

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	84	Host: mag2, Sample ID: 85, Task ID: 84
Risk Level:	6	
Date Processed:	2016-04-18 13:04:03 (UTC)	
Processing Time:	70.44 seconds	
Virtual Environment:	IntelliVM	
Execution Arguments:	"c:\windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe"	

Sample ID:	85
Type:	basic
Owner:	admin
Label:	007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33
Date Added:	2016-04-18 13:04:02 (UTC)
File Type:	PE32:win32:gui:.net
File Size:	137728 bytes
MD5:	118c855cfe81b7d76dc946e84ad8172a
SHA256:	007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33
Description:	None

Pattern Matching Results

- 6 Modifies firewall
- 4 Terminates process under Windows subfolder
- 3 Connects to local host
- 5 Adds autostart object
- 6 Starts process from Application Data folder
- 2 .NET compiled executable
- 6 Creates executable in application data folder
- 6 Modifies registry autorun entries

Process/Thread Events

Creates process:	
C:\windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe	
["C:\windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe"]	
Creates process:	C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe
["C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe"]	
Creates process:	C:\Windows\SysWOW64\netsh.exe [netsh firewall add allowedprogram
"C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe" "ProtocolPc1.exe" ENABLE]	
Terminates process:	
C:\Windows\Temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe	
Terminates process: C:\Windows\SysWOW64\netsh.exe	

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\d0b7ff2d863d1a546f17291f4911b563
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:	\BaseNamedObjects\3a886eb8-fe40-4d0a-b78b-9e0bcb683fb7
Creates mutex:	\Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex:	\BaseNamedObjects\.net clr networking
Creates event:	\BaseNamedObjects\CorDBIPCSyncEvent_2960
Creates event:	\KernelObjects\LowMemoryCondition
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\BaseNamedObjects\CorDBIPCSyncEvent_732
Creates event:	\BaseNamedObjects\ConsoleEvent-0x0000000000000738
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\d0b7ff2d863d1a546f17291f4911b563.exe
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\SysWOW64\mscoree.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\MSCOREE.DLL.local
Opens:	C:\Windows\Microsoft.NET\Framework\v4.0.30319
Opens:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
Opens:	C:\Windows\Microsoft.NET\Framework
Opens:	C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe.config
Opens:	C:\Windows\Temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe
Opens:	C:\windows\temp\api-ms-win-appmodel-runtime-l1-1-0.dll
Opens:	C:\Windows\SysWOW64\api-ms-win-appmodel-runtime-l1-1-0.dll
Opens:	C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
Opens:	C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll

```

Opens: C:\Windows\SysWOW64\Bem\api-ms-win-appmodel-runtime-l1-1-0.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-
11-1-0.dll
Opens: C:\Program Files (x86)\QuickTime\QTSystem\api-ms-win-appmodel-runtime-
11-1-0.dll
Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe.Local\
Opens: C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
Opens: C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
Opens: C:\
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config.cch
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\indexf8.dat
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
Opens: C:\Windows\assembly\GAC_32\mscorlib\v2.0.0.0__b77a5c561934e089
Opens: C:\Windows\Temp
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Opens: C:\windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.config
Opens: C:\Windows\SysWOW64\l_intl.nls
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
Opens: C:\Windows\Globalization\en-us.nlp
Opens: C:\Windows\assembly\GAC_32\mscorlib\v2.0.0.0__b77a5c561934e089\sorttbls.nlp
Opens: C:\Windows\assembly\GAC_32\mscorlib\v2.0.0.0__b77a5c561934e089\sortkey.nlp
Opens: C:\Windows\assembly\pubpol138.dat
Opens: C:\Windows\assembly\GAC\PublisherPolicy.tme
Opens: C:\windows\temp\en-US\j.resources.dll
Opens: C:\windows\temp\en-US\j.resources\j.resources.dll
Opens: C:\windows\temp\en-US\j.resources.exe
Opens: C:\windows\temp\en-US\j.resources\j.resources.exe
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\Culture.dll
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\en-US\mscorrc.dll
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\en-US\mscorrc.dll.DLL
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\en\mscorrc.dll
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\en\mscorrc.dll.DLL
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll
Opens: C:\Windows\Globalization\en.nlp
Opens: C:\windows\temp\en\j.resources.dll
Opens: C:\windows\temp\en\j.resources\j.resources.dll
Opens: C:\windows\temp\en\j.resources.exe
Opens: C:\windows\temp\en\j.resources\j.resources.exe
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
Opens: C:\Windows\assembly\GAC_MSIL\System\v2.0.0.0__b77a5c561934e089
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBasic\08d608378aa405adc844f3cf36974b8c\Microsoft.VisualBasic.ni.dll
Opens: C:\Windows\assembly\GAC_MSIL\Microsoft.VisualBasic\8.0.0.0__b03f5f7f11d50a3a
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
Opens: C:\Windows\assembly\GAC_MSIL\System\v2.0.0.0__b77a5c561934e089\ntdll.dll
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll
Opens: C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\v2.0.0.0__b77a5c561934e089
Opens: C:\Windows\assembly\GAC_MSIL\System.Drawing\v2.0.0.0__b03f5f7f11d50a3a
Opens: C:\Users\Admin\AppData\Roaming\ProtocolPc.exe
Opens: C:\Windows\assembly\GAC_MSIL\System\v2.0.0.0__b77a5c561934e089\shell132.dll
Opens: C:\windows\temp\PROPSYS.dll
Opens: C:\Windows\SysWOW64\propsys.dll
Opens: C:\Windows\SysWOW64\shell132.dll
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\comctl132.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\Registration\R000000000000004.clb
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
Opens: C:\windows\temp\ntmarta.dll
Opens: C:\Windows\SysWOW64\ntmarta.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000018.db
Opens: C:\Users\Admin\Desktop\desktop.ini
Opens: C:\Windows\System32\propsys.dll
Opens: C:\Users\desktop.ini
Opens: C:\Users

