

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3303, Task ID: 721

Task ID:	721
Risk Level:	10
Date Processed:	2016-05-18 10:30:52 (UTC)
Processing Time:	62.63 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\70b2225f430facf31ca65621c234f09e.exe"
Sample ID:	3303
Type:	basic
Owner:	admin
Label:	70b2225f430facf31ca65621c234f09e
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	855552 bytes
MD5:	70b2225f430facf31ca65621c234f09e
SHA256:	375c6e3dfa967d9d6760d4e8ca0868c864fecde2735ce0d1f189b3b2aef512b7
Description:	None

Pattern Matching Results

6	Modifies registry autorun entries
6	Tries to detect VM environment
10	Creates malicious events: Kelihos trojan 2 [Spam]
3	Connects to local host
5	PE: Contains compressed section
5	Adds autostart object

Process/Thread Events

Creates process:	C:\windows\temp\70b2225f430facf31ca65621c234f09e.exe
	["C:\windows\temp\70b2225f430facf31ca65621c234f09e.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED

File System Events

Creates:	C:\Windows\Temp\tmp.exe
Opens:	C:\Windows\Prefetch\70B2225F430FACF31CA65621C234F-988C8555.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\UFAT.dll
Opens:	C:\Windows\System32\ufat.dll
Opens:	C:\windows\temp\ulib.dll
Opens:	C:\Windows\System32\ulib.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\ifsutil.dll
Opens:	C:\Windows\System32\ifsutil.dll
Opens:	C:\windows\temp\MMCBASE.dll
Opens:	C:\Windows\System32\mmcbase.dll
Opens:	C:\windows\temp\MFC42u.dll
Opens:	C:\Windows\System32\mfc42u.dll
Opens:	C:\windows\temp\ODBC32.dll
Opens:	C:\Windows\System32\odbc32.dll
Opens:	C:\windows\temp\RPCNS4.dll
Opens:	C:\Windows\System32\RpcNs4.dll
Opens:	C:\windows\temp\SQLUNIRL.dll
Opens:	C:\Windows\System32\sqlunirl.dll
Opens:	C:\windows\temp\WINSPOOL.DRV
Opens:	C:\Windows\System32\winspool.drv
Opens:	C:\windows\temp\70b2225f430facf31ca65621c234f09e.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af	
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\en-US\setupapi.dll.mui
Opens:	C:\Windows\System32\en-US\ulib.dll.mui
Opens:	C:\Windows\System32\odbcint.dll
Opens:	C:\Windows\System32\en-US\odbcint.dll.mui
Opens:	C:\Windows\System32\en-US\MFC42u.dll.mui
Opens:	C:\Windows\system32\MFC42LOC.DLL
Opens:	C:\Windows\system32\MFC42LOC.DLL.DLL
Opens:	C:\Windows\System32\en-US\mmcbase.dll.mui
Opens:	C:\Windows\System32\DWWIN.EXE
Opens:	C:\Windows\System32\nddeapi.dll

Opens: C:\windows\temp\cmDial32.dll
 Opens: C:\Windows\System32\cmdial32.dll
 Opens: C:\windows\temp\cmpbk32.dll
 Opens: C:\Windows\System32\cmpbk32.dll
 Opens: C:\windows\temp\cmutil.dll
 Opens: C:\Windows\System32\cmutil.dll
 Opens: C:\windows\temp\eappcf.dll
 Opens: C:\Windows\System32\eappcf.dll
 Opens: C:\windows\temp\USERENV.dll
 Opens: C:\Windows\System32\userenv.dll
 Opens: C:\windows\temp\profapi.dll
 Opens: C:\Windows\System32\profapi.dll
 Opens: C:\windows\temp\DNSAPI.dll
 Opens: C:\Windows\System32\dnsapi.dll
 Opens: C:\windows\temp\IPHLPAPI.DLL
 Opens: C:\Windows\System32\IPHLPAPI.DLL
 Opens: C:\windows\temp\WINNSI.DLL
 Opens: C:\Windows\System32\winnsi.dll
 Opens: C:\windows\temp\MSWSOCK.dll
 Opens: C:\Windows\System32\mswsock.dll
 Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens: C:\Windows\System32\WSHTCPIP.DLL
 Opens: C:\Windows\Temp\70b2225f430facf31ca65621c234f09e.exe
 Opens: C:\Windows\Temp
 Opens: C:\Windows\Temp\tmp.exe
 Opens: C:\Windows\System32\en-US\KernelBase.dll.mui
 Opens: C:\Windows\System32\C_1256.NLS
 Opens: C:\Windows\System32\C_1251.NLS
 Opens: C:\Windows\System32\C_950.NLS
 Opens: C:\Windows\System32\C_1250.NLS
 Opens: C:\Windows\System32\C_1253.NLS
 Opens: C:\Windows\System32\C_1255.NLS
 Opens: C:\Windows\System32\C_932.NLS
 Opens: C:\Windows\System32\C_949.NLS
 Opens: C:\dev\urandom
 Opens: C:\windows\temp\dhcpcsvc.DLL
 Opens: C:\Windows\System32\dhcpcsvc.dll
 Opens: C:\windows\temp\wpcap.dll
 Opens: C:\Windows\system32\wpcap.dll
 Opens: C:\Windows\system\wpcap.dll
 Opens: C:\Windows\wpcap.dll
 Opens: C:\Windows\System32\Wbem\wpcap.dll
 Opens: C:\Windows\System32\WindowsPowerShell\v1.0\wpcap.dll
 Opens: C:\Windows\wcx_ftp.ini
 Opens: C:\
 Opens: C:\Users\Admin
 Opens: C:\Users\Admin\wcx_ftp.ini
 Opens: C:\Users\Admin\AppData\Roaming
 Opens: C:\Users\Admin\AppData\Roaming\FlashFXP\3\Sites.dat
 Opens: C:\Users\Admin\AppData\Roaming\FlashFXP\3\Quick.dat
 Opens: C:\Users\Admin\AppData\Roaming\FlashFXP\3\History.dat
 Opens: C:\Users\Admin\AppData\Roaming\FlashFXP\4\Sites.dat
 Opens: C:\Users\Admin\AppData\Roaming\FlashFXP\4\Quick.dat
 Opens: C:\Users\Admin\AppData\Roaming\FlashFXP\4\History.dat
 Opens: C:\Users\Admin\AppData\Local
 Opens: C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP Client
 2009\sites\Bookmarks\
 Opens: C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
 Client\2009\sites\Bookmarks\
 Opens: C:\ProgramData
 Opens: C:\ProgramData\BulletProof Software\BulletProof FTP Client
 2009\sites\Bookmarks\
 Opens: C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP
 Client\2010\sites\Bookmarks\
 Opens: C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
 Client\2010\sites\Bookmarks\
 Opens: C:\ProgramData\BulletProof Software\BulletProof FTP
 Client\2010\sites\Bookmarks\
 Opens: C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP Client
 2009\Default.bps
 Opens: C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
 Client\2009\Default.bps
 Opens: C:\ProgramData\BulletProof Software\BulletProof FTP Client
 2009\Default.bps
 Opens: C:\Users\Admin\AppData\Local\BulletProof Software\BulletProof FTP
 Client\2010\Default.bps
 Opens: C:\Users\Admin\AppData\Roaming\BulletProof Software\BulletProof FTP
 Client\2010\Default.bps
 Opens: C:\ProgramData\BulletProof Software\BulletProof FTP
 Client\2010\Default.bps
 Opens: C:\Users\Admin\AppData\Roaming\TurboFTP\addrbk.dat
 Opens: C:\windows\temp\SspiCli.dll
 Opens: C:\Windows\System32\sspicli.dll

```

Opens: C:\Users\Admin\AppData\Roaming\GPSSoftware\Directory
Opus\ConfigFiles\ftp.oxc
Opens: C:\Users\Admin\AppData\Roaming\GPSSoftware\Directory
Opus\Layouts\System\default.oll
Opens: C:\Users\Admin\AppData\Local\GPSSoftware\Directory
Opus\ConfigFiles\ftp.oxc
Opens: C:\Users\Admin\AppData\Local\GPSSoftware\Directory
Opus\Layouts\System\default.oll
Opens: C:\ProgramData\GPSSoftware\Directory Opus\ConfigFiles\ftp.oxc
Opens: C:\ProgramData\GPSSoftware\Directory Opus\Layouts\System\default.oll
Opens: C:\Windows\32BitFtp.ini
Opens: C:\Users\Admin\AppData\Roaming\VanDyke\Config\Sessions
Opens: C:\Users\Admin\AppData\Roaming\BitKinex\bitkinex.ds
Opens: C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP
Opens: C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP Pro
Opens: C:\Users\Admin\AppData\Roaming\GlobalSCAPE\CuteFTP Lite
Opens: C:\ProgramData\GlobalSCAPE\CuteFTP
Opens: C:\ProgramData\GlobalSCAPE\CuteFTP Pro
Opens: C:\ProgramData\GlobalSCAPE\CuteFTP Lite
Opens: C:\Program Files
Opens: C:\Program Files\CuteFTP
Opens: C:\Windows\win.ini
Opens: C:\Program Files\Common Files
Opens: C:\Program Files\Common Files\Ipswitch\WS_FTP
Opens: C:\Users\Admin\AppData\Roaming\Ipswitch\WS_FTP\Sites
Opens: C:\Users\Admin\AppData\Roaming\Ipswitch\WS_FTP Home\Sites
Opens: C:\ProgramData\Ipswitch\WS_FTP\Sites
Opens: C:\ProgramData\Ipswitch\WS_FTP Home\Sites
Opens: C:\Users\Admin\AppData\Local\Ipswitch\WS_FTP\Sites
Opens: C:\Users\Admin\AppData\Local\Ipswitch\WS_FTP Home\Sites
Opens: C:\Users\Admin\AppData\Roaming\NetDrive\NDSites.ini
Opens: C:\ProgramData\NetDrive\NDSites.ini
Opens: C:\Users\Admin\AppData\Local\NetDrive\NDSites.ini
Opens: C:\Users\Admin\AppData\Roaming\FileZilla\sitemanager.xml
Opens: C:\Users\Admin\AppData\Roaming\FileZilla\recentservers.xml
Opens: C:\Users\Admin\AppData\Roaming\FTP Explorer\profiles.xml
Opens: C:\ProgramData\FTP Explorer\profiles.xml
Opens: C:\Users\Admin\AppData\Local\FTP Explorer\profiles.xml
Opens: C:\Users\Admin\AppData\Roaming\SmartFTP\Favorites.dat
Opens: C:\Users\Admin\AppData\Roaming\SmartFTP\Client
2.0\Favorites\Favorites.dat
Opens: C:\Users\Admin\AppData\Roaming\SmartFTP\History.dat
Opens: C:\Users\Admin\AppData\Roaming\SmartFTP\Client 2.0\Favorites\
Opens: C:\ProgramData\SmartFTP\Favorites.dat
Opens: C:\ProgramData\SmartFTP\Client 2.0\Favorites\Favorites.dat
Opens: C:\ProgramData\SmartFTP\History.dat
Opens: C:\ProgramData\SmartFTP\Client 2.0\Favorites\
Opens: C:\Users\Admin\AppData\Roaming\FTPRush\RushSite.xml
Opens: C:\Users\Admin\AppData\Roaming\Frigate3\FtpSite.XML
Opens: C:\Documents and Settings\
Opens: C:\Users
Opens: C:\Users\All Users
Opens: C:\Users\Default User
Opens: C:\Users\Default
Opens: C:\Users\Admin\AppData\Roaming\Bitcoin\wallet.dat
Opens: C:\ProgramData\APPDATA\ROAMING\BITCOIN\WALLET.DAT
Opens: C:\Users\Default\AppData\Roaming\Bitcoin\wallet.dat
Opens: C:\Users\Public\AppData\Roaming\Bitcoin\wallet.dat
Opens: C:\Windows\System32\tzres.dll
Opens: C:\Windows\System32\en-US\tzres.dll.mui
Opens: C:\Windows\System32\wship6.dll
Reads from: C:\Windows\win.ini
Deletes: C:\Windows\Temp\tmp.exe

