

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3310, Task ID: 750

Task ID:	750
Risk Level:	10
Date Processed:	2016-05-18 10:33:46 (UTC)
Processing Time:	23.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6b1383f452de6d7b6d9a656c24904858.exe"
Sample ID:	3310
Type:	basic
Owner:	admin
Label:	6b1383f452de6d7b6d9a656c24904858
Date Added:	2016-05-18 10:30:49 (UTC)
File Type:	PE32:win32:gui
File Size:	86016 bytes
MD5:	6b1383f452de6d7b6d9a656c24904858
SHA256:	6bfd319db22de02b3658e3618808b2e72ac4ddc8937ac2fd046a6b7e87b768a7
Description:	None

Pattern Matching Results

- 3 Long sleep detected
- 4 Terminates process under Windows subfolder
- 10 Creates malicious events: Beebone [Trojan]
- 6 Checks task list from command line

Process/Thread Events

Creates process:	C:\windows\temp\6b1383f452de6d7b6d9a656c24904858.exe
["C:\windows\temp\6b1383f452de6d7b6d9a656c24904858.exe"]	
Creates process:	C:\Windows\SysWOW64\cmd.exe ["C:\Windows\System32\cmd.exe" /c tasklist&&del 6b1383f452de6d7b6d9a656c24904858.exe]
Creates process:	C:\Windows\SysWOW64\tasklist.exe [tasklist]
Terminates process:	C:\Windows\Temp\6b1383f452de6d7b6d9a656c24904858.exe
Terminates process:	C:\Windows\SysWOW64\tasklist.exe
Terminates process:	C:\Windows\SysWOW64\cmd.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\!MSFTHISTORY!_
Creates mutex:	\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!roaming!microsoft!windows!cookies!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:\users\admin!appdata!local!microsoft!windows!history!history.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\!IETId!Mutex
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\Sessions\1\BaseNamedObjects\DINPUTWINMM
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\BaseNamedObjects\ConsoleEvent-0x00000000000000974
Creates event:	\BaseNamedObjects\TermSrvReadyEvent
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:\WINDOWS?TEMP?

6B1383F452DE6D7B6D9A656C24904858.EXE

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
Opens:	C:\Windows\Prefetch\6B1383F452DE6D7B6D9A656C24904-B353A3C0.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\MSVBVM60.DLL
 Opens: C:\Windows\SysWOW64\msvbvm60.dll
 Opens: C:\Windows\SysWOW64\sechost.dll
 Opens: C:\Windows\SysWOW64\imm32.dll
 Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens: C:\Windows\SysWOW64\rpcss.dll
 Opens: C:\Windows\SysWOW64\uxtheme.dll
 Opens: C:\Windows\temp\6b1383f452de6d7b6d9a656c24904858.exe.cfg
 Opens: C:\Windows\temp\SXS.DLL
 Opens: C:\Windows\SysWOW64\sxs.dll
 Opens: C:\Windows\System32\C_932.NLS
 Opens: C:\Windows\System32\C_949.NLS
 Opens: C:\Windows\System32\C_950.NLS
 Opens: C:\Windows\System32\C_936.NLS
 Opens: C:\Windows\temp\WINMM.DLL
 Opens: C:\Windows\SysWOW64\winmm.dll
 Opens: C:\Windows\temp\MMDevAPI.DLL
 Opens: C:\Windows\SysWOW64\MMDevAPI.dll
 Opens: C:\Windows\temp\PROPSYS.dll
 Opens: C:\Windows\SysWOW64\propsys.dll
 Opens: C:\Windows\SysWOW64\kernel32.dll
 Opens: C:\Windows\temp\LZ32.DLL
 Opens: C:\Windows\SysWOW64\lz32.dll
 Opens: C:\Windows\Temp\6b1383f452de6d7b6d9a656c24904858.exe
 Opens: C:\
 Opens: C:\Windows\SysWOW64\wininet.dll
 Opens: C:\Windows\temp\6b1383f452de6d7b6d9a656c24904858.exe.Local\
 Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
 controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
 Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
 controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
 Opens: C:\Windows\WindowsShell.Manifest
 Opens: C:\Windows\temp\profapi.dll
 Opens: C:\Windows\SysWOW64\profapi.dll
 Opens: C:\Users\Admin
 Opens: C:\Users\Admin\AppData\Local
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Files\desktop.ini
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Files\Content.IE5
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Files\Content.IE5\desktop.ini
 Opens: C:\Users\Admin\AppData\Roaming
 Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Files\Content.IE5\index.dat
 Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
 Opens: C:\Windows\temp\ntmarta.dll
 Opens: C:\Windows\SysWOW64\ntmarta.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\RASAPI32.dll
 Opens: C:\Windows\SysWOW64\rasapi32.dll
 Opens: C:\Windows\temp\rasman.dll
 Opens: C:\Windows\SysWOW64\rasman.dll
 Opens: C:\Windows\temp\rtutils.dll
 Opens: C:\Windows\SysWOW64\rtutils.dll
 Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\
 Opens: C:\Windows\SysWOW64\ras
 Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
 Opens: C:\Windows\temp\sensapi.dll
 Opens: C:\Windows\SysWOW64\SensApi.dll
 Opens: C:\Windows\SysWOW64\nlaapi.dll
 Opens: C:\Windows\temp\rasadhlp.dll
 Opens: C:\Windows\SysWOW64\rasadhlp.dll
 Opens: C:\Windows\temp\VERSION.dll
 Opens: C:\Windows\SysWOW64\version.dll
 Opens: C:\Windows\SysWOW64\en-US\urlmon.dll.mui
 Opens: C:\Windows\SysWOW64\mswsock.dll