```

Opens: C:\Users\Admin\Searches\desktop.ini
Opens: C:\Users\Admin\Videos\desktop.ini
Opens: C:\Users\Admin\Pictures\desktop.ini
Opens: C:\Users\Admin\Contacts\desktop.ini
Opens: C:\Users\Admin\Favorites\desktop.ini
Opens: C:\Users\Admin\Music\desktop.ini
Opens: C:\Users\Admin\Downloads\desktop.ini
Opens: C:\Users\Admin\Documents\desktop.ini
Opens: C:\Users\Admin\Links\desktop.ini
Opens: C:\Users\Admin\Saved Games\desktop.ini
Opens: C:\Windows\temp\apphelp.dll
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\SysWOW64\shdocvw.dll
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\Windows\SysWOW64\urlmon.dll
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Opens: C:\Users\Admin\AppData
Opens: C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe:Zone.Identifier
Opens: C:\Windows\SysWOW64\embdtrst.dll
Opens: C:\Users\Admin\AppData\Roaming\ui\SwDRM.dll
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2960.88031
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2960.88031
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config.cch.2960.88046
Opens: C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe.config
Opens: C:\Users\Admin\AppData\Roaming\api-ms-win-appmodel-runtime-l1-1-0.dll
Opens: C:\Users\Admin\AppData\Roaming\VERSION.dll
Opens: C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe.Local\
Opens: C:\Windows\temp\CRYPTSP.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\Windows\temp\RpcRtRemote.dll
Opens: C:\Windows\SysWOW64\RpcRtRemote.dll
Opens: C:\Users\Admin\AppData\Roaming\profapi.dll
Opens: C:\Users\Admin\AppData\Roaming\ProtocolPc1.config
Opens: C:\Users\Admin\AppData\Roaming\en-US\j.resources.dll
Opens: C:\Users\Admin\AppData\Roaming\en-US\j.resources\j.resources.dll
Opens: C:\Users\Admin\AppData\Roaming\en-US\j.resources.exe
Opens: C:\Users\Admin\AppData\Roaming\en-US\j.resources\j.resources.exe
Opens: C:\Users\Admin\AppData\Roaming\en\j.resources.dll
Opens: C:\Users\Admin\AppData\Roaming\en\j.resources\j.resources.dll
Opens: C:\Users\Admin\AppData\Roaming\en\j.resources.exe
Opens: C:\Users\Admin\AppData\Roaming\en\j.resources\j.resources.exe
Opens: C:\Users\Admin\AppData\Roaming\netsh.exe
Opens: C:\Windows\SysWOW64\netsh.exe
Opens: C:\Windows\SysWOW64\ui\SwDRM.dll
Opens: C:\Windows\SysWOW64\credui.dll
Opens: C:\Windows\SysWOW64\mpr.dll
Opens: C:\Windows\SysWOW64\en-US\netsh.exe.mui
Opens: C:\Windows\SysWOW64\netsh.exe.Local\
Opens: C:\Windows\SysWOW64\nshwfp.dll
Opens: C:\Windows\SysWOW64\FWPUCFLT.DLL
Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens: C:\Windows\SysWOW64\winnsi.dll
Opens: C:\Windows\SysWOW64\slc.dll
Opens: C:\Windows\SysWOW64\dhcpcmonitor.dll
Opens: C:\Windows\SysWOW64\dhcpcsvc.dll
Opens: C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens: C:\Windows\SysWOW64\DHCPQEC.DLL
Opens: C:\Windows\SysWOW64\QUTIL.DLL
Opens: C:\Windows\SysWOW64\wevtapi.dll
Opens: C:\Windows\SysWOW64\wshelper.dll
Opens: C:\Windows\SysWOW64\ws2help.dll
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens: C:\Windows\SysWOW64\nshhttp.dll
Opens: C:\Windows\SysWOW64\httpapi.dll
Opens: C:\Windows\SysWOW64\ifmon.dll
Opens: C:\Windows\SysWOW64\mprapi.dll
Opens: C:\Windows\SysWOW64\nci.dll
Opens: C:\Windows\SysWOW64\devrtl.dll
Opens: C:\Windows\SysWOW64\netiohlp.dll
Opens: C:\Windows\SysWOW64\dnsapi.dll
Opens: C:\Windows\SysWOW64\rpcnsh.dll
Opens: C:\Windows\SysWOW64\hnetmon.dll
Opens: C:\Windows\SysWOW64\netshell.dll
Opens: C:\Windows\SysWOW64\nlaapi.dll
Opens: C:\Windows\SysWOW64\dot3cfg.dll
Opens: C:\Windows\SysWOW64\dot3api.dll
Opens: C:\Windows\SysWOW64\atl.dll
Opens: C:\Windows\SysWOW64\eapcfg.dll
Opens: C:\Windows\SysWOW64\onex.dll
Opens: C:\Windows\SysWOW64\eappprxy.dll
Opens: C:\Windows\SysWOW64\authfwcfg.dll
Opens: C:\Windows\SysWOW64\bcrypt.dll
Opens: C:\Windows\SysWOW64\FirewallAPI.dll
Opens: C:\Windows\SysWOW64\winipsec.dll
Opens: C:\Windows\SysWOW64\p2pnetsh.dll
Opens: C:\Windows\SysWOW64\P2P.dll
Opens: C:\Windows\SysWOW64\p2pcollab.dll
Opens: C:\Windows\SysWOW64\whhelper.dll
Opens: C:\Windows\SysWOW64\winhttp.dll
Opens: C:\Windows\SysWOW64\webio.dll
Opens: C:\Windows\SysWOW64\nshipsec.dll
Opens: C:\Windows\SysWOW64\netapi32.dll
Opens: C:\Windows\SysWOW64\netutils.dll
Opens: C:\Windows\SysWOW64\svrcli.dll
Opens: C:\Windows\SysWOW64\wkscli.dll
Opens: C:\Windows\SysWOW64\logoncli.dll
Opens: C:\Windows\SysWOW64\userenv.dll
Opens: C:\Windows\SysWOW64\activeds.dll