```

Network Events

Connects to:	127.0.0.1:49160
Connects to:	202.69.41.22:80
Connects to:	127.0.0.1:49163
Connects to:	78.139.153.136:80
Connects to:	127.0.0.1:49166
Connects to:	178.89.132.134:80
Connects to:	127.0.0.1:49169
Connects to:	123.200.28.134:80
Connects to:	127.0.0.1:49172
Connects to:	41.32.15.139:80
Connects to:	127.0.0.1:49175
Connects to:	58.146.205.132:80
Connects to:	127.0.0.1:49178
Connects to:	115.252.34.140:80
Connects to:	127.0.0.1:49181
Connects to:	188.231.142.132:80
Connects to:	127.0.0.1:49184

Connects to:	182.234.66.140:80
Connects to:	127.0.0.1:49187
Connects to:	31.25.90.132:80
Connects to:	127.0.0.1:49190
Connects to:	178.91.76.140:80
Connects to:	127.0.0.1:49193
Connects to:	217.23.203.95:80
Connects to:	127.0.0.1:49196
Connects to:	109.162.67.96:80
Connects to:	127.0.0.1:49199
Connects to:	188.73.171.98:80
Connects to:	127.0.0.1:49202
Connects to:	176.112.10.93:80
Connects to:	127.0.0.1:49205
Connects to:	190.198.41.99:80
Connects to:	127.0.0.1:49208
Connects to:	123.140.179.100:80
Connects to:	127.0.0.1:49211
Connects to:	50.128.222.92:80
Connects to:	127.0.0.1:49214
Connects to:	89.72.239.100:80
Connects to:	127.0.0.1:49217
Connects to:	180.149.209.103:80
Connects to:	111.125.235.23:80
Sends data to:	127.0.0.1:49160
Sends data to:	202.69.41.22:80
Sends data to:	127.0.0.1:49163
Sends data to:	78.139.153.136:80
Sends data to:	127.0.0.1:49166
Sends data to:	178.89.132.134:80
Sends data to:	127.0.0.1:49169
Sends data to:	123.200.28.134:80
Sends data to:	127.0.0.1:49172
Sends data to:	41.32.15.139:80
Sends data to:	127.0.0.1:49175
Sends data to:	58.146.205.132:80
Sends data to:	127.0.0.1:49178
Sends data to:	115.252.34.140:80
Sends data to:	127.0.0.1:49181
Sends data to:	188.231.142.132:80
Sends data to:	127.0.0.1:49184
Sends data to:	182.234.66.140:80
Sends data to:	127.0.0.1:49187
Sends data to:	31.25.90.132:80
Sends data to:	127.0.0.1:49190
Sends data to:	178.91.76.140:80
Sends data to:	127.0.0.1:49193
Sends data to:	217.23.203.95:80
Sends data to:	127.0.0.1:49196
Sends data to:	109.162.67.96:80
Sends data to:	127.0.0.1:49199
Sends data to:	188.73.171.98:80
Sends data to:	127.0.0.1:49202
Sends data to:	176.112.10.93:80
Sends data to:	127.0.0.1:49205
Sends data to:	190.198.41.99:80
Sends data to:	127.0.0.1:49208
Sends data to:	123.140.179.100:80
Sends data to:	127.0.0.1:49211
Sends data to:	50.128.222.92:80
Sends data to:	127.0.0.1:49214
Sends data to:	89.72.239.100:80
Sends data to:	127.0.0.1:49217
Sends data to:	180.149.209.103:80
Sends data to:	111.125.235.23:80
Receives data from:	127.0.0.1:49161
Receives data from:	202.69.41.22:80
Receives data from:	127.0.0.1:49164
Receives data from:	78.139.153.136:80
Receives data from:	127.0.0.1:49167
Receives data from:	178.89.132.134:80
Receives data from:	127.0.0.1:49170
Receives data from:	123.200.28.134:80
Receives data from:	127.0.0.1:49173
Receives data from:	41.32.15.139:80
Receives data from:	127.0.0.1:49176
Receives data from:	58.146.205.132:80
Receives data from:	127.0.0.1:49179
Receives data from:	115.252.34.140:80
Receives data from:	127.0.0.1:49182
Receives data from:	188.231.142.132:80
Receives data from:	127.0.0.1:49185
Receives data from:	182.234.66.140:80