Opens:	C:\Windows\SysWOW64\WSHTCPIP.DLL
Opens:	C:\Windows\SysWOW64\wship6.dll
Opens:	C:\Windows\temp\dhcpcsvc6.DLL
Opens:	C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens:	C:\Windows\temp\dhcpcsvc.DLL
Opens:	C:\Windows\SysWOW64\dhcpcsvc.dll
Opens:	C:\Windows\System32\drivers\etc\hosts
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\temp\apphelp.dll
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\SysWOW64\ieframe.dll
Opens:	C:\Windows\SysWOW64\oleacc.dll
Opens:	C:\Windows\temp\OLEACCRC.DLL
Opens:	C:\Windows\SysWOW64\oleaccrc.dll
Opens:	C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
Opens:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000001.db
Opens:	C:\Users\Admin\Desktop\desktop.ini
Opens:	C:\Windows\System32\propsys.dll
Opens:	C:\Windows\SysWOW64\en-US\propsys.dll.mui
Opens:	C:\Windows\SysWOW64\cmd.exe
Opens:	C:\Windows\SysWOW64\cmd.exe:Zone.Identifier
Opens:	C:\Windows\AppPatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\ui\SdDRM.dll
Opens:	C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Opens:	C:\Windows\WINHELP.INI
Opens:	C:\Windows\SysWOW64\HLP
Opens:	C:\Windows\Help\HLP
Opens:	C:\Windows\SysWOW64\winbrand.dll
Opens:	C:\Windows\SysWOW64\en-US\cmd.exe.mui
Opens:	C:\Windows\SysWOW64\tasklist.exe
Opens:	C:\Windows\Prefetch\TASKLIST.EXE-178413B7.pf
Opens:	C:\Windows\SysWOW64\mpr.dll
Opens:	C:\Windows\SysWOW64\secur32.dll
Opens:	C:\Windows\SysWOW64\framedynos.dll
Opens:	C:\Windows\SysWOW64\wtsapi32.dll
Opens:	C:\Windows\SysWOW64\netapi32.dll
Opens:	C:\Windows\SysWOW64\netutils.dll
Opens:	C:\Windows\SysWOW64\srcvcli.dll
Opens:	C:\Windows\SysWOW64\wkscli.dll
Opens:	C:\Windows\SysWOW64\dbghelp.dll
Opens:	C:\Windows\SysWOW64\en-US\tasklist.exe.mui
Opens:	C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
Opens:	C:\Windows\SysWOW64\wbem\wbemprox.dll
Opens:	C:\Windows\SysWOW64\wbem\wbemcomn.dll
Opens:	C:\Windows\SysWOW64\wbemcomn.dll
Opens:	C:\Windows\SysWOW64\wbem\Logs
Opens:	C:\Windows\SysWOW64\winsta.dll
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\Windows\SysWOW64\RpcRtRemote.dll
Opens:	C:\Windows\SysWOW64\wbem\wbemsvc.dll
Opens:	C:\Windows\SysWOW64\wbem\fastprox.dll
Opens:	C:\Windows\SysWOW64\wbem\NTDSAPI.dll
Opens:	C:\Windows\SysWOW64\ntdsapi.dll
Opens:	C:\Windows\SysWOW64\wbem\wmiutils.dll
Opens:	C:\Windows\SysWOW64\wbem\en-US\wmiutils.dll.mui
Opens:	C:\Windows\SysWOW64\6b1383f452de6d7b6d9a656c24904858.exe
Reads from:	C:\Windows\Temp\6b1383f452de6d7b6d9a656c24904858.exe
Reads from:	C:\Windows\System32\drivers\etc\hosts
Reads from:	C:\Users\Admin\Desktop\desktop.ini
Reads from:	C:\Windows\SysWOW64\cmd.exe
Reads from:	C:\Windows\SysWOW64\tasklist.exe

