\System Volume Information\catalog.wci\CiSL0001.001
Opens: C:\System Volume Information\catalog.wci\CiSL0001.002
Opens: C:\System Volume Information\catalog.wci\CiSP0000.002
Opens: C:\System Volume Information\catalog.wci\CiSP0000.001
Opens: C:\System Volume Information\catalog.wci\CiP10000.001
Opens: C:\System Volume Information\catalog.wci\CiP20000.001
Opens: C:\System Volume Information\catalog.wci\CiPT0000.001
Opens: C:\System Volume Information\catalog.wci\CiST0000.001
Opens: C:\System Volume Information\catalog.wci\CiP10000.002
Opens: C:\system volume information\catalog.wci\00000001.ci
Opens: C:\system volume information\catalog.wci\00000001.hsh
Opens: C:\system volume information\catalog.wci\00000001.ps1
Opens: C:\system volume information\catalog.wci\00000001.ps2
Opens: C:\System Volume Information\catalog.wci\CiP20000.002
Opens: C:\System Volume Information\catalog.wci\CiVP0000.001
Opens: C:\windows\SysWOW64\imapi.exe
Opens: C:\WINDOWS\system32\imapi.exe
Opens: C:\WINDOWS\system32\imapi.vir
Opens: C:\System Volume Information\catalog.wci\00000001.ps1
Opens: C:\System Volume Information\catalog.wci\CiPT0000.002
Opens: C:\system volume information\catalog.wci\00000002.ci
Opens: C:\system volume information\catalog.wci\00000002.hsh
Opens: C:\system volume information\catalog.wci\00000002.ps1
Opens: C:\system volume information\catalog.wci\00000002.ps2
Opens: C:\System Volume Information\catalog.wci\00000001.ps2
Opens: C:\WINDOWS\system32\drprov.dll
Opens: C:\windows\SysWOW64\mnmsrvc.exe
Opens: C:\WINDOWS\system32\mnmsrvc.exe
Opens: C:\WINDOWS\system32\ntlanman.dll
Opens: C:\WINDOWS\system32\netui0.dll
Opens: C:\WINDOWS\system32\netui1.dll
Opens: C:\WINDOWS\system32\netrap.dll
Opens: C:\WINDOWS\system32\davclnt.dll
Opens: C:\WINDOWS\system32\mnmsrvc.vir
Opens: C:\WINDOWS\system32\cidaemon.exe
Opens: C:\windows\SysWOW64\msdtc.exe
Opens: C:\WINDOWS\system32\msdtc.exe
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\windows\SysWOW64\msiexec.exe
Opens: C:\WINDOWS\system32\msiexec.exe
Opens: C:\WINDOWS\system32\cidaemon.exe.Manifest
Opens: C:\WINDOWS\Prefetch\CIDAEMON.EXE-27AE97A4.pf
Opens: C:\WINDOWS\system32\msiexec.vir
Opens: C:\windows\SysWOW64\netdde.exe
Opens: C:\WINDOWS\system32\netdde.exe
Opens: C:\Documents and Settings
Opens: C:\WINDOWS\system32\netdde.vir
Opens: C:\windows\SysWOW64\lsass.exe
Opens: C:\windows\system32\lsass.exe
Opens: C:\WINDOWS\system32\lsass.exe
Opens: C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
Opens: C:\Program Files\Common Files\Microsoft Shared\Source Engine
Opens: C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
Opens: C:\windows\SysWOW64\sessmgr.exe
Opens: C:\WINDOWS\system32\sessmgr.exe
Opens: C:\WINDOWS\system32\sessmgr.vir
Opens: C:\Documents and Settings\Administrator
Opens: C:\Documents and Settings\All Users
Opens: C:\Documents and Settings\Default User
Opens: C:\Documents and Settings\LocalService
Opens: C:\windows\SysWOW64\locator.exe
Opens: C:\WINDOWS\system32\locator.exe

```
  Opens:                  C:\Documents and Settings\NetworkService
  Opens:                  C:\WINDOWS\system32\locator.vir
  Opens:                  C:\Documents and Settings\NetworkService\Application Data
  Opens:                  C:\Documents and Settings\NetworkService\Cookies
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings
  Opens:                  C:\Documents and Settings\NetworkService\NTUSER.DAT
  Opens:                  C:\Documents and Settings\NetworkService\ntuser.dat.LOG
  Opens:                  C:\Documents and Settings\NetworkService\ntuser.ini
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings\Application Data
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings\desktop.ini
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings\History
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings\Temp
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings\Temporary
Internet Files
  Opens:                  C:\Documents and Settings\NetworkService\Application Data\Microsoft
  Opens:                  C:\Documents and Settings\LocalService\Application Data
  Opens:                  C:\Documents and Settings\LocalService\Cookies
  Opens:                  C:\Documents and Settings\LocalService\Local Settings
  Opens:                  C:\Documents and Settings\LocalService\NTUSER.DAT
  Opens:                  C:\Documents and Settings\LocalService\ntuser.dat.LOG
  Opens:                  C:\Documents and Settings\LocalService\ntuser.ini
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\Application Data
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\desktop.ini
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\History
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\Temp
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\Temporary Internet
Files
  Opens:                  C:\Documents and Settings\LocalService\Cookies\index.dat
  Opens:                  C:\windows\SysWOW64\scardsvr.exe
  Opens:                  C:\WINDOWS\system32\scardsvr.exe
  Opens:                  C:\Documents and Settings\LocalService\Application Data\Microsoft
  Opens:                  C:\WINDOWS\system32\scardsvr.vir
  Opens:                  C:\windows\SysWOW64\smlogsvc.exe
  Opens:                  C:\WINDOWS\system32\smlogsvc.exe
  Opens:                  C:\WINDOWS\system32\smlogsvc.vir
  Opens:                  C:\windows\SysWOW64\ups.exe
  Opens:                  C:\WINDOWS\system32\ups.exe
  Opens:                  C:\windows\SysWOW64\vssvc.exe
  Opens:                  C:\WINDOWS\system32\vssvc.exe
  Opens:                  C:\Documents and Settings\Default User\Application Data
  Opens:                  C:\Documents and Settings\Default User\Cookies
  Opens:                  C:\documents and settings
  Opens:                  C:\Documents and Settings\Default User\Desktop
  Opens:                  C:\WINDOWS\system32\vssvc.vir
  Opens:                  C:\Documents and Settings\Default User\Favorites
  Opens:                  C:\Documents and Settings\Default User\Local Settings
  Opens:                  C:\Documents and Settings\Default User\My Documents
  Opens:                  C:\Documents and Settings\Default User\NetHood
  Opens:                  C:\Documents and Settings\Default User\NTUSER.DAT
  Opens:                  C:\Documents and Settings\Default User\NTUSER.DAT.LOG
  Opens:                  C:\windows\SysWOW64\wbem\wmiapsrv.exe
  Opens:                  C:\WINDOWS\system32\wbem\wmiapsrv.exe
  Opens:                  C:\Documents and Settings\Default User\PrintHood
  Opens:                  C:\WINDOWS\system32\wbem
  Opens:                  C:\Documents and Settings\Default User\Recent
  Opens:                  C:\WINDOWS\system32\wbem\wmiapsrv.vir
  Opens:                  C:\Documents and Settings\Default User\SendTo
  Opens:                  C:\Documents and Settings\Default User\Start Menu
  Opens:                  C:\Documents and Settings\Default User\Templates
  Opens:                  C:\System Volume Information\catalog.wci\CiST0000.002
  Opens:                  C:\Documents and Settings\Default User\Templates\amipro.sam
  Opens:                  C:\Documents and Settings\Default User\Templates\excel.xls
  Opens:                  C:\Documents and Settings\Default User\Templates\excel4.xls
  Opens:                  C:\Documents and Settings\Default User\Templates\lotus.wk4
  Opens:                  C:\Documents and Settings\Default User\Templates\powerpnt.ppt
  Opens:                  C:\Documents and Settings\Default User\Templates\presenta.shw
  Opens:                  C:\Documents and Settings\Default User\Templates\quattro.wb2
  Opens:                  C:\Documents and Settings\Default User\Templates\sndrec.wav
  Opens:                  C:\AUTOEXEC.BAT\
  Opens:                  C:\boot.ini\
  Opens:                  C:\CONFIG.SYS\
  Opens:                  C:\Documents and Settings\Default User\Templates\winword.doc
  Opens:                  C:\documents and settings\admin
  Opens:                  C:\Documents and Settings\Admin\Application Data
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeCMapFnt09.lst\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\AdobeSysFnt09.lst\
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Acrobat\9.0\Forms
  Opens:                  C:\Documents and Settings\Default User\Templates\winword2.doc
```

```
  Opens:                  C:\Documents and Settings\Default User\Templates\wordpfct.wpd
  Opens:                  C:\Documents and Settings\Default User\Templates\wordpfct.wpg
  Opens:                  C:\Documents and Settings\Default User\Start Menu\desktop.ini
  Opens:                  C:\Documents and Settings\Default User\Start Menu\Programs
  Opens:                  C:\documents and settings\administrator
  Opens:                  C:\Documents and Settings\Default User\Start Menu\Programs\Accessories
  Opens:                  C:\Documents and Settings\Default User\Start Menu\Programs\desktop.ini
  Opens:                  C:\Documents and Settings\Default User\Start Menu\Programs\Remote
Assistance.lnk
  Opens:                  C:\Documents and Settings\Default User\Start Menu\Programs\Startup
  Opens:                  C:\Documents and Settings\Default User\Start Menu\Programs\Windows Media
Player.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Startup\desktop.ini
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Command Prompt.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\desktop.ini
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Entertainment
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Notepad.lnk
  Opens:                  C:\documents and settings\all users
  Opens:                  C:\documents and settings\default user
  Opens:                  C:\documents and settings\localservice
  Opens:                  C:\documents and settings\networkservice
  Opens:                  C:\documents and settings\networkservice\application data
  Opens:                  C:\documents and settings\networkservice\cookies
  Opens:                  C:\documents and settings\networkservice\local settings
  Opens:                  C:\WINDOWS\system32\noise.dat
  Opens:                  C:\Documents and
Settings\NetworkService\ntuser.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C::{4c8cc155-6c1e-11d1-8e41-00c04fb9386d}:$DATA
  Opens:                  C:: DocumentSummaryInformation:$DATA
  Opens:                  C::Docf_ DocumentSummaryInformation:$DATA
  Opens:                  C:\documents and settings\localservice\application data
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts\glob.js\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\JavaScripts\glob.settings.js\
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Synchronize.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Tour Windows XP.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Windows Explorer.lnk
  Opens:                  C:\documents and settings\localservice\local settings
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
  Opens:                  C:\Documents and
Settings\LocalService\ntuser.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Default User\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
  Opens:                  C:\documents and settings\localservice\cookies\index.dat
  Opens:                  C:\Documents and Settings\Default User\SendTo\Desktop (create
shortcut).DeskLink
  Opens:                  C:\Documents and Settings\Default User\SendTo\desktop.ini
  Opens:                  C:\Documents and Settings\Default User\SendTo\Mail Recipient.MAPIMail
  Opens:                  C:\documents and settings\default user\application data
  Opens:                  C:\Documents and Settings\Default User\Local Settings\Application Data
  Opens:                  C:\Documents and Settings\Default User\Local Settings\desktop.ini
  Opens:                  C:\Documents and Settings\Default User\Local Settings\History
  Opens:                  C:\Documents and Settings\Default User\Local Settings\Temp
  Opens:                  C:\Documents and Settings\Default User\Local Settings\Temporary Internet
Files
```

Opens: C:\Documents and Settings\Default User\Cookies\index.dat
Opens: C:\Documents and Settings\Default User\Application Data\desktop.ini
Opens: C:\Documents and Settings\Default User\Application Data\Microsoft
Opens: C:\Documents and Settings\All Users\Application Data
Opens: C:\documents and settings\default user\cookies
Opens: C:\documents and settings\default user\desktop
Opens: C:\documents and settings\default user\favorites
Opens: C:\documents and settings\default user\local settings
Opens: C:\documents and settings\default user\my documents
Opens: C:\documents and settings\default user\nethood
Opens: C:\documents and settings\default user\printhood
Opens: C:\documents and settings\default user\recent
Opens: C:\documents and settings\default user\sendto
Opens: C:\documents and settings\default user\start menu
Opens: C:\documents and settings\default user\templates
Opens: C:\Documents and Settings\Default
User\Templates\amipro.sam: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\system32\noise.enu
Opens: C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\SharedDataEvents\
Opens: C:\Documents and Settings\Admin\Application
Data\Adobe\Acrobat\9.0\UserCache.bin\
Opens: C:\Documents and Settings\Default
User\Templates\excel4.xls: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default
User\Templates\lotus.wk4: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default
User\Templates\presenta.shw: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default
User\Templates\quattro.wb2: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\system32\verclsid.exe
Opens: C:\WINDOWS\system32\verclsid.exe.Manifest
Opens: C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf
Opens: C:\WINDOWS
Opens: C:\WINDOWS\Registration
Opens: C:\WINDOWS\WinSxS
Opens: C:\WINDOWS\system32\ntdll.dll
Opens: C:\WINDOWS\system32\kernel32.dll
Opens: C:\WINDOWS\system32\unicode.nls
Opens: C:\WINDOWS\system32\locale.nls
Opens: C:\WINDOWS\system32\sorttbls.nls
Opens: C:\WINDOWS\system32\ole32.dll
Opens: C:\WINDOWS\system32\advapi32.dll
Opens: C:\WINDOWS\system32\rpcrt4.dll
Opens: C:\WINDOWS\system32\secur32.dll
Opens: C:\WINDOWS\system32\gdi32.dll
Opens: C:\WINDOWS\system32\user32.dll
Opens: C:\WINDOWS\system32\msvcrt.dll
Opens: C:\WINDOWS\system32\ctype.nls
Opens: C:\WINDOWS\system32\sortkey.nls
Opens: C:\WINDOWS\system32\oleaut32.dll
Opens: C:\WINDOWS\system32\version.dll
Opens: C:\WINDOWS\system32\shlwapi.dll
Opens: C:\WINDOWS\system32\shdocvw.dll
Opens: C:\WINDOWS\system32\cryptui.dll
Opens: C:\WINDOWS\system32\wininet.dll
Opens: C:\WINDOWS\system32\imagehlp.dll
Opens: C:\WINDOWS\system32\wldap32.dll
Opens: C:\WINDOWS\system32\riched20.dll
Opens: C:\WINDOWS\system32\userenv.dll
Opens: C:\Documents and Settings\All Users\Desktop
Opens: C:\Documents and Settings\All Users\Documents
Opens: C:\Documents and Settings\All Users\DRM
Opens: C:\Documents and Settings\All Users\Favorites
Opens: C:\Documents and Settings\All Users\ntuser.pol
Opens: C:\Documents and Settings\All Users\Start Menu
Opens: C:\Documents and Settings\All Users\Templates
Opens: C:\Documents and Settings\All Users\Start Menu\desktop.ini
Opens: C:\Documents and Settings\All Users\Start Menu\Programs
Opens: C:\Documents and Settings\All Users\Start Menu\Set Program Access and
Defaults.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Windows Catalog.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Windows Update.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Adobe Reader
9.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\desktop.ini
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
Excel Viewer.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office

```
Word Viewer 2003.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft
PowerPoint Viewer .lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\MSN.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Startup
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Windows
Messenger.lnk
  Opens:                  C:\WINDOWS\system32\shmedia.dll
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Windows Movie
Maker.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Startup\desktop.ini
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\IDLE
(Python GUI).lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Module Docs.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python (command line).lnk
  Opens:                  C:\WINDOWS\system32\msvfw32.dll
  Opens:                  C:\WINDOWS\system32\avifil32.dll
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python for Windows Documentation.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python Manuals.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\PythonWin.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Uninstall Python.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Games\desktop.ini
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Freecell.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Games\Hearts.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Backgammon.lnk
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Checkers.lnk
  Opens:                  C:\WINDOWS\system32\verclsid.exe.124.Manifest
  Opens:                  C:\Documents and Settings\Default
User\Templates\winword2.doc: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Default
User\Templates\wordpfct.wpd: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Default
User\Templates\wordpfct.wpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\default user\start menu\programs
  Opens:                  C:\documents and settings\default user\start menu\programs\accessories
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\WINDOWS\system32\winlogon.exe
  Opens:                  C:\WINDOWS\system32\xpsp2res.dll
  Opens:                  C:\WINDOWS\system32\linkinfo.dll
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Flash Player
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\Flash
Player\AssetCache\7PLTA3CP
  Opens:                  C:\WINDOWS\system32\ntshrui.dll
  Opens:                  C:\WINDOWS\system32\ntshrui.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\ntshrui.dll.123.Config
  Opens:                  C:\Documents and Settings\Default User\Start Menu\Programs\Remote
Assistance.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\default user\start menu\programs\startup
  Opens:                  C:\Documents and Settings\Default User\Start Menu\Programs\Windows Media
Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Startup\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\default user\start
menu\programs\accessories\accessibility
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Command Prompt.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\default user\start
menu\programs\accessories\entertainment
  Opens:                  C:\Documents and Settings\Default User\Start
Menu\Programs\Accessories\Notepad.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\WINDOWS\system32\ieframe.dll
  Opens:                  C:\Program Files\Internet Explorer\iexplore.exe
  Opens:                  C:\WINDOWS\system32\ieframe.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\ieframe.dll.123.Config
```

Opens: C:\WINDOWS\system32\en-US\ieframe.dll.mui
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Program Compatibility Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Hearts.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Reversi.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Spades.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Minesweeper.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Pinball.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Solitaire.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Spider Solitaire.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Component Services.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Computer Management.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Data Sources (ODBC).lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\desktop.ini
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Event Viewer.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Local Security Policy.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Performance.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Services.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Accessibility
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Calculator.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Synchronize.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\desktop.ini
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Entertainment
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Paint.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Remote Desktop Connection.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\WordPad.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Activate Windows.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Backup.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Character Map.lnk
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Tour Windows XP.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\desktop.ini
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Disk Cleanup.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Disk Defragmenter.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Files and Settings Transfer Wizard.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Scheduled Tasks.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Security Center.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\System Information.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\System Restore.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Entertainment\desktop.ini
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Entertainment\Sound Recorder.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Entertainment\Volume Control.lnk

Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Windows Explorer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications\desktop.ini
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications\HyperTerminal.lnk
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Entertainment\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\Magnifier.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\Utility Manager.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\SendTo\Compressed (zipped) Folder.ZFSendToTarget: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Set Program Access and Defaults.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Windows Catalog.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Windows Update.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\start menu\programs\accessories
Opens: C:\documents and settings\all users\start menu\programs\administrative tools
Opens: C:\WINDOWS\Installer
Opens: C:\WINDOWS\Installer\{AC76BA86-7AD7-1033-7B44-A93000000001}
Opens: C:\Documents and Settings\All Users\Documents\desktop.ini
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Adobe Reader 9.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\start menu\programs\games
Opens: C:\WINDOWS\Installer\{95120000-003F-0409-0000-0000000FF1CE}
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office Excel Viewer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\Installer\{90850409-6000-11D3-8CFE-0150048383C9}
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office Word Viewer 2003.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\Installer\{95140000-00AF-0409-0000-0000000FF1CE}
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft PowerPoint Viewer .lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\MSN.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\start menu\programs\python 2.7
Opens: C:\documents and settings\all users\start menu\programs\startup
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Windows Messenger.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Windows Movie Maker.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Startup\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\Installer\{C3CC4DF5-39A5-4027-B136-2B3E1F5AB6E2}
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\IDLE (Python GUI).lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Module Docs.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Python (command line).lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics
Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics\Dictionaries
Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary
Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\all
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications\Network Connections.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications\Network Setup Wizard.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications\New Connection Wizard.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications\Wireless Network Setup Wizard.lnk
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Accessibility\Accessibility Wizard.lnk

Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Accessibility\desktop.ini
Opens: C:\Documents and Settings\All Users\DRM\drmv2.lic
Opens: C:\Documents and Settings\All Users\DRM\drmv2.sst
Opens: C:\Documents and Settings\All Users\Documents\My Music
Opens: C:\Documents and Settings\All Users\Documents\My Pictures
Opens: C:\Documents and Settings\All Users\Documents\My Videos
Opens: C:\Documents and Settings\All Users\Documents\My Videos\Desktop.ini
Opens: C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
Opens: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Python for Windows Documentation.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Python Manuals.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Blue hills.jpg
Opens: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\desktop.ini
Opens: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Sunset.jpg
Opens: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Water lilies.jpg
Opens: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Winter.jpg
Opens: C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
Opens: C:\Documents and Settings\All Users\Documents\My Music\My Playlists
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Music
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst1.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst10.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst11.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst12.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst13.wpl
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\PythonWin.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Uninstall Python.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Freecell.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Hearts.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Backgammon.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Checkers.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Hearts.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Reversi.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Spades.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Minesweeper.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Pinball.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\brt
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Solitaire.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Spider Solitaire.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Component Services.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Computer Management.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Data Sources (ODBC).lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Event Viewer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Local Security Policy.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA

Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Performance.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Services.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\start menu\programs\accessories\accessibility
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Calculator.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\start menu\programs\accessories\communications
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\start menu\programs\accessories\entertainment
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Paint.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Remote Desktop Connection.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\start menu\programs\accessories\system tools
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\WordPad.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst14.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst15.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst2.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst3.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst4.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst5.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst6.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst7.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst8.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst9.wpl
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\Beethoven's Symphony No. 9 (Scherzo).wma
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\desktop.ini
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\New Stories (Highway Blues).wma
Opens: C:\Documents and Settings\All Users\Desktop\Adobe Reader 9.lnk
Opens: C:\Documents and Settings\All Users\Application Data\Adobe
Opens: C:\Documents and Settings\All Users\Application Data\desktop.ini
Opens: C:\Documents and Settings\All Users\Application Data\Microsoft
Opens: C:\Documents and Settings\All Users\Application Data\Sun
Opens: C:\Documents and Settings\Administrator\Application Data
Opens: C:\Documents and Settings\Administrator\Cookies
Opens: C:\Documents and Settings\Administrator\Desktop
Opens: C:\Documents and Settings\Administrator\Favorites
Opens: C:\Documents and Settings\Administrator\Local Settings
Opens: C:\Documents and Settings\Administrator\My Documents
Opens: C:\Documents and Settings\Administrator\NetHood
Opens: C:\Documents and Settings\Administrator\NTUSER.DAT
Opens: C:\Documents and Settings\Administrator\NTUSER.DAT.LOG
Opens: C:\Documents and Settings\Administrator\ntuser.ini
Opens: C:\Documents and Settings\Administrator\PrintHood
Opens: C:\Documents and Settings\Administrator\Recent
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Activate Windows.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Administrator\SendTo
Opens: C:\Documents and Settings\Administrator\Start Menu
Opens: C:\Documents and Settings\Administrator\Templates
Opens: C:\Documents and Settings\Admin\Application Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\can
Opens: C:\Documents and Settings\Administrator\Templates\amipro.sam
Opens: C:\Documents and Settings\Administrator\Templates\excel.xls
Opens: C:\Documents and Settings\Administrator\Templates\excel4.xls
Opens: C:\Documents and Settings\Administrator\Templates\lotus.wk4
Opens: C:\Documents and Settings\Administrator\Templates\powerpnt.ppt
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Backup.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Character Map.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA

Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Disk Cleanup.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Disk Defragmenter.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Files and Settings Transfer
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Scheduled Tasks.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Security Center.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\System Information.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\System Restore.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\SendTo\Desktop (create
shortcut).DeskLink: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default
User\SendTo\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default User\SendTo\Mail
Recipient.MAPIMail: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Default
User\Cookies\index.dat: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\application data
Opens: C:\documents and settings\all users\desktop
Opens: C:\documents and settings\all users\documents
Opens: C:\documents and settings\all users\drm
Opens: C:\documents and settings\all users\favorites
Opens: C:\Documents and Settings\All
Users\ntuser.pol: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\start menu
Opens: C:\documents and settings\all users\templates
Opens: C:\Documents and Settings\All Users\Start
Menu\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application
Data\Adobe\Linguistics\Dictionaries\Adobe Custom Dictionary\eng
Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\Sound Recorder.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\all users\documents\my videos
Opens: C:\Documents and Settings\Administrator\Templates\presenta.shw
Opens: C:\Documents and Settings\Administrator\Templates\quattro.wb2
Opens: C:\Documents and Settings\Administrator\Templates\sndrec.wav
Opens: C:\Documents and Settings\Administrator\Templates\winword.doc
Opens: C:\Documents and Settings\Administrator\Templates\winword2.doc
Opens: C:\Documents and Settings\Administrator\Templates\wordpfct.wpd
Opens: C:\Documents and Settings\Administrator\Templates\wordpfct.wpg
Opens: C:\Documents and Settings\Administrator\Start Menu\desktop.ini
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Remote
Assistance.lnk
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Startup
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
Media Player.lnk
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Startup\desktop.ini
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Command Prompt.lnk
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\desktop.ini
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Entertainment
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Notepad.lnk
Opens: C:\Documents and Settings\All Users\Documents\My
Videos\Desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Synchronize.lnk
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Tour Windows XP.lnk
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Windows Explorer.lnk
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
Opens: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk

```
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
  Opens:                  C:\Documents and Settings\Administrator\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
  Opens:                  C:\Documents and Settings\Administrator\SendTo\Desktop (create
shortcut).DeskLink
  Opens:                  C:\Documents and Settings\Administrator\SendTo\desktop.ini
  Opens:                  C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail
  Opens:                  C:\Documents and Settings\All Users\Documents\My
Pictures\Desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\all users\documents\my pictures\sample
pictures
  Opens:                  C:\WINDOWS\system32\shimgvw.dll
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-
ww_dfb54e0c\GdiPlus.dll
  Opens:                  C:\Documents and Settings\Administrator\Local Settings\Application Data
  Opens:                  C:\Documents and Settings\Administrator\Local Settings\desktop.ini
  Opens:                  C:\Documents and Settings\Administrator\Local Settings\History
  Opens:                  C:\Documents and Settings\Administrator\Local Settings\Temp
  Opens:                  C:\Documents and Settings\Administrator\Local Settings\Temporary
Internet Files
  Opens:                  C:\Documents and Settings\Administrator\Cookies\index.dat
  Opens:                  C:\Documents and Settings\Administrator\Application Data\desktop.ini
  Opens:                  C:\Documents and Settings\Administrator\Application Data\Microsoft
  Opens:                  C:\Documents and Settings\Admin\Cookies
  Opens:                  C:\Documents and Settings\Admin\Desktop
  Opens:                  C:\Documents and Settings\Admin\Favorites
  Opens:                  C:\Documents and Settings\Admin\IECompatCache
  Opens:                  C:\Documents and Settings\Admin\IETldCache
  Opens:                  C:\Documents and Settings\Admin\Local Settings
  Opens:                  C:\Documents and Settings\Admin\My Documents
  Opens:                  C:\Documents and Settings\Admin\NetHood
  Opens:                  C:\Documents and Settings\Admin\NTUSER.DAT
  Opens:                  C:\Documents and Settings\Admin\NTUSER.DAT.LOG
  Opens:                  C:\Documents and Settings\Admin\ntuser.ini
  Opens:                  C:\Documents and Settings\Admin\PrintHood
  Opens:                  C:\Documents and Settings\Admin\PrivacIE
  Opens:                  C:\Documents and Settings\Admin\Recent
  Opens:                  C:\Documents and Settings\Admin\SendTo
  Opens:                  C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Blue hills.jpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Start Menu
  Opens:                  C:\Documents and Settings\Admin\Templates
  Opens:                  C:\Documents and Settings\Admin\Templates\amipro.sam
  Opens:                  C:\Documents and Settings\Admin\Templates\excel.xls
  Opens:                  C:\Documents and Settings\Admin\Templates\excel4.xls
  Opens:                  C:\Documents and Settings\Admin\Application Data\Adobe\LogTransport2
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Adobe\LogTransport2\Logs
  Opens:                  C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Sunset.jpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Water lilies.jpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Winter.jpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My
Music\Desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\all users\documents\my music\my playlists
  Opens:                  C:\documents and settings\all users\documents\my music\sample music
  Opens:                  C:\documents and settings\all users\documents\my music\sample playlists
  Opens:                  C:\documents and settings\all users\documents\my music\sample
playlists\000c5a7a
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst1.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst10.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst11.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst12.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
```