Receives data from: 127.0.0.1:49188
Receives data from: 31.25.90.132:80
Receives data from: 127.0.0.1:49191
Receives data from: 178.91.76.140:80
Receives data from: 127.0.0.1:49194
Receives data from: 217.23.203.95:80
Receives data from: 127.0.0.1:49197
Receives data from: 109.162.67.96:80
Receives data from: 127.0.0.1:49200
Receives data from: 188.73.171.98:80
Receives data from: 127.0.0.1:49203
Receives data from: 176.112.10.93:80
Receives data from: 127.0.0.1:49206
Receives data from: 190.198.41.99:80
Receives data from: 127.0.0.1:49209
Receives data from: 123.140.179.100:80
Receives data from: 127.0.0.1:49212
Receives data from: 50.128.222.92:80
Receives data from: 127.0.0.1:49215
Receives data from: 89.72.239.100:80
Receives data from: 127.0.0.1:49218
Receives data from: 180.149.209.103:80

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\ime\imtc70
Creates key:	HKLM\software\microsoft\windows\currentversion\run
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\ddl
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop\languageconfiguration
Opens key:	HKCU\control panel\desktop
Opens key:	HKCU\control panel\desktop\muicached
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key:	
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots	
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllexoptions	
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\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\locale
Opens key:	HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key:	HKLM\system\currentcontrolset\control\nls\language groups
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\system\currentcontrolset\control\cmf\config
Opens key:	HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:	HKLM\software\microsoft\windows\currentversion\setup
Opens key:	HKLM\software\microsoft\windows\currentversion
Opens key:	HKLM\hardware\description\system
Opens key:	HKLM\software\microsoft\bidinterface\loader
Opens key:	HKCU\software\odbc\odbc.ini\odbc
Opens key:	HKLM\software\odbc\odbc.ini\odbc
Opens key:	HKCU\software\microsoft\microsoft sql server\80\tools\client
Opens key:	HKCU\software\microsoft\microsoft sql server\80\tools\sqlstr
Opens key:	HKLM\system\currentcontrolset\services\crypt32
Opens key:	HKLM\software\microsoft\windows\currentversion\internet settings
Opens key:	HKLM\software\policies\microsoft\windows\currentversion\internet
settings	
Opens key:	HKLM\software\policies\microsoft\sqmclient\windows
Opens key:	HKLM\software\microsoft\sqmclient\windows
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key:	HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:	

[illegible]

Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral\cdockables
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars
 Opens key: HKCU\software\adobe\acrobat
 reader\9.0\avgeneral\ctoolbars\cadvcommenting
 Opens key: HKCU\software\adobe\acrobat
 reader\9.0\avgeneral\ctoolbars\cbasiccommenting
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avgeneral\ctoolbars\ccommenting
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avtracker
 Opens key: HKCU\software\adobe\acrobat reader\9.0\collab
 Opens key: HKCU\software\adobe\acrobat reader\9.0\collab\cdocumentcenter
 Opens key: HKCU\software\adobe\acrobat reader\9.0\collab\cdocumentcenter\csettings
 Opens key: HKCU\software\adobe\acrobat reader\9.0\collab\cemaildistribution
 Opens key: HKCU\software\adobe\acrobat
 reader\9.0\collab\cemaildistribution\csettings
 Opens key: HKCU\software\adobe\acrobat
 reader\9.0\collab\cinitiationwizardfirstlaunch
 Opens key: HKCU\software\adobe\acrobat reader\9.0\collab\cserversettings
 Opens key: HKCU\software\adobe\acrobat reader\9.0\installer
 Opens key: HKCU\software\adobe\acrobat reader\9.0\installer\migrated
 Opens key: HKCU\software\adobe\acrobat reader\9.0\installpath
 Opens key: HKCU\software\adobe\acrobat reader\9.0\language
 Opens key: HKCU\software\adobe\acrobat reader\9.0\language\current
 Opens key: HKCU\software\adobe\acrobat reader\9.0\language\next
 Opens key: HKCU\software\adobe\acrobat reader\9.0\multimedia
 Opens key: HKCU\software\adobe\acrobat reader\9.0\multimedia\ccolorandborder
 Opens key: HKCU\software\adobe\acrobat reader\9.0\originals
 Opens key: HKCU\software\adobe\acrobat reader\9.0\prefsdialog
 Opens key: HKCU\software\adobe\acrobat reader\9.0\sdi
 Opens key: HKCU\software\adobe\acrobat reader\9.0\selection
 Opens key: HKCU\software\adobe\acrobat reader\9.0\usagemeasurement
 Opens key: HKCU\software\adobe\adobe acrobat
 Opens key: HKCU\software\adobe\adobe acrobat\9.0
 Opens key: HKCU\software\adobe\adobe acrobat\9.0\diskcabs
 Opens key: HKCU\software\adobe\adobe arm
 Opens key: HKCU\software\adobe\adobe arm\1.0
 Opens key: HKCU\software\adobe\adobe arm\1.0\arm
 Opens key: HKCU\software\adobe\adobe synchronizer
 Opens key: HKCU\software\adobe\adobe synchronizer\9.0
 Opens key: HKCU\software\adobe\adobe synchronizer\9.0\acrobat.com
 Opens key: HKCU\software\adobe\commonfiles
 Opens key: HKCU\software\adobe\commonfiles\usage
 Opens key: HKCU\software\adobe\commonfiles\usage\demographic
 Opens key: HKCU\software\adobe\commonfiles\usage\reader 9
 Opens key: HKCU\software\appdata\low
 Opens key: HKCU\software\appdata\low\software
 Opens key: HKCU\software\appdata\low\software\microsoft
 Opens key: HKCU\software\appdata\low\software\microsoft\internet explorer
 Opens key: HKCU\software\appdata\low\software\microsoft\internet explorer\security
 Opens key: HKCU\software\appdata\low\software\microsoft\internet
 explorer\security\antiphishing
 Opens key: HKCU\software\javasoft
 Opens key: HKCU\software\javasoft\java update
 Opens key: HKCU\software\javasoft\java update\policy
 Opens key: HKCU\software\javasoft\prefs
 Opens key: HKCU\software\macromedia
 Opens key: HKCU\software\macromedia\flashplayer
 Opens key: HKCU\software\microsoft
 Opens key: HKCU\software\microsoft\active setup
 Opens key: HKCU\software\microsoft\active setup\installed components
 Opens key: HKCU\software\microsoft\active setup\installed components\>{26923b43-
 4d38-484f-9b9e-de460746276c}
 Opens key: HKCU\software\microsoft\active setup\installed components\>{60b49e34-
 c7cc-11d0-8953-00a0c90347ff}
 Opens key: HKCU\software\microsoft\active setup\installed components\{2c7339cf-
 2b09-4501-b3f3-f3508c9228ed}
 Opens key: HKCU\software\microsoft\active setup\installed components\{44bba840-
 cc51-11cf-aafa-00aa00b6015c}
 Opens key: HKCU\software\microsoft\active setup\installed components\{6bf52a52-
 394a-11d3-b153-00c04f79faa6}
 Opens key: HKCU\software\microsoft\active setup\installed components\{89820200-
 ecbd-11cf-8b85-00aa005b4340}
 Opens key: HKCU\software\microsoft\active setup\installed components\{89820200-
 ecbd-11cf-8b85-00aa005b4383}
 Opens key: HKCU\software\microsoft\active setup\installed components\{89b4c1cd-
 b018-4511-b0a1-5476dbf70820}
 Opens key: HKCU\software\microsoft\assistance
 Opens key: HKCU\software\microsoft\assistance\client
 Opens key: HKCU\software\microsoft\assistance\client\1.0
 Opens key: HKCU\software\microsoft\assistance\client\1.0\settings
 Opens key: HKCU\software\microsoft\command processor
 Opens key: HKCU\software\microsoft\ctf
 Opens key: HKCU\software\microsoft\ctf\assemblies

