

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 620, Task ID: 2428

Task ID:	2428
Risk Level:	10
Date Processed:	2016-02-22 05:29:30 (UTC)
Processing Time:	77.07 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe"
Sample ID:	620
Type:	basic
Owner:	admin
Label:	188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5
Date Added:	2016-02-22 05:26:49 (UTC)
File Type:	PE32:win32:gui
File Size:	838656 bytes
MD5:	0feaaa4adc31728e54b006ab9a7e6afa
SHA256:	188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5
Description:	None

Pattern Matching Results

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

Process/Thread Events

Creates process:
C:\windows\temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe
["C:\windows\temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.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\188AB310143D0C0C9673D957FCFE7-4BAD8990.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\windows\temp\CLUSAPI.dll
Opens: C:\Windows\SysWOW64\clusapi.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\windows\temp\cryptdll.dll
Opens: C:\Windows\SysWOW64\cryptdll.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\windows\temp\CMUTIL.DLL
Opens: C:\Windows\SysWOW64\cmutil.dll
Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\windows\temp\DNSAPI.dll
Opens: C:\Windows\SysWOW64\dnsapi.dll
Opens: C:\windows\temp\IPHLPAPI.DLL
Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens: C:\windows\temp\WINNSI.DLL
Opens: C:\Windows\SysWOW64\winnsi.dll
Opens: C:\windows\temp\MSWSOCK.dll
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL
C:\Windows\Temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe
Opens: C:\Windows\Temp
Opens: C:\Windows\Temp\tmp.exe
Opens: C:\Windows\SysWOW64\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\SysWOW64\dhcpcsvc.dll
 Opens: C:\windows\temp\wpcap.dll
 Opens: C:\Windows\SysWOW64\wpcap.dll
 Opens: C:\Windows\system\wpcap.dll
 Opens: C:\Windows\wpcap.dll
 Opens: C:\Windows\SysWOW64\Wbem\wpcap.dll
 Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\wpcap.dll
 Opens: C:\Windows\wcx_ftp.ini
 Opens: C:\windows\temp\profapi.dll
 Opens: C:\Windows\SysWOW64\profapi.dll
 Opens: C:\Users\Admin
 Opens: C:\Users\Admin\wcx_ftp.ini
 Opens: C:\
 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:\Users\Admin\AppData\Roaming\GPSSoftware\Directory
 Opus\ConfigFiles\ftp.oxc
 Opens: C:\Users\Admin\AppData\Roaming\GPSSoftware\Directory
 Opus\Layouts\System\default.o1l
 Opens: C:\Users\Admin\AppData\Local\GPSSoftware\Directory
 Opus\ConfigFiles\ftp.oxc
 Opens: C:\Users\Admin\AppData\Local\GPSSoftware\Directory
 Opus\Layouts\System\default.o1l
 Opens: C:\ProgramData\GPSSoftware\Directory Opus\ConfigFiles\ftp.oxc
 Opens: C:\ProgramData\GPSSoftware\Directory Opus\Layouts\System\default.o1l
 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 (x86)
 Opens: C:\Program Files (x86)\CuteFTP
 Opens: C:\Windows\win.ini
 Opens: C:\Program Files (x86)\Common Files
 Opens: C:\Program Files (x86)\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\SysWOW64\tzres.dll
Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens: C:\Windows\SysWOW64\wship6.dll
Reads from: C:\Windows\win.ini
Deletes: C:\Windows\Temp\tmp.exe

```

Network Events

Connects to:	127.0.0.1:49161
Connects to:	178.168.143.47:80
Connects to:	127.0.0.1:49164
Connects to:	178.168.41.15:80
Connects to:	127.0.0.1:49167
Connects to:	109.87.17.182:80
Sends data to:	127.0.0.1:49161
Sends data to:	127.0.0.1:49164
Sends data to:	127.0.0.1:49167
Receives data from:	127.0.0.1:49162
Receives data from:	127.0.0.1:49165
Receives data from:	127.0.0.1:49168

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\ime\imtc70
Creates key:	HKLM\software\wow6432node\microsoft\windows\currentversion\run
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\language
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key:	HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
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\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\software\wow6432node\microsoft\windows

nt\currentversion\gre_initialize
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
Opens key:
HKLM\software\wow6432node\policies\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:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2fd5577c
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKCU\software
Opens key: HKCU\software\adobe
Opens key: HKCU\software\adobe\acrobat reader
Opens key: HKCU\software\adobe\acrobat reader\9.0

Opens key: HKCU\software\adobe\acrobat reader\9.0\adobeviewer
 Opens key: HKCU\software\adobe\acrobat reader\9.0\annots
 Opens key: HKCU\software\adobe\acrobat reader\9.0\annots\cannots
 Opens key: HKCU\software\adobe\acrobat reader\9.0\annots\cannots\cannot
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avconversionfrompdf\csettings
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avconversiontopdf\csettings
 Opens key: HKCU\software\adobe\acrobat reader\9.0\avdisplay
 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\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\java update\policy\javafx
 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\declined install on demand iev5
 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\activemovie

Opens key: HKCU\software\microsoft\activemovie\devenum 64-bit

Opens key: HKCU\software\microsoft\activemovie\devenum 64-bit\{4efe2452-168a-11d1-bc76-00c04fb9453b}

Opens key: HKCU\software\microsoft\activemovie\devenum 64-bit\{4efe2452-168a-11d1-bc76-00c04fb9453b}\default midiout device

Opens key: HKCU\software\microsoft\activemovie\devenum 64-bit\{e0f158e1-cb04-11d0-bd4e-00a0c911ce86}

Opens key: HKCU\software\microsoft\activemovie\devenum 64-bit\{e0f158e1-cb04-11d0-bd4e-00a0c911ce86}\default directsound device

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\caret browsing

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\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\{5adc2714-2975-4245-b68a-3721298c1e70}
Opens key:	HKCU\software\microsoft\internet	explorer\main\default feeds\{728bab62-50c0-4a2a-b9a6-951f2355feb2}
Opens key:	HKCU\software\microsoft\internet	explorer\main\default feeds\{bab07688-e349-461a-b4f5-b4674114d3a6}
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\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\typedurls
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\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\multimedia
Opens key: HKCU\software\microsoft\multimedia\activemovie