Opens: C:\Documents and Settings\Admin\Templates\lotus.wk4
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst13.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Templates\powerpnt.ppt
Opens: C:\Documents and Settings\Admin\Templates\presenta.shw
Opens: C:\Documents and Settings\Admin\Templates\quattro.wb2
Opens: C:\Documents and Settings\Admin\Templates\sndrec.wav
Opens: C:\Documents and Settings\Admin\Templates\winword.doc
Opens: C:\Documents and Settings\Admin\Templates\winword2.doc
Opens: C:\Documents and Settings\Admin\Templates\wordpfct.wpd
Opens: C:\Documents and Settings\Admin\Templates\wordpfct.wpg
Opens: C:\Documents and Settings\Admin\Start Menu\desktop.ini
Opens: C:\Documents and Settings\Admin\Start Menu\Programs
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Internet Explorer.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Outlook Express.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Remote Assistance.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Startup
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media Player.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Accessibility
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Address Book.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Command Prompt.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\desktop.ini
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Entertainment
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Notepad.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Program Compatibility Wizard.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Synchronize.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System Tools
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst14.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\desktop.ini\
Opens: C:\Documents and Settings\Admin\Application Data\Identities
Opens: C:\Documents and Settings\Admin\Application Data\Identities\{5792731B-1E8B-4ECF-8560-0E560368800D}
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst15.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\#SharedObjects
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\#SharedObjects\45PY3TTW
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst2.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\macromedia.com
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\macromedia.com\support
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\macromedia.com\support\flashplayer
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys
Opens: C:\Documents and Settings\Admin\Application Data\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol\
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Tour Windows XP.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Windows Explorer.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System Tools\Internet Explorer (No Add-ons).lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Entertainment\desktop.ini
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Accessibility\desktop.ini
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Accessibility\Magnifier.lnk
Opens: C:\Documents and Settings\Admin\Start

```
Menu\Programs\Accessories\Accessibility\Narrator.lnk
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst3.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\AddIns
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst4.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Credentials
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst5.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst6.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\0797C381B2F87EB5A1D5573BD15BA4F4\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\135BD6A358680A7BF1CCEC7C0172393D\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\2BF68F4714092295550497DD56F57004\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\3130B1871A126520A8C47861EFE3ED4D\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\60E31627FDA0A46932B0E5948949F2A5\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\62B5AF9BE9ADC1085C3C56EC07A82BF6\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\7B2238AACCEDC3F1FFE8E7EB5F575EC9\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\8DFDF057024880D7A081AFBF6D26B92F\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\A44F4E7CB3133FF765C39A53AD8FCFDD\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\Content\F482C95F83F1B59228F1B1E720F2EDF1\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\0797C381B2F87EB5A1D5573BD15BA4F4\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\135BD6A358680A7BF1CCEC7C0172393D\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\2BF68F4714092295550497DD56F57004\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\3130B1871A126520A8C47861EFE3ED4D\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\60E31627FDA0A46932B0E5948949F2A5\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\62B5AF9BE9ADC1085C3C56EC07A82BF6\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\7B2238AACCEDC3F1FFE8E7EB5F575EC9\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB92015\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\A44F4E7CB3133FF765C39A53AD8FCFDD\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\CryptnetUrlCache\MetaData\F482C95F83F1B59228F1B1E720F2EDF1\
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst7.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst8.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-
1-5-21-1757981266-507921405-1957994488-1003\6b29ae44e85efac3c72ff4d1865d73f1_fa860dc5-a965-4200-
a9d4-fb930ff1911b\
```

Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Crypto\RSA\S-1-5-21-1757981266-507921405-1957994488-1003\83aa4cc77f591dfc2374580bbd95f6ba_fa860dc5-a965-4200-a9d4-fb930ff1911b\
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\000C5A7A\Plylst9.wpl: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\brndlog.bak\
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\brndlog.txt\
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\Desktop.htt\
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\Quick Launch
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\Quick Launch\desktop.ini\
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\Beethoven's Symphony No. 9 (Scherzo).wma: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Program Files\Internet Explorer
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\New Stories (Highway Blues).wma: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Program Files\Internet Explorer\iexplore.vir
Opens: C:\Documents and Settings\All Users\Desktop\Adobe Reader 9.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\administrator\application data
Opens: C:\documents and settings\administrator\cookies
Opens: C:\documents and settings\administrator\desktop
Opens: C:\documents and settings\administrator\favorites
Opens: C:\documents and settings\administrator\local settings
Opens: C:\documents and settings\administrator\my documents
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk\
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet Explorer\Quick Launch\Show Desktop.scf\
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
Opens: C:\Documents and Settings\Admin\SendTo\Compressed (zipped) Folder.ZFSendToTarget
Opens: C:\Documents and Settings\Admin\SendTo\Desktop (create shortcut).DeskLink
Opens: C:\Documents and Settings\Admin\SendTo\desktop.ini
Opens: C:\Documents and Settings\Admin\SendTo\Mail Recipient.MAPIMail
Opens: C:\Documents and Settings\Admin\SendTo\My Documents.mydocs
Opens: C:\Documents and Settings\Admin\Recent\Desktop.ini
Opens: C:\Documents and Settings\Admin\Recent\fp_11.0.1.152_archive.lnk
Opens: C:\Documents and Settings\Admin\PrivacIE\index.dat
Opens: C:\Documents and Settings\Admin\My Documents\desktop.ini
Opens: C:\Documents and Settings\Admin\My Documents\My Music
Opens: C:\Documents and Settings\Admin\My Documents\My Pictures
Opens: C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
Opens: C:\Documents and Settings\Admin\My Documents\My Pictures\Sample Pictures.lnk
Opens: C:\Documents and Settings\Admin\My Documents\My Music\Desktop.ini
Opens: C:\Documents and Settings\Admin\My Documents\My Music\Sample Music.lnk
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data
Opens: C:\Documents and Settings\Admin\Local Settings\desktop.ini
Opens: C:\Documents and Settings\Admin\Local Settings\History
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
Opens: C:\Documents and Settings\Admin\IETldCache\index.dat
Opens: C:\Documents and Settings\Admin\IECompatCache\index.dat
Opens: C:\Documents and Settings\Admin\Favorites\Desktop.ini
Opens: C:\Documents and Settings\Admin\Favorites\Links
Opens: C:\documents and settings\administrator\nethood
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Media Player
Opens: C:\Documents and Settings\Administrator\ntuser.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\MMC
Opens: C:\documents and settings\administrator\printhood
Opens: C:\documents and settings\administrator\recent
Opens: C:\documents and settings\administrator\sendto
Opens: C:\documents and settings\administrator\start menu
Opens: C:\documents and settings\administrator\templates
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Office
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\Office\Excel12.pip\

```
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Office\Recent
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Office\Recent\Desktop.ini\
  Opens:                  C:\Documents and
Settings\Administrator\Templates\amipro.sam: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Protect\CREDHIST\
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3\
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1\
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\fe1a937a-0ac9-4cf1-978d-5d0742ed2858\
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\Preferred\
  Opens:                  C:\documents and settings\administrator\start menu\programs\startup
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Speech
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Speech\Files
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat\
  Opens:                  C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
Media Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Startup\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\administrator\start
menu\programs\accessories\accessibility
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\Certificates
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Command Prompt.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CRLs
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\administrator\start
menu\programs\accessories\entertainment
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CTLs
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Notepad.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Templates
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Windows
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Windows\Themes\Custom.theme\
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Synchronize.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Tour Windows XP.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Application Data\Oracle
  Opens:                  C:\Documents and Settings\Admin\Application Data\Oracle\Java
  Opens:                  C:\Documents and Settings\Admin\Application Data\Oracle\Java\Uninstall
  Opens:                  C:\Documents and Settings\Admin\Application Data\Sun
  Opens:                  C:\Documents and Settings\Admin\Application Data\Sun\Java
  Opens:                  C:\Documents and Settings\Admin\Application Data\Sun\Java\AU
  Opens:                  C:\Documents and Settings\Admin\Application Data\Sun\Java\AU\au.cab\
  Opens:                  C:\Documents and Settings\Admin\Application Data\Sun\Java\AU\au.msi\
  Opens:                  C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
  Opens:                  C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Windows Explorer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Favorites\Microsoft Websites
  Opens:                  C:\Documents and Settings\Admin\Favorites\MSN.com.url
  Opens:                  C:\Documents and Settings\Admin\Favorites\Radio Station Guide.url
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\cache\6.0\0
  Opens:                  C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
site.url
```

Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on Microsoft.com.url
Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft At Home.url
Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft At Work.url
Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft Store.url
Opens: C:\Documents and Settings\Admin\Favorites\Links\desktop.ini
Opens: C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\1
Opens: C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url
Opens: C:\Documents and Settings\Admin\Favorites\Links\Web Slice Gallery.url
Opens: C:\Documents and Settings\Admin\Cookies\admin@c1.microsoft[2].txt
Opens: C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
Opens: C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[1].txt
Opens: C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt
Opens: C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
Opens: C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[3].txt
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Entertainment\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\10
Opens: C:\Documents and Settings\Admin\Cookies\index.dat
Opens: C:\Documents and Settings\Admin\Application Data\desktop.ini
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\11
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\12
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\12\eef218c-550e9171.idx\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\13
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\14
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\15
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\16
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\17
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\17\49a00451-1036314c.idx\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\17\49a00451-6.0.lap\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\18
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\19
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-42ff70b1.idx\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\19\3602b4d3-6.0.lap\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\2
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\20
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\21
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\22
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\23
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\24
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\25
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Magnifier.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\26

Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\27
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\28
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\29
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\3
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\30
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\31
Opens: C:\Documents and Settings\Administrator\Start Menu\Programs\Accessories\Accessibility\Utility Manager.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\32
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\33
Opens: C:\Documents and Settings\Administrator\SendTo\Compressed (zipped) Folder.ZFSendToTarget: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\34
Opens: C:\Documents and Settings\Administrator\SendTo\Desktop (create shortcut).DeskLink: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\35
Opens: C:\Documents and Settings\Administrator\SendTo\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\36
Opens: C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\37
Opens: C:\Documents and Settings\Administrator\Cookies\index.dat: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\admin\application data
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\38
Opens: C:\documents and settings\admin\desktop
Opens: C:\documents and settings\admin\favorites
Opens: C:\documents and settings\admin\local settings
Opens: C:\documents and settings\admin\my documents
Opens: C:\documents and settings\admin\nethood
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\39
Opens: C:\Documents and Settings\Admin\ntuser.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\4
Opens: C:\documents and settings\admin\printhood
Opens: C:\documents and settings\admin\recent
Opens: C:\documents and settings\admin\sendto
Opens: C:\documents and settings\admin\start menu
Opens: C:\documents and settings\admin\templates
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\40
Opens: C:\Documents and Settings\Admin\Templates\amipro.sam: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\41
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\42
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\43
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\43\1ca2666b-2c59609d.idx\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\44
Opens: C:\Documents and Settings\Admin\Templates\excel4.xls: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\45
Opens: C:\Documents and Settings\Admin\Templates\lotus.wk4: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\46

Opens: C:\AUTOEXEC.BAT
Opens: C:\boot.ini
Opens: C:\CONFIG.SYS
Opens: C:\dump.pcap
Opens: C:\exception.log
Opens: C:\IO.SYS
Opens: C:\MSDOS.SYS
Opens: C:\NTDETECT.COM
Opens: C:\ntldr
Opens: C:\pagefile.sys
Opens: C:\Program Files
Opens: C:\static_events.gpb
Opens: C:\System Volume Information
Opens: C:\WINDOWS\0.log
Opens: C:\WINDOWS\addins
Opens: C:\WINDOWS\AppPatch
Opens: C:\WINDOWS\assembly
Opens: C:\WINDOWS\Blue Lace 16.bmp
Opens: C:\WINDOWS\bootstat.dat
Opens: C:\WINDOWS\clock.avi
Opens: C:\WINDOWS\cmsetacl.log
Opens: C:\WINDOWS\Coffee Bean.bmp
Opens: C:\WINDOWS\comsetup.log
Opens: C:\WINDOWS\Config
Opens: C:\WINDOWS\Connection Wizard
Opens: C:\WINDOWS\control.ini
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\47
Opens: C:\WINDOWS\CSC
Opens: C:\WINDOWS\Cursors
Opens: C:\WINDOWS\Debug
Opens: C:\WINDOWS\desktop.ini
Opens: C:\WINDOWS\Downloaded Program Files
Opens: C:\WINDOWS\Driver Cache
Opens: C:\WINDOWS\DtcInstall.log
Opens: C:\WINDOWS\ehome
Opens: C:\WINDOWS\explorer.exe
Opens: C:\WINDOWS\explorer.scf
Opens: C:\WINDOWS\FaxSetup.log
Opens: C:\WINDOWS\FeatherTexture.bmp
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\48
Opens: C:\WINDOWS\Fonts
Opens: C:\WINDOWS\Gone Fishing.bmp
Opens: C:\WINDOWS\Greenstone.bmp
Opens: C:\WINDOWS\Help
Opens: C:\WINDOWS\hh.exe
Opens: C:\WINDOWS\ie8
Opens: C:\WINDOWS\ie8.log
Opens: C:\Documents and Settings\Admin\Templates\presenta.shw: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\49
Opens: C:\Documents and Settings\Admin\Templates\quattro.wb2: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\5
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\50
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\51
Opens: C:\Documents and Settings\Admin\Templates\winword2.doc: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Templates\wordpfct.wpd: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\52
Opens: C:\Documents and Settings\Admin\Templates\wordpfct.wpg: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\53
Opens: C:\Documents and Settings\Admin\Start Menu\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\admin\start menu\programs
Opens: C:\documents and settings\admin\start menu\programs\accessories
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\54
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\55
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\56

Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Internet Explorer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\57
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Outlook Express.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\58
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\59
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Remote Assistance.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\admin\start menu\programs\startup
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\6
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\60
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\61
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\62
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\documents and settings\admin\start menu\programs\accessories\accessibility
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\63
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\7
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Address Book.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\8
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\9
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Command Prompt.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\host
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\lastAccessed\
Opens: C:\documents and settings\admin\start menu\programs\accessories\entertainment
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\muffin
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\cache\6.0\tmp
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Notepad.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Program Compatibility Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\deployment.properties\
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\ext
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\log
Opens: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Synchronize.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\security
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\security\trusted.certs\
Opens: C:\documents and settings\admin\start menu\programs\accessories\system tools
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\tmp
Opens: C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment\tmp\si
Opens: C:\WINDOWS\ie8_main.log
Opens: C:\WINDOWS\iis6.log
Opens: C:\WINDOWS\ime
Opens: C:\WINDOWS\imsins.BAK
Opens: C:\WINDOWS\imsins.log
Opens: C:\WINDOWS\inf
Opens: C:\WINDOWS\java
Opens: C:\WINDOWS\L2Schemas
Opens: C:\WINDOWS\MedCtrOC.log
Opens: C:\WINDOWS\Media
Opens: C:\WINDOWS\Microsoft.NET
Opens: C:\WINDOWS\msagent
Opens: C:\WINDOWS\msapps

```
  Opens:                  C:\WINDOWS\msdfmap.ini
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Tour
Windows XP.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\WINDOWS\msgsocm.log
  Opens:                  C:\WINDOWS\msmqinst.log
  Opens:                  C:\WINDOWS\mui
  Opens:                  C:\WINDOWS\netfxocm.log
  Opens:                  C:\WINDOWS\Network Diagnostic
  Opens:                  C:\WINDOWS\NOTEPAD.EXE
  Opens:                  C:\WINDOWS\ntbtlog.txt
  Opens:                  C:\WINDOWS\ntdtcsetup.log
  Opens:                  C:\WINDOWS\ocgen.log
  Opens:                  C:\WINDOWS\ocmsn.log
  Opens:                  C:\WINDOWS\ODBCINST.INI
  Opens:                  C:\WINDOWS\OEWABLog.txt
  Opens:                  C:\WINDOWS\Offline Web Pages
  Opens:                  C:\WINDOWS\pchealth
  Opens:                  C:\WINDOWS\PeerNet
  Opens:                  C:\WINDOWS\Prairie Wind.bmp
  Opens:                  C:\WINDOWS\Prefetch
  Opens:                  C:\WINDOWS\Provisioning
  Opens:                  C:\WINDOWS\regedit.exe
  Opens:                  C:\WINDOWS\REGLOCS.OLD
  Opens:                  C:\WINDOWS\regopt.log
  Opens:                  C:\WINDOWS\repair
  Opens:                  C:\WINDOWS\Resources
  Opens:                  C:\WINDOWS\Rhododendron.bmp
  Opens:                  C:\WINDOWS\River Sumida.bmp
  Opens:                  C:\WINDOWS\Santa Fe Stucco.bmp
  Opens:                  C:\WINDOWS\SchedLgU.Txt
  Opens:                  C:\WINDOWS\security
  Opens:                  C:\WINDOWS\sessmgr.setup.log
  Opens:                  C:\WINDOWS\SET3.tmp
  Opens:                  C:\WINDOWS\SET4.tmp
  Opens:                  C:\WINDOWS\SET8.tmp
  Opens:                  C:\WINDOWS\setupact.log
  Opens:                  C:\WINDOWS\setupapi.log
  Opens:                  C:\Documents and Settings\Admin\Application Data\Sun\Java\jre1.7.0_02
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Sun\Java\jre1.7.0_02\Data1.cab\
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Sun\Java\jre1.7.0_02\jre1.7.0_02.msi\
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Windows
Explorer.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System
Tools\Internet Explorer (No Add-ons).lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Cookies\admin@c1.microsoft[2].txt\
  Opens:                  C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt\
  Opens:                  C:\Documents and Settings\Admin\Cookies\admin@rto.microsoft[1].txt\
  Opens:                  C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt\
  Opens:                  C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt\
  Opens:                  C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[3].txt\
  Opens:                  C:\Documents and Settings\Admin\Cookies\index.dat\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Desktop.ini\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Links\desktop.ini\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Links\Web Slice Gallery.url\
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
site.url\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
Microsoft.com.url\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Home.url\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Work.url\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
Store.url\
  Opens:                  C:\Documents and Settings\Admin\Favorites\MSN.com.url\
  Opens:                  C:\Documents and Settings\Admin\Favorites\Radio Station Guide.url\
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\Windows Media
Player.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\IECompatCache\index.dat\
  Opens:                  C:\Documents and Settings\Admin\IETldCache\index.dat\
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
```

```
Data\Adobe\Acrobat\9.0
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\AcroFnt09.lst\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Cache\Search
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Updater
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Acrobat\9.0\Updater\updater.log\
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Color
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Color\ACECache10.lst\
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\aum.log\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\aumLib.log\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\Updater6\Install
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\SendTo\Compressed (zipped)
Folder.ZFSendToTarget: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\GDIPFONTCACHEV1.DAT\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\IconCache.db\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\CD Burning
  Opens:                  C:\Documents and Settings\Admin\SendTo\Desktop (create
shortcut).DeskLink: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Credentials\S-1-5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\Documents and
Settings\Admin\SendTo\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\documents and settings\all users\start menu\programs
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\FeedsStore.feedsdb-ms\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Home~.feed-ms\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\Microsoft Feeds~\Microsoft at Work~.feed-ms\
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\Volume Control.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Suggested Sites~.feed-ms\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\Web Slice Gallery~.feed-
ms\
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\desktop.ini\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW\desktop.ini\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\FBANKAIW\fwlink[1]\
```

Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications\HyperTerminal.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\G4DZ1I7H
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\G4DZ1I7H\desktop.ini\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\G4DZ1I7H\fwlink[1]\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\index.dat\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\J3XY1QNV
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\J3XY1QNV\desktop.ini\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\J3XY1QNV\fwlink[1]\
Opens: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Communications\Network Connections.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\TLMHA51J
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\TLMHA51J\desktop.ini\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Feeds Cache\TLMHA51J\ieonline.microsoft[1]\
Opens: C:\WINDOWS\setuperr.log
Opens: C:\WINDOWS\setuplog.txt
Opens: C:\WINDOWS\Soap Bubbles.bmp
Opens: C:\WINDOWS\SoftwareDistribution
Opens: C:\WINDOWS\spupdsvc.log
Opens: C:\WINDOWS\srchasst
Opens: C:\WINDOWS\Sti_Trace.log
Opens: C:\WINDOWS\Sun
Opens: C:\WINDOWS\SxsCaPendDel
Opens: C:\WINDOWS\system
Opens: C:\WINDOWS\system.ini
Opens: C:\WINDOWS\tabletoc.log
Opens: C:\WINDOWS\TASKMAN.EXE
Opens: C:\WINDOWS\Tasks
Opens: C:\WINDOWS\Temp
Opens: C:\WINDOWS\tsoc.log
Opens: C:\WINDOWS\twain.dll
Opens: C:\WINDOWS\twain_32
Opens: C:\WINDOWS\twain_32.dll
Opens: C:\WINDOWS\twunk_16.exe
Opens: C:\WINDOWS\twunk_32.exe
Opens: C:\WINDOWS\unins000.dat
Opens: C:\WINDOWS\unins000.exe
Opens: C:\WINDOWS\unins001.dat
Opens: C:\WINDOWS\unins001.exe
Opens: C:\WINDOWS\updspapi.log
Opens: C:\WINDOWS\vb.ini
Opens: C:\WINDOWS\vbaddin.ini
Opens: C:\WINDOWS\vmmreg32.dll
Opens: C:\WINDOWS\WBEM
Opens: C:\WINDOWS\Web
Opens: C:\WINDOWS\wiadebug.log
Opens: C:\WINDOWS\wiaservc.log
Opens: C:\WINDOWS\win.ini
Opens: C:\WINDOWS\WindowsUpdate.log
Opens: C:\WINDOWS\winhelp.exe
Opens: C:\WINDOWS\winhlp32.exe
Opens: C:\WINDOWS\winnt.bmp
Opens: C:\WINDOWS\winnt256.bmp
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\brndlog.bak\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\brndlog.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Custom Settings
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Custom Settings\Custom0
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Custom Settings\Custom0\install.ins\
Opens: C:\WINDOWS\wmsetup.log
Opens: C:\WINDOWS\WMSysPr9.prx
Opens: C:\WINDOWS\Zapotec.bmp
Opens: C:\WINDOWS_default.pif
Opens: C:\WINDOWS\WinSxS\InstallTemp
Opens: C:\WINDOWS\WinSxS\Manifests
Opens: C:\Documents and Settings\All Users\Start

```
Menu\Programs\Accessories\Communications\Network Setup
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\0WORJP5C
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\31VE7QYK\www.microsoft[1].xml\
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\New Connection
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\3FDD734T
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Wireless Network Setup
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\index.dat\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\DOMStore\LQLIM8KB
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Accessibility\Accessibility
Wizard.lnk: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\frameiconcache.dat\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active\{49831954-C276-11E3-AE24-08002733366F}.dat\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{80236AC0-AAD6-11E3-AE20-
08002733366F}.dat\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Last Active\{69EE14A0-C276-11E3-AE24-08002733366F}.dat\
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Accessibility\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\rsoplog.bak\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\rsoplog.txt\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Services
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Media Player
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Media Player\CurrentDatabase_59R.wmdb\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office\12.0
  Opens:                  C:\Documents and Settings\All
Users\Documents\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Office\14.0
  Opens:                  C:\Documents and Settings\Admin\SendTo\Mail
Recipient.MAPIMail: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Silverlight
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Silverlight\mssl.lck\
  Opens:                  C:\Documents and Settings\Admin\SendTo\My
Documents.mydocs: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat.LOG\
  Opens:                  C:\Documents and
Settings\Admin\Recent\Desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
```

Data\Microsoft\Windows Media\9.0
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.DTD\
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows Media\9.0\WMSDKNS.XML\
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\0
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\1
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\10
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\11
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\12
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\13
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\14
Opens: C:\WINDOWS\WinSxS\MSIL_IEExecRemote_b03f5f7f11d50a3a_2.0.0.0_x-
ww_6e57c34e
Opens: C:\WINDOWS\WinSxS\Policies
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualCPlusPlus.Runtime-
Libraries_6595b64144ccf1df_6.0.0.0_x-ww_ff9986d7
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_353599c2
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.21022.8_x-
ww_d08d0375
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_15fc9313
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.0.0_x-ww_2726e76a
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.2600.5512_x-
ww_3fd60d63
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.0.0_x-ww_8d353f13
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_5.2.2.3_x-ww_468466a7
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcDll_6595b64144ccf1df_5.2.2.3_x-ww_d6bd8b95
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcRes_6595b64144ccf1df_5.2.2.3_en_16a24bc0
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\15
Opens:
C:\WINDOWS\WinSxS\x86_System.EnterpriseServices_b03f5f7f11d50a3a_2.0.0.0_x-ww_7d5f3790
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\16
Opens:
C:\WINDOWS\WinSxS\x86_System.EnterpriseServices_b03f5f7f11d50a3a_2.0.0.0_x-
ww_7d5f3790\System.EnterpriseServices.dll
Opens:
C:\WINDOWS\WinSxS\x86_System.EnterpriseServices_b03f5f7f11d50a3a_2.0.0.0_x-
ww_7d5f3790\System.EnterpriseServices.Wrapper.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcRes_6595b64144ccf1df_5.2.2.3_en_16a24bc0\rtcres.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcDll_6595b64144ccf1df_5.2.2.3_x-
ww_d6bd8b95\rtcdll.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_5.2.2.3_x-
ww_468466a7\dxmrtp.dll

Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.0.0_x-
ww_8d353f13\GdiPlus.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.2600.5512_x-
ww_3fd60d63\msvcirt.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.2600.5512_x-
ww_3fd60d63\msvcrt.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.0.0_x-
ww_2726e76a\msvcirt.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.0.0_x-
ww_2726e76a\msvcrt.dll
Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
site.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\17
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\18
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\19
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\2
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\20
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\21
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\22
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\23
Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
Microsoft.com.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\24
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\25
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\26
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\27
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\28
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\29
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\3
Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Home.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\30
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\31
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\32
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\33
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\34
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\35
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\36
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\37
Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Work.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\38
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\39
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\4
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\40
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\41
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\42
Opens: C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment\cache\6.0\43

Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\44
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\45
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\45\7e60542d-6963afcc.idx\
Opens: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft Store.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\46
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\47
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\47\15572e2f-21932044.idx\
Opens: C:\Documents and Settings\Admin\Favorites\Links\desktop.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\48
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\49
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\5
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\50
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\51
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\52
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\53
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\54
Opens: C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\55
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\56
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\57
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\58
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\59
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\6
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\60
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\61
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\62
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\63
Opens: C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\7
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\7\2bbaaf87-5ca9d237.idx\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\8
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\9
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\host
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\lastAccessed\
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\muffin
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\tmp
Opens: C:\Documents and Settings\Admin\Local Settings\desktop.ini\
Opens: C:\Documents and Settings\Admin\Local Settings\History\desktop.ini\
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\desktop.ini\

Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\index.dat\
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014031220140313
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014031220140313\index.dat\
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014033120140407
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014033120140407\index.dat\
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014041220140413
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014041220140413\index.dat\
Opens: C:\Documents and Settings\Admin\Favorites\Links\Web Slice Gallery.url: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\296c0.msp\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM_NotLocked.log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ASPNETSetup_00000.log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ASPNETSetup_00001.log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\AUCHECK_PARSER.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Compatibility Pack for the 2007 Office system (0).log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_clwireg.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_depcheck_NETFX_EXP_35.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_dotnetfx35error.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_dotnetfx35install.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_NET_Framework20_Setup164F.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_NET_Framework30_Setup16AE.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_NET_Framework35_MSI16E2.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_NET_Framework35_MSI63E0.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_RGB9RAST_x86.msi601E.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA2A49.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA3565.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_wcf_retCA35A0.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\dd_XPS.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\gen_py
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7\dicts.dat\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\gen_py\2.7__init__.py\
Opens: C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Cookies\index.dat: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\JAUReg.log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\java_install.log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\java_install_reg.log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\jusched.log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft PowerPoint Viewer (0).log\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_10.0.30319
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20131223_035827352-MSI_vc_red.msi.txt\
Opens: C:\AUTOEXEC.BAT: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20131223_035827352.html\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20140312_152314679-MSI_vc_red.msi.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20140312_152314679.html\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++ 2010 x86 Redistributable Setup_20140312_152634747-MSI_vc_red.msi.txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++

```
2010 x86 Redistributable Setup_20140312_152634747.html\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_154212618-MSI_vc_red.msi.txt\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\Microsoft Visual C++
2010 x86 Redistributable Setup_20140312_154212618.html\
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\pywin32_postinstall.log\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\setup.log\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\Silverlight0.log\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\SilverlightMSI.log\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\uxeventlog.txt\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\AntiPhishing\2CEDBFBC-DBA8-43AA-B1FD-CC8E6316E3E2.dat\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\180x150_WP_NokiaReinvented_EN_US[1].gif\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[1].json\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\300lo[2].json\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\33975792-bade-4cf2-b676-3b0eee2cf2ed_16[1].jpg\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\3ef01e72-0832-46f0-a6e1-23f9d5a07d86_5[1].png\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\871d9c8a-b403-40aa-aeb8-9ecd40181833_15[1].jpg\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\88666cc6-d578-45c8-baf0-89d3837f41c3_89[1].css\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\93e33485-fea3-4687-a642-2c5dd233522f_12[1].eot\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\access-web-bg-grey[1].jpg\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\access_dev_center_new[1].jpg\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\accordion_icon_sprites[1].png\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[1].txt\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[2].txt\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[3].txt\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[4].txt\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\ADSAdClient31[5].txt\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\adServer[1].htm\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\auth016[1].js\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\bimapping[2].js\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\broker[1].js\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CA9ATUDW.css\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CAMLW29Z.jsx\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CATM568T.jsx\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\CAVLZJ9D.jsx\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\click-to-install-right[1].png\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\Closed_btn_21x21[1].png\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[1].js\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\core114[2].js\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[1].css\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[2].css\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\css[3].css\
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\daf22230-6bbc-4982-87b3-6da3f5e6e8b4_28[1].jpg\
```

Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\DataList[1].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\desktop.ini\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\dotnetfx35setup[1].exe
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\dotnetfx35setup[1].exe\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\e64030e7-ad8c-4be8-a45a-b69a2df3caef_13[1].eot\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\eb4f0171-7cb7-428a-afcc-d93a6b84525c_33[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\event[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\event[2].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\event[3].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\event[5].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\false[1].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\favicon[1].ico\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\General[1].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\General[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\georedirect[1].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\georedirect[2].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\georedirect[3].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\georedirect[4].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\gl_social[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\icon_plus_hover[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\icon_to_right_arrow[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\info_tip_16x16[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\install[1].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\js[2].ashx\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\LoginStatus[1].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\microsoft-accessibility_2[1].jpg\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\microsoft_symbol_clr_56x56[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\microsoft_update_icon[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ms-silverlight-logo-rev[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\Nebula[1].js\
Opens: C:\boot.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\omnibase[2].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\oneMscomBlade[2].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\onemscomfooter[2].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[2].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\oneMscomJsCssLoader[3].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\page_bg_mid[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\page_top[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\request[1].php\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ScriptResource[1].axd\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ScriptResource[2].axd\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ScriptResource[3].axd\

Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ScriptResource[4].axd\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\ScriptResource[5].axd\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\script[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\script[1].jsx\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\script[2].jsx\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\top-nav-right[1].jpg\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\top-nav-seperator[1].gif\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\true[1].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\true[2].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\views[1]\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\WebResource[1].axd\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\wtid[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\CXCXW1MR\wt_capi[2].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\desktop.ini\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\index.dat\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\35a5f647-c96d-4bbf-b9f4-ca71e16add70_28[1].jpg\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\5a7873a1-fd4e-4462-8ab2-32bd729117c6_7[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\736e3781-6a19-4119-b717-e61f0d8982c0_12[1].eot\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\accessibility_logo[1].jpg\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\ADSAdClient31[1].txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\ADSAdClient31[2].txt\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\auth016[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\auth016[2].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\bgLineTile[1].jpg\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\bing[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\bing_logo[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\blind-low-vision-thumb[1].jpg\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\broker-config_s1[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\broker-config_s1[2].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\broker-config_s1[3].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\CA39W67Q.jsx\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\CAANG12B.css\
Opens: C:\CONFIG.SYS: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\CAU35S9Y.jsx\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\cbc6f38d-b79c-4bff-8b67-b81eb9676ab3_5[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\ChangePassword[1].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\click-to-install-left[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\ClickToInstall[1].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\ClientBiSettings.Wol[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\confirmation[1].aspx\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\core114[1].js\

Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\counter017[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\counter017[2].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\css[1].ashx\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\css[1].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\css[2].css\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\desktop.ini\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\details[1].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\details[2].htm\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\e9979a8b-c439-452a-a09f-d3b32df0e5b1_13[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\email[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\en-us[1].gif\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\event[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\event[3].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\event[6].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\facebook[1].gif\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\favicon[1].ico\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\favicon[2].ico\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\favicon[4].ico\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\favicon[5].ico\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\General[1].js\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\gl_site[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\gl_social[1].svg\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\hero_bg_index[1].png\
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\icon_minus_hover[1].png\
Opens: C:\system volume information\catalog.wci\00010001.dir
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\ONWV4FIP\IE8-WindowsXP-x86-ENU[1].exe
Opens: C:\System Volume Information\catalog.wci\00010001.dir
Opens: C:\System Volume Information\catalog.wci\00010001.ci
Opens: C:\System Volume Information\catalog.wci\CiFLfffc.002
Opens: C:\System Volume Information\catalog.wci\CiFLfffc.001
Opens: C:\exception.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\IO.SYS: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\MSDOS.SYS: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\NTDETECT.COM: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\ntldr: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\program files
Opens: C:\system volume information
Opens: C:\windows
Opens: C:\WINDOWS\0.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\addins
Opens: C:\windows\apppatch
Opens: C:\windows\assembly
Opens: C:\WINDOWS\Blue Lace 16.bmp: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\bootstat.dat: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\system32\wsock32.dll
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\wbem\wbemprox.dll
Opens: C:\WINDOWS\system32\wbem\wbemcomn.dll
Opens: C:\WINDOWS\system32\wbem\wbemsvc.dll
Opens: C:\WINDOWS\explorer.exe: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\system32\wbem\fastprox.dll
Opens: C:\WINDOWS\system32\msvcp60.dll
Opens: C:\WINDOWS\system32\ntdsapi.dll
Opens: C:\WINDOWS\system32\dnsapi.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll
Opens: C:\WINDOWS\explorer.scf: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA

Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53\mfc90.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53\mfc90u.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53\mfcm90.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_a57c1f53\mfcm90u.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90chs.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90cht.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90deu.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90enu.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90esn.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90esp.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90fra.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90ita.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90jpn.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90kor.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_15fc9313\mfc90rus.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_d495ac4e\msvcm90.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_d495ac4e\msvcp90.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_d495ac4e\msvcr90.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.21022.8_x-
ww_d08d0375\msvcm90.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.21022.8_x-
ww_d08d0375\msvcp90.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.21022.8_x-
ww_d08d0375\msvcr90.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_353599c2\atl90.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700\msvcm80.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700\msvcp80.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700\msvcr80.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcm80.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcp80.dll
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcr80.dll
Opens: C:\WINDOWS\FaxSetup.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualCPlusPlus.Runtime-
Libraries_6595b64144ccf1df_6.0.0.0_x-ww_ff9986d7\atl.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualCPlusPlus.Runtime-
Libraries_6595b64144ccf1df_6.0.0.0_x-ww_ff9986d7\mfc42.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualCPlusPlus.Runtime-
Libraries_6595b64144ccf1df_6.0.0.0_x-ww_ff9986d7\mfc42u.dll
Opens: C:\WINDOWS\FeatherTexture.bmp: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\fonts

Opens: C:\WINDOWS\Gone Fishing.bmp: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\Greenstone.bmp: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\help
Opens: C:\WINDOWS\hh.exe: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\ie8
Opens: C:\WINDOWS\ie8.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\ie8_main.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\iis6.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\ime
Opens: C:\WINDOWS\imsins.BAK: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\imsins.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\inf
Opens: C:\windows\installer
Opens: C:\windows\java
Opens: C:\windows\l2schemas
Opens: C:\WINDOWS\MedCtrOC.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\media
Opens: C:\windows\microsoft.net
Opens: C:\windows\msagent
Opens: C:\windows\msapps
Opens: C:\WINDOWS\system32\mswsock.dll
Opens: C:\WINDOWS\system32\hnetcfg.dll
Opens: C:\WINDOWS\system32\wshtcpip.dll
Opens: C:\WINDOWS\system32\iphlpapi.dll
Opens: C:\WINDOWS\msdfmap.ini: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\msgsocm.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\system32\winrnr.dll
Opens: C:\WINDOWS\system32\drivers\etc\hosts
Opens: C:\WINDOWS\system32\rsaenh.dll
Opens: C:\WINDOWS\msmqinst.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\mui
Opens: C:\WINDOWS\netfxocm.log: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\windows\network diagnostic
Opens: C:\WINDOWS\NOTEPAD.EXE: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualCPlusPlus.Runtime-Libraries_6595b64144ccf1df_6.0.0.0_x-ww_ff9986d7\msvcp60.dll
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.1.0.Microsoft.Windows.GdiPlus_6595b64144ccf1df_x-ww_4e8510ac
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.5.1.Microsoft.Windows.SystemCompatible_6595b64144ccf1df_x-ww_a0111510
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_x-ww_362e60dd
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Rtcdll_6595b64144ccf1df_x-ww_c7b7206f
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.6.0.Microsoft.Windows.Common-Controls_6595b64144ccf1df_x-ww_5ddad775
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.7.0.Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_x-ww_a317e4b3
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-ww_77c24773
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_x-ww_9e7eb501
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-ww_b7353f75
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_x-ww_b8438ace
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_x-ww_4ee8bb30
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_x-ww_4ee8bb30\9.0.30729.4148.cat
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_x-ww_4ee8bb30\9.0.30729.4148.policy
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_x-ww_b8438ace\9.0.30729.4148.cat
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.MFCLOC_1fc8b3b9a1e18e3b_x-ww_b8438ace\9.0.30729.4148.policy
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-ww_b7353f75\9.0.21022.8.cat
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-ww_b7353f75\9.0.21022.8.policy
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-

ww_b7353f75\9.0.30729.4148.cat
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-ww_b7353f75\9.0.30729.4148.policy
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_x-ww_9e7eb501\9.0.30729.4148.cat
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_x-ww_9e7eb501\9.0.30729.4148.policy
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-ww_77c24773\8.0.50727.3053.cat
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-ww_77c24773\8.0.50727.3053.policy
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-ww_77c24773\8.0.50727.762.cat
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-ww_77c24773\8.0.50727.762.policy
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.7.0.Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_x-ww_a317e4b3\7.0.2600.5512.cat
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.7.0.Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_x-ww_a317e4b3\7.0.2600.5512.Policy
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.6.0.Microsoft.Windows.Common-Controls_6595b64144ccf1df_x-ww_5ddad775\6.0.2600.5512.cat
Opens: C:\WINDOWS\WinSxS\Policies\x86_policy.6.0.Microsoft.Windows.Common-Controls_6595b64144ccf1df_x-ww_5ddad775\6.0.2600.5512.Policy
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Rtcdll_6595b64144ccf1df_x-ww_c7b7206f\5.2.2.3.cat
Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Rtcdll_6595b64144ccf1df_x-ww_c7b7206f\5.2.2.3.Policy
Opens: C:\WINDOWS\ntbtlog.txt: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
Writes to: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
Writes to: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe
Writes to: C:\WINDOWS\system32\cisvc.vir
Writes to: C:\WINDOWS\system32\cisvc.exe
Writes to: C:\WINDOWS\system32\clipsrv.vir
Writes to: C:\WINDOWS\system32\clipsrv.exe
Writes to: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
Writes to: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
Writes to: C:\WINDOWS\system32\dmadmin.vir
Writes to: C:\System Volume Information\catalog.wci\CiSP0000.000
Writes to: C:\WINDOWS\system32\dmadmin.exe
Writes to: C:\System Volume Information\catalog.wci\INDEX.000
Writes to: C:\System Volume Information\catalog.wci\INDEX.002
Writes to: C:\System Volume Information\catalog.wci\INDEX.001
Writes to: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.vir
Writes to: C:\System Volume Information\catalog.wci\CiFLfffd.000
Writes to: C:\System Volume Information\catalog.wci\CiCL0001.000
Writes to: C:\System Volume Information\catalog.wci\CiSL0001.000
Writes to: C:\System Volume Information\catalog.wci\CiP10000.000
Writes to: C:\System Volume Information\catalog.wci\CiP20000.000
Writes to: C:\System Volume Information\catalog.wci\CiPT0000.000
Writes to: C:\System Volume Information\catalog.wci\CiST0000.000
Writes to: C:\System Volume Information\catalog.wci\propstor.bk1
Writes to: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.exe
Writes to: C:\System Volume Information\catalog.wci\CiP10000.002
Writes to: C:\System Volume Information\catalog.wci\CiP10000.001
Writes to: C:\System Volume Information\catalog.wci\propstor.bk2
Writes to: C:\System Volume Information\catalog.wci\CiP20000.002
Writes to: C:\System Volume Information\catalog.wci\CiP20000.001
Writes to: C:\System Volume Information\catalog.wci\CiVP0000.000
Writes to: C:\WINDOWS\system32\imapi.vir
Writes to: C:\WINDOWS\system32\imapi.exe
Writes to: C:\System Volume Information\catalog.wci\CiPT0000.002
Writes to: C:\System Volume Information\catalog.wci\CiPT0000.001
Writes to: C:\System Volume Information\catalog.wci\cicat.hsh
Writes to: C:\System Volume Information\catalog.wci\cicat.fid
Writes to: C:\WINDOWS\system32\mnmsrvc.vir
Writes to: C:\WINDOWS\system32\mnmsrvc.exe
Writes to: C:\System Volume Information\catalog.wci\CiSP0000.001
Writes to: C:\WINDOWS\system32\msiexec.vir
Writes to: C:\System Volume Information\catalog.wci\CiSP0000.002
Writes to: C:\WINDOWS\system32\msiexec.exe

Writes to: C:\WINDOWS\system32\netdde.vir
Writes to: C:\WINDOWS\system32\netdde.exe
Writes to: C:\System Volume Information\catalog.wci\00000002.ps1
Writes to: C:\System Volume Information\catalog.wci\00000002.ps2
Writes to: C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
Writes to: C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
Writes to: C:\WINDOWS\system32\sessmgr.vir
Writes to: C:\WINDOWS\system32\sessmgr.exe
Writes to: C:\WINDOWS\system32\locator.vir
Writes to: C:\WINDOWS\system32\locator.exe
Writes to: C:\WINDOWS\system32\scardsvr.vir
Writes to: C:\WINDOWS\system32\scardsvr.exe
Writes to: C:\WINDOWS\system32\smlogsvc.vir
Writes to: C:\WINDOWS\system32\vssvc.vir
Writes to: C:\WINDOWS\system32\vssvc.exe
Writes to: C:\WINDOWS\system32\wbem\wmiapsrv.vir
Writes to: C:\WINDOWS\system32\wbem\wmiapsrv.exe
Writes to: C:\System Volume Information\catalog.wci\CiST0000.002
Writes to: C:\System Volume Information\catalog.wci\CiST0000.001
Writes to: C:\System Volume Information\catalog.wci\CiCL0001.002
Writes to: C:\System Volume Information\catalog.wci\CiCL0001.001
Writes to: C:\Program Files\Internet Explorer\iexplore.vir
Writes to: C:\Program Files\Internet Explorer\iexplore.exe
Writes to: C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf
Writes to: C:\System Volume Information\catalog.wci\00010001.dir
Writes to: C:\System Volume Information\catalog.wci\00010001.ci
Writes to: C:\System Volume Information\catalog.wci\CiFLfffc.000
Writes to: C:\System Volume Information\catalog.wci\CiFLfffc.002
Writes to: C:\System Volume Information\catalog.wci\CiFLfffc.001
Reads from: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe
Reads from: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
Reads from: C:\WINDOWS\system32\cisvc.exe
Reads from: C:\WINDOWS\system32\cisvc.vir
Reads from: C:\WINDOWS\Registration\R000000000007.clb
Reads from: C:\WINDOWS\system32\ixsso.dll
Reads from: C:\WINDOWS\system32\clipsrv.exe
Reads from: C:\WINDOWS\system32\clipsrv.vir
Reads from: C:\WINDOWS\system32\ciodm.dll
Reads from: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
Reads from: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
Reads from: C:\WINDOWS\system32\langwrbk.dll
Reads from: C:\WINDOWS\system32\dllhost.exe
Reads from: C:\WINDOWS\system32\dmadmin.exe
Reads from: C:\WINDOWS\system32\dmadmin.vir
Reads from: C:\WINDOWS\Microsoft.NET\Framework\v3.0\WPF\PresentationFontCache.exe
Reads from: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.exe
Reads from: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.vir
Reads from: C:\WINDOWS\system32\imapi.exe
Reads from: C:\WINDOWS\system32\imapi.vir
Reads from: C:\WINDOWS\system32\mnmsrvc.exe
Reads from: C:\WINDOWS\system32\mnmsrvc.vir
Reads from: C:\WINDOWS\system32\msdtc.exe
Reads from: C:\WINDOWS\system32\msiexec.exe
Reads from: C:\WINDOWS\system32\msiexec.vir
Reads from: C:\WINDOWS\system32\netdde.exe
Reads from: C:\WINDOWS\system32\netdde.vir
Reads from: C:\System Volume Information\catalog.wci\propstor.bk1
Reads from: C:\System Volume Information\catalog.wci\propstor.bk2
Reads from: C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE
Reads from: C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
Reads from: C:\WINDOWS\system32\sessmgr.exe
Reads from: C:\WINDOWS\system32\sessmgr.vir
Reads from: C:\WINDOWS\system32\locator.exe
Reads from: C:\WINDOWS\system32\locator.vir
Reads from: C:\WINDOWS\system32\scardsvr.exe
Reads from: C:\WINDOWS\system32\scardsvr.vir
Reads from: C:\WINDOWS\system32\smlogsvc.exe
Reads from: C:\WINDOWS\system32\ups.exe
Reads from: C:\WINDOWS\system32\vssvc.exe
Reads from: C:\WINDOWS\system32\vssvc.vir
Reads from: C:\WINDOWS\system32\wbem\wmiapsrv.exe
Reads from: C:\WINDOWS\system32\wbem\wmiapsrv.vir
Reads from: C:\WINDOWS\system32\noise.dat
Reads from: C:\Documents and Settings\NetworkService\ntuser.ini
Reads from: C:\Documents and Settings\LocalService\ntuser.ini
Reads from: C:\Documents and Settings\Default User\Templates\amipro.sam
Reads from: C:\WINDOWS\system32\noise.enu
Reads from: C:\Documents and Settings\Default User\Templates\excel.xls
Reads from: C:\Documents and Settings\Default User\Templates\excel4.xls
Reads from: C:\Documents and Settings\Default User\Templates\lotus.wk4
Reads from: C:\Documents and Settings\Default User\Templates\presenta.shw

Reads from: C:\Documents and Settings\Default User\Templates\quattro.wb2
Reads from: C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf
Reads from: C:\Documents and Settings\Default User\Templates\winword.doc
Reads from: C:\Documents and Settings\Default User\Templates\winword2.doc
Reads from: C:\Documents and Settings\Default User\Templates\wordpfct.wpd
Reads from: C:\Documents and Settings\Default User\Templates\wordpfct.wpg
Reads from: C:\Documents and Settings\Default User\Start Menu\desktop.ini
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\desktop.ini
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Remote Assistance.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Windows Media Player.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Startup\desktop.ini
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Command Prompt.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\desktop.ini
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Notepad.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Program Compatibility Wizard.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Synchronize.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Tour Windows XP.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Windows Explorer.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Entertainment\desktop.ini
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\desktop.ini
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\Magnifier.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\Narrator.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
Reads from: C:\Documents and Settings\Default User\Start Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
Reads from: C:\Documents and Settings\Default User\SendTo\desktop.ini
Reads from: C:\Documents and Settings\Default User\SendTo\Compressed (zipped) Folder.ZFSendToTarget
Reads from: C:\Documents and Settings\All Users\Start Menu\Set Program Access and Defaults.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\desktop.ini
Reads from: C:\Documents and Settings\All Users\Start Menu\Windows Catalog.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Windows Update.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Adobe Reader 9.lnk
Reads from: C:\Documents and Settings\All Users\Documents\desktop.ini
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\desktop.ini
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office Excel Viewer.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office Word Viewer 2003.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft PowerPoint Viewer .lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\MSN.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Windows Messenger.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Windows Movie Maker.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Startup\desktop.ini
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\IDLE (Python GUI).lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Module Docs.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Python (command line).lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Python for Windows Documentation.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Python Manuals.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\PythonWin.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\Uninstall Python.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\desktop.ini

Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Freecell.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Hearts.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Backgammon.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Checkers.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Hearts.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Reversi.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet Spades.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Minesweeper.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Pinball.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Solitaire.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Games\Spider Solitaire.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Component Services.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\desktop.ini
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Computer Management.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Data Sources (ODBC).lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Event Viewer.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Local Security Policy.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Performance.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\Services.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Calculator.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\desktop.ini
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Paint.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Remote Desktop Connection.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\WordPad.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Activate Windows.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\desktop.ini
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Backup.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Character Map.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Disk Cleanup.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Disk Defragmenter.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Files and Settings Transfer Wizard.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Scheduled Tasks.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\Security Center.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\System Information.lnk
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\System Restore.lnk
Reads from: C:\Documents and Settings\Default User\SendTo\Desktop (create shortcut).DeskLink
Reads from: C:\Documents and Settings\Default User\SendTo\Mail Recipient.MAPIMail
Reads from: C:\Documents and Settings\Default User\Cookies\index.dat
Reads from: C:\Documents and Settings\All Users\ntuser.pol
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Entertainment\desktop.ini
Reads from: C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Entertainment\Sound Recorder.lnk
Reads from: C:\Documents and Settings\All Users\Documents\My Videos\Desktop.ini
Reads from: C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
Reads from: C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\desktop.ini
Reads from: C:\Documents and Settings\All Users\Documents\My Pictures\Sample

Pictures\Blue hills.jpg
  Reads from: C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Sunset.jpg
  Reads from: C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Water lilies.jpg
  Reads from: C:\Documents and Settings\All Users\Documents\My Pictures\Sample
Pictures\Winter.jpg
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst1.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst10.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst11.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst12.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst13.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst14.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst15.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst2.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst3.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst4.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst5.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst6.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst7.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst8.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\000C5A7A\Plylst9.wpl
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Music\desktop.ini
  Reads from: C:\Documents and Settings\Admin\Application Data\Microsoft\Internet
Explorer\Quick Launch\Launch Internet Explorer Browser.lnk
  Reads from: C:\Program Files\Internet Explorer\iexplore.exe
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample
Music\Beethoven's Symphony No. 9 (Scherzo).wma
  Reads from: C:\Documents and Settings\All Users\Documents\My Music\Sample Music\New
Stories (Highway Blues).wma
  Reads from: C:\Documents and Settings\All Users\Desktop\Adobe Reader 9.lnk
  Reads from: C:\Program Files\Internet Explorer\iexplore.vir
  Reads from: C:\Documents and Settings\Administrator\ntuser.ini
  Reads from: C:\Documents and Settings\Administrator\Templates\amipro.sam
  Reads from: C:\Documents and Settings\Administrator\Templates\excel.xls
  Reads from: C:\Documents and Settings\Administrator\Start Menu\Programs\Windows
Media Player.lnk
  Reads from: C:\Documents and Settings\Administrator\Start Menu\desktop.ini
  Reads from: C:\Documents and Settings\Administrator\Start Menu\Programs\desktop.ini
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Startup\desktop.ini
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Command Prompt.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\desktop.ini
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Notepad.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Program Compatibility Wizard.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Synchronize.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Tour Windows XP.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Windows Explorer.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
  Reads from: C:\Documents and Settings\Administrator\Start

Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
  Reads from: C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
  Reads from: C:\Documents and Settings\Administrator\SendTo\desktop.ini
  Reads from: C:\Documents and Settings\Administrator\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
  Reads from: C:\Documents and Settings\Administrator\SendTo\Desktop (create
shortcut).DeskLink
  Reads from: C:\Documents and Settings\Administrator\SendTo\Mail Recipient.MAPIMail
  Reads from: C:\Documents and Settings\Administrator\Cookies\index.dat
  Reads from: C:\Documents and Settings\Admin\ntuser.ini
  Reads from: C:\Documents and Settings\Admin\Templates\amipro.sam
  Reads from: C:\Documents and Settings\Admin\Templates\excel.xls
  Reads from: C:\Documents and Settings\Admin\Templates\excel4.xls
  Reads from: C:\Documents and Settings\Admin\Templates\lotus.wk4
  Reads from: C:\Documents and Settings\Admin\Templates\presenta.shw
  Reads from: C:\Documents and Settings\Admin\Templates\quattro.wb2
  Reads from: C:\Documents and Settings\Admin\Templates\winword.doc
  Reads from: C:\Documents and Settings\Admin\Templates\winword2.doc
  Reads from: C:\Documents and Settings\Admin\Templates\wordpfct.wpd
  Reads from: C:\Documents and Settings\Admin\Templates\wordpfct.wpg
  Reads from: C:\Documents and Settings\Admin\Start Menu\desktop.ini
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Internet
Explorer.lnk
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Outlook Express.lnk
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Remote
Assistance.lnk
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media
Player.lnk
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Address
Book.lnk
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\desktop.ini
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Command
Prompt.lnk
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Notepad.lnk
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Program
Compatibility Wizard.lnk
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Synchronize.lnk
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Tour
Windows XP.lnk
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Windows
Explorer.lnk
  Reads from: C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System
Tools\Internet Explorer (No Add-ons).lnk
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
  Reads from: C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
  Reads from: C:\Documents and Settings\Admin\SendTo\desktop.ini
  Reads from: C:\Documents and Settings\Admin\SendTo\Compressed (zipped)
Folder.ZFSendToTarget
  Reads from: C:\Documents and Settings\Admin\SendTo\Desktop (create
shortcut).DeskLink
  Reads from: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\Volume Control.lnk
  Reads from: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\desktop.ini
  Reads from: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\HyperTerminal.lnk
  Reads from: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Network Connections.lnk
  Reads from: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Network Setup Wizard.lnk
  Reads from: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\New Connection Wizard.lnk
  Reads from: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Wireless Network Setup Wizard.lnk
  Reads from: C:\Documents and Settings\All Users\Start