Opens key:	HKCU\software\microsoft\ctf\assemblies\0x00000409
Opens key:	HKCU\software\microsoft\ctf\assemblies\0x00000409\{34745c63-b2f0-4784-8b67-5e12c8701a31}
Opens key:	HKCU\software\microsoft\ctf\directswitchhotkeys
Opens key:	HKCU\software\microsoft\ctf\hiddendummylayouts
Opens key:	HKCU\software\microsoft\ctf\msutb
Opens key:	HKCU\software\microsoft\ctf\sortorder
Opens key:	HKCU\software\microsoft\ctf\sortorder\language
Opens key:	HKCU\software\microsoft\ctf\tip
Opens key:	HKCU\software\microsoft\direct3d
Opens key:	HKCU\software\microsoft\direct3d\mostrecentapplication
Opens key:	HKCU\software\microsoft\eventsystem
Opens key:	HKCU\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}
Opens key:	HKCU\software\microsoft\fax
Opens key:	HKCU\software\microsoft\fax\faxoptions
Opens key:	HKCU\software\microsoft\fax\fxscInt
Opens key:	HKCU\software\microsoft\fax\fxscInt\archive
Opens key:	HKCU\software\microsoft\fax\fxscInt\confirm
Opens key:	HKCU\software\microsoft\fax\setup
Opens key:	HKCU\software\microsoft\fax\userinfo
Opens key:	HKCU\software\microsoft\feeds
Opens key:	HKCU\software\microsoft\ftp
Opens key:	HKCU\software\microsoft\gdiplus
Opens key:	HKCU\software\microsoft\iam
Opens key:	HKCU\software\microsoft\iam\accounts
Opens key:	HKCU\software\microsoft\iam\accounts\active directory gc
Opens key:	HKCU\software\microsoft\iam\accounts\active directory gc\windows mail account id
Opens key:	HKCU\software\microsoft\iam\accounts\verisign
Opens key:	HKCU\software\microsoft\iam\accounts\verisign\windows mail account id
Opens key:	HKCU\software\microsoft\ime
Opens key:	HKCU\software\microsoft\ime\imesc
Opens key:	HKCU\software\microsoft\ime\imesc\5.0
Opens key:	HKCU\software\microsoft\imejp
Opens key:	HKCU\software\microsoft\imejp\10.0
Opens key:	HKCU\software\microsoft\imejp\10.0\dictonaries
Opens key:	HKCU\software\microsoft\imejp\10.0\manage
Opens key:	HKCU\software\microsoft\imejp\10.0\msime
Opens key:	HKCU\software\microsoft\imejp\10.0\msime\autocharwidth
Opens key:	HKCU\software\microsoft\imejp\10.0\romadef
Opens key:	HKCU\software\microsoft\imejp\10.0\romadef\ms-ime
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\atok
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\atok\color
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\ms-ime2000
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\ms-ime2000\color
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\natural
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\natural\color
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\vje
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\vje\color
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\wx
Opens key:	HKCU\software\microsoft\imejp\10.0\stylelist\wx\color
Opens key:	HKCU\software\microsoft\imejp\10.0>window
Opens key:	HKCU\software\microsoft\imejp\10.0>window\pltsmall
Opens key:	HKCU\software\microsoft\imejp\10.0>window\plttiny
Opens key:	HKCU\software\microsoft\imejp\colors
Opens key:	HKCU\software\microsoft\internet connection wizard
Opens key:	HKCU\software\microsoft\internet explorer
Opens key:	HKCU\software\microsoft\internet explorer\browseremulation
Opens key:	HKCU\software\microsoft\internet explorer\browseremulation\lowmic
Opens key:	HKCU\software\microsoft\internet explorer\caretbrowsing
Opens key:	HKCU\software\microsoft\internet explorer\desktop
Opens key:	HKCU\software\microsoft\internet explorer\desktop\general
Opens key:	HKCU\software\microsoft\internet explorer\document windows
Opens key:	HKCU\software\microsoft\internet explorer\domstorage
Opens key:	HKCU\software\microsoft\internet explorer\domstorage\total
Opens key:	HKCU\software\microsoft\internet explorer\download
Opens key:	HKCU\software\microsoft\internet explorer\help_menu_urls
Opens key:	HKCU\software\microsoft\internet explorer\ietld
Opens key:	HKCU\software\microsoft\internet explorer\ietld\lowmic
Opens key:	HKCU\software\microsoft\internet explorer\intelliforms
Opens key:	HKCU\software\microsoft\internet explorer\international
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\10
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\11
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\12
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\13
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\14
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\15
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\16
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\17
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\18

Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\19
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\20
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\21
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\22
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\23
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\24
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\25
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\26
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\27
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\28
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\29
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\3
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\30
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\34
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\35
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\37
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\38
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\39
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\4
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\5
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\6
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\7
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\8
Opens key:	HKCU\software\microsoft\internet explorer\international\scripts\9
Opens key:	HKCU\software\microsoft\internet explorer\internetregistry
Opens key:	HKCU\software\microsoft\internet explorer\linksbar
Opens key:	HKCU\software\microsoft\internet explorer\linksbar\itemcache
Opens key:	HKCU\software\microsoft\internet explorer\linksbar\itemcache\0
Opens key:	HKCU\software\microsoft\internet explorer\linksbar\itemcache\1
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\domstorage
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\domstorage\total
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\dontshowmethisdialogagain
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\errorreporting
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\shell extensions
Opens key:	HKCU\software\microsoft\internet explorer\lowregistry\shell extensions\cached
Opens key:	HKCU\software\microsoft\internet explorer\main
Opens key:	HKCU\software\microsoft\internet explorer\main\default feeds
Opens key:	HKCU\software\microsoft\internet explorer\main\default feeds\{63711043-1e15-4eee-9c89-d029e7a92f34}
Opens key:	HKCU\software\microsoft\internet explorer\main\default feeds\{69ced929-f2f8-4103-9c1f-a4de6b351877}
Opens key:	HKCU\software\microsoft\internet explorer\main\default feeds\{a320a889-8e25-4619-830c-9ebebeb4339d}
Opens key:	HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key:	HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key:	HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown\settings
Opens key:	HKCU\software\microsoft\internet explorer\main\windowssearch
Opens key:	HKCU\software\microsoft\internet explorer\new windows
Opens key:	HKCU\software\microsoft\internet explorer\new windows\allow
Opens key:	HKCU\software\microsoft\internet explorer\pagesetup
Opens key:	HKCU\software\microsoft\internet explorer\phishingfilter
Opens key:	HKCU\software\microsoft\internet explorer\privacy
Opens key:	HKCU\software\microsoft\internet explorer\recovery
Opens key:	HKCU\software\microsoft\internet explorer\recovery\active
Opens key:	HKCU\software\microsoft\internet explorer\recovery\adminactive
Opens key:	HKCU\software\microsoft\internet explorer\searchscopes
Opens key:	HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
Opens key:	HKCU\software\microsoft\internet explorer\searchurl
Opens key:	HKCU\software\microsoft\internet explorer\security
Opens key:	HKCU\software\microsoft\internet explorer\security\antiphishing
Opens key:	HKCU\software\microsoft\internet explorer\security\antiphishing\2cedbfbcbda8-43aa-b1fd-cc8e6316e3e2
Opens key:	HKCU\software\microsoft\internet explorer\services
Opens key:	HKCU\software\microsoft\internet explorer\settings
Opens key:	HKCU\software\microsoft\internet explorer\setup
Opens key:	HKCU\software\microsoft\internet explorer\sqm
Opens key:	HKCU\software\microsoft\internet explorer\suggested sites
Opens key:	HKCU\software\microsoft\internet explorer\tabbedbrowsing
Opens key:	HKCU\software\microsoft\internet explorer\toolbar
Opens key:	HKCU\software\microsoft\internet explorer\toolbar\shellbrowser
Opens key:	HKCU\software\microsoft\internet explorer\toolbar\webbrowser
Opens key:	HKCU\software\microsoft\internet explorer\urlsearchhooks
Opens key:	HKCU\software\microsoft\internet explorer\user preferences
Opens key:	HKCU\software\microsoft\internet explorer\zoom
Opens key:	HKCU\software\microsoft\java vm
Opens key:	HKCU\software\microsoft\keyboard
Opens key:	HKCU\software\microsoft\keyboard\native media players

