Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 34, Task ID: 134

Task ID:	134
Risk Level:	6
Date Processed:	2016-04-28 12:50:35 (UTC)
Processing Time:	61.2 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\4221e71f07b19e015be63e5e85c7048e.exe"
Sample ID:	34
Type:	basic
Owner:	admin
Label:	4221e71f07b19e015be63e5e85c7048e
Date Added:	2016-04-28 12:44:53 (UTC)
File Type:	PE32:win32:gui
File Size:	659504 bytes
MD5:	4221e71f07b19e015be63e5e85c7048e
SHA256:	0fdbfdf3a384ff2424ccd281acab7caa1cab55145bfa68de95d10b115222f78a
Description:	None

Pattern Matching Results

6 Tries to detect VM environment
5 Creates process in suspicious location
5 PE: Contains compressed section
5 Opens Copy Hook Handlers key
5 Packer: UPX
2 PE: Nonstandard section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process: C:\WINDOWS\Temp\4221e71f07b19e015be63e5e85c7048e.exe ["c:\windows\temp\4221e71f07b19e015be63e5e85c7048e.exe"]
Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\startup.exe ["C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\startup.exe"]
Creates process: C:\WINDOWS\system32\ntvdm.exe ["C:\WINDOWS\system32\ntvdm.exe" -f -i1 -w -a C:\WINDOWS\system32\krnl386.exe]
Terminates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\startup.exe
Terminates process: C:\WINDOWS\Temp\4221e71f07b19e015be63e5e85c7048e.exe

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.IN
Creates mutex: \BaseNamedObjects\ZonesCounterMutex
Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates event: \BaseNamedObjects\userenv: User Profile setup event
Creates event: \BaseNamedObjects\ShellCopyEngineRunning
Creates event: \BaseNamedObjects\ShellCopyEngineFinished
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

Creates semaphore: \BaseNamedObjects\C:?DOCUME~1?ADMIN?LOCALS~1?TEMP?RARSFX0?STARTUP.EXE

File System Events

Creates: C:\Documents and Settings\Admin
Creates: C:\DOCUME~1
Creates: C:\DOCUME~1\Admin
Creates: C:\DOCUME~1\Admin\LOCALS~1
Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_user1.cab
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_ISDEL.EXE
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_setup.dll
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_sys1.cab
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_INST32I.EX_
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\DATA.TAG
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\data1.cab
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\lang.dat
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\layout.bin
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\os.dat
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\SETUP.EXE
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\SETUP.INI
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\setup.ins
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\setup.lid
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\startup.exe
Creates: C:\WINDOWS\Temp\scs1.tmp
Creates: C:\WINDOWS\Temp\scs2.tmp
Opens: C:\WINDOWS\Prefetch\4221E71F07B19E015BE63E5E85C70-22313389.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\Temp\4221e71f07b19e015be63e5e85c7048e.exe
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\SHELL32.DLL.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.DLL.124.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
Opens: C:\WINDOWS\system32\riched32.dll
Opens: C:\WINDOWS\system32\riched20.dll
Opens: C:\WINDOWS\Fonts\sserife.fon
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\system32\ole32.dll
Opens: C:\WINDOWS\win.ini
Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_user1.cab
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_ISDEL.EXE
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_setup.dll
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_sys1.cab
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_INST32I.EX_
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\DATA.TAG
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\data1.cab
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\lang.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\layout.bin
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\os.dat
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\SETUP.EXE
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\SETUP.INI
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\setup.ins
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\setup.lid
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\startup.exe
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\netapi32.dll
Opens: C:\WINDOWS\system32\setupapi.dll
Opens: C:\
Opens: C:\Documents and Settings
Opens: C:\Documents and Settings\Admin\My Documents\desktop.ini
Opens: C:\Documents and Settings\All Users