Network Events

DNS query:	domai.1noip.org
Sends data to:	8.8.8.8:53
Receives data from:	8.8.8.8:53

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKLM\software\wow6432node\microsoft\tracing
Creates key:	HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32
Creates key:	HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key:	HKCU\software\microsoft\windows nt\currentversion\network\location awareness

Creates key: HKCU\software\microsoft\visual basic\6.0
 Creates key: HKCU\software
 Creates key: HKCU\software\microsoft
 Creates key: HKCU\software\microsoft\visual basic
 Creates key: HKLM\software\wow6432node\microsoft\wbem\cimom
 Deletes value: HKCU\software\microsoft\windows\currentversion\internet
 settings[proxyserver]
 Deletes value: HKCU\software\microsoft\windows\currentversion\internet
 settings[proxyoverride]
 Deletes value: HKCU\software\microsoft\windows\currentversion\internet
 settings[autoconfigurl]
 Deletes value: HKCU\software\microsoft\windows\currentversion\internet
 settings\zonemap[proxybypass]
 Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings\zonemap[proxybypass]
 Deletes value: HKCU\software\microsoft\windows\currentversion\internet
 settings\zonemap[intranetname]
 Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings\zonemap[intranetname]
 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\ddl
 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\locale\nls\customlocale
 Opens key: HKLM\system\currentcontrolset\control\locale\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\locale\nls\sorting\versions
 Opens key: HKLM\
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\diagnostics
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\dlloptions
 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\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\control\locale\nls\extendedlocale
 Opens key: HKLM\system\currentcontrolset\control\locale\nls\locale
 Opens key: HKLM\system\currentcontrolset\control\locale\nls\locale\alternate sorts
 Opens key: HKLM\system\currentcontrolset\control\locale\nls\language groups
 Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens key: HKLM\system\currentcontrolset\control\locale\nls\codepage
 Opens key: HKLM\software\wow6432node\microsoft\vba\monitors
 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\software\policies\microsoft\sqlclient\windows
 Opens key: HKLM\software\microsoft\sqlclient\windows
 Opens key: HKLM\system\currentcontrolset\control\sqlservicelist
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\drivers32
 Opens key:
 HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
 Opens key: HKCU\software\microsoft\windows\currentversion\multimedia\midimap

Opens key: HKLM\software\wow6432node\microsoft\oleaut\userera
Opens key: HKCU\software\policies\microsoft\control
panel\international\calendars\twodigityearmax
Opens key: HKCU\control panel\international\calendars\twodigityearmax
Opens key: HKLM\system\currentcontrolset\services\disk\enum
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\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\wow6432node\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software\wow6432node
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer
Opens key: HKLM\software\policies\microsoft\internet explorer
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main
Opens key: HKLM\software\policies\microsoft\internet explorer\main
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\main\featurecontrol
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer
Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer
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\{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\knownfolderssettings
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}
Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag
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\internet
settings\5.0\cache\history
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders

Opens key: HKLM\system\currentcontrolset\services\ldap

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\20eb7494

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: HKCU\software\microsoft\windows\currentversion\internet settings\wpad

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32

Opens key: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\profilelist
Opens key: HKLM\software\microsoft\sqlclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqlclient\windows\disabledsessions\
Opens key: HKU\
Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\system\currentcontrolset\services\dns
Opens key: HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
Opens key:
HKLM\system\currentcontrolset\services\dnsclient\parameters\dnspolicyconfig
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet

[illegible]

Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solids_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solids_in_userinfo_kb932562
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKCU\software\microsoft\internet explorer\ietld
Opens key: HKLM\system\currentcontrolset\control\cmf\config
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
migration\providers\tcpip6
Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters\dnsclient
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
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\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5bae0b1}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\services\netbt\linkage
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\6b1383f452de6d7b6d9a656c24904858.exe
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\delegatefolders
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{031e4825-
7b94-4dc3-b131-e946b44c8dd5}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{04731b67-
d933-450a-90e6-4acd2e9408fe}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{11016101-
e366-4d22-bc06-4ada335c892b}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{26ee0668-
a00a-44d7-9371-beb064c98683}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{4336a54d-
038b-4685-ab02-99bb52d3fb8b}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{450d8fba-
ad25-11d0-98a8-0800361b1103}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{5399e694-
6ce5-4d6c-8fce-1d8870fdbcba0}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{59031a47-
3f72-44a7-89c5-5595fe6b30ee}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{645ff040-
5081-101b-9f08-00aa002f954e}
Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{89d83576-6bd1-4c86-9454-beb04e94c819}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{9343812e-1c37-4a49-a12e-4b2d810d956b}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{daf95313-e44d-46af-be1b-cbacea2c3065}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{e345f35f-9397-435c-8f95-4e922c26259e}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\delegatefolders
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace\delegatefolders
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder
Opens key:
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum
Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKCU\software\classes\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder
Opens key: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder
Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shell extensions\blocked
Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags\custom\ieframe.dll
Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached
Opens key: HKLM\software\microsoft\com3
Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas

Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\progid
Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\progid
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler
Opens key: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-
42a0-1069-a2ea-08002b30309d}
Opens key: HKCU\software\classes\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder
Opens key: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{645ff040-
5081-101b-9f08-00aa002f954e}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{645ff040-5081-101b-
9f08-00aa002f954e}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder
Opens key: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{26ee0668-
a00a-44d7-9371-beb064c98683}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{26ee0668-a00a-44d7-
9371-beb064c98683}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder
Opens key: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-
3f72-44a7-89c5-5595fe6b30ee}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-
89c5-5595fe6b30ee}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder
Opens key: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{031e4825-
7b94-4dc3-b131-e946b44c8dd5}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{031e4825-7b94-4dc3-
b131-e946b44c8dd5}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder
Opens key: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{04731b67-
d933-450a-90e6-4acd2e9408fe}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{04731b67-d933-450a-
90e6-4acd2e9408fe}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder
Opens key: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{11016101-
e366-4d22-bc06-4ada335c892b}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{11016101-e366-4d22-
bc06-4ada335c892b}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder
Opens key: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{4336a54d-
038b-4685-ab02-99bb52d3fb8b}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{4336a54d-038b-4685-
ab02-99bb52d3fb8b}\shellfolder

Opens key: HKCU\software\classes\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder
Opens key: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder
Opens key: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{89d83576-6bd1-4c86-9454-beb04e94c819}\shellfolder
Opens key: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-beb04e94c819}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{89d83576-6bd1-4c86-9454-beb04e94c819}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{89d83576-6bd1-4c86-9454-beb04e94c819}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder
Opens key: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder
Opens key: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder
Opens key: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{daf95313-e44d-46af-be1b-cbacea2c3065}\shellfolder
Opens key: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-cbacea2c3065}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{daf95313-e44d-46af-be1b-cbacea2c3065}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{daf95313-e44d-46af-be1b-cbacea2c3065}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder
Opens key: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder
Opens key: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder

Opens key: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\app_paths\cmd.exe

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app_paths\cmd.exe

Opens key: HKLM\software\microsoft\windows\currentversion\app_paths\cmd.exe

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

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

Opens key: HKCU\software\classes\drive\shellex\folderextensions

Opens key: HKCR\drive\shellex\folderextensions

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}

Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion

Opens key: HKLM\software\wow6432node\microsoft\windows\shell\registeredapplications\urlassociations\directory\openwithprogids

Opens key: HKCU\software\microsoft\windows\shell\associations\urlassociations\directory