Opens key: HKCU\software\microsoft\keyboard\native media players\wmp
 Opens key: HKCU\software\microsoft\mediaplayer
 Opens key: HKCU\software\microsoft\mediaplayer\health
 Opens key: HKCU\software\microsoft\mediaplayer\player
 Opens key: HKCU\software\microsoft\mediaplayer\player\settings
 Opens key: HKCU\software\microsoft\mediaplayer\player\tasks
 Opens key: HKCU\software\microsoft\mediaplayer\player\tasks\nowplaying
 Opens key: HKCU\software\microsoft\mediaplayer\preferences
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\hme
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\hme\errorfolders
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\hme\lastsharedfolders
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\hme\sharefolders
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\hme\unsharefolders
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http
 Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp
 Opens key: HKCU\software\microsoft\mediaplayer\setup
 Opens key: HKCU\software\microsoft\mediaplayer\setup\createdlinks
 Opens key: HKCU\software\microsoft\microsoft management console
 Opens key: HKCU\software\microsoft\microsoft management console\recent file list
 Opens key: HKCU\software\microsoft\microsoft management console\settings
 Opens key: HKCU\software\microsoft\ms design tools
 Opens key: HKCU\software\microsoft\ms design tools\mdtdbd
 Opens key: HKCU\software\microsoft\msdaipp
 Opens key: HKCU\software\microsoft\msdaipp\providers
 Opens key: HKCU\software\microsoft\msdaipp\providers\{9fec570-b9d4-11d1-9c78-0000f875ac61}
 Opens key: HKCU\software\microsoft\msdaipp\providers\{9fec571-b9d4-11d1-9c78-0000f875ac61}
 Opens key: HKCU\software\microsoft\msf
 Opens key: HKCU\software\microsoft\msf\registration
 Opens key: HKCU\software\microsoft\msf\registration\listen
 Opens key: HKCU\software\microsoft\notepad
 Opens key: HKCU\software\microsoft\office
 Opens key: HKCU\software\microsoft\office\11.0
 Opens key: HKCU\software\microsoft\office\11.0\common
 Opens key: HKCU\software\microsoft\office\11.0\common\drawalerts
 Opens key: HKCU\software\microsoft\office\11.0\common\drawalerts\ftp sites
 Opens key: HKCU\software\microsoft\office\11.0\common\dsadaptermru
 Opens key: HKCU\software\microsoft\office\11.0\common\general
 Opens key: HKCU\software\microsoft\office\11.0\common\languageresources
 Opens key: HKCU\software\microsoft\office\11.0\common\migration
 Opens key: HKCU\software\microsoft\office\11.0\common\migration\office
 Opens key: HKCU\software\microsoft\office\11.0\common\migration\word
 Opens key: HKCU\software\microsoft\office\11.0\common\open find
 Opens key: HKCU\software\microsoft\office\11.0\common\open find\microsoft office word
 Opens key: HKCU\software\microsoft\office\11.0\common\open find\places
 Opens key: HKCU\software\microsoft\office\11.0\common\research
 Opens key: HKCU\software\microsoft\office\11.0\common\research\translation
 Opens key: HKCU\software\microsoft\office\11.0\common\toolbars
 Opens key: HKCU\software\microsoft\office\11.0\common\toolbars\settings
 Opens key: HKCU\software\microsoft\office\11.0\common\userinfo
 Opens key: HKCU\software\microsoft\office\11.0\word
 Opens key: HKCU\software\microsoft\office\11.0\word\options
 Opens key: HKCU\software\microsoft\office\11.0\word\userinfo
 Opens key: HKCU\software\microsoft\office\11.0\word\wizards
 Opens key: HKCU\software\microsoft\office\11.0\wordview
 Opens key: HKCU\software\microsoft\office\11.0\wordview\data
 Opens key: HKCU\software\microsoft\office\12.0
 Opens key: HKCU\software\microsoft\office\12.0\common
 Opens key: HKCU\software\microsoft\office\12.0\common\drawalerts
 Opens key: HKCU\software\microsoft\office\12.0\common\drawalerts\ftp sites
 Opens key: HKCU\software\microsoft\office\12.0\common\general
 Opens key: HKCU\software\microsoft\office\12.0\common\languageresources
 Opens key: HKCU\software\microsoft\office\12.0\common\languageresources\enabledlanguages
 Opens key: HKCU\software\microsoft\office\12.0\common\migration
 Opens key: HKCU\software\microsoft\office\12.0\common\migration\excel
 Opens key: HKCU\software\microsoft\office\12.0\common\migration\office
 Opens key: HKCU\software\microsoft\office\12.0\common\open find
 Opens key: HKCU\software\microsoft\office\12.0\common\open find\microsoft office excel viewer
 Opens key: HKCU\software\microsoft\office\12.0\common\research
 Opens key: HKCU\software\microsoft\office\12.0\common\research\translation
 Opens key: HKCU\software\microsoft\office\12.0\excel
 Opens key: HKCU\software\microsoft\office\12.0\excel\options
 Opens key: HKCU\software\microsoft\office\12.0\excel viewer
 Opens key: HKCU\software\microsoft\office\12.0\excel viewer\viewer options
 Opens key: HKCU\software\microsoft\office\12.0\user settings
 Opens key: HKCU\software\microsoft\office\12.0\user settings\excel_intl
 Opens key: HKCU\software\microsoft\office\12.0\user settings\msso_intl
 Opens key: HKCU\software\microsoft\office\12.0\user settings\powerpoint_intl

Opens key: HKCU\software\microsoft\office\14.0
 Opens key: HKCU\software\microsoft\office\14.0\common
 Opens key: HKCU\software\microsoft\office\14.0\common\drawalerts
 Opens key: HKCU\software\microsoft\office\14.0\common\drawalerts\ftp_sites
 Opens key: HKCU\software\microsoft\office\14.0\common\general
 Opens key: HKCU\software\microsoft\office\14.0\common\languageresources
 Opens key:
 HKCU\software\microsoft\office\14.0\common\languageresources\enabledlanguages
 Opens key: HKCU\software\microsoft\office\14.0\common\open_find
 Opens key: HKCU\software\microsoft\office\14.0\common\open_find\microsoft
 powerpoint viewer
 Opens key: HKCU\software\microsoft\office\14.0\common\research
 Opens key: HKCU\software\microsoft\office\14.0\common\research\translation
 Opens key: HKCU\software\microsoft\office\14.0\powerpoint
 Opens key: HKCU\software\microsoft\office\14.0\powerpoint viewer
 Opens key: HKCU\software\microsoft\office\14.0\powerpoint viewer\options
 Opens key: HKCU\software\microsoft\office\common
 Opens key: HKCU\software\microsoft\office\common\offdiag
 Opens key: HKCU\software\microsoft\office\common\smart_tag
 Opens key: HKCU\software\microsoft\office\common\smart_tag\actions
 Opens key: HKCU\software\microsoft\office\common\smart_tag\actions\{339361cd-6723-455d-a40b-c95f1f91ff8a}
 Opens key: HKCU\software\microsoft\office\common\smart_tag\actions\{49df3409-46b3-4b0c-b7bf-fec0f9401edd}
 Opens key: HKCU\software\microsoft\office\common\smart_tag\actions\{64ab6c69-b40e-40af-9b7f-f5687b48e2b6}
 Opens key: HKCU\software\microsoft\office\common\smart_tag\actions\{c3754d1a-04d3-4085-8cfb-97705b57a98f}
 Opens key: HKCU\software\microsoft\office\common\smart_tag\actions\{f114ae61-1331-4238-92c9-bbe330af25fd}
 Opens key: HKCU\software\microsoft\office\common\smart_tag\recognizers
 Opens key: HKCU\software\microsoft\office\common\smart_tag\recognizers\{64ab6c69-b40e-40af-9b7f-f5687b48e2b6}
 Opens key: HKCU\software\microsoft\office\common\smart_tag\recognizers\{87ef1cfe-51ca-4e6b-8c76-e576aa926888}
 Opens key: HKCU\software\microsoft\office\common\userinfo
 Opens key: HKCU\software\microsoft\peernet
 Opens key: HKCU\software\microsoft\peernet\event_config
 Opens key: HKCU\software\microsoft\protected storage system provider
 Opens key: HKCU\software\microsoft\protected storage system provider\s-1-5-21-2160590473-689474908-1361669368-1002
 Opens key: HKCU\software\microsoft\ras_autodial
 Opens key: HKCU\software\microsoft\ras_autodial\default
 Opens key: HKCU\software\microsoft\remote assistance
 Opens key: HKCU\software\microsoft\shared
 Opens key: HKCU\software\microsoft\shared tools
 Opens key: HKCU\software\microsoft\shared tools\font mapping
 Opens key: HKCU\software\microsoft\shared tools\proofing tools
 Opens key: HKCU\software\microsoft\shared tools\proofing tools\custom dictionaries
 Opens key: HKCU\software\microsoft\sideshow
 Opens key: HKCU\software\microsoft\sideshow\gadgets
 Opens key: HKCU\software\microsoft\speech
 Opens key: HKCU\software\microsoft\speech\preferences
 Opens key: HKCU\software\microsoft\speech\preferences\appcompatdisabledictation
 Opens key: HKCU\software\microsoft\speech\preferences\appcompatdisablemsaa
 Opens key: HKCU\software\microsoft\sqmclient
 Opens key: HKCU\software\microsoft\systemcertificates
 Opens key: HKCU\software\microsoft\systemcertificates\ca
 Opens key: HKCU\software\microsoft\systemcertificates\ca\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\ca\crls
 Opens key: HKCU\software\microsoft\systemcertificates\ca\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\disallowed
 Opens key: HKCU\software\microsoft\systemcertificates\disallowed\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\disallowed\crls
 Opens key: HKCU\software\microsoft\systemcertificates\disallowed\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\my
 Opens key: HKCU\software\microsoft\systemcertificates\root
 Opens key: HKCU\software\microsoft\systemcertificates\root\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\root\crls
 Opens key: HKCU\software\microsoft\systemcertificates\root\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\root\protectedroots
 Opens key: HKCU\software\microsoft\systemcertificates\smartcardroot
 Opens key: HKCU\software\microsoft\systemcertificates\smartcardroot\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\smartcardroot\crls
 Opens key: HKCU\software\microsoft\systemcertificates\smartcardroot\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\trust
 Opens key: HKCU\software\microsoft\systemcertificates\trust\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\trust\crls
 Opens key: HKCU\software\microsoft\systemcertificates\trust\ctls
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople\crls
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpeople\ctls