Opens: C:\Windows\SysWOW64\adslrpc.dll
Opens: C:\Windows\SysWOW64\polstore.dll
Opens: C:\Windows\SysWOW64\rasmontr.dll
Opens: C:\Windows\SysWOW64\rasapi32.dll
Opens: C:\Windows\SysWOW64\rasman.dll
Opens: C:\Windows\SysWOW64\mfcd2u.dll
Opens: C:\Windows\SysWOW64\odbc32.dll
Opens: C:\Windows\SysWOW64\odbcint.dll
Opens: C:\Windows\SysWOW64\MFC42LOC.DLL
Opens: C:\Windows\SysWOW64\MFC42LOC.DLL.DLL
Opens: C:\Windows\system32\MFC42LOC.DLL
Opens: C:\Windows\system32\MFC42LOC.DLL.DLL
Opens: C:\Windows\SysWOW64\PeerDistSh.dll
Opens: C:\Windows\SysWOW64\fwcfg.dll
Opens: C:\Windows\SysWOW64\wlancfg.dll
Opens: C:\Windows\SysWOW64\wlanapi.dll
Opens: C:\Windows\SysWOW64\wlanutil.dll
Opens: C:\Windows\SysWOW64\wlanhlp.dll
Opens: C:\Windows\SysWOW64\en-US\p2pnetsh.dll.mui
Opens: C:\Windows\SysWOW64\gpapi.dll
Opens: C:\Windows\SysWOW64\bccryptprimitives.dll
Opens: C:\Windows\SysWOW64\mprmsg.dll
Opens: C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
Opens: C:\Users\Admin\AppData\Roaming\shfolder.dll
Opens: C:\Windows\SysWOW64\shfolder.dll
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\d0b7ff2d863d1a546f17291f4911b563.exe
Opens: C:\Users\Admin\AppData\Roaming\ntdll.DLL
Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\bc09ad2d49d8535371845cd7532f9271\System.Configuration.ni.dll
Opens:
C:\Windows\assembly\GAC_MSIL\System.Configuration\2.0.0.0__b03f5f7f11d50a3a
Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\461d3b6b3f43e6fbe6c897d5936e17e4\System.Xml.ni.dll
Opens: C:\Windows\assembly\GAC_MSIL\System.Xml\2.0.0.0__b77a5c561934e089
Opens: C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\ws2_32.dll
Opens: C:\Windows\SysWOW64\WSH_TCPIP.DLL
Opens: C:\Windows\SysWOW64\wship6.dll
Opens: C:\Windows\SysWOW64\tzres.dll
Opens: C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\psapi.dll
Writes to: C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe
Writes to: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\d0b7ff2d863d1a546f17291f4911b563.exe
Reads from: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Reads from:
C:\Windows\Temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe
Reads from: C:\Users\Admin\Desktop\desktop.ini
Reads from: C:\Users\desktop.ini
Reads from: C:\Users\Admin\Searches\desktop.ini
Reads from: C:\Users\Admin\Videos\desktop.ini
Reads from: C:\Users\Admin\Pictures\desktop.ini
Reads from: C:\Users\Admin\Contacts\desktop.ini
Reads from: C:\Users\Admin\Favorites\desktop.ini
Reads from: C:\Users\Admin\Music\desktop.ini
Reads from: C:\Users\Admin\Downloads\desktop.ini
Reads from: C:\Users\Admin\Documents\desktop.ini
Reads from: C:\Users\Admin\Links\desktop.ini
Reads from: C:\Users\Admin\Saved Games\desktop.ini
Reads from: C:\Windows\SysWOW64\shdocvw.dll
Reads from: C:\Users\Admin\AppData\Roaming\ProtocolPc1.exe
Reads from: C:\Windows\SysWOW64\netsh.exe

Network Events

Connects to: 127.0.0.1:1177

Windows Registry Events

Creates key: HKLM\software\microsoft\fusion\gacchangenotification\default
Creates key: HKCU\software\d0b7ff2d863d1a546f17291f4911b563
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\microsoft\windows nt\currentversion\image file execution
options\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe
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\nls\sorting\versions
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\v4.0
Opens key: HKLM\software\wow6432node\microsoft\.netframework
Opens key: HKCU\software\microsoft\.netframework
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\.netframework\policy\standards
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\standards\v2.0.50727
Opens key: HKLM\software\wow6432node\microsoft\fusion
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch\v4.0.30319.00000
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch\v4.0.30319.00000\mscorwks.dll
Opens key: HKLM\software\microsoft\fusion
Opens key: HKCU\software\microsoft\fusion
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets\localintranet
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-2469590586-531574596-741558139-1004
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2469590586-531574596-741558139-1004
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
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\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
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\system\currentcontrolset\control\locale\extendedlocale
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\{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\currentversion\explorer\knownfolderssettings
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\v2.0.50727\security\policy
Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32
Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\indexf8
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\1
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloxptions
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:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6a\68a8ac6a
Opens key: HKLM\software\wow6432node\microsoft\strongname
Opens key: HKLM\software\microsoft\fusion\publisherpolicy\default
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\770a8281\4ebac521
Opens key: HKLM\software\microsoft\windows\currentversion\installer\managed\s-1-5-21-2469590586-531574596-741558139-1004\installer\assemblies\c:\windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe

Opens key:
HKCU\software\microsoft\installer\assemblies\c:\windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe

Opens key:
HKCR\installer\assemblies\c:\windows\temp\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe

Opens key:
HKLM\software\microsoft\windows\currentversion\installer\managed\5-21-2469590586-531574596-741558139-1004\installer\assemblies\global

Opens key:
HKCU\software\microsoft\installer\assemblies\global

Opens key:
HKCR\installer\assemblies\global

Opens key:
HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\770a8281\49ca294a

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system__b77a5c561934e089

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\5

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\6

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\7

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.xml__b77a5c561934e089

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.configuration__b03f5f7f11d50a3a

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.8.0.microsoft.visualbasic__b03f5f7f11d50a3a

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\16

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\5cd4db\5

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\1a

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6e8397\46ad0879\7

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2b1a4e4\38a3212c\2a

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\24bf93f6\455bab30\b

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\4f99a7c9\53bea2b0\73

Opens key:
HKLM\software\wow6432node\microsoft\framework\policy\aptca

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.web__b03f5f7f11d50a3a

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.management__b03f5f7f11d50a3a

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.runtime.remoting__b77a5c561934e089

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.deployment__b03f5f7f11d50a3a

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.drawing__b03f5f7f11d50a3a

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.windows.forms__b77a5c561934e089

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\3

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\1b

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\1e

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d

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\sqmclient\windows

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.runtime.serialization.formatters.soap__b03f5f7f11d50a3a

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.accessibility__b03f5f7f11d50a3a

Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.security__b03f5f7f11d50a3a

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

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

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

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

Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe

Opens key:
HKCU\software\classes\

Opens key:
HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shell\folder

Opens key:
HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shell\folder

Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shell\folder

Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shell\folder

Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum
 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: 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: HKLM\software\microsoft\com3
 Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
 Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\
 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\system\currentcontrolset\control\lsa\accessproviders
 Opens key: HKLM\system\currentcontrolset\services\ldap
 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: 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:
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\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}\propertybag
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\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
ea55d8994f1a}
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\progid
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\progid
Opens key: HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
Opens key: HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
Opens key: HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\progid
Opens key: HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler
Opens key: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f7f1ed05-9f6d-47a2-aaae-29d317c6f066}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2112ab0a-c86a-4ffe-a368-0de96e47012e}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{48daf80b-e6cf-4f4e-b800-0e69d84ee384}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{48daf80b-e6cf-4f4e-b800-0e69d84ee384}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4aa340d-f20f-4863-afef-f87ef2e6ba25}\propertybag
Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9e52ab10-f80d-49df-acb8-4330f5687855}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9e52ab10-f80d-49df-acb8-4330f5687855}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{98ec0e18-2098-4d44-8644-66979315a281}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{98ec0e18-2098-4d44-8644-66979315a281}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a4115719-d62e-491d-aa7c-e74b8be3b067}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{cac52c1a-b53d-4edc-92d7-6b2e8ac19434}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{cac52c1a-b53d-4edc-92d7-6b2e8ac19434}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{18989b1d-99b5-455b-841c-ab7c74e4ddfc}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{18989b1d-99b5-455b-841c-ab7c74e4ddfc}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de974d24-d9c6-4d3e-bf91-f4455120b917}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{6f0cd92b-2e97-45d1-88ff-b0d186b8dedd}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{6f0cd92b-2e97-45d1-88ff-b0d186b8dedd}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{76fc4e2d-d6ad-4519-a663-37bd56068185}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{76fc4e2d-d6ad-4519-a663-37bd56068185}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a75d362e-50fc-4fb7-ac2c-a8beaa314493}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a75d362e-50fc-4fb7-ac2c-a8beaa314493}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{491e922f-5643-4af4-a7eb-4e7a138d8174}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{491e922f-5643-4af4-a7eb-4e7a138d8174}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{debf2536-e1a8-4c59-b6a2-414586476aea}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0f214138-b1d3-4a90-bba9-27cbc0c5389a}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2400183a-6185-49fb-a2d8-4a392a602ba3}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2400183a-6185-49fb-a2d8-4a392a602ba3}\propertybag