Opens key: HKCU\software\microsoft\multimedia\activemovie\filter cache64
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\mso_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-1-5-21-980053277-1733835069-2361817685-1001
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\appcompatdisablesaa
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\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\{59031a47-3f72-44a7-89c5-5595fe6b30ee}
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{645ff040-5081-101b-9f08-00aa002f954e}
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\comdlg32
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\cidsize mru
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\firstfolder
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedpidlmru
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\opensavepidlmru
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\controlpanel
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\discardable
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\discardable\postsetup
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\3g2
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\3gp
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\3gp2
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\3gpp
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\aac
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\adt
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\adts
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\aif
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\afc
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\aiif
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\asf
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\asx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\au
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\avi
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\bmp
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\cab
 Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\fileexts\contact
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\css
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\dib
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\dll
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\doc
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\docm
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\docx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\dot
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\dvr
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\dvr-ms
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\dwfx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\eamx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\edrx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\emf
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\eptrx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\exe
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\fon
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\gif
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\htm
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\html
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ico
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ini
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\jfif
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\jpe
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\jpeg
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\jpg
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\jtx
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\lnk
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\m1v

[illegible]

HKCU\software\microsoft\windows\currentversion\explorer\modules\commonplaces
Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\modules\globalsettings
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\modules\navpane
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc
Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{8063a3d4-8213-11e3-a68e-806e6f6e6963}
Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{8063a3d7-8213-11e3-a68e-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\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\animatemax
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\{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\{cfbfae00-17a6-11d0-99cb-00c04fd64497}
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\group policy objects
Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects\{f2660594-63ea-4618-8650-1a5a4fb9ca52}machine
Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects\{f2660594-63ea-4618-8650-1a5a4fb9ca52}machine\software
Opens key: HKCU\software\microsoft\windows\currentversion\group policy objects\{f2660594-63ea-4618-8650-1a5a4fb9ca52}user
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\ui\statuscache
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\3e-68-f6-0d-2d-0f
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\9e-87-70-29-a3-67
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\e2-c2-d0-09-69-0f
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{4dc0ee17-9725-46c6-9208-9e741c29932a}
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{97510e62-091a-49b5-9797-24fe4dde0abc}
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{c034e4b5-6859-46ca-b262-e1e2cfd7fcab}
  Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{f9145a4d-b491-47f1-8afa-50f81461036d}
  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:
HKCU\software\microsoft\windows\currentversion\screensavers\bubbles\screen 2
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\mystify
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\mystify\screen 1
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\mystify\screen 2
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\ribbons
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\ribbons\screen 1
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\ribbons\screen 2
  Opens key: HKCU\software\microsoft\windows\currentversion\screensavers\sstext3d
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\sstext3d\screen 1
  Opens key:
HKCU\software\microsoft\windows\currentversion\screensavers\sstext3d\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:
HKCU\software\microsoft\windows\currentversion\telephony\handoffpriorities
  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:
HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleoff
  Opens key:

```

```

HKCU\software\microsoft\windows\currentversion\themes\defaultvisualstyleon
  Opens key: HKCU\software\microsoft\windows\currentversion\themes\installedthemes
  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\dwmm
  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\windows error reporting\hangs\nhrtimes
  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
  Opens key: HKCU\software\microsoft\windows
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\softwareprotectionplatform
  Opens key: HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\activation
  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\wow6432node
Opens key: HKCU\software\wow6432node\microsoft
Opens key: HKCU\software\wow6432node\microsoft\active setup
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components\>{26923b43-4d38-484f-9b9e-de460746276c}
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components\>{60b49e34-c7cc-11d0-8953-00a0c90347ff}
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components\{2c7339cf-2b09-4501-b3f3-f3508c9228ed}
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components\{44bba840-cc51-11cf-aafa-00aa00b6015c}
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components\{6bf52a52-394a-11d3-b153-00c04f79faa6}
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4340}
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components\{89820200-ecbd-11cf-8b85-00aa005b4383}
Opens key: HKCU\software\wow6432node\microsoft\active setup\installed components\{89b4c1cd-b018-4511-b0a1-5476dbf70820}
Opens key: HKCU\software\classes
Opens key: HKCU\software\classes\wow6432node\clsid
Opens key: HKCU\software\classes\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}
Opens key: HKCU\software\classes\wow6432node\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0003-abcdeffedcba}
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0003-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0004-abcdeffedcba}
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0004-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0005-abcdeffedcba}
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0000-0005-abcdeffedcba}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0000-abcdeffedcba}
Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0013-0001-0000-

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```

abcdeffedcbb}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbc}
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0000-
abcdeffedcbc}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcba}
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcba}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbb}
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbb}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbc}
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0001-
abcdeffedcbc}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbc}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}
  Opens key: HKCU\software\classes\wow6432node\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{e19f9331-3110-11d4-991c-
005004d3b3db}
  Opens key: HKCU\software\classes\wow6432node\clsid\{e19f9331-3110-11d4-991c-
005004d3b3db}\inprocserver32
  Opens key: HKCU\software\classes\javaplugin.1020
  Opens key: HKCU\software\classes\javaplugin.1020\clsid
  Opens key: HKCU\software\classes\local settings
  Opens key: HKCU\software\classes\local settings\muicache
  Opens key: HKCU\software\classes\local settings\muicache\16
  Opens key: HKCU\software\classes\local settings\muicache\16\52c64b7e
  Opens key: HKCU\software\classes\local settings\software
  Opens key: HKCU\software\classes\local settings\software\microsoft
  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\wow6432node
  Opens key:
HKCU\software\classes\virtualstore\machine\software\wow6432node\microsoft
  Opens key: HKCU\software\classes\wow6432node
  Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\run
  Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
  Opens key: HKLM\software\wow6432node\microsoft\rpc
  Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key: HKLM\system\setup
  Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
  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\ftp\host
  Opens key: HKCU\software\far2\saveddialoghistory\ftp\host
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-