Opens key: HKCU\software\microsoft\systemcertificates\trustedpublisher
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpublisher\certificates
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpublisher\crls
 Opens key: HKCU\software\microsoft\systemcertificates\trustedpublisher\ctls
 Opens key: HKCU\software\microsoft\wab
 Opens key: HKCU\software\microsoft\wab\me
 Opens key: HKCU\software\microsoft\wab\wab4
 Opens key: HKCU\software\microsoft\wab\wab4\wab file name
 Opens key: HKCU\software\microsoft\wfs
 Opens key: HKCU\software\microsoft\wfs\draftsview
 Opens key: HKCU\software\microsoft\wfs\inboxview
 Opens key: HKCU\software\microsoft\wfs\incomingview
 Opens key: HKCU\software\microsoft\wfs\outboxview
 Opens key: HKCU\software\microsoft\wfs\sentitemsview
 Opens key: HKCU\software\microsoft\windows
 Opens key: HKCU\software\microsoft\windows\currentversion
 Opens key: HKCU\software\microsoft\windows\currentversion\action center
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{945a8954-c147-4acd-923f-40c45405a658}.check.42
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\providers
 Opens key: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog
 Opens key: HKCU\software\microsoft\windows\currentversion\app paths
 Opens key: HKCU\software\microsoft\windows\currentversion\app paths\pythonwin.exe
 Opens key: HKCU\software\microsoft\windows\currentversion\applets
 Opens key: HKCU\software\microsoft\windows\currentversion\applets\regedit
 Opens key: HKCU\software\microsoft\windows\currentversion\applets\systray
 Opens key: HKCU\software\microsoft\windows\currentversion\controls folder
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\applicationdestinations
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\autoplayhandlers
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\autoplayhandlers\eventhandlersdefaultselection
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\autoplayhandlers\userchosenexecutehandlers
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\bitbucket
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\bitbucket\volume
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\cabinetstate
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\cd burning
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\cd
 burning\drives
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\cd
 burning\staginginfo
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\cidopen
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\cidopen\modules
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\cidsave
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\cidsave\modules
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-

[illegible]

[illegible]

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{89745146-9299-11e3-ba80-806e6f6e6963}
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\newshortcuthandlers
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\recentdocs
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\recentdocs\.zip
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\recentdocs\folder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\runmru
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\searchplatform
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\searchplatform\preferences
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\startpage
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\startpage\newshortcuts
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\startpage2
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\streams
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\streams\desktop
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\stuckrects2
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\taskband
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\typedpaths
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\userassist
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{f4e57c4b-2036-45f0-a9ab-443bcfe33d9f}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\visualeffects
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\animateminmax
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\comboboxanimation
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\controlanimations
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\cursorshadow
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dragfullwindows
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dropshadow
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dwmaeropeekenabled
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dwmenabled
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\dwmsavethumbnailenabled
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\fontsmoothing
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listboxsmoothscrolling
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewalphaselect
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\listviewshadow
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\menuanimation
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\selectionfade
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\taskbaranimations
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\themes
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\thumbnailsoricon
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\tooltipanimation
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\visualeffects\transparentglass
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\wallpapers
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\wallpapers\images
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\wallpapers\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\ext
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-e8ad-4283-a596-fa578c2ebdc3}

Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{761497bb-d6f0-462c-b6eb-d4daf1d92d43}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-4283-a596-fa578c2ebdc3}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{761497bb-d6f0-462c-b6eb-d4daf1d92d43}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{8856f961-340a-11d0-a96b-00c04fd705a2}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{cfbfae00-17a6-11d0-99cb-00c04fd64497}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{d27cdb6e-ae6d-11cf-96b8-444553540000}
Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-435b-bc74-9c25c1c588a9}
Opens key: HKCU\software\microsoft\windows\currentversion\group policy
Opens key: HKCU\software\microsoft\windows\currentversion\group
policy\groupmembership
Opens key: HKCU\software\microsoft\windows\currentversion\group policy\history
Opens key: HKCU\software\microsoft\windows\currentversion\group
policy\policyapplicationstate
Opens key: HKCU\software\microsoft\windows\currentversion\group policy editor
Opens key: HKCU\software\microsoft\windows\currentversion\group policy editor\admx
filter
Opens key: HKCU\software\microsoft\windows\currentversion\group policy editor\admx
filter.cache
Opens key: HKCU\software\microsoft\windows\currentversion\homegroup
Opens key: HKCU\software\microsoft\windows\currentversion\homegroup\printers
Opens key: HKCU\software\microsoft\windows\currentversion\homegroup\uistatuscache
Opens key: HKCU\software\microsoft\windows\currentversion\ime
Opens key: HKCU\software\microsoft\windows\currentversion\ime\imtc70
Opens key: HKCU\software\microsoft\windows\currentversion\ime\imtc70\fuzzyscheme
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\activities
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\activities\blog
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\activities\email
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\activities\map
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\activities\translate
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\connections
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\http
filters
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
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: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\p3p
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\passport
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\passport\lowdamap
Opens key: HKCU\software\microsoft\windows\currentversion\internet


```

settings\protocols
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\protocols\mailto
  Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\5e-19-d5-f1-94-00
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\ce-24-88-5f-90-5e
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\fe-54-5a-c1-01-d0
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{1701d862-74bd-40ea-8107-be3313fdd529}
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{8dfa6cf1-5379-431e-aa1b-11fda2af808d}
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{eb978a0c-1694-44cd-91c4-0d1bb526b865}
  Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\escdomains
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges
  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: HKCU\software\microsoft\windows\currentversion\mct
  Opens key: HKCU\software\microsoft\windows\currentversion\mct\us
  Opens key: HKCU\software\microsoft\windows\currentversion\mct\us\link
  Opens key: HKCU\software\microsoft\windows\currentversion\mct\us\rssfeed
  Opens key: HKCU\software\microsoft\windows\currentversion\mct\us\theme
  Opens key: HKCU\software\microsoft\windows\currentversion\mct\us\wallpaper
  Opens key: HKCU\software\microsoft\windows\currentversion\netcache
  Opens key: HKCU\software\microsoft\windows\currentversion\policies
  Opens key: HKCU\software\microsoft\windows\currentversion\radar
  Opens key: HKCU\software\microsoft\windows\currentversion\run
  Opens key: HKCU\software\microsoft\windows\currentversion\runonce
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\bubbles
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\bubbles\screen 1
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\bubbles\screen 2
    Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\mystify
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\mystify\screen 1
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\mystify\screen 2
    Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\ribbons
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\ribbons\screen 1
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\ribbons\screen 2
    Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\ssstext3d
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\ssstext3d\screen 1
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\ssstext3d\screen 2
    Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions
    Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached
    Opens key: HKCU\software\microsoft\windows\currentversion\sidebar
    Opens key: HKCU\software\microsoft\windows\currentversion\sidebar\settings
    Opens key: HKCU\software\microsoft\windows\currentversion\telephony
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities\mediamodes
    Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
    Opens key: HKCU\software\microsoft\windows\currentversion\themes
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleoff
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleon
    Opens key: HKCU\software\microsoft\windows\currentversion\themes\installedthemes
    Opens key:
  Opens key: HKCU\software\microsoft\windows\currentversion\themes\installedthemes\mct
    Opens key: HKCU\software\microsoft\windows\currentversion\wintrust
    Opens key: HKCU\software\microsoft\windows\currentversion\wintrust\trust providers