Menu\Programs\Accessories\Accessibility\Accessibility Wizard.lnk
  Reads from: C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
  Reads from: C:\Documents and Settings\All Users\DRM\drmv2.lic
  Reads from: C:\Documents and Settings\All Users\DRM\drmv2.sst
  Reads from: C:\Documents and Settings\Admin\SendTo\Mail Recipient.MAPIMail
  Reads from: C:\Documents and Settings\Admin\SendTo\My Documents.mydocs
  Reads from: C:\Documents and Settings\Admin\Recent\Desktop.ini
  Reads from: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE Add-on
site.url
  Reads from: C:\Documents and Settings\Admin\Favorites\Desktop.ini
  Reads from: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\IE site on
Microsoft.com.url
  Reads from: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Home.url
  Reads from: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
At Work.url
  Reads from: C:\Documents and Settings\Admin\Favorites\Microsoft Websites\Microsoft
Store.url
  Reads from: C:\Documents and Settings\Admin\Favorites\Links\desktop.ini
  Reads from: C:\Documents and Settings\Admin\Favorites\Links\Free Hotmail.url
  Reads from: C:\Documents and Settings\Admin\Favorites\Links\Suggested Sites.url
  Reads from: C:\Documents and Settings\Admin\Favorites\Links\Web Slice Gallery.url
  Reads from: C:\Documents and Settings\Admin\Cookies\admin@search.microsoft[1].txt
  Reads from: C:\Documents and Settings\Admin\Cookies\index.dat
  Reads from: C:\AUTOEXEC.BAT
  Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\dotnetfx35setup[1].exe
  Reads from: C:\boot.ini
  Reads from: C:\CONFIG.SYS
  Reads from: C:\System Volume Information\catalog.wci\00010001.ci
  Reads from: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\ONWV4FIP\IE8-WindowsXP-x86-ENU[1].exe
  Reads from: C:\exception.log
  Reads from: C:\IO.SYS
  Reads from: C:\MSDOS.SYS
  Reads from: C:\NTDETECT.COM
  Reads from: C:\ntldr
  Reads from: C:\WINDOWS\0.log
  Reads from: C:\WINDOWS\Blue Lace 16.bmp
  Reads from: C:\WINDOWS\bootstat.dat
  Reads from: C:\WINDOWS\explorer.exe
  Reads from: C:\WINDOWS\explorer.scf
  Reads from: C:\WINDOWS\FaxSetup.log
  Reads from: C:\WINDOWS\FeatherTexture.bmp
  Reads from: C:\WINDOWS\Gone Fishing.bmp
  Reads from: C:\WINDOWS\Greenstone.bmp
  Reads from: C:\WINDOWS\hh.exe
  Reads from: C:\WINDOWS\ie8.log
  Reads from: C:\WINDOWS\ie8_main.log
  Reads from: C:\WINDOWS\iis6.log
  Reads from: C:\WINDOWS\imsins.BAK
  Reads from: C:\WINDOWS\imsins.log
  Reads from: C:\WINDOWS\MedCtrOC.log
  Reads from: C:\WINDOWS\msdfmap.ini
  Reads from: C:\WINDOWS\msgsocm.log
  Reads from: C:\WINDOWS\system32\drivers\etc\hosts
  Reads from: C:\WINDOWS\system32\rsaenh.dll
  Reads from: C:\WINDOWS\msmqinst.log
  Reads from: C:\WINDOWS\netfxocm.log
  Reads from: C:\WINDOWS\NOTEPAD.EXE
  Reads from: C:\WINDOWS\ntbtlog.txt
  Deletes: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.vir
  Deletes: C:\WINDOWS\system32\cisvc.vir
  Deletes: C:\WINDOWS\system32\clipsrv.vir
  Deletes: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.vir
  Deletes: C:\WINDOWS\system32\dmadmin.vir
  Deletes: C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\infocard.vir
  Deletes: C:\System Volume Information\catalog.wci\00000001.ps1
  Deletes: C:\WINDOWS\system32\imapi.vir
  Deletes: C:\System Volume Information\catalog.wci\00000001.ps2
  Deletes: C:\WINDOWS\system32\mnmsrvc.vir
  Deletes: C:\WINDOWS\system32\msiexec.vir
  Deletes: C:\WINDOWS\system32\netdde.vir
  Deletes: C:\Program Files\Common Files\Microsoft Shared\Source Engine\ose.vir
  Deletes: C:\WINDOWS\system32\sessmgr.vir
  Deletes: C:\WINDOWS\system32\locator.vir
  Deletes: C:\WINDOWS\system32\scardsvr.vir
  Deletes: C:\WINDOWS\system32\smlogsvc.vir
  Deletes: C:\WINDOWS\system32\vssvc.vir
  Deletes: C:\WINDOWS\system32\wbem\wmiapsrv.vir
  Deletes: C:\Program Files\Internet Explorer\iexplore.vir

Deletes: C:\System Volume Information\catalog.wci\CiFLfffd.000
Deletes: C:\System Volume Information\catalog.wci\CiFLfffd.001
Deletes: C:\System Volume Information\catalog.wci\CiFLfffd.002

Windows Registry Events

Creates key: HKU\.default\software\microsoft\multimedia\audio
Creates key: HKU\.default\software\microsoft\multimedia\audio compression manager\
Creates key: HKU\.default\software\microsoft\multimedia\audio compression manager\msacm
Creates key: HKU\.default\software\microsoft\multimedia\audio compression manager\priority v4.00
Creates key: HKLM\software\classes
Creates key: HKCR\msidxs
Creates key: HKCR\msidxs\clsid
Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}
Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\progid
Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\versionindependentprogid
Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\inprocserver32
Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\ole db provider
Creates key: HKCR\msidxs errorlookup
Creates key: HKCR\msidxs errorlookup\clsid
Creates key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}
Creates key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\progid
Creates key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\versionindependentprogid
Creates key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\inprocserver32
Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors
Creates key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors\{f9ae8981-7e52-11d0-8964-00c04fd611d7}
Creates key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}
Creates key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\progid
Creates key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\versionindependentprogid
Creates key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\inprocserver32
Creates key: HKLM\system\currentcontrolset\control\contentindexcommon
Creates key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}
Creates key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprocserver32
Creates key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}
Creates key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32
Creates key: HKCR\clsid\{098f2470-bae0-11cd-b579-08002b30bfeb}
Creates key: HKCR\clsid\{098f2470-bae0-11cd-b579-08002b30bfeb}\persistentaddinsregistered
Creates key: HKCR\clsid\{098f2470-bae0-11cd-b579-08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Creates key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}
Creates key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32
Creates key: HKCR\.386
Creates key: HKCR\.386\persistenthandler
Creates key: HKCR\.audiocd
Creates key: HKCR\.audiocd\persistenthandler
Creates key: HKCR\.desklink
Creates key: HKCR\.desklink\persistenthandler
Creates key: HKCR\.folder
Creates key: HKCR\.folder\persistenthandler
Creates key: HKCR\.mapimail
Creates key: HKCR\.mapimail\persistenthandler
Creates key: HKCR\.zfsendtotarget
Creates key: HKCR\.zfsendtotarget\persistenthandler
Creates key: HKCR\.aif
Creates key: HKCR\.aif\persistenthandler
Creates key: HKCR\.aifc
Creates key: HKCR\.aifc\persistenthandler
Creates key: HKCR\.aiff
Creates key: HKCR\.aiff\persistenthandler
Creates key: HKCR\.aps
Creates key: HKCR\.aps\persistenthandler
Creates key: HKCR\.asf
Creates key: HKCR\.asf\persistenthandler
Creates key: HKCR\.asx
Creates key: HKCR\.asx\persistenthandler
Creates key: HKCR\.au
Creates key: HKCR\.au\persistenthandler
Creates key: HKCR\.avi
Creates key: HKCR\.avi\persistenthandler
Creates key: HKCR\clsid\{00022602-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\.bin
Creates key: HKCR\.bin\persistenthandler
Creates key: HKCR\.bkf
Creates key: HKCR\.bkf\persistenthandler
Creates key: HKCR\.bmp
Creates key: HKCR\.bmp\persistenthandler

Creates key: HKCR\clsid\{d3e34b21-9d75-101a-8c3d-00aa001a1652}\persistenthandler
Creates key: HKCR\.bsc
Creates key: HKCR\.bsc\persistenthandler
Creates key: HKCR\.cab
Creates key: HKCR\.cab\persistenthandler
Creates key: HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262}\persistenthandler
Creates key: HKCR\.cda
Creates key: HKCR\.cda\persistenthandler
Creates key: HKCR\.cgm
Creates key: HKCR\.cgm\persistenthandler
Creates key: HKCR\.com
Creates key: HKCR\.com\persistenthandler
Creates key: HKCR\.cpl
Creates key: HKCR\.cpl\persistenthandler
Creates key: HKCR\.cur
Creates key: HKCR\.cur\persistenthandler
Creates key: HKCR\.dbg
Creates key: HKCR\.dbg\persistenthandler
Creates key: HKCR\.dct
Creates key: HKCR\.dct\persistenthandler
Creates key: HKCR\.dib
Creates key: HKCR\.dib\persistenthandler
Creates key: HKCR\.dl_
Creates key: HKCR\.dl_\persistenthandler
Creates key: HKCR\.dll
Creates key: HKCR\.dll\persistenthandler
Creates key: HKCR\.drv
Creates key: HKCR\.drv\persistenthandler
Creates key: HKCR\.dvd
Creates key: HKCR\.dvd\persistenthandler
Creates key: HKCR\.emf
Creates key: HKCR\.emf\persistenthandler
Creates key: HKCR\.eps
Creates key: HKCR\.eps\persistenthandler
Creates key: HKCR\.ex_
Creates key: HKCR\.ex_\persistenthandler
Creates key: HKCR\.exe
Creates key: HKCR\.exe\persistenthandler
Creates key: HKCR\.exp
Creates key: HKCR\.exp\persistenthandler
Creates key: HKCR\.eyb
Creates key: HKCR\.eyb\persistenthandler
Creates key: HKCR\.fnd
Creates key: HKCR\.fnd\persistenthandler
Creates key: HKCR\.fnt
Creates key: HKCR\.fnt\persistenthandler
Creates key: HKCR\.fon
Creates key: HKCR\.fon\persistenthandler
Creates key: HKCR\.ghi
Creates key: HKCR\.ghi\persistenthandler
Creates key: HKCR\.gif
Creates key: HKCR\.gif\persistenthandler
Creates key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\persistenthandler
Creates key: HKCR\.gz
Creates key: HKCR\.gz\persistenthandler
Creates key: HKCR\.hqx
Creates key: HKCR\.hqx\persistenthandler
Creates key: HKCR\.icm
Creates key: HKCR\.icm\persistenthandler
Creates key: HKCR\.ico
Creates key: HKCR\.ico\persistenthandler
Creates key: HKCR\.idb
Creates key: HKCR\.idb\persistenthandler
Creates key: HKCR\.ilk
Creates key: HKCR\.ilk\persistenthandler
Creates key: HKCR\.imc
Creates key: HKCR\.imc\persistenthandler
Creates key: HKCR\.in_
Creates key: HKCR\.in_\persistenthandler
Creates key: HKCR\.inv
Creates key: HKCR\.inv\persistenthandler
Creates key: HKCR\.ivf
Creates key: HKCR\.ivf\persistenthandler
Creates key: HKCR\.jbf
Creates key: HKCR\.jbf\persistenthandler
Creates key: HKCR\.jfif
Creates key: HKCR\.jfif\persistenthandler
Creates key: HKCR\.jpe
Creates key: HKCR\.jpe\persistenthandler
Creates key: HKCR\.jpeg
Creates key: HKCR\.jpeg\persistenthandler
Creates key: HKCR\.jpg
Creates key: HKCR\.jpg\persistenthandler

Creates key: HKCR\.latex
Creates key: HKCR\.latex\persistenthandler
Creates key: HKCR\.lib
Creates key: HKCR\.lib\persistenthandler
Creates key: HKCR\.m14
Creates key: HKCR\.m14\persistenthandler
Creates key: HKCR\.m1v
Creates key: HKCR\.m1v\persistenthandler
Creates key: HKCR\.m3u
Creates key: HKCR\.m3u\persistenthandler
Creates key: HKCR\.mdb
Creates key: HKCR\.mdb\persistenthandler
Creates key: HKCR\.mid
Creates key: HKCR\.mid\persistenthandler
Creates key: HKCR\clsid\{00022603-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\.midi
Creates key: HKCR\.midi\persistenthandler
Creates key: HKCR\.mmf
Creates key: HKCR\.mmf\persistenthandler
Creates key: HKCR\.mov
Creates key: HKCR\.mov\persistenthandler
Creates key: HKCR\.movie
Creates key: HKCR\.movie\persistenthandler
Creates key: HKCR\.mp2
Creates key: HKCR\.mp2\persistenthandler
Creates key: HKCR\.mp2v
Creates key: HKCR\.mp2v\persistenthandler
Creates key: HKCR\.mp3
Creates key: HKCR\.mp3\persistenthandler
Creates key: HKCR\.mpa
Creates key: HKCR\.mpa\persistenthandler
Creates key: HKCR\.mpe
Creates key: HKCR\.mpe\persistenthandler
Creates key: HKCR\.mpeg
Creates key: HKCR\.mpeg\persistenthandler
Creates key: HKCR\.mpg
Creates key: HKCR\.mpg\persistenthandler
Creates key: HKCR\.mpv2
Creates key: HKCR\.mpv2\persistenthandler
Creates key: HKCR\.msg
Creates key: HKCR\.msg\persistenthandler
Creates key: HKCR\.mv
Creates key: HKCR\.mv\persistenthandler
Creates key: HKCR\.mydocs
Creates key: HKCR\.mydocs\persistenthandler
Creates key: HKCR\.ncb
Creates key: HKCR\.ncb\persistenthandler
Creates key: HKCR\.obj
Creates key: HKCR\.obj\persistenthandler
Creates key: HKCR\.oc_
Creates key: HKCR\.oc_\persistenthandler
Creates key: HKCR\.ocx
Creates key: HKCR\.ocx\persistenthandler
Creates key: HKCR\.pch
Creates key: HKCR\.pch\persistenthandler
Creates key: HKCR\.pdb
Creates key: HKCR\.pdb\persistenthandler
Creates key: HKCR\.pds
Creates key: HKCR\.pds\persistenthandler
Creates key: HKCR\.pic
Creates key: HKCR\.pic\persistenthandler
Creates key: HKCR\.pma
Creates key: HKCR\.pma\persistenthandler
Creates key: HKCR\.pmc
Creates key: HKCR\.pmc\persistenthandler
Creates key: HKCR\.pml
Creates key: HKCR\.pml\persistenthandler
Creates key: HKCR\.pmr
Creates key: HKCR\.pmr\persistenthandler
Creates key: HKCR\.png
Creates key: HKCR\.png\persistenthandler
Creates key: HKCR\.psd
Creates key: HKCR\.psd\persistenthandler
Creates key: HKCR\.res
Creates key: HKCR\.res\persistenthandler
Creates key: HKCR\.rle
Creates key: HKCR\.rle\persistenthandler
Creates key: HKCR\.rmi
Creates key: HKCR\.rmi\persistenthandler
Creates key: HKCR\.rpc
Creates key: HKCR\.rpc\persistenthandler
Creates key: HKCR\.rsp
Creates key: HKCR\.rsp\persistenthandler

Creates key: HKCR\.sbr
Creates key: HKCR\.sbr\persistenthandler
Creates key: HKCR\.sc2
Creates key: HKCR\.sc2\persistenthandler
Creates key: HKCR\.sit
Creates key: HKCR\.sit\persistenthandler
Creates key: HKCR\.snd
Creates key: HKCR\.snd\persistenthandler
Creates key: HKCR\.sr_
Creates key: HKCR\.sr_\persistenthandler
Creates key: HKCR\.sy_
Creates key: HKCR\.sy_\persistenthandler
Creates key: HKCR\.sym
Creates key: HKCR\.sym\persistenthandler
Creates key: HKCR\.sys
Creates key: HKCR\.sys\persistenthandler
Creates key: HKCR\.tar
Creates key: HKCR\.tar\persistenthandler
Creates key: HKCR\.tgz
Creates key: HKCR\.tgz\persistenthandler
Creates key: HKCR\.tif
Creates key: HKCR\.tif\persistenthandler
Creates key: HKCR\.tiff
Creates key: HKCR\.tiff\persistenthandler
Creates key: HKCR\.tlb
Creates key: HKCR\.tlb\persistenthandler
Creates key: HKCR\.tsp
Creates key: HKCR\.tsp\persistenthandler
Creates key: HKCR\.ttc
Creates key: HKCR\.ttc\persistenthandler
Creates key: HKCR\.ttf
Creates key: HKCR\.ttf\persistenthandler
Creates key: HKCR\.vbx
Creates key: HKCR\.vbx\persistenthandler
Creates key: HKCR\.vxd
Creates key: HKCR\.vxd\persistenthandler
Creates key: HKCR\.wav
Creates key: HKCR\.wav\persistenthandler
Creates key: HKCR\clsid\{00020c01-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\.wax
Creates key: HKCR\.wax\persistenthandler
Creates key: HKCR\.wll
Creates key: HKCR\.wll\persistenthandler
Creates key: HKCR\.wlt
Creates key: HKCR\.wlt\persistenthandler
Creates key: HKCR\.wm
Creates key: HKCR\.wm\persistenthandler
Creates key: HKCR\.wma
Creates key: HKCR\.wma\persistenthandler
Creates key: HKCR\.wmf
Creates key: HKCR\.wmf\persistenthandler
Creates key: HKCR\.wmp
Creates key: HKCR\.wmp\persistenthandler
Creates key: HKCR\.wmv
Creates key: HKCR\.wmv\persistenthandler
Creates key: HKCR\.wmx
Creates key: HKCR\.wmx\persistenthandler
Creates key: HKCR\.wmz
Creates key: HKCR\.wmz\persistenthandler
Creates key: HKCR\.wsz
Creates key: HKCR\.wsz\persistenthandler
Creates key: HKCR\.wvx
Creates key: HKCR\.wvx\persistenthandler
Creates key: HKCR\.xbm
Creates key: HKCR\.xbm\persistenthandler
Creates key: HKCR\.xix
Creates key: HKCR\.xix\persistenthandler
Creates key: HKCR\.z
Creates key: HKCR\.z\persistenthandler
Creates key: HKCR\.z96
Creates key: HKCR\.z96\persistenthandler
Creates key: HKCR\.zip
Creates key: HKCR\.zip\persistenthandler
Creates key: HKCR\clsid\{e88dcce0-b7b3-11d1-a9f0-00aa0060fa31}\persistenthandler
Creates key: HKCR\clsid\{5e941d80-bf96-11cd-b579-08002b30bfeb}
Creates key: HKCR\clsid\{5e941d80-bf96-11cd-b579-08002b30bfeb}\persistentaddinsregistered
Creates key: HKCR\clsid\{5e941d80-bf96-11cd-b579-08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Creates key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}
Creates key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32
Creates key: HKCR\clsid\{73fddc80-aea9-101a-98a7-00aa00374959}\persistenthandler
Creates key: HKCR\clsid\{48123bc4-99d9-11d1-a6b3-00c04fd91555}\persistenthandler

Creates key: HKCR\.dic
Creates key: HKCR\.dic\persistenthandler
Creates key: HKCR\.txt
Creates key: HKCR\.txt\persistenthandler
Creates key: HKCR\.wtx
Creates key: HKCR\.wtx\persistenthandler
Creates key: HKCR\.bat
Creates key: HKCR\.bat\persistenthandler
Creates key: HKCR\.cmd
Creates key: HKCR\.cmd\persistenthandler
Creates key: HKCR\.idq
Creates key: HKCR\.idq\persistenthandler
Creates key: HKCR\.ini
Creates key: HKCR\.ini\persistenthandler
Creates key: HKCR\.inx
Creates key: HKCR\.inx\persistenthandler
Creates key: HKCR\.reg
Creates key: HKCR\.reg\persistenthandler
Creates key: HKCR\.inf
Creates key: HKCR\.inf\persistenthandler
Creates key: HKCR\.vbs
Creates key: HKCR\.vbs\persistenthandler
Creates key: HKCR\.asm
Creates key: HKCR\.asm\persistenthandler
Creates key: HKCR\.c
Creates key: HKCR\.c\persistenthandler
Creates key: HKCR\.cpp
Creates key: HKCR\.cpp\persistenthandler
Creates key: HKCR\.cxx
Creates key: HKCR\.cxx\persistenthandler
Creates key: HKCR\.def
Creates key: HKCR\.def\persistenthandler
Creates key: HKCR\.h
Creates key: HKCR\.h\persistenthandler
Creates key: HKCR\.hpp
Creates key: HKCR\.hpp\persistenthandler
Creates key: HKCR\.hxx
Creates key: HKCR\.hxx\persistenthandler
Creates key: HKCR\.idl
Creates key: HKCR\.idl\persistenthandler
Creates key: HKCR\.inc
Creates key: HKCR\.inc\persistenthandler
Creates key: HKCR\.js
Creates key: HKCR\.js\persistenthandler
Creates key: HKCR\.log
Creates key: HKCR\.log\persistenthandler
Creates key: HKCR\.pl
Creates key: HKCR\.pl\persistenthandler
Creates key: HKCR\.rc
Creates key: HKCR\.rc\persistenthandler
Creates key: HKCR\.rtf
Creates key: HKCR\.rtf\persistenthandler
Creates key: HKCR\.url
Creates key: HKCR\.url\persistenthandler
Creates key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\persistenthandler
Creates key: HKCR\.xml
Creates key: HKCR\.xml\persistenthandler
Creates key: HKCR\.xsl
Creates key: HKCR\.xsl\persistenthandler
Creates key: HKLM\system\currentcontrolset\control\contentindex\language\neutral
Creates key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}
Creates key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserver32
Creates key: HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}
Creates key: HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}\inprocserver32
Creates key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}
Creates key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprocserver32
Creates key: HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}
Creates key: HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}\inprocserver32
Creates key: HKCR\clsid
Creates key: HKCR\clsid\{c04efa90-e221-11d2-985e-00c04f575153}
Creates key: HKCR\clsid\{c04efa90-e221-11d2-985e-00c04f575153}\inprocserver32
Creates key: HKCR\interface
Creates key: HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}
Creates key: HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}\proxystubclsid32
Creates key: HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}\nummethods
Creates key: HKCR\clsid\{95ad72f0-44ce-11d0-ae29-00aa004b9986}
Creates key: HKCR\clsid\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\inprocserver32
Creates key: HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-00aa004b9986}
Creates key: HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\extension
Creates key: HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\standalone

Creates key: HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\nodetypes
Creates key: HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\nodetypes\{5401e3e9-f5f6-11d1-b4f7-00c04fc2db8d}
Creates key: HKLM\software\microsoft\mmc\nodetypes\{5401e3e9-f5f6-11d1-b4f7-00c04fc2db8d}
Creates key: HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-00c04fd8d5b0}
Creates key: HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-00c04fd8d5b0}\extensions
Creates key: HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-00c04fd8d5b0}\extensions\namespace
Creates key: HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-00c04fd8d5b0}\dynamic extensions
Creates key: HKLM\system\currentcontrolset\control\server applications
Creates key: HKCR\ixsso.query
Creates key: HKCR\ixsso.query\clsid
Creates key: HKCR\ixsso.query\curver
Creates key: HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}
Creates key: HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\inprocserver32
Creates key: HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\progid
Creates key: HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\implemented categories
Creates key: HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\implemented categories\{7dd95801-9882-11cf-9fa9-00aa006c42c4}
Creates key: HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\implemented categories\{7dd95802-9882-11cf-9fa9-00aa006c42c4}
Creates key: HKCR\ixsso.query.3
Creates key: HKCR\ixsso.query.3\clsid
Creates key: HKCR\ixsso.query.2
Creates key: HKCR\ixsso.query.2\clsid
Creates key: HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}
Creates key: HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\inprocserver32
Creates key: HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\progid
Creates key: HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\implemented categories
Creates key: HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\implemented categories\{7dd95801-9882-11cf-9fa9-00aa006c42c4}
Creates key: HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\implemented categories\{7dd95802-9882-11cf-9fa9-00aa006c42c4}
Creates key: HKCR\ixsso.util
Creates key: HKCR\ixsso.util\clsid
Creates key: HKCR\ixsso.util\curver
Creates key: HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}
Creates key: HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\inprocserver32
Creates key: HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\progid
Creates key: HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\implemented categories
Creates key: HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\implemented categories\{7dd95801-9882-11cf-9fa9-00aa006c42c4}
Creates key: HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\implemented categories\{7dd95802-9882-11cf-9fa9-00aa006c42c4}
Creates key: HKCR\ixsso.util.2
Creates key: HKCR\ixsso.util.2\clsid
Creates key: HKCR\clsid\{eec97550-47a9-11cf-b952-00aa0051fe20}
Creates key: HKCR\clsid\{eec97550-47a9-11cf-b952-00aa0051fe20}\persistentaddinsregistered
Creates key: HKCR\clsid\{eec97550-47a9-11cf-b952-00aa0051fe20}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Creates key: HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}
Creates key: HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}\inprocserver32
Creates key: HKCR\clsid\{3050f4d8-98b5-11cf-bb82-00aa00bdce0b}\persistenthandler
Creates key: HKCR\.odc
Creates key: HKCR\.odc\persistenthandler
Creates key: HKCR\.hhc
Creates key: HKCR\.hhc\persistenthandler
Creates key: HKCR\.htm
Creates key: HKCR\.htm\persistenthandler
Creates key: HKCR\.html
Creates key: HKCR\.html\persistenthandler
Creates key: HKCR\.htx
Creates key: HKCR\.htx\persistenthandler
Creates key: HKCR\.stm
Creates key: HKCR\.stm\persistenthandler
Creates key: HKCR\.htw
Creates key: HKCR\.htw\persistenthandler
Creates key: HKCR\.asp
Creates key: HKCR\.asp\persistenthandler
Creates key: HKCR\.aspx
Creates key: HKCR\.aspx\persistenthandler
Creates key: HKCR\.ascx
Creates key: HKCR\.ascx\persistenthandler
Creates key: HKCR\.css
Creates key: HKCR\.css\persistenthandler
Creates key: HKCR\.hta
Creates key: HKCR\.hta\persistenthandler