Opens: C:\Documents and Settings\All Users\Documents\desktop.ini
Opens: C:\WINDOWS\system32\clbcatq.dll
Opens: C:\WINDOWS\system32\comres.dll
Opens: C:\WINDOWS\Registration\R000000000007.clb
Opens: C:\WINDOWS\system32\urlmon.dll
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\Documents and Settings\Admin\Local Settings
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\systest.sdb
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\startup.exe.Manifest
Opens: C:\WINDOWS\Prefetch\STARTUP.EXE-0A79CD8C.pf
Opens: C:\WINDOWS\system32\msvbvm60.dll
Opens: C:\WINDOWS\system32\sxs.dll
Opens: C:\WINDOWS\system32\ntvdm.exe
Opens: C:\WINDOWS\system32\ntvdm.exe.Manifest
Opens: C:\WINDOWS\Prefetch\NTVDM.EXE-1A10A423.pf
Opens: C:\WINDOWS_default.pif
Opens: C:\WINDOWS\system32\ntvdmd.dll
Opens: C:\WINDOWS\system32\ntio.sys
Opens: C:\WINDOWS\system32\ntdos.sys
Opens: C:\WINDOWS\system32\CONFIG.NT
Opens: C:\WINDOWS\Temp\scs1.tmp
Opens: C:\WINDOWS\system32\himem.sys
Opens: C:\WINDOWS\system32\country.sys
Opens: C:
Opens: C:\WINDOWS\system32\command.com
Opens: C:\WINDOWS\SYSTEM32
Opens: C:\WINDOWS\system32\AUTOEXEC.NT
Opens: C:\WINDOWS\Temp\scs2.tmp
Opens: C:\Program Files
Opens: C:\WINDOWS\system32
Opens: C:\WINDOWS\system32\mscdexnt.exe
Opens: C:\WINDOWS\system32\redir.exe
Opens: C:\WINDOWS\system32\dosx.exe
Opens: C:\WINDOWS\system.ini
Opens: C:\WINDOWS\WINHELP.INI
Opens: C:\WINDOWS\system32\shdocvw.dll
Opens: C:\WINDOWS\system32\mydocs.dll
Opens: C:\WINDOWS\system32\mydocs.dll.123.Manifest
Opens: C:\WINDOWS\system32\mydocs.dll.123.Config
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\ntshrui.dll
Opens: C:\WINDOWS\Temp\bc8b46bf-dfae-4199-b4c2-593ea8b15843
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_user1.cab
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_ISDEL.EXE
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_setup.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_sys1.cab
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_INST32I.EX_
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\DATA.TAG
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\data1.cab
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\lang.dat
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\layout.bin
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\os.dat
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\SETUP.EXE
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\SETUP.INI
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\setup.ins
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\setup.lid
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\startup.exe
Writes to: C:\WINDOWS\Temp\scs1.tmp
Writes to: C:\WINDOWS\Temp\scs2.tmp
Reads from: C:\WINDOWS\Temp\4221e71f07b19e015be63e5e85c7048e.exe
Reads from: C:\WINDOWS\win.ini
Reads from: C:\Documents and Settings\Admin\My Documents\desktop.ini
Reads from: C:\Documents and Settings\All Users\Documents\desktop.ini
Reads from: C:\WINDOWS\Registration\R000000000007.clb
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\startup.exe
Reads from: C:\WINDOWS_default.pif
Reads from: C:\WINDOWS\system32\ntio.sys
Reads from: C:\WINDOWS\system32\ntdos.sys
Reads from: C:\WINDOWS\system32\CONFIG.NT
Reads from: C:\WINDOWS\Temp\scs1.tmp
Reads from: C:\WINDOWS\system32\himem.sys