```

Opens key: HKCU\software\microsoft\windows\currentversion\wintrust\trust providers\software publishing

Opens key: HKCU\software\microsoft\windows\dwm

Opens key: HKCU\software\microsoft\windows\shell

Opens key: HKCU\software\microsoft\windows\shell\bagmru

Opens key: HKCU\software\microsoft\windows\shell\bags

Opens key: HKCU\software\microsoft\windows\shell\bags\1

Opens key: HKCU\software\microsoft\windows\shell\bags\1\desktop

Opens key: HKCU\software\microsoft\windows\tabletpc

Opens key: HKCU\software\microsoft\windows\tabletpc\tabsetup

Opens key: HKCU\software\microsoft\windows\windows error reporting

Opens key: HKCU\software\microsoft\windows\windows error reporting\consent

Opens key: HKCU\software\microsoft\windows\windows error reporting\hangs

Opens key: HKCU\software\microsoft\windows mail

Opens key: HKCU\software\microsoft\windows mail\mail

Opens key: HKCU\software\microsoft\windows mail\news

Opens key: HKCU\software\microsoft\windows mail\trident

Opens key: HKCU\software\microsoft\windows mail\trident\main

Opens key: HKCU\software\microsoft\windows mail\trident\settings

Opens key: HKCU\software\microsoft\windows media

Opens key: HKCU\software\microsoft\windows media\wmsdk

Opens key: HKCU\software\microsoft\windows media\wmsdk\general

Opens key: HKCU\software\microsoft\windows media\wmsdk\namespace

Opens key: HKCU\software\microsoft\windows nt

Opens key: HKCU\software\microsoft\windows nt\currentversion

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

nt\currentversion\appcompatflags\compatibility assistant

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant\persisted

Opens key: HKCU\software\microsoft\windows nt\currentversion\devices

Opens key: HKCU\software\microsoft\windows nt\currentversion\efs

Opens key: HKCU\software\microsoft\windows nt\currentversion\msicorruptedfilerecovery

Opens key: HKCU\software\microsoft\windows nt\currentversion\msicorruptedfilerecovery\repairedproducts

Opens key: HKCU\software\microsoft\windows nt\currentversion\network

Opens key: HKCU\software\microsoft\windows nt\currentversion\network\location

awareness

Opens key: HKCU\software\microsoft\windows nt\currentversion\peernet

Opens key: HKCU\software\microsoft\windows nt\currentversion\peernet\collabhost

Opens key: HKCU\software\microsoft\windows nt\currentversion\printerports

Opens key: HKCU\software\microsoft\windows nt\currentversion\taskmanager

Opens key: HKCU\software\microsoft\windows nt\currentversion\windows

Opens key: HKCU\software\microsoft\windows nt\currentversion\winlogon

Opens key: HKCU\software\microsoft\windows script

Opens key: HKCU\software\microsoft\windows script\settings

Opens key: HKCU\software\microsoft\windows search

Opens key: HKCU\software\microsoft\windows search\processedsearchroots

Opens key: HKCU\software\microsoft\windows search\processedsearchroots\0000

Opens key: HKCU\software\microsoft\windows search\processedsearchroots\0001

Opens key: HKCU\software\microsoft\windows search\processedsearchroots\0002

Opens key: HKCU\software\microsoft\windows search\processedsearchroots\0003

Opens key: HKCU\software\microsoft\windows sidebar

Opens key: HKCU\software\microsoft\windows sidebar\ieoverride

Opens key: HKCU\software\microsoft\windows sidebar\ieoverride\main

Opens key: HKCU\software\microsoft\windows sidebar\ieoverride\settings

Opens key: HKCU\software\microsoft\windows sidebar\ieoverride\styles

Opens key: HKCU\software\microsoft\wisp

Opens key: HKCU\software\microsoft\wisp\multitouch

Opens key: HKCU\software\microsoft\wisp\pen

Opens key: HKCU\software\microsoft\wisp\pen\syseventparameters

Opens key: HKCU\software\microsoft\wisp\pen\syseventparameters\customflickcommands

Opens key: HKCU\software\microsoft\wisp\pen\syseventparameters\flickcommands

Opens key: HKCU\software\microsoft\wisp\touch

Opens key: HKCU\software\netscape

Opens key: HKCU\software\netscape\netscape navigator

Opens key: HKCU\software\netscape\netscape navigator\suffixes

Opens key: HKCU\software\netscape\netscape navigator\user trusted external

applications

Opens key: HKCU\software\netscape\netscape navigator\viewers

Opens key: HKCU\software\policies

Opens key: HKCU\software\policies\microsoft

Opens key: HKCU\software\policies\microsoft\systemcertificates

Opens key: HKCU\software\policies\microsoft\systemcertificates\ca

Opens key: HKCU\software\policies\microsoft\systemcertificates\ca\certificates

Opens key: HKCU\software\policies\microsoft\systemcertificates\ca\crls

Opens key: HKCU\software\policies\microsoft\systemcertificates\ca\ctls

Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed

Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed\certificates

Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed\crls

Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed\ctls

Opens key: HKCU\software\policies\microsoft\systemcertificates\trust
Opens key: HKCU\software\policies\microsoft\systemcertificates\trust\certificates
Opens key: HKCU\software\policies\microsoft\systemcertificates\trust\crls
Opens key: HKCU\software\policies\microsoft\systemcertificates\trust\ctls
Opens key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople
Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpeople\certificates
Opens key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople\crls
Opens key: HKCU\software\policies\microsoft\systemcertificates\trustedpeople\ctls
Opens key: HKCU\software\policies\microsoft\systemcertificates\trustedpublisher
Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\certificates
Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\crls
Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\ctls
Opens key: HKCU\software\policies\microsoft\windows
Opens key: HKCU\software\policies\microsoft\windows\currentversion
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\cache
Opens key: HKCU\software\policies\power
Opens key: HKCU\software\policies\power\powersettings
Opens key: HKCU\software\python
Opens key: HKCU\software\python\pythoncore
Opens key: HKCU\software\python\pythoncore\2.7
Opens key: HKCU\software\python\pythoncore\2.7\help
Opens key: HKCU\software\python\pythoncore\2.7\help\pythonwin reference
Opens key: HKCU\software\classes
Opens key: HKCU\software\classes\clsid
Opens key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}
Opens key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0000-0003-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0000-0003-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0000-0004-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0000-0004-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0000-0005-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0000-0005-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0000-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0000-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcbb}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0001-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-abcdeffedcbb}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0002-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-abcdeffedcbb}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0003-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-abcdeffedcbb}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0004-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-abcdeffedcbb}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0005-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-abcdeffedcba}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-abcdeffedcbb}
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-abcdeffedcbb}\inprocserver32
Opens key: HKCU\software\classes\clsid\{cafeefac-0013-0001-0006-abcdeffedcbb}\inprocserver32