```

0e22-4760-9afe-ea3317b67173}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key: HKCU\software\ghisler\windows commander
Opens key: HKCU\software\ghisler\total commander
Opens key: HKLM\software\wow6432node\ghisler\windows commander
Opens key: HKLM\software\wow6432node\ghisler\total commander
Opens key: HKCU\software\flashfxp
Opens key: HKCU\software\flashfxp\3
Opens key: HKCU\software\flashfxp\4
Opens key: HKLM\software\wow6432node\flashfxp
Opens key: HKLM\software\wow6432node\flashfxp\3
Opens key: HKLM\software\wow6432node\flashfxp\4
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key:
HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\uninstall
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\addressbook
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\adobe flash player activex
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\connection manager
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\directdrawex
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\fontcore
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie40
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie4data
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie5bakex
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\iedata
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mobileoptionpack
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\schedulingagent
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wic
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-befc77a11a1e}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-2f83217002ff}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-5f2748764d10}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-0000000ff1ce}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-0150048383c9}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-0000000ff1ce}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}
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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}\propertybag
Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-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\nch software\classicftp\ftpaccounts
Opens key: HKLM\software\wow6432node\nch 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\wow6432node\microsoft\windows\currentversion\uninstall\ultrafxp
Opens key: HKLM\software\wow6432node
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
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: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatencodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\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\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5]

Queries value: HKLM\software\wow6432node\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\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\wow6432node\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\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storeserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storeserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
Queries value:

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

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[mincompressedkey]
Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[languagecompletedprev]
Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[userplayedactive]
Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[pathupdatedcurrent]
Queries value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[bufferupdatedquick]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\run[sonyagent]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-

0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\uninstall\addressbook[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\adobe flash player
activex[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\adobe flash player
activex[displayname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\connection
manager[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\directdrawex[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\fontcore[uninstallstring]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie40[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie4data[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\ie5bakex[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\iedata[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mobileoptionpack[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\schedulingagent[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wic[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-befc77a11a1e}[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{196bb40d-1578-3d01-b289-befc77a11a1e}[displayname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-2f83217002ff}[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{26a24ae4-039d-4ca4-87b4-2f83217002ff}[displayname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{4a03706f-666a-4037-7777-5f2748764d10}[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-0000000ff1ce}[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90120000-0020-0409-0000-0000000ff1ce}[displayname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-0150048383c9}[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{90850409-6000-11d3-8cfe-0150048383c9}[displayname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-0000000ff1ce}[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95120000-003f-0409-0000-0000000ff1ce}[displayname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{95140000-00af-0409-0000-0000000ff1ce}[displayname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}[uninstallstring]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{ac76ba86-7ad7-1033-7b44-a93000000001}[displayname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localizedname]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[precreate]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
Queries value:
HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[name]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[description]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[parsiname]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[security]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[category]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[name]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[parentfolder]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[description]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[relativepath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[parsiname]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[infotip]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[localizedname]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}[icon]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaaa-29d317c6f066}[initfolderhandler]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software\wow6432node[debuglogpath]
Queries value: HKLM\software\wow6432node[debugloglevel]
Queries value: HKLM\software\wow6432node[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[mincompressedkey]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[languagecompletedprev]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[userplayedactive]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[pathupdatedcurrent]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\ime\imtc70[bufferupdatedquick]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\windows\currentversion\run[sonyagent]