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:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4900540-2379-4c75-844b-64e6faf8716b}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c4900540-2379-4c75-844b-64e6faf8716b}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{289a9a43-be44-4057-a41b-587a76d7e7f9}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{289a9a43-be44-4057-a41b-587a76d7e7f9}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bfebf45-347d-4006-a5be-ac0cb0567192}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bfebf45-347d-4006-a5be-ac0cb0567192}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b7534046-3ecb-4c18-be4e-64cd4cb7d6ac}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ee32e446-31ca-4aba-814f-a5ebd2fd6d5e}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c870044b-f49e-4126-a9c3-b52a1ff411e8}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c5abbf53-e17f-4121-8900-86626fc2c973}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{56784854-c6cb-462b-8169-88e350acb882}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{56784854-c6cb-462b-8169-88e350acb882}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7b396e54-9ec5-4300-be0a-2482ebae1a26}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7b396e54-9ec5-4300-be0a-2482ebae1a26}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bcbd3057-ca5c-4622-b42d-bc56db0ae516}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bcbd3057-ca5c-4622-b42d-bc56db0ae516}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a302545d-deff-464b-abe8-61c8648d939b}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a302545d-deff-464b-abe8-61c8648d939b}\propertybag

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\{2a00375e-224c-49de-b8d1-440df7ef3ddc}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2a00375e-224c-49de-b8d1-440df7ef3ddc}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{e555ab60-153b-4d17-9f04-a5fe99fc15ec}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{e555ab60-153b-4d17-9f04-a5fe99fc15ec}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{054fae61-4dd8-4787-80b6-090220c4b700}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b250c668-f57d-4ee1-a63c-290ee7d1aa1f}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b250c668-f57d-4ee1-a63c-290ee7d1aa1f}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52528a6b-b9e3-4add-b60d-588c2dba842d}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{52528a6b-b9e3-4add-b60d-588c2dba842d}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8983036c-27c0-404b-8f08-102d10dcfd74}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8983036c-27c0-404b-8f08-102d10dcfd74}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bcb5256f-79f6-4cee-b725-dc34e402fd46}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bcb5256f-79f6-4cee-b725-dc34e402fd46}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{724ef170-a42d-4fef-9f26-b60e846fba4f}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{724ef170-a42d-4fef-9f26-b60e846fba4f}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-422220080e43}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-422220080e43}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4d9f7874-4e0c-4904-967b-40b0d20c3e4b}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4d9f7874-4e0c-4904-967b-40b0d20c3e4b}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a77f5d77-2e2b-44c3-a6a2-aba601054a51}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0ac0837c-bbf8-452a-850d-79d08e667ca7}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d0384e7d-bac3-4797-8f14-cba229b392b5}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d0384e7d-bac3-4797-8f14-cba229b392b5}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7b0db17d-9cd2-4a93-9733-46cc89022e7c}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7b0db17d-9cd2-4a93-9733-46cc89022e7c}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ae50c081-ebd2-438a-8655-8a092e34987a}