Creates key: HKCR\.htt
Creates key: HKCR\.htt\persistenthandler
Creates key: HKCR\clsid\{98de59a0-d175-11cd-a7bd-00006b827d94}
Creates key: HKCR\clsid\{98de59a0-d175-11cd-a7bd-00006b827d94}\persistentaddinsregistered
Creates key: HKCR\clsid\{98de59a0-d175-11cd-a7bd-00006b827d94}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Creates key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}
Creates key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32
Creates key: HKCR\clsid\{00020906-0000-0000-c000-000000000046}
Creates key: HKCR\clsid\{00020906-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\clsid\{64818d11-4f9b-11cf-86ea-00aa00b929e8}
Creates key: HKCR\clsid\{64818d11-4f9b-11cf-86ea-00aa00b929e8}\persistenthandler
Creates key: HKCR\clsid\{64818d10-4f9b-11cf-86ea-00aa00b929e8}
Creates key: HKCR\clsid\{64818d10-4f9b-11cf-86ea-00aa00b929e8}\persistenthandler
Creates key: HKCR\clsid\{00020820-0000-0000-c000-000000000046}
Creates key: HKCR\clsid\{00020820-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\clsid\{00020821-0000-0000-c000-000000000046}
Creates key: HKCR\clsid\{00020821-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\clsid\{00020900-0000-0000-c000-000000000046}
Creates key: HKCR\clsid\{00020900-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\clsid\{ea7bae70-fb3b-11cd-a903-00aa00510ea3}
Creates key: HKCR\clsid\{ea7bae70-fb3b-11cd-a903-00aa00510ea3}\persistenthandler
Creates key: HKCR\clsid\{ea7bae71-fb3b-11cd-a903-00aa00510ea3}
Creates key: HKCR\clsid\{ea7bae71-fb3b-11cd-a903-00aa00510ea3}\persistenthandler
Creates key: HKCR\clsid\{00020811-0000-0000-c000-000000000046}
Creates key: HKCR\clsid\{00020811-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\clsid\{00020810-0000-0000-c000-000000000046}
Creates key: HKCR\clsid\{00020810-0000-0000-c000-000000000046}\persistenthandler
Creates key: HKCR\.doc
Creates key: HKCR\.doc\persistenthandler
Creates key: HKCR\.dot
Creates key: HKCR\.dot\persistenthandler
Creates key: HKCR\.pot
Creates key: HKCR\.pot\persistenthandler
Creates key: HKCR\.ppt
Creates key: HKCR\.ppt\persistenthandler
Creates key: HKCR\.pps
Creates key: HKCR\.pps\persistenthandler
Creates key: HKCR\.xlb
Creates key: HKCR\.xlb\persistenthandler
Creates key: HKCR\.xlc
Creates key: HKCR\.xlc\persistenthandler
Creates key: HKCR\.xls
Creates key: HKCR\.xls\persistenthandler
Creates key: HKCR\.xlt
Creates key: HKCR\.xlt\persistenthandler
Creates key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}
Creates key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\progid
Creates key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid
Creates key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\programmable
Creates key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
Creates key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}
Creates key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\progid
Creates key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid
Creates key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\programmable
Creates key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
Creates key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}
Creates key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\progid
Creates key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid
Creates key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\programmable
Creates key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
Creates key: HKLM\system\currentcontrolset\control\contentindex\language\english_us
Creates key: HKCR\clsid\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}
Creates key: HKCR\clsid\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}\inprocserver32
Creates key: HKLM\system\currentcontrolset\control\contentindex\language\english_uk
Creates key: HKCR\clsid\{d99f7670-7f1a-11ce-be57-00aa0051fe20}
Creates key: HKCR\clsid\{d99f7670-7f1a-11ce-be57-00aa0051fe20}\inprocserver32
Creates key: HKLM\system\currentcontrolset\control\contentindex\language\french_french
Creates key: HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}
Creates key: HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}\inprocserver32
Creates key: HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}
Creates key: HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Creates key: HKLM\system\currentcontrolset\control\contentindex\language\german_german
Creates key: HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}
Creates key: HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}\inprocserver32
Creates key: HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}
Creates key: HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}\inprocserver32

Creates key:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian
Creates key: HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}
Creates key: HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}\inprocserver32
Creates key: HKCR\clsid\{6d36ce10-7f1c-11ce-be57-00aa0051fe20}
Creates key: HKCR\clsid\{6d36ce10-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Creates key:
HKLM\system\currentcontrolset\control\contentindex\language\swedish_default
Creates key: HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}
Creates key: HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32
Creates key: HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}
Creates key: HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Creates key:
HKLM\system\currentcontrolset\control\contentindex\language\spanish_modern
Creates key: HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}
Creates key: HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32
Creates key: HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}
Creates key: HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Creates key: HKLM\system\currentcontrolset\control\contentindex\language\dutch_dutch
Creates key: HKCR\clsid\{66b37110-8bf2-11ce-be59-00aa0051fe20}
Creates key: HKCR\clsid\{66b37110-8bf2-11ce-be59-00aa0051fe20}\inprocserver32
Creates key: HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}
Creates key: HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}\inprocserver32
Creates key: HKCR\.nws
Creates key: HKCR\microsoft internet news message
Creates key: HKCR\microsoft internet news message\clsid
Creates key: HKCR\clsid\{5645c8c0-e277-11cf-8fda-00aa00a14f93}
Creates key: HKCR\clsid\{5645c8c0-e277-11cf-8fda-00aa00a14f93}\persistenthandler
Creates key: HKCR\clsid\{5645c8c1-e277-11cf-8fda-
00aa00a14f93}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Creates key: HKCR\clsid\{5645c8c2-e277-11cf-8fda-00aa00a14f93}\inprocserver32
Creates key: HKCR\.eml
Creates key: HKCR\microsoft internet mail message
Creates key: HKCR\microsoft internet mail message\clsid
Creates key: HKCR\clsid\{5645c8c3-e277-11cf-8fda-00aa00a14f93}
Creates key: HKCR\clsid\{5645c8c3-e277-11cf-8fda-00aa00a14f93}\persistenthandler
Creates key: HKCR\clsid\{5645c8c4-e277-11cf-8fda-
00aa00a14f93}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Creates key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}
Creates key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\progid
Creates key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-
0090272fa362}\versionindependentprogid
Creates key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32
Creates key: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}
Creates key: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\progid
Creates key: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-
29634f378a42}\versionindependentprogid
Creates key: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\inprocserver32
Creates key: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}
Creates key: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\progid
Creates key: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-
7829d4f7e43b}\versionindependentprogid
Creates key: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\inprocserver32
Creates key: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}
Creates key: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\progid
Creates key: HKCR\clsid\{91870674-de84-4313-b07d-
a387415bb4f5}\versionindependentprogid
Creates key: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\inprocserver32
Creates key: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}
Creates key: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\progid
Creates key: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-
c4825abbe5cf}\versionindependentprogid
Creates key: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\inprocserver32
Creates key:
HKU\.default\software\microsoft\windows\currentversion\explorer\mountpoints2\c
Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key: HKU\.default\software\microsoft\windows\currentversion\shell
extensions\blocked
Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached
Creates key: HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached
Creates key: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
Creates key: HKU\.default\software\microsoft\windows\currentversion\explorer\shell
folders
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKLM\software\microsoft\wbem\cimom
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\35644f3d0029f81c3d478d3c2407fac3.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server

Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comdlg32.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\software\microsoft\windows nt\currentversion\image file execution options\odbc32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\odbcbcp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\pdh.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: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\system\setup
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\system\currentcontrolset\services\crypt32\performance
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\microsoft\bidinterface\loader
Opens key: HKLM\software\microsoft\mdac
Opens key: HKLM\software
Opens key: HKCU\software\odbc\odbc.ini\odbc
Opens key: HKLM\software\odbc\odbc.ini\odbc
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKLM\software\microsoft\rpc\pagedbuffers
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\35644f3d0029f81c3d478d3c2407fac3.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\microsoft\windows nt\currentversion\pdh
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\odbcint.dll
Opens key: HKLM\system\currentcontrolset\control\servicecurrent
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imagehlp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sfc_os.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\pstorec.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crtdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sfc.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
Opens key:
HKLM\software\microsoft\ctf\compatibility\35644f3d0029f81c3d478d3c2407fac3.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
Opens key: HKCU\software\microsoft\ctf
Opens key: HKLM\software\microsoft\ctf\systemshared
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cisvc.exe
Opens key: HKLM\system\wpa\tabletpc
Opens key: HKLM\system\wpa\mediacenter
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\query.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
Opens key: HKU\.default\software\policies\microsoft\control panel\desktop
Opens key: HKU\.default\control panel\desktop
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32
Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm
Opens key: HKLM\system\currentcontrolset\control\productoptions
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKU\.default\software\microsoft\windows\currentversion\thememanager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cisvc.exe\rpcthreadpoolthrottle

Opens key: HKLM\system\currentcontrolset\control\contentindex
Opens key: HKLM\system\currentcontrolset\control\contentindex\catalogs
Opens key: HKLM\system\currentcontrolset\control\contentindex\catalogs\system
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi.dll
Opens key: HKLM\system\currentcontrolset\control\minint
Opens key: HKLM\system\wpa\pnp
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
Opens key: HKLM\system\currentcontrolset\control\contentindex\catalogs\system\scopes
Opens key: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comres.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\clbcatq.dll
Opens key: HKLM\software\microsoft\com3\debug
Opens key: HKCU\software\classes\
Opens key: HKLM\software\classes
Opens key: HKU\
Opens key: HKCR\clsid
Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}
Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\treatas
Opens key: HKCR\
Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32
Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserverx86
Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\localserver32
Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprochandler32
Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprochandlerx86
Opens key: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\localserver
Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors\{f9ae8981-7e52-11d0-8964-00c04fd611d7}
Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors
Opens key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\inprocserver32
Opens key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\versionindependentprogid
Opens key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\progid
Opens key: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}
Opens key: HKCR\msidxs errorlookup\clsid
Opens key: HKCR\msidxs errorlookup
Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\ole db provider
Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\inprocserver32
Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\versionindependentprogid
Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\progid
Opens key: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}
Opens key: HKCR\msidxs\clsid
Opens key: HKCR\msidxs
Opens key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\inprocserver32
Opens key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\versionindependentprogid
Opens key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\progid
Opens key: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}
Opens key: HKLM\system\currentcontrolset\control
Opens key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprocserver32
Opens key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32
Opens key: HKCR\clsid\{08c524e0-89b0-11cf-88a1-00aa004b9986}
Opens key: HKCR\binaryfile
Opens key: HKCR\vxdfile
Opens key: HKCR\vxdfile\clsid
Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}
Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\clsid
Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}
Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\clsid
Opens key: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}
Opens key: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}\clsid
Opens key: HKCR\aifffile
Opens key: HKCR\aifffile\clsid
Opens key: HKCR\asffile
Opens key: HKCR\asffile\clsid
Opens key: HKCR\asxfile
Opens key: HKCR\asxfile\clsid
Opens key: HKCR\aufile
Opens key: HKCR\aufile\clsid
Opens key: HKCR\avifile
Opens key: HKCR\avifile\clsid
Opens key: HKCR\clsid\{00022602-0000-0000-c000-000000000046}
Opens key: HKCR\msbackupfile
Opens key: HKCR\msbackupfile\clsid
Opens key: HKCR\paint.picture
Opens key: HKCR\paint.picture\clsid
Opens key: HKCR\clsid\{d3e34b21-9d75-101a-8c3d-00aa001a1652}

Opens key: HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262}
Opens key: HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262}\clsid
Opens key: HKCR\cdafile
Opens key: HKCR\cdafile\clsid
Opens key: HKCR\comfile
Opens key: HKCR\comfile\clsid
Opens key: HKCR\cplfile
Opens key: HKCR\cplfile\clsid
Opens key: HKCR\curfile
Opens key: HKCR\curfile\clsid
Opens key: HKCR\dllfile
Opens key: HKCR\dllfile\clsid
Opens key: HKCR\drvfile
Opens key: HKCR\drvfile\clsid
Opens key: HKCR\emffile
Opens key: HKCR\emffile\clsid
Opens key: HKCR\exefile
Opens key: HKCR\exefile\clsid
Opens key: HKCR\fndfile
Opens key: HKCR\fndfile\clsid
Opens key: HKCR\fonfile
Opens key: HKCR\fonfile\clsid
Opens key: HKCR\giffile
Opens key: HKCR\giffile\clsid
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
Opens key: HKCR\icmfile
Opens key: HKCR\icmfile\clsid
Opens key: HKCR\icofile
Opens key: HKCR\icofile\clsid
Opens key: HKCR\ivffile
Opens key: HKCR\ivffile\clsid
Opens key: HKCR\pjpegfile
Opens key: HKCR\pjpegfile\clsid
Opens key: HKCR\jpegfile
Opens key: HKCR\jpegfile\clsid
Opens key: HKCR\mpegfile
Opens key: HKCR\mpegfile\clsid
Opens key: HKCR\m3ufile
Opens key: HKCR\m3ufile\clsid
Opens key: HKCR\midfile
Opens key: HKCR\midfile\clsid
Opens key: HKCR\clsid\{00022603-0000-0000-c000-000000000046}
Opens key: HKCR\mp3file
Opens key: HKCR\mp3file\clsid
Opens key: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}
Opens key: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}\clsid
Opens key: HKCR\ocxfile
Opens key: HKCR\ocxfile\clsid
Opens key: HKCR\perffile
Opens key: HKCR\perffile\clsid
Opens key: HKCR\pngfile
Opens key: HKCR\pngfile\clsid
Opens key: HKCR\sysfile
Opens key: HKCR\sysfile\clsid
Opens key: HKCR\tifimage.document
Opens key: HKCR\tifimage.document\clsid
Opens key: HKCR\ttcfile
Opens key: HKCR\ttcfile\clsid
Opens key: HKCR\ttffile
Opens key: HKCR\ttffile\clsid
Opens key: HKCR\soundrec
Opens key: HKCR\soundrec\clsid
Opens key: HKCR\clsid\{00020c01-0000-0000-c000-000000000046}
Opens key: HKCR\waxfile
Opens key: HKCR\waxfile\clsid
Opens key: HKCR\wmafile
Opens key: HKCR\wmafile\clsid
Opens key: HKCR\wmffile
Opens key: HKCR\wmffile\clsid
Opens key: HKCR\wmvfile
Opens key: HKCR\wmvfile\clsid
Opens key: HKCR\wmzfile
Opens key: HKCR\wmzfile\clsid
Opens key: HKCR\wvxfile
Opens key: HKCR\wvxfile\clsid
Opens key: HKCR\.xbm
Opens key: HKCR\.xbm\clsid
Opens key: HKCR\compressedfolder
Opens key: HKCR\compressedfolder\clsid
Opens key: HKCR\clsid\{e88dcce0-b7b3-11d1-a9f0-00aa0060fa31}
Opens key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32
Opens key: HKCR\clsid\{89bcb7a4-6119-101a-bcb7-00dd010655af}
Opens key: HKCR\clsid\{89bcb7a5-6119-101a-bcb7-00dd010655af}

Opens key: HKCR\clsid\{89bcb7a6-6119-101a-bcb7-00dd010655af}
Opens key: HKCR\clsid\{961c1130-89ad-11cf-88a1-00aa004b9986}
Opens key: HKCR\clsid\{8c9e8e1c-90f0-11d1-ba0f-00a0c906b239}
Opens key: HKCR\clsid\{95876eb0-90f0-11d1-ba0f-00a0c906b239}
Opens key: HKCR\clsid\{9e704f44-90f0-11d1-ba0f-00a0c906b239}
Opens key: HKCR\clsid\{9ed4692c-90f0-11d1-ba0f-00a0c906b239}
Opens key: HKCR\clsid\{87db1ada-aa39-11d1-829f-00a0c906b239}
Opens key: HKCR\plaintext
Opens key: HKCR\batfile
Opens key: HKCR\batfile\clsid
Opens key: HKCR\cmdfile
Opens key: HKCR\cmdfile\clsid
Opens key: HKCR\idqfile
Opens key: HKCR\inifile
Opens key: HKCR\inifile\clsid
Opens key: HKCR\inxfile
Opens key: HKCR\regfile
Opens key: HKCR\regfile\clsid
Opens key: HKCR\inffile
Opens key: HKCR\inffile\clsid
Opens key: HKCR\vbsfile
Opens key: HKCR\vbsfile\clsid
Opens key: HKCR\asmfile
Opens key: HKCR\cfile
Opens key: HKCR\cppfile
Opens key: HKCR\cxxfile
Opens key: HKCR\deffile
Opens key: HKCR\hfile
Opens key: HKCR\hppfile
Opens key: HKCR\hxxfile
Opens key: HKCR\idlfile
Opens key: HKCR\incfile
Opens key: HKCR\jsfile
Opens key: HKCR\jsfile\clsid
Opens key: HKCR\logfile
Opens key: HKCR\plfile
Opens key: HKCR\rcfile
Opens key: HKCR\rtffile
Opens key: HKCR\rtffile\clsid
Opens key: HKCR\clsid\{73fddc80-aea9-101a-98a7-00aa00374959}
Opens key: HKCR\urlfile
Opens key: HKCR\xmlfile
Opens key: HKCR\xmlfile\clsid
Opens key: HKCR\clsid\{48123bc4-99d9-11d1-a6b3-00c04fd91555}
Opens key: HKCR\xlsfile
Opens key: HKCR\txtfile
Opens key: HKCR\txtfile\clsid
Opens key: HKCR\wordview.rtf.8
Opens key: HKCR\wordview.rtf.8\clsid
Opens key: HKCR\internetshortcut
Opens key: HKCR\internetshortcut\clsid
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}
Opens key: HKCR\xslfile
Opens key: HKCR\xslfile\clsid
Opens key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserver32
Opens key: HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}\inprocserver32
Opens key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprocserver32
Opens key: HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ciadmin.dll
Opens key: HKLM\software\microsoft\mmc\snapins
Opens key: HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-00aa004b9986}
Opens key: HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\nodetypes
Opens key: HKLM\software\microsoft\mmc\nodetypes
Opens key: HKLM\software\microsoft\mmc\nodetypes\{5401e3e9-f5f6-11d1-b4f7-00c04fc2db8d}
Opens key: HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-00c04fd8d5b0}
Opens key: HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-00c04fd8d5b0}\extensions
Opens key: HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-00c04fd8d5b0}\extensions\namespace
Opens key: HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-00c04fd8d5b0}\dynamic extensions
Opens key: HKLM\system\currentcontrolset\control\
Opens key: HKLM\system\currentcontrolset\control\server applications
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ixsso.dll
Opens key: HKCR\typelib
Opens key: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}
Opens key: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0

Opens key: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\flags
Opens key: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\409
Opens key: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\409\win32
Opens key: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\helpdir
Opens key: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}
Opens key: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\proxystubclsid
Opens key: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\proxystubclsid32
Opens key: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\typelib
Opens key: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}
Opens key: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\proxystubclsid
Opens key: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\proxystubclsid32
Opens key: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\typelib
Opens key: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}
Opens key: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\proxystubclsid
Opens key: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\proxystubclsid32
Opens key: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\typelib
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\nlhtml.dll
Opens key: HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{7f73b8f6-c19c-11d0-aa66-00c04fc2eddc}
Opens key: HKCR\clsid\{bd70c020-2d24-11d0-9110-00004c752752}
Opens key: HKCR\clsid\{ffb10349-5267-4c96-8ad7-01b52a2de434}
Opens key: HKCR\clsid\{ea2510f-12f5-4460-a10a-19e48fff1da5}
Opens key: HKCR\odcfile
Opens key: HKCR\odcfile\clsid
Opens key: HKCR\hhcfile
Opens key: HKCR\htmlfile
Opens key: HKCR\htmlfile\clsid
Opens key: HKCR\asp_auto_file
Opens key: HKCR\aspxfile
Opens key: HKCR\ascxfile
Opens key: HKCR\cssfile
Opens key: HKCR\cssfile\clsid
Opens key: HKCR\htafile
Opens key: HKCR\htafile\clsid
Opens key: HKCR\clsid\{3050f4d8-98b5-11cf-bb82-00aa00bdce0b}
Opens key: HKCR\httfile
Opens key: HKCR\httfile\clsid
Opens key: HKCR\aspfile
Opens key: HKCR\aspfile\clsid
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\offfilt.dll
Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32
Opens key: HKCR\word.document.8
Opens key: HKCR\word.document.8\clsid
Opens key: HKCR\word.template.8
Opens key: HKCR\powerpoint.template.8
Opens key: HKCR\powerpoint.template.8\clsid
Opens key: HKCR\powerpoint.show.8
Opens key: HKCR\powerpoint.show.8\clsid
Opens key: HKCR\powerpoint.slideshow.8
Opens key: HKCR\powerpoint.slideshow.8\clsid
Opens key: HKCR\excel.sheet.8
Opens key: HKCR\excel.sheet.8\clsid
Opens key: HKCR\excel.chart.8
Opens key: HKCR\excel.template.8
Opens key: HKCR\word.document.6
Opens key: HKCR\word.template
Opens key: HKCR\powerpoint.show.7
Opens key: HKCR\powerpoint.template
Opens key: HKCR\excel.chart.5
Opens key: HKCR\excel.sheet.5
Opens key: HKCR\wordview.document.8
Opens key: HKCR\wordview.document.8\clsid
Opens key: HKCR\wordview.template.8
Opens key: HKCR\wordview.template.8\clsid
Opens key: HKCR\powerpointviewer.template.11
Opens key: HKCR\powerpointviewer.template.11\clsid
Opens key: HKCR\powerpointviewer.show.11
Opens key: HKCR\powerpointviewer.show.11\clsid
Opens key: HKCR\powerpointviewer.slideshow.11
Opens key: HKCR\powerpointviewer.slideshow.11\clsid
Opens key: HKCR\excelviewer.sheet.8
Opens key: HKCR\excelviewer.sheet.8\clsid
Opens key: HKCR\excelviewer.template.8
Opens key: HKCR\excelviewer.template.8\clsid
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ciodm.dll
Opens key: HKCR\microsoft.isadm.1
Opens key: HKCR\microsoft.isadm.1\clsid
Opens key: HKCR\microsoft.isadm
Opens key: HKCR\microsoft.isadm\curver
Opens key: HKCR\microsoft.isadm\clsid

Opens key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}
Opens key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
Opens key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\progid
Opens key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\programmable
Opens key: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid
Opens key: HKCR\microsoft.iscatadm.1
Opens key: HKCR\microsoft.iscatadm.1\clsid
Opens key: HKCR\microsoft.iscatadm
Opens key: HKCR\microsoft.iscatadm\curver
Opens key: HKCR\microsoft.iscatadm\clsid
Opens key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}
Opens key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
Opens key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\progid
Opens key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\programmable
Opens key: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid
Opens key: HKCR\microsoft.isscopeadm.1
Opens key: HKCR\microsoft.isscopeadm.1\clsid
Opens key: HKCR\microsoft.isscopeadm
Opens key: HKCR\microsoft.isscopeadm\curver
Opens key: HKCR\microsoft.isscopeadm\clsid
Opens key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}
Opens key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32
Opens key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\progid
Opens key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\programmable
Opens key: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid
Opens key: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}
Opens key: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0
Opens key: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\flags
Opens key: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\0
Opens key: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\0\win32
Opens key: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\helpdir
Opens key: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}
Opens key: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid
Opens key: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid32
Opens key: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\typelib
Opens key: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}
Opens key: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid
Opens key: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid32
Opens key: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}\typelib
Opens key: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}
Opens key: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid
Opens key: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid32
Opens key: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\typelib
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\infosoft.dll
Opens key: HKCR\clsid\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{d99f7670-7f1a-11ce-be57-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}\inprocserver32
Opens key: HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}\inprocserver32
Opens key: HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}\inprocserver32
Opens key: HKCR\clsid\{6d36ce10-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32
Opens key: HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32
Opens key: HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{66b37110-8bf2-11ce-be59-00aa0051fe20}\inprocserver32
Opens key: HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mimefilt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\langwrbk.dll
Opens key: HKCR\enguswrdbrk.enguswrdbrk.1
Opens key: HKCR\enguswrdbrk.enguswrdbrk.1\clsid
Opens key: HKCR\enguswrdbrk.enguswrdbrk
Opens key: HKCR\enguswrdbrk.enguswrdbrk\curver
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\progid
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\versionindependentprogid
Opens key: HKCR\engukwrdbrk.engukwrdbrk.1
Opens key: HKCR\engukwrdbrk.engukwrdbrk.1\clsid
Opens key: HKCR\engukwrdbrk.engukwrdbrk
Opens key: HKCR\engukwrdbrk.engukwrdbrk\curver
Opens key: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}
Opens key: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\inprocserver32
Opens key: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\progid
Opens key: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-

29634f378a42}\versionindependentprogid
Opens key: HKCR\frnfrnwrdbrk.frnfrnwrdbrk.1
Opens key: HKCR\frnfrnwrdbrk.frnfrnwrdbrk.1\clsid
Opens key: HKCR\frnfrnwrdbrk.frnfrnwrdbrk
Opens key: HKCR\frnfrnwrdbrk.frnfrnwrdbrk\curver
Opens key: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}
Opens key: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\inprocserver32
Opens key: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\progid
Opens key: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-
7829d4f7e43b}\versionindependentprogid
Opens key: HKCR\itlitlwrdbrk.itlitlwrdbrk.1
Opens key: HKCR\itlitlwrdbrk.itlitlwrdbrk.1\clsid
Opens key: HKCR\itlitlwrdbrk.itlitlwrdbrk
Opens key: HKCR\itlitlwrdbrk.itlitlwrdbrk\curver
Opens key: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}
Opens key: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\inprocserver32
Opens key: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\progid
Opens key: HKCR\clsid\{91870674-de84-4313-b07d-
a387415bb4f5}\versionindependentprogid
Opens key: HKCR\spnmdrwrdbrk.spnmdrwrdbrk.1
Opens key: HKCR\spnmdrwrdbrk.spnmdrwrdbrk.1\clsid
Opens key: HKCR\spnmdrwrdbrk.spnmdrwrdbrk
Opens key: HKCR\spnmdrwrdbrk.spnmdrwrdbrk\curver
Opens key: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}
Opens key: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\inprocserver32
Opens key: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\progid
Opens key: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-
c4825abbe5cf}\versionindependentprogid
Opens key: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}
Opens key: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0
Opens key: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\flags
Opens key: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\0
Opens key: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\0\win32
Opens key: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\helpdir
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\samlib.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
Opens key: HKLM\system\currentcontrolset\services\ldap
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntmarta.dll
Opens key: HKLM\system\currentcontrolset\services\contentindex\performance
Opens key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}
Opens key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\treatas
Opens key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprocserverx86
Opens key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\localserver32
Opens key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprochandler32
Opens key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprochandlerx86
Opens key: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\localserver
Opens key:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system\properties
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\system\currentcontrolset
Opens key: HKLM\system\currentcontrolset\services\rdpnp\networkprovider
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider
Opens key: HKLM\system\currentcontrolset\services\webclient\networkprovider
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\drprov.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netui0.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\network\world full
access shared parameters
Opens key: HKU\.default\control panel\international
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netrap.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netui1.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntlanman.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\davclnt.dll
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cidaemon.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cidaemon.exe
Opens key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}
Opens key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\treatas
Opens key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprocserverx86
Opens key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\localserver32
Opens key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprochandler32
Opens key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprochandlerx86
Opens key: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\localserver
Opens key: HKLM\system\currentcontrolset\control\contentindex\language
Opens key: HKLM\system\currentcontrolset\control\contentindex\language\dutch_dutch
Opens key: HKLM\system\currentcontrolset\control\contentindex\language\english_uk
Opens key: HKLM\system\currentcontrolset\control\contentindex\language\english_us
Opens key: HKLM\system\currentcontrolset\control\contentindex\language\french_french
Opens key: HKLM\system\currentcontrolset\control\contentindex\language\german_german
Opens key: HKLM\system\currentcontrolset\control\contentindex\language\italian_italian
Opens key: HKLM\system\currentcontrolset\control\contentindex\language\neutral
Opens key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}
Opens key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\treatas
Opens key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserverx86
Opens key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\localserver32
Opens key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprochandler32
Opens key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprochandlerx86
Opens key: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\localserver
Opens key: HKLM\software\microsoft\security center\svc
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-befc77a11a1e}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-2f83217002ff}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-4ee8-baa9-00bcb3d54227}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-5f2748764d10}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-0000000ff1ce}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-0150048383c9}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-0000000ff1ce}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-3813-a88d-b8dccde8f8c7}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-3f2d-899a-6a1d67f2073f}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-4027-b136-2b3e1f5ab6e2}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-36ca-84d3-9f4dcf5c5bd9}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-36ca-84d3-9f4dcf5c5bd9}.kb953595
Opens key: HKCR\.ini\persistenthandler
Opens key: HKCR\clsid\{5e941d80-bf96-11cd-b579-08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Opens key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}
Opens key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\treatas
Opens key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserverx86
Opens key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\localserver32
Opens key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprochandler32
Opens key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprochandlerx86
Opens key: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\localserver
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKU\.default\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cidaemon.exe\rpcthreadpoolthrottle
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
Opens key: HKCR\directory
Opens key: HKCR\directory\curver
Opens key: HKCR\directory\
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer

Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\
Opens key: HKU\.default\software\microsoft\internet explorer\desktop\scheme
Opens key: HKU\.default\software\microsoft\internet explorer\desktop\components
Opens key:
HKU\.default\software\microsoft\windows\currentversion\explorer\startmenu\startpanel
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\startmenu\startpanel
Opens key: HKU\.default\software\microsoft\windows\currentversion\policies\system
Opens key: HKCR\directory\shellex\iconhandler
Opens key: HKCR\directory\clsid
Opens key: HKCR\folder
Opens key: HKCR\folder\clsid
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\fileexts
Opens key: HKCR\.ini
Opens key: HKCR\inifile\curver
Opens key: HKCR\inifile\
Opens key: HKCR\inifile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.ini
Opens key: HKCR*
Opens key: HKCR*\clsid
Opens key: HKCR\inifile\shellex\propertyhandler
Opens key: HKCR\.ini\shellex\propertyhandler
Opens key: HKCR*\shellex\propertyhandler
Opens key: HKCR\.sam\persistenthandler
Opens key: HKCR\.sam
Opens key: HKCR\.sam\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.sam
Opens key: HKCR\.sam\clsid
Opens key: HKCR\.sam\shellex\propertyhandler
Opens key: HKCR\.xls\persistenthandler
Opens key: HKCR\clsid\{98de59a0-d175-11cd-a7bd-
00006b827d94}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}
Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\treatas
Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserverx86
Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\localserver32
Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprochandler32
Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprochandlerx86
Opens key: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\localserver
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\treatas
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserverx86
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\localserver32
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprochandler32
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprochandlerx86
Opens key: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\localserver
Opens key: HKCR\.xls
Opens key: HKCR\excelviewer.sheet.8\curver
Opens key: HKCR\excelviewer.sheet.8\
Opens key: HKCR\excelviewer.sheet.8\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.xls
Opens key: HKCR\systemfileassociations\.xls\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.xls\clsid
Opens key: HKCR\excelviewer.sheet.8\shellex\propertyhandler
Opens key: HKCR\.xls\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\.xls\shellex\propertyhandler
Opens key: HKCR\.wk4\persistenthandler
Opens key: HKCR\.wk4
Opens key: HKCR\.wk4\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wk4
Opens key: HKCR\.wk4\clsid
Opens key: HKCR\.wk4\shellex\propertyhandler
Opens key: HKCR\.ppt\persistenthandler
Opens key: HKCR\.shw\persistenthandler
Opens key: HKCR\.shw
Opens key: HKCR\.shw\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.shw
Opens key: HKCR\.shw\clsid
Opens key: HKCR\.shw\shellex\propertyhandler
Opens key: HKCR\.wb2\persistenthandler
Opens key: HKCR\.wb2
Opens key: HKCR\.wb2\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wb2
Opens key: HKCR\.wb2\clsid
Opens key: HKCR\.wb2\shellex\propertyhandler
Opens key: HKCR\.wav\persistenthandler
Opens key: HKCR\clsid\{098f2470-bae0-11cd-b579-
08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Opens key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}
Opens key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\treatas
Opens key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserverx86
Opens key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\localserver32
Opens key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprochandler32
Opens key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprochandlerx86

Opens key: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\localserver
Opens key: HKCR\.wav
Opens key: HKCR\soundrec\curver
Opens key: HKCR\soundrec\
Opens key: HKCR\soundrec\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wav
Opens key: HKCR\systemfileassociations\.wav\shellex\iconhandler
Opens key: HKCR\systemfileassociations\audio
Opens key: HKCR\systemfileassociations\audio\shellex\iconhandler
Opens key: HKCR\clsid\{00020c01-0000-0000-c000-000000000046}\implemented categories\{00021490-0000-0000-c000-000000000046}
Opens key: HKCR\soundrec\shellex\propertyhandler
Opens key: HKCR\.wav\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\.wav\shellex\propertyhandler
Opens key: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\verclsid.exe
Opens key: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}
Opens key: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\treatas
Opens key: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprocserverx86
Opens key: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\localserver32
Opens key: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprochandler32
Opens key: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprochandlerx86
Opens key: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvfw32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\avifil32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shmedia.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\vfw
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\shmedia.dll
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{e4b29f9d-d390-480b-92fd-7ddb47101d71}
Opens key: HKCR\.doc\persistenthandler
Opens key: HKCR\.doc
Opens key: HKCR\wordview.document.8\curver
Opens key: HKCR\wordview.document.8\
Opens key: HKCR\wordview.document.8\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.doc
Opens key: HKCR\systemfileassociations\.doc\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.doc\clsid
Opens key: HKCR\wordview.document.8\shellex\propertyhandler
Opens key: HKCR\.doc\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\.doc\shellex\propertyhandler
Opens key: HKCR\.wpd\persistenthandler
Opens key: HKCR\.wpd
Opens key: HKCR\.wpd\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wpd
Opens key: HKCR\.wpd\clsid
Opens key: HKCR\.wpd\shellex\propertyhandler
Opens key: HKCR\.wpg\persistenthandler
Opens key: HKCR\.wpg
Opens key: HKCR\.wpg\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wpg
Opens key: HKCR\.wpg\clsid
Opens key: HKCR\.wpg\shellex\propertyhandler
Opens key: HKCR\.lnk\persistenthandler
Opens key: HKCR\.lnk
Opens key: HKCR\lnkfile\clsid
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\persistenthandler
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserver32
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\treatas
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserverx86
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\localserver32
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprochandler32
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprochandlerx86
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\localserver
Opens key: HKCR\appid\cidaemon.exe
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKCR\interface\{0000010b-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{0000010b-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\linkinfo.dll
Opens key: HKCR\network\sharinghandler
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntshrui.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\xpsp2res.dll
Opens key: HKCR\.exe
Opens key: HKCR\exefile\curver
Opens key: HKCR\exefile\
Opens key: HKCR\exefile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.exe
Opens key: HKCR\systemfileassociations\application
Opens key: HKCR\interface\{89bcb740-6119-101a-bcb7-00dd010655af}
Opens key: HKCR\lnkfile
Opens key: HKCR\lnkfile\curver
Opens key: HKCR\lnkfile\
Opens key: HKCR\lnkfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.lnk
Opens key: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\implemented
categories\{00021490-0000-0000-c000-000000000046}
Opens key: HKCR\lnkfile\shellex\propertyhandler
Opens key: HKCR\.lnk\shellex\propertyhandler
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-
a2ea-08002b30309d}
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ieframe.dll
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
Opens key: HKLM\software\microsoft\internet explorer\setup
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
Opens key: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32
Opens key: HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
Opens key: HKCR\.zfsendtotarget
Opens key: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}\curver
Opens key: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}\
Opens key: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.zfsendtotarget
Opens key: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-
00c04fd7d062}\shellex\propertyhandler
Opens key: HKCR\.zfsendtotarget\shellex\propertyhandler
Opens key: HKCR\drive\shellex\folderextensions
Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
Opens key: HKCR\.ico
Opens key: HKCR\icofile\curver
Opens key: HKCR\icofile\
Opens key: HKCR\icofile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.ico
Opens key: HKCR\systemfileassociations\image
Opens key: HKCR\systemfileassociations\image\shellex\iconhandler
Opens key: HKCR\systemfileassociations\image\clsid
Opens key: HKCR\.chm
Opens key: HKCR\chm.file
Opens key: HKCR\chm.file\curver
Opens key: HKCR\chm.file\
Opens key: HKCR\chm.file\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.chm
Opens key: HKCR\chm.file\clsid
Opens key: HKCR\.msc
Opens key: HKCR\mscfile
Opens key: HKCR\mscfile\curver
Opens key: HKCR\mscfile\
Opens key: HKCR\mscfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.msc
Opens key: HKCR\mscfile\clsid
Opens key: HKCR\.cpl
Opens key: HKCR\cplfile\curver
Opens key: HKCR\cplfile\
Opens key: HKCR\cplfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.cpl
Opens key: HKCR\.desklink\persistenthandler
Opens key: HKCR\.desklink
Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\curver
Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\

Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.desklink
Opens key: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}\shellex\propertyhandler
Opens key: HKCR\.desklink\shellex\propertyhandler
Opens key: HKCR\.mapimail\persistenthandler
Opens key: HKCR\.mapimail
Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\curver
Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\
Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.mapimail
Opens key: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}\shellex\propertyhandler
Opens key: HKCR\.mapimail\shellex\propertyhandler
Opens key: HKCR\.dat\persistenthandler
Opens key: HKCR\.dat
Opens key: HKCR\.dat\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.dat
Opens key: HKCR\.dat\clsid
Opens key: HKCR\.dat\shellex\propertyhandler
Opens key: HKCR\.pol\persistenthandler
Opens key: HKCR\.pol
Opens key: HKCR\systemfileassociations\.pol
Opens key: HKCR\.jpg\persistenthandler
Opens key: HKCR\.jpg
Opens key: HKCR\jpegfile\curver
Opens key: HKCR\jpegfile\
Opens key: HKCR\jpegfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.jpg
Opens key: HKCR\systemfileassociations\.jpg\shellex\iconhandler
Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046}
Opens key: HKCR\jpegfile\shellex\propertyhandler
Opens key: HKCR\.jpg\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\.jpg\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\image\shellex\propertyhandler
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserver32
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\treatas
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserverx86
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\localserver32
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprochandler32
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprochandlerx86
Opens key: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdiplus.dll
Opens key: HKCR\.wpl\persistenthandler
Opens key: HKCR\.wpl
Opens key: HKCR\wplfile\clsid
Opens key: HKCR\wplfile
Opens key: HKCR\wplfile\curver
Opens key: HKCR\wplfile\
Opens key: HKCR\wplfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wpl
Opens key: HKCR\systemfileassociations\.wpl\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wpl\clsid
Opens key: HKCR\wplfile\shellex\propertyhandler
Opens key: HKCR\.wpl\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\.wpl\shellex\propertyhandler
Opens key: HKCR\.wma\persistenthandler
Opens key: HKCR\.wma
Opens key: HKCR\wmafile\curver
Opens key: HKCR\wmafile\
Opens key: HKCR\wmafile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wma
Opens key: HKCR\systemfileassociations\.wma\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.wma\clsid
Opens key: HKCR\systemfileassociations\audio\clsid
Opens key: HKCR\wmafile\shellex\propertyhandler
Opens key: HKCR\.wma\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\.wma\shellex\propertyhandler
Opens key: HKCR\clsid\{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}\inprocserver32
Opens key: HKCR\.lic\persistenthandler
Opens key: HKCR\.lic
Opens key: HKCR\systemfileassociations\.lic
Opens key: HKCR\.sst\persistenthandler
Opens key: HKCR\.sst
Opens key: HKCR\certificatestorefile\clsid
Opens key: HKCR\certificatestorefile
Opens key: HKCR\certificatestorefile\curver
Opens key: HKCR\certificatestorefile\
Opens key: HKCR\certificatestorefile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.sst

Opens key: HKCR\certificatestorefile\shellex\propertyhandler
Opens key: HKCR\.sst\shellex\propertyhandler
Opens key: HKCR\.mydocs\persistenthandler
Opens key: HKCR\.mydocs
Opens key: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}\curver
Opens key: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}\
Opens key: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.mydocs
Opens key: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}\shellex\propertyhandler
Opens key: HKCR\.mydocs\shellex\propertyhandler
Opens key: HKCR\.url\persistenthandler
Opens key: HKCR\clsid\{8cd34779-9f10-4f9b-adfb-b3faeabdab5a}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}
Opens key: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\inprocserver32
Opens key: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}
Opens key: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\treatas
Opens key: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\inprocserverx86
Opens key: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\localserver32
Opens key: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\inprochandler32
Opens key: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\inprochandlerx86
Opens key: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\localserver
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\treatas
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserver32
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserverx86
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\localserver32
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprochandler32
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprochandlerx86
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\localserver
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\treatas
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserver32
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserverx86
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\localserver32
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprochandler32
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprochandlerx86
Opens key: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\localserver
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\initpropertybag
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKU\.default\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKU\.default\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_urlfile_cacheflush_kb936881
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll
Opens key: HKCR\protocols\name-space handler\
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKU\.default\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\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: HKU\.default\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKU\.default\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKU\.default\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\treatas
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserver32
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserverx86

Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\localserver32
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprochandler32
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprochandlerx86
Opens key: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\localserver
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\treatas
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserver32
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserverx86
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\localserver32
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprochandler32
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprochandlerx86
Opens key: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\localserver
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}
Opens key: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2
Opens key: HKCR\.url
Opens key: HKCR\internetshortcut\curver
Opens key: HKCR\internetshortcut\
Opens key: HKCR\internetshortcut\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.url
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\implemented categories\{00021490-0000-0000-c000-000000000046}
Opens key: HKCR\internetshortcut\shellex\propertyhandler
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprocserver32
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\treatas
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprocserverx86
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\localserver32
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprochandler32
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprochandlerx86
Opens key: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\localserver
Opens key: HKCR\appid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}
Opens key: HKCR\.txt\persistenthandler
Opens key: HKCR\.txt
Opens key: HKCR\txtfile\curver
Opens key: HKCR\txtfile\
Opens key: HKCR\txtfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.txt
Opens key: HKCR\systemfileassociations\text
Opens key: HKCR\systemfileassociations\text\shellex\iconhandler
Opens key: HKCR\systemfileassociations\text\clsid
Opens key: HKCR\txtfile\shellex\propertyhandler
Opens key: HKCR\.txt\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\text\shellex\propertyhandler
Opens key: HKCR\.bat\persistenthandler
Opens key: HKCR\.bat
Opens key: HKCR\batfile\curver
Opens key: HKCR\batfile\
Opens key: HKCR\batfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.bat
Opens key: HKCR\batfile\shellex\propertyhandler
Opens key: HKCR\.bat\shellex\propertyhandler
Opens key: HKCR\.sys\persistenthandler
Opens key: HKCR\.sys
Opens key: HKCR\sysfile\curver
Opens key: HKCR\sysfile\
Opens key: HKCR\sysfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.sys
Opens key: HKCR\sysfile\shellex\propertyhandler
Opens key: HKCR\.sys\shellex\propertyhandler
Opens key: HKCR\.log\persistenthandler
Opens key: HKCR\.log
Opens key: HKCR\systemfileassociations\.log
Opens key: HKCR\.log\shellex\propertyhandler
Opens key: HKCR\.com\persistenthandler
Opens key: HKCR\.com
Opens key: HKCR\comfile\curver
Opens key: HKCR\comfile\
Opens key: HKCR\comfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.com
Opens key: HKCR\comfile\shellex\propertyhandler
Opens key: HKCR\.com\shellex\propertyhandler
Opens key: HKCR\.\persistenthandler
Opens key: HKCR\.
Opens key: HKCR\.bmp\persistenthandler
Opens key: HKCR\.bmp
Opens key: HKCR\paint.picture\curver
Opens key: HKCR\paint.picture\
Opens key: HKCR\paint.picture\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.bmp
Opens key: HKCR\systemfileassociations\.bmp\shellex\iconhandler
Opens key: HKCR\clsid\{d3e34b21-9d75-101a-8c3d-00aa001a1652}\implemented categories\{00021490-0000-0000-c000-000000000046}

Opens key: HKCR\paint.picture\shellex\propertyhandler
Opens key: HKCR\.bmp\shellex\propertyhandler
Opens key: HKCR\systemfileassociations\.bmp\shellex\propertyhandler
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\wsock32.dll
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wbemcomn.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wbemprox.dll
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandlerx86
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
Opens key: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\appid\cisvc.exe
Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32
Opens key: HKCR\.exe\persistenthandler
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wbemsvc.dll
Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32
Opens key: HKCR\exefile\shellex\propertyhandler
Opens key: HKCR\.exe\shellex\propertyhandler
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserverx86
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandlerx86
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver
Opens key: HKCR\.scf\persistenthandler
Opens key: HKCR\.scf
Opens key: HKCR\shcmdfile\clsid
Opens key: HKCR\clsid\{57651662-ce3e-11d0-8d77-00c04fc99d61}\persistenthandler
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcp60.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKCR\shcmdfile
Opens key: HKCR\shcmdfile\curver
Opens key: HKCR\shcmdfile\
Opens key: HKCR\shcmdfile\shellex\iconhandler
Opens key: HKCR\systemfileassociations\.scf
Opens key: HKCR\clsid\{57651662-ce3e-11d0-8d77-00c04fc99d61}\implemented categories\{00021490-0000-0000-c000-000000000046}
Opens key: HKCR\shcmdfile\shellex\propertyhandler
Opens key: HKCR\.scf\shellex\propertyhandler
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\fastprox.dll
Opens key: HKLM\software\microsoft\wbem\cimom
Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver
Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32
Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32
Opens key: HKCR\.bak\persistenthandler
Opens key: HKCR\.bak
Opens key: HKCR\systemfileassociations\.bak
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: 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\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winrnr.dll
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
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[35644f3d0029f81c3d478d3c2407fac3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[35644f3d0029f81c3d478d3c2407fac3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\currentcontrolset\control\servicecurrent[]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[cisvc]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cisvc]
Queries value: HKU\.default\control panel\desktop[multiuilanguageid]
Queries value: HKU\.default\control panel\desktop[smoothscroll]
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: HKU\.default\software\microsoft\multimedia\audio[systemformats]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.imaadpcm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msadpcm]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg711]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msgsm610]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.trspch]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg723]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.sl_anet]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
Queries value: HKU\.default\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
Queries value: HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00[priority1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[personal]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local settings]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
Queries value:
HKU\.default\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKU\.default\control panel\desktop[lamebuttontext]
Queries value: HKLM\system\currentcontrolset\control\contentindex[donotstartcisvc]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[cataloginactive]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[location]
Queries value: HKLM\system\wpa\pnp[seed]
Queries value: HKLM\system\setup[osloaderpath]
Queries value: HKLM\system\setup[systempartition]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[mountremovablecatalogs]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxcachedpipes]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxsimultaneousrequests]
Queries value: HKLM\system\currentcontrolset\control\contentindex[requesttimeout]
Queries value: HKLM\system\currentcontrolset\control\contentindex[minimizeworkingset]
Queries value: HKLM\system\currentcontrolset\control\contentindex[minclientidletime]
Queries value: HKLM\system\currentcontrolset\control\contentindex[startupdelay]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxactiverequestthreads]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[minidlerequestthreads]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKCR\clsid\{2a488070-6fd9-11d0-a808-
00a0c906241a}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32[]
Queries value: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}[appid]
Queries value: HKCR\clsid\{2a488070-6fd9-11d0-a808-
00a0c906241a}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\control\contentindex[dllstoregister]
Queries value: HKCR\.386[]
Queries value: HKCR\.audiocd[]
Queries value: HKCR\.desklink[]
Queries value: HKCR\.folder[]

Queries value: HKCR\.mapimail[]
Queries value: HKCR\.zfsendtotarget[]
Queries value: HKCR\.aif[]
Queries value: HKCR\.aifc[]
Queries value: HKCR\.aiff[]
Queries value: HKCR\.aps[]
Queries value: HKCR\.asf[]
Queries value: HKCR\.asx[]
Queries value: HKCR\.au[]
Queries value: HKCR\.avi[]
Queries value: HKCR\avifile\clsid[]
Queries value: HKCR\.bin[]
Queries value: HKCR\.bkf[]
Queries value: HKCR\.bmp[]
Queries value: HKCR\paint.picture\clsid[]
Queries value: HKCR\.bsc[]
Queries value: HKCR\.cab[]
Queries value: HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262}\clsid[]
Queries value: HKCR\.cda[]
Queries value: HKCR\.cgm[]
Queries value: HKCR\.com[]
Queries value: HKCR\.cpl[]
Queries value: HKCR\.cur[]
Queries value: HKCR\.dbg[]
Queries value: HKCR\.dct[]
Queries value: HKCR\.dib[]
Queries value: HKCR\.dl_[]
Queries value: HKCR\.dll[]
Queries value: HKCR\.drv[]
Queries value: HKCR\.dvd[]
Queries value: HKCR\.emf[]
Queries value: HKCR\.eps[]
Queries value: HKCR\.ex_[]
Queries value: HKCR\.exe[]
Queries value: HKCR\.exp[]
Queries value: HKCR\.eyb[]
Queries value: HKCR\.fnd[]
Queries value: HKCR\.fnt[]
Queries value: HKCR\.fon[]
Queries value: HKCR\.ghi[]
Queries value: HKCR\.gif[]
Queries value: HKCR\giffile\clsid[]
Queries value: HKCR\.gz[]
Queries value: HKCR\.hqx[]
Queries value: HKCR\.icm[]
Queries value: HKCR\.ico[]
Queries value: HKCR\.idb[]
Queries value: HKCR\.ilk[]
Queries value: HKCR\.imc[]
Queries value: HKCR\.in_[]
Queries value: HKCR\.inv[]
Queries value: HKCR\.ivf[]
Queries value: HKCR\.jbf[]
Queries value: HKCR\.jfif[]
Queries value: HKCR\pjpegfile\clsid[]
Queries value: HKCR\.jpe[]
Queries value: HKCR\jpegfile\clsid[]
Queries value: HKCR\.jpeg[]
Queries value: HKCR\.jpg[]
Queries value: HKCR\.latex[]
Queries value: HKCR\.lib[]
Queries value: HKCR\.m14[]
Queries value: HKCR\.m1v[]
Queries value: HKCR\.m3u[]
Queries value: HKCR\.mdb[]
Queries value: HKCR\.mid[]
Queries value: HKCR\midfile\clsid[]
Queries value: HKCR\.midi[]
Queries value: HKCR\.mmf[]
Queries value: HKCR\.mov[]
Queries value: HKCR\.movie[]
Queries value: HKCR\.mp2[]
Queries value: HKCR\.mp2v[]
Queries value: HKCR\.mp3[]
Queries value: HKCR\.mpa[]
Queries value: HKCR\.mpe[]
Queries value: HKCR\.mpeg[]
Queries value: HKCR\.mpg[]
Queries value: HKCR\.mpv2[]
Queries value: HKCR\.msg[]
Queries value: HKCR\.mv[]
Queries value: HKCR\.mydocs[]
Queries value: HKCR\.ncb[]

Queries value: HKCR\.obj[]
Queries value: HKCR\.oc_[]
Queries value: HKCR\.ocx[]
Queries value: HKCR\.pch[]
Queries value: HKCR\.pdb[]
Queries value: HKCR\.pds[]
Queries value: HKCR\.pic[]
Queries value: HKCR\.pma[]
Queries value: HKCR\.pmc[]
Queries value: HKCR\.pml[]
Queries value: HKCR\.pmr[]
Queries value: HKCR\.png[]
Queries value: HKCR\pngfile\clsid[]
Queries value: HKCR\.psd[]
Queries value: HKCR\.res[]
Queries value: HKCR\.rle[]
Queries value: HKCR\.rmi[]
Queries value: HKCR\.rpc[]
Queries value: HKCR\.rsp[]
Queries value: HKCR\.sbr[]
Queries value: HKCR\.sc2[]
Queries value: HKCR\.sit[]
Queries value: HKCR\.snd[]
Queries value: HKCR\.sr_[]
Queries value: HKCR\.sy_[]
Queries value: HKCR\.sym[]
Queries value: HKCR\.sys[]
Queries value: HKCR\.tar[]
Queries value: HKCR\.tgz[]
Queries value: HKCR\.tif[]
Queries value: HKCR\.tiff[]
Queries value: HKCR\.tlb[]
Queries value: HKCR\.tsp[]
Queries value: HKCR\.ttc[]
Queries value: HKCR\.ttf[]
Queries value: HKCR\.vbx[]
Queries value: HKCR\.vxd[]
Queries value: HKCR\.wav[]
Queries value: HKCR\soundrec\clsid[]
Queries value: HKCR\.wax[]
Queries value: HKCR\.wll[]
Queries value: HKCR\.wlt[]
Queries value: HKCR\.wm[]
Queries value: HKCR\.wma[]
Queries value: HKCR\.wmf[]
Queries value: HKCR\.wmp[]
Queries value: HKCR\.wmv[]
Queries value: HKCR\.wmx[]
Queries value: HKCR\.wmz[]
Queries value: HKCR\.wsz[]
Queries value: HKCR\.wvx[]
Queries value: HKCR\.xix[]
Queries value: HKCR\.z[]
Queries value: HKCR\.z96[]
Queries value: HKCR\.zip[]
Queries value: HKCR\compressedfolder\clsid[]
Queries value: HKCR\rtffile\clsid[]
Queries value: HKCR\xmlfile\clsid[]
Queries value: HKCR\.dic[]
Queries value: HKCR\.txt[]
Queries value: HKCR\.wtx[]
Queries value: HKCR\.bat[]
Queries value: HKCR\.cmd[]
Queries value: HKCR\.idq[]
Queries value: HKCR\.ini[]
Queries value: HKCR\.inx[]
Queries value: HKCR\.reg[]
Queries value: HKCR\.inf[]
Queries value: HKCR\.vbs[]
Queries value: HKCR\.asm[]
Queries value: HKCR\.c[]
Queries value: HKCR\.cpp[]
Queries value: HKCR\.cxx[]
Queries value: HKCR\.def[]
Queries value: HKCR\.h[]
Queries value: HKCR\.hpp[]
Queries value: HKCR\.hxx[]
Queries value: HKCR\.idl[]
Queries value: HKCR\.inc[]
Queries value: HKCR\.js[]
Queries value: HKCR\.log[]
Queries value: HKCR\.pl[]
Queries value: HKCR\.rc[]

Queries value: HKCR\.rtf[]
Queries value: HKCR\.url[]
Queries value: HKCR\internetshortcut\clsid[]
Queries value: HKCR\.xml[]
Queries value: HKCR\.xsl[]
Queries value: HKCR\xslfile\clsid[]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0[]
Queries value: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\flags[]
Queries value: HKCR\typelib\{4e469dd1-2b6f-11d0-bfbc-0020f8008024}\1.0\409\win32[]
Queries value: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}[]
Queries value: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\proxystubclsid[]
Queries value: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\proxystubclsid32[]
Queries value: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\typelib[]
Queries value: HKCR\interface\{f7456c32-6ff0-11d1-a260-0000f8753d7c}\typelib[version]
Queries value: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}[]
Queries value: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\proxystubclsid[]
Queries value: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\proxystubclsid32[]
Queries value: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\typelib[]
Queries value: HKCR\interface\{7d74218f-4858-42f9-99cc-ef2ba840425a}\typelib[version]
Queries value: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}[]
Queries value: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\proxystubclsid[]
Queries value: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\proxystubclsid32[]
Queries value: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\typelib[]
Queries value: HKCR\interface\{3b34e346-6cf1-11d1-a260-0000f8753d7c}\typelib[version]
Queries value: HKCR\htmlfile\clsid[]
Queries value: HKCR\htafile\clsid[]
Queries value: HKCR\.odc[]
Queries value: HKCR\.hhc[]
Queries value: HKCR\.htm[]
Queries value: HKCR\.html[]
Queries value: HKCR\.htx[]
Queries value: HKCR\.stm[]
Queries value: HKCR\.htw[]
Queries value: HKCR\.asp[]
Queries value: HKCR\.aspx[]
Queries value: HKCR\.ascx[]
Queries value: HKCR\.css[]
Queries value: HKCR\.hta[]
Queries value: HKCR\.htt[]
Queries value: HKCR\.doc[]
Queries value: HKCR\.dot[]
Queries value: HKCR\.pot[]
Queries value: HKCR\.ppt[]
Queries value: HKCR\.pps[]
Queries value: HKCR\.xlb[]
Queries value: HKCR\.xlc[]
Queries value: HKCR\.xls[]
Queries value: HKCR\.xlt[]
Queries value: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0[]
Queries value: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\flags[]
Queries value: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\0\win32[]
Queries value: HKCR\typelib\{3bc4f393-652a-11d1-b4d4-00c04fc2db8d}\1.0\helpdir[]
Queries value: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}[]
Queries value: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid[]
Queries value: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid32[]
Queries value: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\typelib[]
Queries value: HKCR\interface\{3bc4f3a0-652a-11d1-b4d4-00c04fc2db8d}\typelib[version]
Queries value: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}[]
Queries value: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid[]
Queries value: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid32[]
Queries value: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}\typelib[]
Queries value: HKCR\interface\{3bc4f3a2-652a-11d1-b4d4-00c04fc2db8d}\typelib[version]
Queries value: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}[]
Queries value: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid[]
Queries value: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\proxystubclsid32[]
Queries value: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\typelib[]
Queries value: HKCR\interface\{3bc4f3a4-652a-11d1-b4d4-00c04fc2db8d}\typelib[version]
Queries value: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0[]
Queries value: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\flags[]
Queries value: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\0\win32[]
Queries value: HKCR\typelib\{613201f0-a246-11d3-bb8c-0090272fa362}\1.0\helpdir[]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxcatalogs]
Queries value: HKLM\system\currentcontrolset\control\contentindex[leavecorruptcatalog]
Queries value: HKLM\system\currentcontrolset\control\contentindex[useole]
Queries value: HKLM\system\currentcontrolset\control\contentindex[filtercontents]
Queries value: HKLM\system\currentcontrolset\control\contentindex[filterdelayinterval]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[filterremainingthreshold]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxfilesizefiltered]
Queries value: HKLM\system\currentcontrolset\control\contentindex[mastermergetime]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxfilesizemultiplier]