Reads from: C:\WINDOWS\system32\country.sys
Reads from: C:\WINDOWS\system32\command.com
Reads from: C:\WINDOWS\system32\AUTOEXEC.NT
Reads from: C:\WINDOWS\Temp\scs2.tmp
Reads from: C:\WINDOWS\system32\mscdexnt.exe
Reads from: C:\WINDOWS\system32\redir.exe
Reads from: C:\WINDOWS\system32\dosx.exe
Reads from: C:\WINDOWS\system.ini
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\DATA.TAG
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\data1.cab
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\lang.dat
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\layout.bin
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\os.dat
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\SETUP.EXE
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\SETUP.INI
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\setup.ins
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\setup.lid
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\startup.exe
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_INST32I.EX_
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_ISDEL.EXE
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_setup.dll
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_sys1.cab
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0_user1.cab
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKCU\software\vb and vba program settings\atstart\preferences
Creates key: HKCU\software
Creates key: HKCU\software\vb and vba program settings
Creates key: HKCU\software\vb and vba program settings\atstart
Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached
Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\4221e71f07b19e015be63e5e85c7048e.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKLM\system\setup
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\riched20.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\riched32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\4221e71f07b19e015be63e5e85c7048e.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCU\software\microsoft\ctf
Opens key: HKLM\software\microsoft\ctf\systemshared
Opens key: HKCU\software\microsoft\windows nt\currentversion\windows
Opens key: HKCU\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\langbaraddin\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\netapi32.dll
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\4221e71f07b19e015be63e5e85c7048e.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\4221e71f07b19e015be63e5e85c7048e.exe
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
Opens key: HKCU\software\classes\drive\shellex\folderextensions
Opens key: HKCR\drive\shellex\folderextensions
Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe
Opens key: HKCU\software\classes\.exe
Opens key: HKCR\.exe
Opens key: HKCU\software\classes\exefile
Opens key: HKCR\exefile
Opens key: HKCU\software\classes\exefile\curver
Opens key: HKCR\exefile\curver
Opens key: HKCR\exefile\
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\
Opens key: HKCU\software\microsoft\windows\currentversion\policies\system
Opens key: HKCU\software\classes\exefile\shellex\iconhandler
Opens key: HKCR\exefile\shellex\iconhandler
Opens key: HKCU\software\classes\systemfileassociations\.exe
Opens key: HKCR\systemfileassociations\.exe
Opens key: HKCU\software\classes\systemfileassociations\application
Opens key: HKCR\systemfileassociations\application
Opens key: HKCU\software\classes\exefile\clsid
Opens key: HKCR\exefile\clsid
Opens key: HKCU\software\classes*
Opens key: HKCR*
Opens key: HKCU\software\classes*\clsid
Opens key: HKCR*\clsid
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\setupapi.dll
Opens key: HKLM\system\currentcontrolset\control\minint
Opens key: HKLM\system\wpa\pnp
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Opens key: HKCU\software\classes\directory
Opens key: HKCR\directory
Opens key: HKCU\software\classes\directory\curver
Opens key: HKCR\directory\curver
Opens key: HKCR\directory\
Opens key: HKCU\software\classes\directory\shellex\iconhandler
Opens key: HKCR\directory\shellex\iconhandler
Opens key: HKCU\software\classes\directory\clsid
Opens key: HKCR\directory\clsid
Opens key: HKCU\software\classes\folder
Opens key: HKCR\folder
Opens key: HKCU\software\classes\folder\clsid
Opens key: HKCR\folder\clsid
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks
Opens key: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
Opens key: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
Opens key: HKLM\software\microsoft\windows\currentversion\policies\associations
Opens key: HKCU\software\microsoft\windows\currentversion\policies\associations
Opens key: HKCU\software\classes\.ade
Opens key: HKCR\.ade
Opens key: HKCU\software\classes\.adp
Opens key: HKCR\.adp
Opens key: HKCU\software\classes\.app
Opens key: HKCR\.app
Opens key: HKCU\software\classes\.asp
Opens key: HKCR\.asp
Opens key: HKCU\software\classes\.bas
Opens key: HKCR\.bas
Opens key: HKCU\software\classes\.bat
Opens key: HKCR\.bat
Opens key: HKCU\software\classes\.cer
Opens key: HKCR\.cer
Opens key: HKCU\software\classes\.chm
Opens key: HKCR\.chm
Opens key: HKCU\software\classes\.cmd