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\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\{b6ebfb86-6907-413c-9af7-4fc2abf07cc5}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b6ebfb86-6907-413c-9af7-4fc2abf07cc5}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9274bd8d-cfd1-41c3-b35e-b13f55a758f4}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9274bd8d-cfd1-41c3-b35e-b13f55a758f4}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{69d2cf90-fc33-4fb7-9a0c-ebb0f0fcb43c}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{69d2cf90-fc33-4fb7-9a0c-ebb0f0fcb43c}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{374de290-123f-4565-9164-39c4925e467b}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{859ead94-2e85-48ad-a71a-0969cb56a6cd}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a305ce99-f527-492b-8b1a-7e76fa98d6e4}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3d644c9b-1fb8-4f30-9b45-f670235f79c0}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a990ae9f-a03b-4e80-94bc-9912d7504104}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{dfd76a2-c82a-4d63-906a-5644ac457385}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{dfd76a2-c82a-4d63-906a-5644ac457385}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1a6fdb2-f42d-4358-a798-b74d745926c5}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1a6fdb2-f42d-4358-a798-b74d745926c5}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a520a1a4-1780-4ff6-bd18-167343c5af16}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b88f4daa-e7bd-49a9-b74d-02885a5dc765}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b88f4daa-e7bd-49a9-b74d-02885a5dc765}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2c36c0aa-5812-4b87-bfd0-4cd0dfb19b39}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2c36c0aa-5812-4b87-bfd0-4cd0dfb19b39}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9e3995ab-1f9c-4f13-b827-48b24b6c7174}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{df7266ac-9274-4867-8d55-3bd661de872d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{df7266ac-9274-4867-8d55-3bd661de872d}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ed4824af-dce4-45a8-81e2-fc7965083634}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{ed4824af-dce4-45a8-81e2-fc7965083634}\propertybag
Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{15ca69b3-30ee-49c1-ace1-6b5ec372afb5}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{15ca69b3-30ee-49c1-ace1-6b5ec372afb5}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3214fab5-9757-4298-bb61-92a9deaa44ff}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3214fab5-9757-4298-bb61-92a9deaa44ff}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fd228cb7-ae11-4ae3-864c-16f3910ab8fe}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b97d20bb-f46a-4c97-ba10-5e3608430854}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b97d20bb-f46a-4c97-ba10-5e3608430854}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{625b53c3-ab48-4ec1-ba1f-a1ef4146fc19}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d20beec4-5ca8-4905-ae3b-bf251ea09b53}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de92c1c7-837f-4f69-a3bb-86e631204a23}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de92c1c7-837f-4f69-a3bb-86e631204a23}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{10c07cd0-ef91-4567-b850-448b77cb37f9}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c1bae2d0-10df-4334-bedd-7aa20b227a9d}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{c1bae2d0-10df-4334-bedd-7aa20b227a9d}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{190337d1-b8ca-4121-a639-6d472d16972a}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{190337d1-b8ca-4121-a639-6d472d16972a}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{54eed2e0-e7ca-4fdb-9148-0f4247291cfa}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{54eed2e0-e7ca-4fdb-9148-0f4247291cfa}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}\propertybag