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Opens key: HKCU\software\classes\local settings\software\microsoft\windows
 Opens key: HKCU\software\classes\local
 settings\software\microsoft\windows\currentversion
 Opens key: HKCU\software\classes\local settings\software\microsoft\windows\shell
 Opens key: HKCU\software\classes\python.file
 Opens key: HKCU\software\classes\python.file\shell
 Opens key: HKCU\software\classes\python.file\shell\edit with pythonwin
 Opens key: HKCU\software\classes\python.file\shell\edit with pythonwin\command
 Opens key: HKCU\software\classes\python.noconfile
 Opens key: HKCU\software\classes\python.noconfile\shell
 Opens key: HKCU\software\classes\python.noconfile\shell\edit with pythonwin
 Opens key: HKCU\software\classes\python.noconfile\shell\edit with pythonwin\command
 Opens key: HKCU\software\classes\virtualstore
 Opens key: HKCU\software\classes\virtualstore\machine
 Opens key: HKCU\software\classes\virtualstore\machine\software
 Opens key: HKCU\software\classes\virtualstore\machine\software\microsoft
 Opens key: HKCU\software\classes\virtualstore\machine\software\microsoft\directdraw
 Opens key: HKCU\software\classes\virtualstore\machine\software\microsoft\downloadmanager
 Opens key: HKLM\software\microsoft\windows\currentversion\run
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}
 Opens key: HKLM\software\microsoft\rpc
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\setup
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
 Opens key: HKCU\software\far\plugins\ftp\hosts
 Opens key: HKCU\software\far2\plugins\ftp\hosts
 Opens key: HKCU\software\far\saveddialoghistory\ftphost
 Opens key: HKCU\software\far2\saveddialoghistory\ftphost
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
 Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
 Opens key: HKCU\software\ghisler\windows commander
 Opens key: HKCU\software\ghisler\total commander
 Opens key: HKLM\software\ghisler\windows commander
 Opens key: HKLM\software\ghisler\total commander
 Opens key: HKCU\software\flashfxp
 Opens key: HKCU\software\flashfxp\3
 Opens key: HKCU\software\flashfxp\4
 Opens key: HKLM\software\flashfxp
 Opens key: HKLM\software\flashfxp\3
 Opens key: HKLM\software\flashfxp\4
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\addressbook
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
 player activex
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\connection
 manager
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\dxm_runtime
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\fontcore
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ie40
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ie4data
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\iedata
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\wic
 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\{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\{ac76ba86-7ad7-1033-7b44-a93000000001}
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-4027-b136-2b3e1f5ab6e2}
Opens key: HKCU\software\bpftp\bullet proof ftp\main
Opens key: HKCU\software\bulletproof software\bulletproof ftp client\main
Opens key: HKCU\software\bpftp\bullet proof ftp\options
Opens key: HKCU\software\bulletproof software\bulletproof ftp client\options
Opens key: HKCU\software\bulletproof software\bulletproof ftp client 2010\options
Opens key: HKCU\software\bpftp
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}\propertybag
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKCU\software\turboftp
Opens key: HKCU\software\cryer\websitepublisher
Opens key: HKU\
Opens key: HKCU\software\ftpclient\sites
Opens key: HKCU\software\softx.org\ftpclient\sites
Opens key: HKCU\software\martin prikryl\winscp 2\sessions
Opens key: HKCU\software\vandyke\securefx
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}\propertybag
Opens key: HKCU\software\globalscape\cuteftp 6 home\qctoolbar
Opens key: HKCU\software\globalscape\cuteftp 6 professional\qctoolbar
Opens key: HKCU\software\globalscape\cuteftp 7 home\qctoolbar
Opens key: HKCU\software\globalscape\cuteftp 7 professional\qctoolbar
Opens key: HKCU\software\globalscape\cuteftp 8 home\qctoolbar
Opens key: HKCU\software\globalscape\cuteftp 8 professional\qctoolbar
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}\propertybag
Opens key: HKCU\software\sota\ffftp\options
Opens key: HKCU\software\ftpware\coreftp\sites
Opens key: HKCU\software\south river technologies\webdrive\connections
Opens key: HKCU\software\vnch software\classicftp\ftpaccounts
Opens key: HKLM\software\vnch software\fling\accounts
Opens key: HKCU\software\filezilla
Opens key: HKCU\software\filezilla\recent servers
Opens key: HKCU\software\filezilla\site manager
Opens key: HKCU\software\ftp explorer\profiles
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\ultraftp
Opens key: HKLM\software
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions[sqlunirl.dll]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[70b2225f430facf31ca65621c234f09e]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapprivate]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\hardware\description\system[identifier]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[6b1db052-734f-4e23-
af5e-6cd8ae459f98]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[9c88041d-349d-4647-
8bfd-2c0a167bfe58]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5f31090b-d990-4e91-
b16d-46121d0255aa]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
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\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]

[illegible]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storiesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storiesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value:

HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
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\control\nls\customlocale[ar]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ar]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ar-sa]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-sa]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bg]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bg]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bg-bg]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bg-bg]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ca]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ca]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ca-es]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ca-es]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[zh-hans]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hans]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-cn]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[cs]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[cs]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[cs-cz]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[cs-cz]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[da]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[da]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[da-dk]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[da-dk]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[de]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[de]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[de-de]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[de-de]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[el]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[el]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[el-gr]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[el-gr]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[wo-sn]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[prs]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[prs]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[prs-af]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[prs-af]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[gd]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gd]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[gd-gb]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gd-gb]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000401]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[d]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000402]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[5]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000403]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[zh-tw]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-tw]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000404]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[9]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000405]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[2]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000406]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000407]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000408]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[4]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-es_tradnl]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-es_tradnl]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000040a]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000040b]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000040c]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000040d]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[c]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000040e]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000040f]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000410]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000411]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[7]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000412]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[8]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000413]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000414]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000415]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000416]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000417]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000418]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000419]
Queries value: HKCU\software\microsoft\windows\currentversion\ime\imtc70[]
Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[persistentsavedflags]
Queries value: HKCU\software\microsoft\windows\currentversion\ime\imtc70[fullplayedmin]
Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[linecompressedcheck]
Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[fieldenablenalocal]
Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[stylecompletedhide]
Queries value: HKLM\software\microsoft\windows\currentversion\run[sonyagent]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[enabledhcp]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup\systemsetupinprogress
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsiname]

Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002[profileimagepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsiname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]

Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\addressbook[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
player activex[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\adobe flash
player activex[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\connection
manager[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\directdrawex[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\dxm_runtime[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\fontcore[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie40[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie4data[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\ie5bakex[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\iedata[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\mobileoptionpack[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\mplayer2[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\schedulingagent[uninstallstring]
Queries value:
HKLM\software\microsoft\windows\currentversion\uninstall\wic[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-befc77a11a1e}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-befc77a11a1e}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-2f83217002ff}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-2f83217002ff}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-5f2748764d10}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-0000000ff1ce}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-0000000ff1ce}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-0150048383c9}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-0150048383c9}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-0000000ff1ce}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-0000000ff1ce}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}[displayname]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}[uninstallstring]
Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}[displayname]

Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-4027-b136-2b3e1f5ab6e2}[uninstallstring]

Queries value: HKLM\software\microsoft\windows\currentversion\uninstall\{c3cc4df5-39a5-4027-b136-2b3e1f5ab6e2}[displayname]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[category]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[relativepath]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parsingname]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[category]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[name]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[description]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[relativepath]

Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-

b29c-65b732d3d21a}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[initfolderhandler]

Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software[debuglogpath]
Queries value: HKLM\software[debugloglevel]
Queries value: HKLM\software[enableddebuglog]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[persistentsavedflags]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\ime\imtc70[fullplayedmin]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[linecompressedcheck]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[fieldenabledlocal]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[stylecompletedhide]
Sets/Creates value: HKLM\software\microsoft\windows\currentversion\run[sonyagent]
Value changes:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[stylecompletedhide]