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\curver

Opens key: HKCR\directory\curver

Opens key: HKCR\directory\

Opens key: HKCU\software\classes\directory\shellex\iconhandler

Opens key: HKCR\directory\shellex\iconhandler

Opens key: HKCU\software\classes\folder

Opens key: HKCR\folder

Opens key: HKCU\software\classes\folder\shellex\iconhandler

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

Opens key: HKCU\software\classes\allfilesystemobjects\shellex\iconhandler

Opens key: HKCR\allfilesystemobjects\shellex\iconhandler

Opens key: HKCU\software\classes\directory\docobject

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}\

Opens key: HKCR\directory\docobject

Opens key: HKCU\software\classes\folder\docobject

Opens key: HKCR\folder\docobject

Opens key: HKCU\software\classes\allfilesystemobjects\docobject

Opens key: HKCR\allfilesystemobjects\docobject

Opens key: HKCU\software\classes\directory\browseinplace

Opens key: HKCR\directory\browseinplace

Opens key: HKCU\software\classes\folder\browseinplace

Opens key: HKCR\folder\browseinplace

Opens key: HKCU\software\classes\allfilesystemobjects\browseinplace

Opens key: HKCR\allfilesystemobjects\browseinplace

Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid

Opens key: HKCU\software\classes\folder\clsid

Opens key: HKCR\folder\clsid

Opens key: HKCU\software\classes\allfilesystemobjects\clsid

Opens key: HKCR\allfilesystemobjects\clsid

Opens key: HKCU\software\classes\ .exe

Opens key: HKCR\ .exe

Opens key: HKCU\software\classes\ .exe\openwithprogids

Opens key: HKCR\ .exe\openwithprogids

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .exe\openwithprogids

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .exe

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .exe\

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\ .exe\userchoice

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

Opens key: HKCU\software\classes\exefile\curver

Opens key: HKCR\exefile\curver

Opens key: HKCR\exefile\

Opens key: HKCU\software\classes\exefile\shellex\iconhandler

Opens key: HKCR\exefile\shellex\iconhandler
 Opens key: HKCU\software\classes\systemfileassociations\.exe
 Opens key: HKCR\systemfileassociations\.exe
 Opens key: HKCU\software\classes\systemfileassociations\.exe\shellex\iconhandler
 Opens key: HKCR\systemfileassociations\.exe\shellex\iconhandler
 Opens key: HKCU\software\classes\exefile\docobject
 Opens key: HKCR\exefile\docobject
 Opens key: HKCU\software\classes\systemfileassociations\.exe\docobject
 Opens key: HKCR\systemfileassociations\.exe\docobject
 Opens key: HKCU\software\classes\exefile\browseinplace
 Opens key: HKCR\exefile\browseinplace
 Opens key: HKCU\software\classes\systemfileassociations\.exe\browseinplace
 Opens key: HKCR\systemfileassociations\.exe\browseinplace
 Opens key: HKCU\software\classes\exefile\clsid
 Opens key: HKCR\exefile\clsid
 Opens key: HKCU\software\classes\systemfileassociations\.exe\clsid
 Opens key: HKCR\systemfileassociations\.exe\clsid
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}\propertybag
 Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
 Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
 Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
 Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
 Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
 Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
 Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
 Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
 Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler32
 Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprochandler
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}\propertybag
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\kindmap
 Opens key: HKCU\software\classes\exefile\shell
 Opens key: HKCR\exefile\shell
 Opens key: HKCU\software\classes\exefile\shell\open
 Opens key: HKCR\exefile\shell\open
 Opens key: HKCR\exefile\shell\open\
 Opens key: HKCU\software\classes\exefile\shell\open\command
 Opens key: HKCR\exefile\shell\open\command
 Opens key: HKCU\software\classes\exefile\shell\open\droptarget
 Opens key: HKCR\exefile\shell\open\droptarget
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\associations
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\associations
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\associations
 Opens key: HKCU\software\classes\.ade
 Opens key: HKCR\.ade
 Opens key: HKCU\software\classes\.adp
 Opens key: HKCR\.adp
 Opens key: HKCU\software\classes\.app
 Opens key: HKCR\.app
 Opens key: HKCU\software\classes\.asp
 Opens key: HKCR\.asp
 Opens key: HKCU\software\classes\.bas
 Opens key: HKCR\.bas
 Opens key: HKCU\software\classes\.bat
 Opens key: HKCR\.bat
 Opens key: HKCU\software\classes\.cer
 Opens key: HKCR\.cer