Queries value: HKLM\system\currentcontrolset\control\contentindex[threadclassfilter]
Queries value: HKLM\system\currentcontrolset\control\contentindex[threadpriorityfilter]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[daemonresponsetimeout]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxcharacterization]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[generatecharacterization]
Queries value: HKLM\system\currentcontrolset\control\contentindex[isautoalias]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxautoaliasrefresh]
Queries value: HKLM\system\currentcontrolset\control\contentindex[isindexingw3svc]
Queries value: HKLM\system\currentcontrolset\control\contentindex[isindexingnntpsvc]
Queries value: HKLM\system\currentcontrolset\control\contentindex[isindexingimapsvc]
Queries value: HKLM\system\currentcontrolset\control\contentindex[isreadonly]
Queries value: HKLM\system\currentcontrolset\control\contentindex[isenumallowed]
Queries value: HKLM\system\currentcontrolset\control\contentindex[filterdirectories]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[filterfileswithunknownextensions]
Queries value: HKLM\system\currentcontrolset\control\contentindex[cataloginactive]
Queries value: HKLM\system\currentcontrolset\control\contentindex[forcepathalias]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[propertystoremappedcache]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[propertystorebackupsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[secpropertystoremappedcache]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[secpropertystorebackupsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[forcednetpathscaninterval]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxmergeinterval]
Queries value: HKLM\system\currentcontrolset\control\contentindex[threadprioritymerge]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxupdates]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxwordlists]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[minsizemergewordlists]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxwordlistsize]
Queries value: HKLM\system\currentcontrolset\control\contentindex[minwordlistmemory]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxwordlistio]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxwordlistiodiskperf]
Queries value: HKLM\system\currentcontrolset\control\contentindex[minwordlistbattery]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[lowresourcecheckinterval]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxfreshdeletes]
Queries value: HKLM\system\currentcontrolset\control\contentindex[lowresourcesleep]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxwordlistmemoryload]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxfreshcount]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxqueuechunks]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[mastermergecheckpointinterval]
Queries value: HKLM\system\currentcontrolset\control\contentindex[filterbuffersize]
Queries value: HKLM\system\currentcontrolset\control\contentindex[filterretries]
Queries value: HKLM\system\currentcontrolset\control\contentindex[filterretryinterval]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxshadowindexsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[mindiskfreeforcemerge]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxshadowfreeforcemerge]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxindexes]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxidealindexes]
Queries value: HKLM\system\currentcontrolset\control\contentindex[minmergeidletime]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxpendingdocuments]
Queries value: HKLM\system\currentcontrolset\control\contentindex[minidlequerythreads]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxactivequerythreads]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxquerytimeslice]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[maxqueryexecutiontime]
Queries value: HKLM\system\currentcontrolset\control\contentindex[w3svcinstance]
Queries value: HKLM\system\currentcontrolset\control\contentindex[nntpsvcinstance]
Queries value: HKLM\system\currentcontrolset\control\contentindex[imapsvcinstance]
Queries value: HKLM\system\currentcontrolset\control\contentindex[eventlogflags]
Queries value: HKLM\system\currentcontrolset\control\contentindex[cimiscflags]
Queries value: HKLM\system\currentcontrolset\control\contentindex[cicatalogflags]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxusnlogsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[usnlogallocationdelta]
Queries value: HKLM\system\currentcontrolset\control\contentindex[scanbackoff]
Queries value: HKLM\system\currentcontrolset\control\contentindex[usnreadtimeout]
Queries value: HKLM\system\currentcontrolset\control\contentindex[usnreadminsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex[delayusnreadonlowresource]

Queries value: HKLM\system\currentcontrolset\control\contentindex[maxdaemonvmuse]
Queries value: HKLM\system\currentcontrolset\control\contentindex[delayedfilterretries]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxrestrictionnodes]
Queries value: HKLM\system\currentcontrolset\control\contentindex[stomplastaccessdelay]
Queries value: HKLM\system\currentcontrolset\control\contentindex[wordlistuseridle]
Queries value: HKLM\system\currentcontrolset\control\contentindex[mindiskspacetoleave]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[useole]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filtercontents]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterdelayinterval]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterremainingthreshold]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxfilesizefiltered]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[mastermergetime]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxfilesizemultiplier]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[threadclassfilter]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[threadpriorityfilter]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[daemonresponsetimeout]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxcharacterization]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[generatecharacterization]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isautoalias]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxautoaliasrefresh]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isindexingw3svc]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isindexingnntpsvc]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isindexingimapsvc]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isreadonly]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[isenumallowed]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterdirectories]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterfileswithunknownextensions]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[forcepathalias]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[propertystoremappedcache]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[propertystorebackupsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[secpropertystoremappedcache]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[secpropertystorebackupsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[forcednetpathscaninterval]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxmergeinterval]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[threadprioritymerge]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxupdates]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxwordlists]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minsizemergewordlists]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxwordlistsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minwordlistmemory]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxwordlistio]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxwordlistiodiskperf]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minwordlistbattery]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[lowresourcecheckinterval]
Queries value:

HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxfreshdeletes]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[lowresourcesleep]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxwordlistmemoryload]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxfreshcount]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxqueuechunks]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[mastermergecheckpointinterval]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterbuffersize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterretries]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filterretryinterval]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxshadowindexsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[mindiskfreeforcemerge]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxshadowfreeforcemerge]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxindexes]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxidealindexes]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minmergeidletime]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxpendingdocuments]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minidlequerythreads]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxactivequerythreads]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxquerytimeslice]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxqueryexecutiontime]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minidlerequestthreads]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minclientidletime]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxactiverequestthreads]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxsimultaneousrequests]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxcachedpipes]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[wordlistuseridle]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[requesttimeout]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[w3svcinstance]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[nntpsvcinstance]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[imapsvcinstance]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[minimizeworkingset]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[eventlogflags]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[cimiscflags]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[cicatalogflags]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxrestrictionnodes]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxusnlogsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[usnlogallocationdelta]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[scanbackoff]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[startupdelay]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[usnreadtimeout]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[usnreadminsize]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[delayusnreadonlowresource]

Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[maxdaemonvmuse]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[delayedfilterretries]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[stomplastaccessdelay]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[mindiskspacetoleave]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-
00c04fc2f410}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprocserver32[]
Queries value: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}[appid]
Queries value: HKCR\clsid\{1e9685e6-db6d-11d0-bb63-
00c04fc2f410}\inprocserver32[threadingmodel]
Queries value:
HKLM\system\currentcontrolset\control\networkprovider\hworder[providerorder]
Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[name]
Queries value: HKLM\system\currentcontrolset\services\rdpnp\networkprovider[class]
Queries value:
HKLM\system\currentcontrolset\services\rdpnp\networkprovider[providerpath]
Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[name]
Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[class]
Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[providerpath]
Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[name]
Queries value: HKLM\system\currentcontrolset\services\webclient\networkprovider[class]
Queries value:
HKLM\system\currentcontrolset\services\webclient\networkprovider[providerpath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\network\world full
access shared parameters[sort hyphens]
Queries value: HKU\.default\control panel\international[locale]
Queries value: HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[cidaemon]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[cidaemon]
Queries value: HKCR\clsid\{aa205a4d-681f-11d0-a243-
08002b36fca4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprocserver32[]
Queries value: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}[appid]
Queries value: HKCR\clsid\{aa205a4d-681f-11d0-a243-
08002b36fca4}\inprocserver32[threadingmodel]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system[filtertrackers]
Queries value: HKLM\system\currentcontrolset\control\contentindex[filtertrackers]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\catalogs\system\scopes[]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\dutch_dutch[locale]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\english_uk[locale]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\english_us[locale]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\french_french[locale]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\german_german[locale]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian[locale]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\neutral[locale]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\neutral[wbreakerclass]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\neutral[stemmerclass]
Queries value:
HKLM\system\currentcontrolset\control\contentindex\language\neutral[noisefile]
Queries value: HKCR\clsid\{369647e0-17b0-11ce-9950-
00aa004bbb1f}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserver32[]
Queries value: HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}[appid]
Queries value: HKCR\clsid\{369647e0-17b0-11ce-9950-
00aa004bbb1f}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-
3d01-b289-befc77a11a1e}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-
4ca4-87b4-2f83217002ff}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{350c97b0-3d7c-
4ee8-baa9-00bcb3d54227}[installlocation]

Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-5f2748764d10}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-0000000ff1ce}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-0150048383c9}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-0000000ff1ce}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{a3051cd0-2f64-3813-a88d-b8dccde8f8c7}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c09fb3cd-3d0c-3f2d-899a-6a1d67f2073f}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-4027-b136-2b3e1f5ab6e2}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-36ca-84d3-9f4dcf5c5bd9}[installlocation]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ce2cdd62-0124-36ca-84d3-9f4dcf5c5bd9}.kb953595[installlocation]
Queries value: HKCR\.ini\persistenthandler[]
Queries value: HKCR\clsid\{5e941d80-bf96-11cd-b579-08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
Queries value: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32[]
Queries value: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}[appid]
Queries value: HKLM\system\currentcontrolset\control\contentindex[maxtextfilterbytes]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nonethood]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\startmenu\startpanel[defaultstartpaneloff]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
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: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
Queries value: HKCR\.ini[perceivedtype]
Queries value: HKCR\inifile[docobject]
Queries value: HKCR\inifile[browseinplace]
Queries value: HKCR\inifile[isshortcut]
Queries value: HKCR\inifile[alwaysshowext]
Queries value: HKCR\inifile[nevershowext]
Queries value: HKCR\.sam[]
Queries value: HKCR\.sam[perceivedtype]
Queries value: HKCR\.sam[docobject]
Queries value: HKCR\.sam[browseinplace]
Queries value: HKCR\.sam[isshortcut]

Queries value: HKCR\.sam[alwaysshowext]
Queries value: HKCR\.sam[nevershowext]
Queries value: HKCR\.xls\persistenthandler[]
Queries value: HKCR\clsid\{98de59a0-d175-11cd-a7bd-00006b827d94}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
Queries value: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32[]
Queries value: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}[appid]
Queries value: HKU\.default\control panel\international[scurrency]
Queries value: HKU\.default\control panel\international[icurrency]
Queries value: HKU\.default\control panel\international[inegcurr]
Queries value: HKU\.default\control panel\international[icurrdigits]
Queries value: HKU\.default\control panel\international[smondecimalsep]
Queries value: HKU\.default\control panel\international[smonthousandsep]
Queries value: HKU\.default\control panel\international[idigits]
Queries value: HKU\.default\control panel\international[ilzero]
Queries value: HKU\.default\control panel\international[sdecimal]
Queries value: HKU\.default\control panel\international[sthousand]
Queries value: HKU\.default\control panel\international[itime]
Queries value: HKU\.default\control panel\international[itlzero]
Queries value: HKU\.default\control panel\international[itimeprefix]
Queries value: HKU\.default\control panel\international[s1159]
Queries value: HKU\.default\control panel\international[s2359]
Queries value: HKU\.default\control panel\international[stime]
Queries value: HKU\.default\control panel\international[sshortdate]
Queries value: HKLM\system\currentcontrolset\control\contentindex\language\english_uk[wbreakerclass]
Queries value: HKLM\system\currentcontrolset\control\contentindex\language\english_uk[stemmerclass]
Queries value: HKLM\system\currentcontrolset\control\contentindex\language\english_uk[noisefile]
Queries value: HKLM\system\currentcontrolset\control\contentindex\language\english_us[wbreakerclass]
Queries value: HKLM\system\currentcontrolset\control\contentindex\language\english_us[stemmerclass]
Queries value: HKLM\system\currentcontrolset\control\contentindex\language\english_us[noisefile]
Queries value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32[]
Queries value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}[appid]
Queries value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32[threadingmodel]
Queries value: HKCR\.xls[perceivedtype]
Queries value: HKCR\excelviewer.sheet.8[docobject]
Queries value: HKCR\systemfileassociations\.xls[docobject]
Queries value: HKCR\excelviewer.sheet.8[browseinplace]
Queries value: HKCR\systemfileassociations\.xls[browseinplace]
Queries value: HKCR\excelviewer.sheet.8[isshortcut]
Queries value: HKCR\systemfileassociations\.xls[isshortcut]
Queries value: HKCR\excelviewer.sheet.8[alwaysshowext]
Queries value: HKCR\systemfileassociations\.xls[alwaysshowext]
Queries value: HKCR\excelviewer.sheet.8[nevershowext]
Queries value: HKCR\systemfileassociations\.xls[nevershowext]
Queries value: HKCR\.wk4[]
Queries value: HKCR\.wk4[perceivedtype]
Queries value: HKCR\.wk4[docobject]
Queries value: HKCR\.wk4[browseinplace]
Queries value: HKCR\.wk4[isshortcut]
Queries value: HKCR\.wk4[alwaysshowext]
Queries value: HKCR\.wk4[nevershowext]
Queries value: HKCR\.ppt\persistenthandler[]
Queries value: HKCR\.shw[]
Queries value: HKCR\.shw[perceivedtype]
Queries value: HKCR\.shw[docobject]
Queries value: HKCR\.shw[browseinplace]
Queries value: HKCR\.shw[isshortcut]
Queries value: HKCR\.shw[alwaysshowext]
Queries value: HKCR\.shw[nevershowext]
Queries value: HKCR\.wb2[]
Queries value: HKCR\.wb2[perceivedtype]
Queries value: HKCR\.wb2[docobject]
Queries value: HKCR\.wb2[browseinplace]
Queries value: HKCR\.wb2[isshortcut]
Queries value: HKCR\.wb2[alwaysshowext]
Queries value: HKCR\.wb2[nevershowext]
Queries value: HKCR\.wav\persistenthandler[]
Queries value: HKCR\clsid\{098f2470-bae0-11cd-b579-08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
Queries value: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32[]

Queries value: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}[appid]
Queries value: HKCR\soundrec[docobject]
Queries value: HKCR\systemfileassociations\.wav[docobject]
Queries value: HKCR\systemfileassociations\audio[docobject]
Queries value: HKCR\soundrec[browseinplace]
Queries value: HKCR\systemfileassociations\.wav[browseinplace]
Queries value: HKCR\systemfileassociations\audio[browseinplace]
Queries value: HKCR\soundrec[isshortcut]
Queries value: HKCR\systemfileassociations\.wav[isshortcut]
Queries value: HKCR\systemfileassociations\audio[isshortcut]
Queries value: HKCR\soundrec[alwaysshowext]
Queries value: HKCR\systemfileassociations\.wav[alwaysshowext]
Queries value: HKCR\systemfileassociations\audio[alwaysshowext]
Queries value: HKCR\soundrec[nevershowext]
Queries value: HKCR\systemfileassociations\.wav[nevershowext]
Queries value: HKCR\systemfileassociations\audio[nevershowext]
Queries value: HKCR\systemfileassociations\.wav\shellex\propertyhandler[]
Queries value: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprocserver32[]
Queries value: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked[{e4b29f9d-d390-480b-92fd-7ddb47101d71}]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\blocked[{e4b29f9d-d390-480b-92fd-7ddb47101d71}]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\cached[{e4b29f9d-d390-480b-92fd-7ddb47101d71} {0000010b-0000-0000-c000-000000000046} 0x401]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\cached[{e4b29f9d-d390-480b-92fd-7ddb47101d71} {0000010b-0000-0000-c000-000000000046} 0x401]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[verclsid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[verclsid]
Queries value: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}[appid]
Queries value: HKCR\clsid\{e4b29f9d-d390-480b-92fd-7ddb47101d71}\inprocserver32[threadingmodel]
Queries value: HKCR\.doc\persistenthandler[]
Queries value: HKCR\.doc[perceivedtype]
Queries value: HKCR\wordview.document.8[docobject]
Queries value: HKCR\systemfileassociations\.doc[docobject]
Queries value: HKCR\wordview.document.8[browseinplace]
Queries value: HKCR\systemfileassociations\.doc[browseinplace]
Queries value: HKCR\wordview.document.8[isshortcut]
Queries value: HKCR\systemfileassociations\.doc[isshortcut]
Queries value: HKCR\wordview.document.8[alwaysshowext]
Queries value: HKCR\systemfileassociations\.doc[alwaysshowext]
Queries value: HKCR\wordview.document.8[nevershowext]
Queries value: HKCR\systemfileassociations\.doc[nevershowext]
Queries value: HKCR\.wpd[]
Queries value: HKCR\.wpd[perceivedtype]
Queries value: HKCR\.wpd[docobject]
Queries value: HKCR\.wpd[browseinplace]
Queries value: HKCR\.wpd[isshortcut]
Queries value: HKCR\.wpd[alwaysshowext]
Queries value: HKCR\.wpd[nevershowext]
Queries value: HKCR\.wpg[]
Queries value: HKCR\.wpg[perceivedtype]
Queries value: HKCR\.wpg[docobject]
Queries value: HKCR\.wpg[browseinplace]
Queries value: HKCR\.wpg[isshortcut]
Queries value: HKCR\.wpg[alwaysshowext]
Queries value: HKCR\.wpg[nevershowext]
Queries value: HKU\.default\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
Queries value: HKCR\.lnk[]
Queries value: HKCR\lnkfile\clsid[]
Queries value: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\persistenthandler[]
Queries value: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
Queries value: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserver32[]
Queries value: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{00021401-0000-0000-c000-000000000046}[appid]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKLM\software\microsoft\com3[gipactivitybypass]
Queries value: HKCR\interface\{0000010b-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[normalizelinknetpidls]
Queries value: HKCR\network\sharinghandler[]
Queries value:
HKU\.default\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness]
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: HKCR\lnkfile\shellex\iconhandler[]
Queries value: HKCR\lnkfile[docobject]
Queries value: HKCR\.lnk[perceivedtype]
Queries value: HKCR\lnkfile[browseinplace]
Queries value: HKCR\lnkfile[isshortcut]
Queries value: HKCR\lnkfile[alwaysshowext]
Queries value: HKCR\lnkfile[nevershowext]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x401]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x401]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
Queries value: HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
Queries value: HKLM\software\microsoft\internet explorer\setup[installstarted]
Queries value: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
Queries value: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
Queries value: HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
Queries value: HKCR\.zfsendtotarget[perceivedtype]
Queries value: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[docobject]
Queries value: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[browseinplace]
Queries value: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[isshortcut]
Queries value: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[alwaysshowext]
Queries value: HKCR\clsid\{888dca60-fc0a-11cf-8f0f-00c04fd7d062}[nevershowext]
Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
Queries value: HKU\.default\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\icofile[docobject]
Queries value: HKCR\systemfileassociations\image[docobject]
Queries value: HKCR\icofile[browseinplace]
Queries value: HKCR\systemfileassociations\image[browseinplace]
Queries value: HKCR\icofile[isshortcut]
Queries value: HKCR\systemfileassociations\image[isshortcut]
Queries value: HKCR\icofile[alwaysshowext]
Queries value: HKCR\systemfileassociations\image[alwaysshowext]
Queries value: HKCR\icofile[nevershowext]
Queries value: HKCR\systemfileassociations\image[nevershowext]
Queries value: HKCR\.chm[]
Queries value: HKCR\.chm[perceivedtype]

Queries value: HKCR\chm.file[docobject]
Queries value: HKCR\chm.file[browseinplace]
Queries value: HKCR\chm.file[isshortcut]
Queries value: HKCR\chm.file[alwaysshowext]
Queries value: HKCR\chm.file[nevershowext]
Queries value: HKCR\.msc[]
Queries value: HKCR\mscfile\shellex\iconhandler[]
Queries value: HKCR\mscfile[docobject]
Queries value: HKCR\.msc[perceivedtype]
Queries value: HKCR\mscfile[browseinplace]
Queries value: HKCR\mscfile[isshortcut]
Queries value: HKCR\mscfile[alwaysshowext]
Queries value: HKCR\mscfile[nevershowext]
Queries value: HKCR\.cpl[perceivedtype]
Queries value: HKCR\cplfile[docobject]
Queries value: HKCR\cplfile[browseinplace]
Queries value: HKCR\cplfile[isshortcut]
Queries value: HKCR\cplfile[alwaysshowext]
Queries value: HKCR\cplfile[nevershowext]
Queries value: HKCR\.desklink\persistenthandler[]
Queries value: HKCR\.desklink[perceivedtype]
Queries value: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[docobject]
Queries value: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[browseinplace]
Queries value: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[isshortcut]
Queries value: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[alwaysshowext]
Queries value: HKCR\clsid\{9e56be61-c50f-11cf-9a2c-00a0c90a90ce}[nevershowext]
Queries value: HKCR\.mapimail\persistenthandler[]
Queries value: HKCR\.mapimail[perceivedtype]
Queries value: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}[docobject]
Queries value: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}[browseinplace]
Queries value: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}[isshortcut]
Queries value: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}[alwaysshowext]
Queries value: HKCR\clsid\{9e56be60-c50f-11cf-9a2c-00a0c90a90ce}[nevershowext]
Queries value: HKCR\.dat[]
Queries value: HKCR\.dat[perceivedtype]
Queries value: HKCR\.dat[docobject]
Queries value: HKCR\.dat[browseinplace]
Queries value: HKCR\.dat[isshortcut]
Queries value: HKCR\.dat[alwaysshowext]
Queries value: HKCR\.dat[nevershowext]
Queries value: HKCR\.jpg\persistenthandler[]
Queries value: HKCR\jpegfile[docobject]
Queries value: HKCR\systemfileassociations\.jpg[docobject]
Queries value: HKCR\jpegfile[browseinplace]
Queries value: HKCR\systemfileassociations\.jpg[browseinplace]
Queries value: HKCR\jpegfile[isshortcut]
Queries value: HKCR\systemfileassociations\.jpg[isshortcut]
Queries value: HKCR\jpegfile[alwaysshowext]
Queries value: HKCR\systemfileassociations\.jpg[alwaysshowext]
Queries value: HKCR\jpegfile[nevershowext]
Queries value: HKCR\systemfileassociations\.jpg[nevershowext]
Queries value: HKCR\systemfileassociations\image\shellex\propertyhandler[]
Queries value: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserver32[]
Queries value: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\blocked[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\cached[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe} {0000010b-0000-0000-c000-000000000046} 0x401]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\cached[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe} {0000010b-0000-0000-c000-000000000046} 0x401]
Queries value: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}[appid]
Queries value: HKCR\clsid\{eb9b1153-3b57-4e68-959a-a3266bc3d7fe}\inprocserver32[threadingmodel]
Queries value: HKCR\.wpl[]
Queries value: HKCR\.wpl[perceivedtype]
Queries value: HKCR\wplfile[docobject]
Queries value: HKCR\systemfileassociations\.wpl[docobject]
Queries value: HKCR\wplfile[browseinplace]
Queries value: HKCR\systemfileassociations\.wpl[browseinplace]
Queries value: HKCR\wplfile[isshortcut]
Queries value: HKCR\systemfileassociations\.wpl[isshortcut]
Queries value: HKCR\wplfile[alwaysshowext]
Queries value: HKCR\systemfileassociations\.wpl[alwaysshowext]
Queries value: HKCR\wplfile[nevershowext]
Queries value: HKCR\systemfileassociations\.wpl[nevershowext]
Queries value: HKCR\.wma\persistenthandler[]

Queries value: HKCR\wmafile[docobject]
Queries value: HKCR\systemfileassociations\.wma[docobject]
Queries value: HKCR\wmafile[browseinplace]
Queries value: HKCR\systemfileassociations\.wma[browseinplace]
Queries value: HKCR\wmafile[isshortcut]
Queries value: HKCR\systemfileassociations\.wma[isshortcut]
Queries value: HKCR\wmafile[alwaysshowext]
Queries value: HKCR\systemfileassociations\.wma[alwaysshowext]
Queries value: HKCR\wmafile[nevershowext]
Queries value: HKCR\systemfileassociations\.wma[nevershowext]
Queries value: HKCR\systemfileassociations\.wma\shellex\propertyhandler[]
Queries value: HKCR\clsid\{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}\inprocserver32[]
Queries value: HKCR\clsid\{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\blocked[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78}]
Queries value: HKLM\software\microsoft\windows\currentversion\shell extensions\cached[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78} {0000010b-0000-0000-c000-000000000046} 0x401]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\cached[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78} {0000010b-0000-0000-c000-000000000046} 0x401]
Queries value: HKCR\.sst[]
Queries value: HKCR\.sst[perceivedtype]
Queries value: HKCR\certificatestorefile[docobject]
Queries value: HKCR\certificatestorefile[browseinplace]
Queries value: HKCR\certificatestorefile[isshortcut]
Queries value: HKCR\certificatestorefile[alwaysshowext]
Queries value: HKCR\certificatestorefile[nevershowext]
Queries value: HKCR\.mydocs\persistenthandler[]
Queries value: HKCR\.mydocs[perceivedtype]
Queries value: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[docobject]
Queries value: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[browseinplace]
Queries value: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[isshortcut]
Queries value: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[alwaysshowext]
Queries value: HKCR\clsid\{ecf03a32-103d-11d2-854d-006008059367}[nevershowext]
Queries value: HKCR\.url\persistenthandler[]
Queries value: HKCR\clsid\{8cd34779-9f10-4f9b-adfb-b3faeabdab5a}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
Queries value: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\inprocserver32[]
Queries value: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7ee0a24e-a8c6-46ae-a875-8e7c3d18aeaf}[appid]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserver32[]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}[appid]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance[clsid]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance[loadwithoutcom]
Queries value: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserver32[]
Queries value: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}[appid]
Queries value: HKCR\clsid\{942bc614-676c-464e-b384-d3202aaa02da}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[cidaemon.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserver32[]
Queries value: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}[appid]
Queries value: HKCR\clsid\{4516cee1-97da-4030-a444-2d8e296b96b6}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserver32[]
Queries value: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}[appid]
Queries value: HKCR\clsid\{6f237df9-9ddb-47ad-b218-400d54c286ad}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2[section]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-