Opens key: HKCR\.cmd
Opens key: HKCU\software\classes\.com
Opens key: HKCR\.com
Opens key: HKCU\software\classes\.cpl
Opens key: HKCR\.cpl
Opens key: HKCU\software\classes\.crt
Opens key: HKCR\.crt
Opens key: HKCU\software\classes\.csh
Opens key: HKCR\.csh
Opens key: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comres.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\clbcatq.dll
Opens key: HKLM\software\microsoft\com3\debug
Opens key: HKLM\software\classes
Opens key: HKU\
Opens key: HKCR\clsid
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll
Opens key: HKCU\software\classes\protocols\name-space handler\
Opens key: HKCR\protocols\name-space handler
Opens key: HKCU\software\classes\protocols\name-space handler
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key: HKLM\software\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com\related
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKCU\software\microsoft\internet explorer\ietld
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key: HKCU\software\classes\exefile\shell
Opens key: HKCR\exefile\shell
Opens key: HKCU\software\classes\exefile\shell\open
Opens key: HKCR\exefile\shell\open
Opens key: HKCU\software\classes\exefile\shell\open\command
Opens key: HKCR\exefile\shell\open\command
Opens key:
HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\startup.exe
Opens key: HKCU\software\classes\exefile\shell\open\ddeexec
Opens key: HKCR\exefile\shell\open\ddeexec
Opens key: HKCU\software\classes\applications\startup.exe
Opens key: HKCR\applications\startup.exe
Opens key: HKCU\software\microsoft\windows\shellnoroam
Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache
Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
Opens key: HKLM\system\wpa\tabletpc
Opens key: HKLM\system\wpa\mediacenter

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

Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\startup.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvbvm60.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\startup.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll
Opens key: HKLM\system\currentcontrolset\control\nls\codepage
Opens key: HKLM\software\microsoft\vba\monitors
Opens key: HKCU\software\microsoft\internet explorer\main
Opens key: HKLM\system\currentcontrolset\control\wow
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntvdm.exe
Opens key: HKLM\system\currentcontrolset\control\wow\cpuenv
Opens key: HKLM\hardware\description\system
Opens key: HKLM\system\currentcontrolset\control\virtualdevicedrivers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntvdmd.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\terminal server
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
Opens key: HKLM\system\currentcontrolset\control\productoptions
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows
Opens key: HKLM\software\microsoft\windows\html help
Opens key: HKLM\software\microsoft\windows\help
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers
Opens key: HKCR\directory\shellex\copyhookhandlers
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\cdf
Opens key: HKCR\directory\shellex\copyhookhandlers\cdf
Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-
00c04fd75d13}\inprocserver32
Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\filesystem
Opens key: HKCR\directory\shellex\copyhookhandlers\filesystem
Opens key: HKCU\software\classes\clsid\{217fc9c0-3aea-1069-a2db-
08002b30309d}\inprocserver32
Opens key: HKCR\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\mydocuments
Opens key: HKCR\directory\shellex\copyhookhandlers\mydocuments
Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-
006008059367}\inprocserver32
Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mydocs.dll
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ecf03a33-103d-11d2-
854d-006008059367}
Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\sharing
Opens key: HKCR\directory\shellex\copyhookhandlers\sharing
Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\inprocserver32
Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\setup.exe
Opens key: HKLM\software\microsoft\windows\currentversion\app paths_isdel.exe
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]

Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[4221e71f07b19e015be63e5e85c7048e]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[4221e71f07b19e015be63e5e85c7048e]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\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: 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: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinterval]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
Queries value: HKCR\.exe[]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]

Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
Queries value: HKCR\exefile[docobject]
Queries value: HKCR\exefile[browseinplace]
Queries value: HKCR\exefile[isshortcut]
Queries value: HKCR\exefile[alwaysshowext]
Queries value: HKCR\exefile[nevershowext]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
Queries value: HKLM\system\wpa\pnp[seed]
Queries value: HKLM\system\setup[osloaderpath]
Queries value: HKLM\system\setup[systempartition]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[generation]
Queries value: HKCR\directory[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32[loadwithoutcom]
Queries value: HKCR\.asp[]
Queries value: HKCR\.bat[]
Queries value: HKCR\.cer[]
Queries value: HKCR\.chm[]
Queries value: HKCR\.cmd[]
Queries value: HKCR\.com[]
Queries value: HKCR\.cpl[]
Queries value: HKCR\.crt[]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]

Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[4221e71f07b19e015be63e5e85c7048e.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[createuricachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enablepunycode]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[enablepunycode]
Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablesecuritysettingscheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[flags]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[4221e71f07b19e015be63e5e85c7048e.exe]
Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[4221e71f07b19e015be63e5e85c7048e.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1806]
Queries value: HKCR\exefile\shell[]
Queries value: HKCR\exefile\shell\open\command[]
Queries value: HKCR\exefile\shell\open\command[command]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\rarsfx0\startup.exe]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]
Queries value: HKLM\system\currentcontrolset\control\session manager\appcompatibility[disableappcompat]
Queries value: HKLM\system\wpa\mediacenter[installed]
Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemsize]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]

Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[startup]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[startup]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value: HKCU\software\microsoft\internet explorer\main[start page]
Queries value: HKLM\system\currentcontrolset\control\wow[wowcmdline]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[ntvdm]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[ntvdm]
Queries value: HKLM\hardware\description\system[identifier]
Queries value: HKLM\hardware\description\system[configuration data]
Queries value: HKLM\system\currentcontrolset\control\wow[romfontpointers]
Queries value: HKLM\system\currentcontrolset\control\virtualdevicedrivers[vdd]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[bootdir]
Queries value: HKLM\software\microsoft\windows nt\currentversion\terminal
server[rootdrive]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
Queries value: HKLM\system\currentcontrolset\control\session manager\environment[temp]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer[nofilefolderconnection]
Queries value: HKCR\directory\shellex\copyhookhandlers\cdf[]
Queries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[]
Queries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-
00c04fd75d13}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{67ea19a0-ccef-11d0-8024-00c04fd75d13}]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{67ea19a0-ccef-11d0-8024-00c04fd75d13}]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{67ea19a0-ccef-11d0-8024-00c04fd75d13} {00000000-0000-0000-c000-000000000046}
0x401]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{67ea19a0-ccef-11d0-8024-00c04fd75d13} {00000000-0000-0000-c000-000000000046}
0x401]
Queries value: HKCR\directory\shellex\copyhookhandlers\filesystem[]
Queries value: HKCR\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32[]
Queries value: HKCR\directory\shellex\copyhookhandlers\mydocuments[]
Queries value: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32[]
Queries value: HKCR\clsid\{ecf03a33-103d-11d2-854d-
006008059367}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{ecf03a33-103d-11d2-854d-006008059367}]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{ecf03a33-103d-11d2-854d-006008059367}]
Queries value: HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{ecf03a33-103d-11d2-854d-006008059367} {00000000-0000-0000-c000-000000000046}
0x401]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{ecf03a33-103d-11d2-854d-006008059367} {00000000-0000-0000-c000-000000000046}
0x401]
Queries value: HKCR\directory\shellex\copyhookhandlers\sharing[]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\inprocserver32[loadwithoutcom]
Queries value: HKLM\software\microsoft\windows\currentversion\shell

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

folders[commonmusic]
  Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[commonvideo]
  Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[oem links]
  Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cd burning]
  Queries value: HKLM\software\microsoft\windows\currentversion\app paths\setup.exe[]
  Sets/Creates value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\rarsfx0\startup.exe]
  Sets/Creates value: HKCU\software\vb and vba program settings\atstart\preferences[homepage]
  Value changes: HKLM\software\microsoft\cryptography\rng[seed]
  Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[personal]
  Value changes: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]
  Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common documents]
  Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[desktop]
  Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common desktop]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[uncasintranet]
  Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[autodetect]
  Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
  Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cookies]