Opens key: HKCU\software\classes\.chm
 Opens key: HKCR\.chm
 Opens key: HKCU\software\classes\.cmd
 Opens key: HKCR\.cmd
 Opens key: HKCU\software\classes\.com
 Opens key: HKCR\.com
 Opens key: HKCU\software\classes\.cpl
 Opens key: HKCR\.cpl
 Opens key: HKCU\software\classes\.crt
 Opens key: HKCR\.crt
 Opens key: HKCU\software\classes\.csh
 Opens key: HKCR\.csh
 Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
 Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
 Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
 Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
 Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
 Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
 Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid
 Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
 Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
 Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
 Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\0
 Opens key: HKCU\software\classes\exefile\progid
 Opens key: HKCR\exefile\progid
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\progids\exefile
 Opens key: HKCU\software\classes\exefile\shell\open\ddeexec
 Opens key: HKCR\exefile\shell\open\ddeexec
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmd.exe
 Opens key: HKLM\system\currentcontrolset\control\session manager\apppcertdlls
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\cmd.exe
 Opens key: HKLM\software\wow6432node\microsoft\windows
 Opens key: HKLM\software\wow6432node\microsoft\windows\html help
 Opens key: HKLM\software\wow6432node\microsoft\windows\help
 Opens key: HKCU\software\policies\microsoft\windows\system
 Opens key: HKLM\software\wow6432node\microsoft\command processor
 Opens key: HKCU\software\microsoft\command processor
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\tasklist.exe
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\tasklist.exe
 Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
 Opens key: HKLM\software\wow6432node\microsoft\wbem\cimom
 Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
 Opens key: HKCU\software\classes\appid\tasklist.exe
 Opens key: HKCR\appid\tasklist.exe
 Opens key: HKLM\system\currentcontrolset\control\lsa
 Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}

Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid
Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler
Opens key: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler
Opens key: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler
Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\system\currentcontrolset\control\lsa\lipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
Opens key: HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
Opens key: HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas

Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid
Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler
Opens key: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
Opens key: HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
Opens key: HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas
Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid
Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid
Opens key: HKCU\software\classes\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
Opens key: HKCU\software\classes\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid
Opens key: HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler
Opens key: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
Opens key: HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
Opens key: HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid
Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler
Opens key: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-000000000001}
Opens key: HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-000000000001}
Opens key: HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler
Opens key: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler
Opens key: HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
Opens key: HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
Opens key: HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32
Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}
Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}
Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\treatas
Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\progid
Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\progid
Opens key: HKCU\software\classes\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}
Opens key: HKCR\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}
Opens key: HKCU\software\classes\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\progid
Opens key: HKCR\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprochandler
Opens key: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprochandler
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\image file execution
options\dlloptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions[msvbvm60.dll]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[6b1383f452de6d7b6d9a656c24904858]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows\loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value: 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\software\microsoft\sqlclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\control\sqlservicelist[sqlservicelist]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave1]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave2]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave3]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave4]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave5]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave6]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave7]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave8]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[wave9]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi1]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi2]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi3]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi4]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi5]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi6]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi7]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi8]

Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\drivers32[midi9]
Queries value:
HKCU\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value: HKLM\system\currentcontrolset\services\disk\enum[0]
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: HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasiccoverclearchannel]
Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-

33be-4251-ba85-6007caedcf9d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
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}[parsingname]
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\{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}[parsiname]
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: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content[cache\limit]
 Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruser\item]
 Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruser\item]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[relativepath]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localizedname]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[security]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
 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}[parsingname]
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: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-

b784-432e-a781-5a1130a75963}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheopath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]

Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbscservername]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbscapiforcrack]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[6b1383f452de6d7b6d9a656c24904858.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

```
settings[leashlegacycookies]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttptnocachecheck]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttptnocachecheck]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrevving]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
  Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
  Queries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  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:
```

[illegible]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storiesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storiesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpiretime]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[6b1383f452de6d7b6d9a656c24904858.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
Queries value: HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[enablefiletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[filetracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[consoletracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[maxfilesize]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[filedirectory]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[enablefiletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[filetracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[enableconsoletracing]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[consoletracingmask]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[maxfilesize]
Queries value:
HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[filedirectory]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[5386cf58]
Queries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
Queries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[queryadaptername]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[usedomainnamedevolution]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[domainnamedevolutionlevel]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[prioritize record data]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritize record data]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[allowunqualifiedquery]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[appendtomultilabelname]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screenbadtlds]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screenunreachableservers]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screendefaultservers]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dynamicserverqueryorder]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[filterclusterip]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usedns]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dnssecurenamequeryfallback]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[enableadaforallnetworks]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[directaccessqueryorder]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[addrconfigcontrol]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disablewanddynamicupdate]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddresstoregister]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatetopleveldomainzones]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[downcasespncauseapiowneristoolazy]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationoverwrite]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxnegativecachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[adaptertimeoutlimit]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[serverprioritytimelimit]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastresponderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsenderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usecompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[cacheallcompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usenewregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistrationonly]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[6b1383f452de6d7b6d9a656c24904858.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[6b1383f452de6d7b6d9a656c24904858.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
Queries value: HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[6b1383f452de6d7b6d9a656c24904858.exe]
Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature_localmachine_lockdown[6b1383f452de6d7b6d9a656c24904858.exe]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
Queries value: HKLM\system\currentcontrolset\control\cmf\config\system
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKLM\system\currentcontrolset\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]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value:
HKLM\system\currentcontrolset\services\dns\parameters\dns[shutdownonidle]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-