1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}[section]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2[key]
Queries value: HKCR\clsid\{06eee834-461c-42c2-8dcf-
1502b527b1f9}\instance\propertysetstorage\{000214a0-0000-0000-c000-000000000046}\2[vartype]
Queries value: HKCR\internetshortcut\shellex\iconhandler[]
Queries value: HKCR\internetshortcut[docobject]
Queries value: HKCR\.url[perceivedtype]
Queries value: HKCR\internetshortcut[browseinplace]
Queries value: HKCR\internetshortcut[isshortcut]
Queries value: HKCR\internetshortcut[alwaysshowext]
Queries value: HKCR\internetshortcut[nevershowext]
Queries value: HKCR\internetshortcut\shellex\propertyhandler[]
Queries value: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\inprocserver32[]
Queries value: HKCR\clsid\{fbf23b40-e3f0-101b-8488-
00aa003e56f8}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{fbf23b40-e3f0-101b-8488-00aa003e56f8}]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell
extensions\blocked[{fbf23b40-e3f0-101b-8488-00aa003e56f8}]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{fbf23b40-e3f0-101b-8488-00aa003e56f8} {0000010b-0000-0000-c000-000000000046}
0x401]
Queries value: HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{fbf23b40-e3f0-101b-8488-00aa003e56f8} {0000010b-0000-0000-c000-000000000046}
0x401]
Queries value: HKCR\clsid\{fbf23b40-e3f0-101b-8488-
00aa003e56f8}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}[appid]
Queries value: HKCR\appid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}[dllsurrogate]
Queries value: HKCR\clsid\{fbf23b40-e3f0-101b-8488-
00aa003e56f8}\inprocserver32[threadingmodel]
Queries value: HKCR\.txt\persistenthandler[]
Queries value: HKCR\.txt[perceivedtype]
Queries value: HKCR\txtfile[docobject]
Queries value: HKCR\systemfileassociations\text[docobject]
Queries value: HKCR\txtfile[browseinplace]
Queries value: HKCR\systemfileassociations\text[browseinplace]
Queries value: HKCR\txtfile[isshortcut]
Queries value: HKCR\systemfileassociations\text[isshortcut]
Queries value: HKCR\txtfile[alwaysshowext]
Queries value: HKCR\systemfileassociations\text[alwaysshowext]
Queries value: HKCR\txtfile[nevershowext]
Queries value: HKCR\systemfileassociations\text[nevershowext]
Queries value: HKCR\.bat\persistenthandler[]
Queries value: HKCR\batfile[docobject]
Queries value: HKCR\batfile[browseinplace]
Queries value: HKCR\batfile[isshortcut]
Queries value: HKCR\batfile[alwaysshowext]
Queries value: HKCR\batfile[nevershowext]
Queries value: HKCR\.sys\persistenthandler[]
Queries value: HKCR\.sys[perceivedtype]
Queries value: HKCR\sysfile[docobject]
Queries value: HKCR\sysfile[browseinplace]
Queries value: HKCR\sysfile[isshortcut]
Queries value: HKCR\sysfile[alwaysshowext]
Queries value: HKCR\sysfile[nevershowext]
Queries value: HKCR\.log\persistenthandler[]
Queries value: HKCR\.log[perceivedtype]
Queries value: HKCR\.com\persistenthandler[]
Queries value: HKCR\comfile[docobject]
Queries value: HKCR\comfile[browseinplace]
Queries value: HKCR\comfile[isshortcut]
Queries value: HKCR\comfile[alwaysshowext]
Queries value: HKCR\comfile[nevershowext]
Queries value: HKCR\.bmp\persistenthandler[]
Queries value: HKCR\paint.picture[docobject]
Queries value: HKCR\systemfileassociations\.bmp[docobject]
Queries value: HKCR\paint.picture[browseinplace]
Queries value: HKCR\systemfileassociations\.bmp[browseinplace]
Queries value: HKCR\paint.picture[isshortcut]
Queries value: HKCR\systemfileassociations\.bmp[isshortcut]
Queries value: HKCR\paint.picture[alwaysshowext]
Queries value: HKCR\systemfileassociations\.bmp[alwaysshowext]
Queries value: HKCR\paint.picture[nevershowext]
Queries value: HKCR\systemfileassociations\.bmp[nevershowext]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\wbem\cimom[logging directory]

Queries value: HKLM\software\microsoft\wbem\cimom[logging]
Queries value: HKLM\software\microsoft\wbem\cimom[log file max size]
Queries value: HKLM\software\microsoft\wbem\cimom[repository directory]
Queries value: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
Queries value: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
Queries value: HKCR\.exe\persistenthandler[]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
Queries value: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
Queries value: HKCR\.scf[]
Queries value: HKCR\shcmdfile\clsid[]
Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[threadingmodel]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
Queries value: HKCR\shcmdfile\shellex\iconhandler[]
Queries value: HKCR\shcmdfile[docobject]
Queries value: HKCR\.scf[perceivedtype]
Queries value: HKCR\shcmdfile[browseinplace]
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: HKCR\shcmdfile[isshortcut]
Queries value: HKCR\shcmdfile[alwaysshowext]
Queries value: HKCR\shcmdfile[nevershowext]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]

Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
Queries value: HKLM\software\microsoft\wbem\cimom[processid]
Queries value: HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
Queries value: HKLM\software\microsoft\wbem\cimom[contextlimit]
Queries value: HKLM\software\microsoft\wbem\cimom[objectlimit]
Queries value: HKLM\software\microsoft\wbem\cimom[identifierlimit]
Queries value: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32[]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
Queries value: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
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\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
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-
c7d49d7cecdc}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipautoconfigurationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
Sets/Creates value: HKCR\msidxs[]
Sets/Creates value: HKCR\msidxs\clsid[]
Sets/Creates value: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}[]
Sets/Creates value: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\progid[]
Sets/Creates value: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\ole db provider[]
Sets/Creates value: HKCR\msidxs errorlookup[]
Sets/Creates value: HKCR\msidxs errorlookup\clsid[]
Sets/Creates value: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}[]
Sets/Creates value: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\progid[]
Sets/Creates value: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{f9ae8981-7e52-11d0-8964-00c04fd611d7}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors[]
Sets/Creates value: HKCR\clsid\{f9ae8980-7e52-11d0-8964-00c04fd611d7}\extendederrors\{f9ae8981-7e52-11d0-8964-00c04fd611d7}[]
Sets/Creates value: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}[]
Sets/Creates value: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\progid[]
Sets/Creates value: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{c7b6c04a-cbb5-11d0-bb4c-00c04fc2f410}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{0cd7a5c0-9f37-11ce-ae65-08002b2e1262}\persistenthandler[]
Sets/Creates value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\persistenthandler[]
Sets/Creates value: HKCR\.xbm\persistenthandler[]
Sets/Creates value: HKCR\clsid\{e88dcce0-b7b3-11d1-a9f0-00aa0060fa31}\persistenthandler[]
Sets/Creates value: HKCR\clsid\{48123bc4-99d9-11d1-a6b3-00c04fd91555}\persistenthandler[]
Sets/Creates value: HKCR\clsid\{fbf23b40-e3f0-101b-8488-00aa003e56f8}\persistenthandler[]
Sets/Creates value: HKCR\.xml\persistenthandler[]
Sets/Creates value: HKCR\.xsl\persistenthandler[]
Sets/Creates value: HKCR\clsid\{3050f4d8-98b5-11cf-bb82-00aa00bdce0b}\persistenthandler[]
Sets/Creates value: HKCR\.hta\persistenthandler[]
Sets/Creates value: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}[]
Sets/Creates value: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\progid[]
Sets/Creates value: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid[]

Sets/Creates value: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{3bc4f3a1-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}[]
Sets/Creates value: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\progid[]
Sets/Creates value: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{3bc4f3a3-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}[]
Sets/Creates value: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\progid[]
Sets/Creates value: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{3bc4f3a7-652a-11d1-b4d4-00c04fc2db8d}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}[]
Sets/Creates value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\progid[]
Sets/Creates value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{80a3e9b0-a246-11d3-bb8c-0090272fa362}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}[]
Sets/Creates value: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\progid[]
Sets/Creates value: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{363f1015-fd5f-4ba8-ac58-29634f378a42}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}[]
Sets/Creates value: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\progid[]
Sets/Creates value: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{f14e6b48-fbca-4d32-bd79-7829d4f7e43b}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}[]
Sets/Creates value: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\progid[]
Sets/Creates value: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{91870674-de84-4313-b07d-a387415bb4f5}\inprocserver32[threadingmodel]
Sets/Creates value: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}[]
Sets/Creates value: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\progid[]
Sets/Creates value: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\versionindependentprogid[]
Sets/Creates value: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\inprocserver32[]
Sets/Creates value: HKCR\clsid\{1f7e6c6d-c3f8-4c80-8d77-c4825abbe5cf}\inprocserver32[threadingmodel]
Sets/Creates value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\cached[{e4b29f9d-d390-480b-92fd-7ddb47101d71} {0000010b-0000-0000-c000-000000000046} 0x401]
Sets/Creates value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\cached[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe} {0000010b-0000-0000-c000-000000000046} 0x401]
Sets/Creates value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\cached[{875cb1a1-0f29-45de-a1ae-cfb4950d0b78} {0000010b-0000-0000-c000-000000000046} 0x401]
Sets/Creates value: HKU\.default\software\microsoft\windows\currentversion\shell extensions\cached[{fbf23b40-e3f0-101b-8488-00aa003e56f8} {0000010b-0000-0000-c000-000000000046} 0x401]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}[]
Value changes: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprocserver32[]
Value changes: HKCR\clsid\{aa205a4d-681f-11d0-a243-08002b36fca4}\inprocserver32[threadingmodel]
Value changes: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}[]
Value changes: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32[]
Value changes: HKCR\clsid\{2a488070-6fd9-11d0-a808-00a0c906241a}\inprocserver32[threadingmodel]
Value changes: HKCR\clsid\{098f2470-bae0-11cd-b579-08002b30bfeb}[]
Value changes: HKCR\clsid\{098f2470-bae0-11cd-b579-08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
Value changes: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}[]
Value changes: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32[]
Value changes: HKCR\clsid\{c3278e90-bea7-11cd-b579-08002b30bfeb}\inprocserver32[threadingmodel]
Value changes: HKCR\clsid\{00022602-0000-0000-c000-000000000046}\persistenthandler[]
Value changes: HKCR\clsid\{d3e34b21-9d75-101a-8c3d-00aa001a1652}\persistenthandler[]
Value changes: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\persistenthandler[]

```
  Value changes:            HKCR\clsid\{00022603-0000-0000-c000-000000000046}\persistenthandler[]
  Value changes:            HKCR\clsid\{00020c01-0000-0000-c000-000000000046}\persistenthandler[]
  Value changes:            HKCR\clsid\{5e941d80-bf96-11cd-b579-08002b30bfeb}[]
  Value changes:            HKCR\clsid\{5e941d80-bf96-11cd-b579-
08002b30bfeb}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
  Value changes:            HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}[]
  Value changes:            HKCR\clsid\{c1243ca0-bf96-11cd-b579-08002b30bfeb}\inprocserver32[]
  Value changes:            HKCR\clsid\{c1243ca0-bf96-11cd-b579-
08002b30bfeb}\inprocserver32[threadingmodel]
  Value changes:            HKCR\clsid\{73fddc80-aea9-101a-98a7-00aa00374959}\persistenthandler[]
  Value changes:            HKCR\clsid\{48123bc4-99d9-11d1-a6b3-00c04fd91555}\persistenthandler[]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\neutral[locale]
  Value changes:            HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}[]
  Value changes:            HKCR\clsid\{369647e0-17b0-11ce-9950-00aa004bbb1f}\inprocserver32[]
  Value changes:            HKCR\clsid\{369647e0-17b0-11ce-9950-
00aa004bbb1f}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\neutral[wbreakerclass]
  Value changes:            HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}[]
  Value changes:            HKCR\clsid\{78fe669a-186e-4108-96e9-77b586c1332f}\inprocserver32[]
  Value changes:            HKCR\clsid\{78fe669a-186e-4108-96e9-
77b586c1332f}\inprocserver32[threadingmodel]
  Value changes:            HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}[]
  Value changes:            HKCR\clsid\{1e9685e6-db6d-11d0-bb63-00c04fc2f410}\inprocserver32[]
  Value changes:            HKCR\clsid\{1e9685e6-db6d-11d0-bb63-
00c04fc2f410}\inprocserver32[threadingmodel]
  Value changes:            HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}[]
  Value changes:            HKCR\clsid\{1f247dc0-902e-11d0-a80c-00a0c906241a}\inprocserver32[]
  Value changes:            HKCR\clsid\{1f247dc0-902e-11d0-a80c-
00a0c906241a}\inprocserver32[threadingmodel]
  Value changes:            HKCR\clsid\{c04efa90-e221-11d2-985e-00c04f575153}\inprocserver32[]
  Value changes:            HKCR\clsid\{c04efa90-e221-11d2-985e-
00c04f575153}\inprocserver32[threadingmodel]
  Value changes:            HKCR\clsid\{c04efa90-e221-11d2-985e-00c04f575153}[]
  Value changes:            HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}\proxystubclsid32[]
  Value changes:            HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}[]
  Value changes:            HKCR\interface\{f4eb8260-8dda-11d1-b3aa-00a0c9063796}\nummethods[]
  Value changes:            HKCR\clsid\{95ad72f0-44ce-11d0-ae29-00aa004b9986}[]
  Value changes:            HKCR\clsid\{95ad72f0-44ce-11d0-ae29-00aa004b9986}\inprocserver32[]
  Value changes:            HKCR\clsid\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}\inprocserver32[threadingmodel]
  Value changes:            HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}[namestring]
  Value changes:            HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}[about]
  Value changes:            HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}[nodetype]
  Value changes:            HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}[provider]
  Value changes:            HKLM\software\microsoft\mmc\snapins\{95ad72f0-44ce-11d0-ae29-
00aa004b9986}[version]
  Value changes:            HKLM\software\microsoft\mmc\nodetypes\{5401e3e9-f5f6-11d1-b4f7-
00c04fc2db8d}[]
  Value changes:            HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-
00c04fd8d5b0}\extensions\namespace[{95ad72f0-44ce-11d0-ae29-00aa004b9986}]
  Value changes:            HKLM\software\microsoft\mmc\nodetypes\{476e6449-aaff-11d0-b944-
00c04fd8d5b0}\dynamic extensions[{95ad72f0-44ce-11d0-ae29-00aa004b9986}]
  Value changes:            HKLM\system\currentcontrolset\control\server applications[{95ad72f0-
44ce-11d0-ae29-00aa004b9986}]
  Value changes:            HKCR\ixsso.query[]
  Value changes:            HKCR\ixsso.query\clsid[]
  Value changes:            HKCR\ixsso.query\curver[]
  Value changes:            HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}[]
  Value changes:            HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\inprocserver32[]
  Value changes:            HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-
1e486b2fef9d}\inprocserver32[threadingmodel]
  Value changes:            HKCR\clsid\{eafdf8b3-3be5-4e05-bf86-1e486b2fef9d}\progid[]
  Value changes:            HKCR\ixsso.query.3[]
  Value changes:            HKCR\ixsso.query.3\clsid[]
  Value changes:            HKCR\ixsso.query.2[]
  Value changes:            HKCR\ixsso.query.2\clsid[]
  Value changes:            HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}[]
  Value changes:            HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\inprocserver32[]
  Value changes:            HKCR\clsid\{a4463024-2b6f-11d0-bfbc-
0020f8008024}\inprocserver32[threadingmodel]
  Value changes:            HKCR\clsid\{a4463024-2b6f-11d0-bfbc-0020f8008024}\progid[]
  Value changes:            HKCR\ixsso.util[]
  Value changes:            HKCR\ixsso.util\clsid[]
  Value changes:            HKCR\ixsso.util\curver[]
  Value changes:            HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}[]
  Value changes:            HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\inprocserver32[]
  Value changes:            HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-
```

0020f8008024}\inprocserver32[threadingmodel]
  Value changes: HKCR\clsid\{0c16c27e-a6e7-11d0-bfc3-0020f8008024}\progid[]
  Value changes: HKCR\ixsso.util.2[]
  Value changes: HKCR\ixsso.util.2\clsid[]
  Value changes: HKCR\clsid\{eec97550-47a9-11cf-b952-00aa0051fe20}[]
  Value changes: HKCR\clsid\{eec97550-47a9-11cf-b952-
00aa0051fe20}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
  Value changes: HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}[]
  Value changes: HKCR\clsid\{e0ca5340-4534-11cf-b952-00aa0051fe20}\inprocserver32[]
  Value changes: HKCR\clsid\{e0ca5340-4534-11cf-b952-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes: HKCR\.odc\persistenthandler[]
  Value changes: HKCR\.hhc\persistenthandler[]
  Value changes: HKCR\.htm\persistenthandler[]
  Value changes: HKCR\.html\persistenthandler[]
  Value changes: HKCR\.htx\persistenthandler[]
  Value changes: HKCR\.stm\persistenthandler[]
  Value changes: HKCR\.htw\persistenthandler[]
  Value changes: HKCR\.asp\persistenthandler[]
  Value changes: HKCR\.aspx\persistenthandler[]
  Value changes: HKCR\.ascx\persistenthandler[]
  Value changes: HKCR\.css\persistenthandler[]
  Value changes: HKCR\clsid\{3050f4d8-98b5-11cf-bb82-00aa00bdce0b}\persistenthandler[]
  Value changes: HKCR\.htt\persistenthandler[]
  Value changes: HKCR\clsid\{98de59a0-d175-11cd-a7bd-00006b827d94}[]
  Value changes: HKCR\clsid\{98de59a0-d175-11cd-a7bd-
00006b827d94}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
  Value changes: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}[]
  Value changes: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-00aa004b9986}\inprocserver32[]
  Value changes: HKCR\clsid\{f07f3920-7b8c-11cf-9be8-
00aa004b9986}\inprocserver32[threadingmodel]
  Value changes: HKCR\clsid\{00020906-0000-0000-c000-000000000046}\persistenthandler[]
  Value changes: HKCR\clsid\{64818d11-4f9b-11cf-86ea-00aa00b929e8}\persistenthandler[]
  Value changes: HKCR\clsid\{64818d10-4f9b-11cf-86ea-00aa00b929e8}\persistenthandler[]
  Value changes: HKCR\clsid\{00020820-0000-0000-c000-000000000046}\persistenthandler[]
  Value changes: HKCR\clsid\{00020821-0000-0000-c000-000000000046}\persistenthandler[]
  Value changes: HKCR\clsid\{00020900-0000-0000-c000-000000000046}\persistenthandler[]
  Value changes: HKCR\clsid\{ea7bae70-fb3b-11cd-a903-00aa00510ea3}\persistenthandler[]
  Value changes: HKCR\clsid\{ea7bae71-fb3b-11cd-a903-00aa00510ea3}\persistenthandler[]
  Value changes: HKCR\clsid\{00020811-0000-0000-c000-000000000046}\persistenthandler[]
  Value changes: HKCR\clsid\{00020810-0000-0000-c000-000000000046}\persistenthandler[]
  Value changes: HKCR\.doc\persistenthandler[]
  Value changes: HKCR\.dot\persistenthandler[]
  Value changes: HKCR\.pot\persistenthandler[]
  Value changes: HKCR\.ppt\persistenthandler[]
  Value changes: HKCR\.pps\persistenthandler[]
  Value changes: HKCR\.xlb\persistenthandler[]
  Value changes: HKCR\.xlc\persistenthandler[]
  Value changes: HKCR\.xls\persistenthandler[]
  Value changes: HKCR\.xlt\persistenthandler[]
  Value changes: HKCR\microsoft.isadm.1[]
  Value changes: HKCR\microsoft.isadm.1\clsid[]
  Value changes: HKCR\microsoft.isadm[]
  Value changes: HKCR\microsoft.isadm\curver[]
  Value changes: HKCR\microsoft.isadm\clsid[]
  Value changes: HKCR\microsoft.iscatadm.1[]
  Value changes: HKCR\microsoft.iscatadm.1\clsid[]
  Value changes: HKCR\microsoft.iscatadm[]
  Value changes: HKCR\microsoft.iscatadm\curver[]
  Value changes: HKCR\microsoft.iscatadm\clsid[]
  Value changes: HKCR\microsoft.isscopeadm.1[]
  Value changes: HKCR\microsoft.isscopeadm.1\clsid[]
  Value changes: HKCR\microsoft.isscopeadm[]
  Value changes: HKCR\microsoft.isscopeadm\curver[]
  Value changes: HKCR\microsoft.isscopeadm\clsid[]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\english_us[locale]
  Value changes: HKCR\clsid\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}[]
  Value changes: HKCR\clsid\{eeed4c20-7f1b-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes: HKCR\clsid\{eeed4c20-7f1b-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\english_us[stemmerclass]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\english_uk[locale]
  Value changes: HKCR\clsid\{d99f7670-7f1a-11ce-be57-00aa0051fe20}[]
  Value changes: HKCR\clsid\{d99f7670-7f1a-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes: HKCR\clsid\{d99f7670-7f1a-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\english_uk[stemmerclass]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\french_french[locale]

```
  Value changes:            HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}[]
  Value changes:            HKCR\clsid\{59e09848-8099-101b-8df3-00000b65c3b5}\inprocserver32[]
  Value changes:            HKCR\clsid\{59e09848-8099-101b-8df3-
00000b65c3b5}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\french_french[wbreakerclass]
  Value changes:            HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:            HKCR\clsid\{2a6eb050-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:            HKCR\clsid\{2a6eb050-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\french_french[stemmerclass]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\german_german[locale]
  Value changes:            HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}[]
  Value changes:            HKCR\clsid\{9b08e210-e51b-11cd-bc7f-00aa003db18e}\inprocserver32[]
  Value changes:            HKCR\clsid\{9b08e210-e51b-11cd-bc7f-
00aa003db18e}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\german_german[wbreakerclass]
  Value changes:            HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:            HKCR\clsid\{510a4910-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:            HKCR\clsid\{510a4910-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\german_german[stemmerclass]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian[locale]
  Value changes:            HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}[]
  Value changes:            HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-00aa004bbb1f}\inprocserver32[]
  Value changes:            HKCR\clsid\{fd86b5d0-12c6-11ce-bd31-
00aa004bbb1f}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian[wbreakerclass]
  Value changes:            HKCR\clsid\{6d36ce10-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:            HKCR\clsid\{6d36ce10-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:            HKCR\clsid\{6d36ce10-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\italian_italian[stemmerclass]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\swedish_default[locale]
  Value changes:            HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}[]
  Value changes:            HKCR\clsid\{01c6b350-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32[]
  Value changes:            HKCR\clsid\{01c6b350-12c7-11ce-bd31-
00aa004bbb1f}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\swedish_default[wbreakerclass]
  Value changes:            HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:            HKCR\clsid\{9478f640-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:            HKCR\clsid\{9478f640-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\swedish_default[stemmerclass]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\spanish_modern[locale]
  Value changes:            HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}[]
  Value changes:            HKCR\clsid\{0285b5c0-12c7-11ce-bd31-00aa004bbb1f}\inprocserver32[]
  Value changes:            HKCR\clsid\{0285b5c0-12c7-11ce-bd31-
00aa004bbb1f}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\spanish_modern[wbreakerclass]
  Value changes:            HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}[]
  Value changes:            HKCR\clsid\{b0516ff0-7f1c-11ce-be57-00aa0051fe20}\inprocserver32[]
  Value changes:            HKCR\clsid\{b0516ff0-7f1c-11ce-be57-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\spanish_modern[stemmerclass]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\dutch_dutch[locale]
  Value changes:            HKCR\clsid\{66b3711d-8bf2-11ce-be59-00aa0051fe20}[]
  Value changes:            HKCR\clsid\{66b3711d-8bf2-11ce-be59-00aa0051fe20}\inprocserver32[]
  Value changes:            HKCR\clsid\{66b3711d-8bf2-11ce-be59-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\dutch_dutch[wbreakerclass]
  Value changes:            HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}[]
  Value changes:            HKCR\clsid\{860d28d0-8bf4-11ce-be59-00aa0051fe20}\inprocserver32[]
  Value changes:            HKCR\clsid\{860d28d0-8bf4-11ce-be59-
00aa0051fe20}\inprocserver32[threadingmodel]
  Value changes:
HKLM\system\currentcontrolset\control\contentindex\language\dutch_dutch[stemmerclass]
  Value changes:            HKCR\.nws[]
```

```
  Value changes:            HKCR\microsoft internet news message[]
  Value changes:            HKCR\microsoft internet news message\clsid[]
  Value changes:            HKCR\clsid\{5645c8c0-e277-11cf-8fda-00aa00a14f93}[]
  Value changes:            HKCR\clsid\{5645c8c0-e277-11cf-8fda-00aa00a14f93}\persistenthandler[]
  Value changes:            HKCR\clsid\{5645c8c1-e277-11cf-8fda-
00aa00a14f93}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
  Value changes:            HKCR\clsid\{5645c8c2-e277-11cf-8fda-00aa00a14f93}\inprocserver32[]
  Value changes:            HKCR\clsid\{5645c8c2-e277-11cf-8fda-
00aa00a14f93}\inprocserver32[threadingmodel]
  Value changes:            HKCR\.eml[]
  Value changes:            HKCR\microsoft internet mail message[]
  Value changes:            HKCR\microsoft internet mail message\clsid[]
  Value changes:            HKCR\clsid\{5645c8c3-e277-11cf-8fda-00aa00a14f93}[]
  Value changes:            HKCR\clsid\{5645c8c3-e277-11cf-8fda-00aa00a14f93}\persistenthandler[]
  Value changes:            HKCR\clsid\{5645c8c4-e277-11cf-8fda-
00aa00a14f93}\persistentaddinsregistered\{89bcb740-6119-101a-bcb7-00dd010655af}[]
  Value changes:            HKCR\enguswrdbrk.enguswrdbrk.1[]
  Value changes:            HKCR\enguswrdbrk.enguswrdbrk.1\clsid[]
  Value changes:            HKCR\enguswrdbrk.enguswrdbrk[]
  Value changes:            HKCR\enguswrdbrk.enguswrdbrk\curver[]
  Value changes:            HKCR\engukwrdbrk.engukwrdbrk.1[]
  Value changes:            HKCR\engukwrdbrk.engukwrdbrk.1\clsid[]
  Value changes:            HKCR\engukwrdbrk.engukwrdbrk[]
  Value changes:            HKCR\engukwrdbrk.engukwrdbrk\curver[]
  Value changes:            HKCR\frnfrnwrdbrk.frnfrnwrdbrk.1[]
  Value changes:            HKCR\frnfrnwrdbrk.frnfrnwrdbrk.1\clsid[]
  Value changes:            HKCR\frnfrnwrdbrk.frnfrnwrdbrk[]
  Value changes:            HKCR\frnfrnwrdbrk.frnfrnwrdbrk\curver[]
  Value changes:            HKCR\itlitlwrdbrk.itlitlwrdbrk.1[]
  Value changes:            HKCR\itlitlwrdbrk.itlitlwrdbrk.1\clsid[]
  Value changes:            HKCR\itlitlwrdbrk.itlitlwrdbrk[]
  Value changes:            HKCR\itlitlwrdbrk.itlitlwrdbrk\curver[]
  Value changes:            HKCR\spnmdrwrdbrk.spnmdrwrdbrk.1[]
  Value changes:            HKCR\spnmdrwrdbrk.spnmdrwrdbrk.1\clsid[]
  Value changes:            HKCR\spnmdrwrdbrk.spnmdrwrdbrk[]
  Value changes:            HKCR\spnmdrwrdbrk.spnmdrwrdbrk\curver[]
  Value changes:
HKU\.default\software\microsoft\windows\currentversion\explorer\mountpoints2\c[baseclass]
  Value changes:            HKU\.default\software\microsoft\windows\currentversion\explorer\shell
folders[personal]
  Value changes:            HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common documents]
  Value changes:            HKU\.default\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
  Value changes:            HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common desktop]
  Value changes:            HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{fbf23b40-e3f0-101b-8488-00aa003e56f8} {0000010b-0000-0000-c000-000000000046}
0x401]
  Value changes:            HKU\.default\software\microsoft\windows\currentversion\shell
extensions\cached[{eb9b1153-3b57-4e68-959a-a3266bc3d7fe} {0000010b-0000-0000-c000-000000000046}
0x401]
  Value changes:            HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
```