e1e01c1f69b5}{dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[maxnumberofaddresstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[maxnumberofaddresstoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enablemulticast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[maximizeapps]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[enableshellexecutehooks]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{04731b67-

d933-450a-90e6-4acd2e9408fe}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{11016101-e366-4d22-bc06-4ada335c892b}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{26ee0668-a00a-44d7-9371-beb064c98683}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{450d8fba-ad25-11d0-98a8-0800361b1103}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{645ff040-5081-101b-9f08-00aa002f954e}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{89d83576-6bd1-4c86-9454-beb04e94c819}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{9343812e-1c37-4a49-a12e-4b2d810d956b}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{daf95313-e44d-46af-be1b-cbacea2c3065}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{e345f35f-9397-435c-8f95-4e922c26259e}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}[suppressionpolicy]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideondektopperuser]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hasnavigationenum]
Queries value:

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-08002b30309d}]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[attributes]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[callforattributes]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[restrictedattributes]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[wantsfordisplay]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[hidefolderverbs]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[usedrophandler]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[wantsforparsing]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[queryforoverlay]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[mapnetdriveverbs]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[queryforinfotip]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[hideinwebview]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[hideondesktopperuser]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[wantsaliasednotifications]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[wantsuniversaldelegate]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[nofilefolderjunction]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[pintonamespacetree]

Queries value: HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[hasnavigationenum]

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{208d2c60-3aea-1069-a2d7-08002b30309d}]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[callforattributes]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[restrictedattributes]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsfordisplay]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hidefolderverbs]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[usedrophandler]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsforparsing]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[queryforoverlay]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[mapnetdriveverbs]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[queryforinfotip]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hideinwebview]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hideondesktopperuser]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsaliasednotifications]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsuniversaldelegate]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[nofilefolderjunction]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[pintonamespacetree]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[hasnavigationenum]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-08002b30309d}]

Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-

08002b30309d}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[loadwithoutcom]
Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0xfffff]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\ole[maxxsxshashcount]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{645ff040-5081-101b-9f08-00aa002f954e}]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-

beb064c98683}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{26ee0668-a00a-44d7-9371-beb064c98683}]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-5595fe6b30ee}]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellfolder[hasnavigationenum]

Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{031e4825-7b94-4dc3-b131-e946b44c8dd5}]

Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-4acd2e9408fe}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{04731b67-d933-450a-90e6-4acd2e9408fe}]

Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{11016101-e366-4d22-bc06-4ada335c892b}]

Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[attributes]

Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{4336a54d-038b-4685-ab02-99bb52d3fb8b}]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{450d8fba-ad25-11d0-98a8-0800361b1103}]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder[restrictedattributes]

1d8870fdcba0}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{89d83576-6bd1-4c86-9454-
beb04e94c819}]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[usedrophandler]

Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-4b2d810d956b}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{9343812e-1c37-4a49-a12e-4b2d810d956b}]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{b4fb3f98-c1ea-428d-a78a-d1f5659cba93}]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-b309680c6b7e}\shellfolder[wantsparsedisplayname]

b309680c6b7e}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{daf95313-e44d-46af-be1b-
cbacea2c3065}]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[queryforinfotip]

Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-4e922c26259e}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{e345f35f-9397-435c-8f95-4e922c26259e}]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{ed228fdf-9ea8-4870-83b1-96b02cfe0d52}]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-7367fc96ef3c}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-

7367fc96ef3c}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[pintonamespacestree]
Queries value: HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[generation]
Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
Queries value: HKCR\directory[docobject]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-
11e3-a68e-806e6f6e6963}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-
11e3-a68e-806e6f6e6963}[generation]
Queries value: HKCR\folder[docobject]
Queries value: HKCR\allfilesystemobjects[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\folder[browseinplace]
Queries value: HKCR\allfilesystemobjects[browseinplace]
Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\folder[isshortcut]
Queries value: HKCR\allfilesystemobjects[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKCR\folder[nevershowext]
Queries value: HKCR\allfilesystemobjects[nevershowext]
Queries value:

```

HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
  Queries value: HKCR\.exe[]
  Queries value: HKCR\exefile[docobject]
  Queries value: HKCR\systemfileassociations\.exe[docobject]
  Queries value: HKCR\exefile[browseinplace]
  Queries value: HKCR\systemfileassociations\.exe[browseinplace]
  Queries value: HKCR\.exe[content type]
  Queries value: HKCR\exefile[isshortcut]
  Queries value: HKCR\systemfileassociations\.exe[isshortcut]
  Queries value: HKCR\exefile[alwaysshowext]
  Queries value: HKCR\systemfileassociations\.exe[alwaysshowext]
  Queries value: HKCR\exefile[nevershowext]
  Queries value: HKCR\systemfileassociations\.exe[nevershowext]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parsiname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[initfolderhandler]
  Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
  Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
  Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[threadingmodel]
  Queries value:

```

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.exe]
Queries value: HKCR\exefile[nostaticdefaultverb]
Queries value: HKCR\exefile\shell[]
Queries value: HKCR\exefile\shell\open[neverdefault]
Queries value: HKCR\exefile\shell\open\command[delegateexecute]
Queries value: HKCR\ .asp[]
Queries value: HKCR\ .bas[]
Queries value: HKCR\ .bat[]
Queries value: HKCR\ .cer[]
Queries value: HKCR\ .chm[]
Queries value: HKCR\ .cmd[]
Queries value: HKCR\ .com[]
Queries value: HKCR\ .cpl[]
Queries value: HKCR\ .crt[]
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

```

settings[specialfolderscachesize]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[6b1383f452de6d7b6d9a656c24904858.exe]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1806]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0[1806]
  Queries value: HKCR\exefile\shell\open\command[command]
  Queries value: HKCR\exefile\shell\open\command[]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
  Queries value: HKCR\exefile\shell\open[setworkingdirectoryfromtarget]
  Queries value: HKCR\exefile\shell\open[noworkingdirectory]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value: HKCU\software\microsoft\visual basic\6.0[allowunsafeobjectpassing]
  Queries value: HKLM\software\wow6432node\microsoft\windows\html help[.hlp]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[cmd]
  Queries value: HKLM\software\wow6432node\microsoft\command processor[disableunccheck]
  Queries value: HKLM\software\wow6432node\microsoft\command processor[enableextensions]
  Queries value: HKLM\software\wow6432node\microsoft\command processor[delayedexpansion]
  Queries value: HKLM\software\wow6432node\microsoft\command processor[defaultcolor]
  Queries value: HKLM\software\wow6432node\microsoft\command processor[completionchar]
  Queries value: HKLM\software\wow6432node\microsoft\command
processor[pathcompletionchar]
  Queries value: HKLM\software\wow6432node\microsoft\command processor[autorun]
  Queries value: HKCU\software\microsoft\command processor[disableunccheck]
  Queries value: HKCU\software\microsoft\command processor[enableextensions]
  Queries value: HKCU\software\microsoft\command processor[delayedexpansion]
  Queries value: HKCU\software\microsoft\command processor[defaultcolor]
  Queries value: HKCU\software\microsoft\command processor[completionchar]
  Queries value: HKCU\software\microsoft\command processor[pathcompletionchar]
  Queries value: HKCU\software\microsoft\command processor[autorun]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[tasklist]
  Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
  Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
  Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
  Queries value: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[logging directory]
  Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[log file max size]
  Queries value: HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
  Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value: HKLM\software\microsoft\cryptography[machineguid]
  Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
  Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]

```


Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[36a1bda3]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
Queries value: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[]
Queries value: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32[threadingmodel]
Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[processid]
Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[enableprivateobjectheap]
Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit]
Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit]
Queries value: HKLM\software\wow6432node\microsoft\wbem\cimom[identifierlimit]
Queries value: HKLM\system\currentcontrolset\control\ls\customlocale[en]
Queries value: HKLM\system\currentcontrolset\control\ls\extendedlocale[en]
Queries value: HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
Queries value: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
Queries value: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[threadingmodel]
Queries value: HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
Queries value: HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
Queries value: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}[]
Queries value: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\inprocserver32[threadingmodel]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[enablefiletracing]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[enableconsoletracing]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[filetracingmask]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[consoletracingmask]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[maxfilesize]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasapi32[filedirectory]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[enablefiletracing]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[enableconsoletracing]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[filetracingmask]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[consoletracingmask]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[maxfilesize]
Sets/Creates value: HKLM\software\wow6432node\microsoft\tracing\6b1383f452de6d7b6d9a656c24904858_rasmancs[filedirectory]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\connections[savedlegacysettings]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[uncasintranet]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[autodetect]