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-664e-48db-a079-df759e0509f7}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{a63293e8-664e-48db-a079-df759e0509f7}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5ce4a5e9-e4eb-479d-b89f-130c02886155}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a74aeb-aeb4-465c-a014-d097ee346d63}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{43668bf8-c14e-49b2-97c9-747784d784b7}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-9efe-4bda-8fd7-f78dca774f87}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{915221fb-9efe-4bda-8fd7-f78dca774f87}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaa4}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaa4}\propertybag
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{e2c3b244-9797-11e5-a31c-806e6f6e6963}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{e2c3b243-9797-11e5-a31c-806e6f6e6963}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\usersfiles\namespace
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders\{dffacdc5-679f-4156-8947-c5c76bc0b67f}
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\usersfiles\namespace
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\usersfiles\namespace\delegatefolders
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\shellfolder
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\shellfolder
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\shellfolder
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\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\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\shdocvw.dll
Opens key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\treatas
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\progid
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\progid
Opens key: HKCU\software\classes\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}

Opens key: HKCR\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}
Opens key: HKCU\software\classes\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\progid
Opens key: HKCR\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\inprochandler
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprocserver32
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\treatas
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\progid
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\progid
Opens key: HKCU\software\classes\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}
Opens key: HKCR\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}
Opens key: HKCU\software\classes\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\progid
Opens key: HKCR\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprochandler32
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprochandler32
Opens key: HKCU\software\classes\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprochandler
Opens key: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}\inprochandler
Opens key: HKCU\software\classes\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance\initpropertybag
Opens key: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}\instance\initpropertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\objects\{dffacdc5-679f-4156-8947-c5c76bc0b67f}
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\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: 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\policies\microsoft\windows\currentversion\internet settings\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: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol

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

Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

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: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

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

Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

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\policies\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\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610

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\windows\currentversion\internet settings

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\policies\microsoft\internet explorer\main\featurecontrol\feature_allow_reverse_solids_in_userinfo_kb932562

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: HKLM\software\wow6432node\policies\microsoft\internet explorer

Opens key: HKLM\software\policies\microsoft\internet explorer

Opens key: HKLM\software\policies\microsoft\internet explorer\security

Opens key: HKCU\software\policies\microsoft\internet explorer

Opens key: HKCU\software\microsoft\internet explorer\security

[illegible]

settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
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: HKCU\software\microsoft\windows\currentversion\app_paths\protocolpc1.exe
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\protocolpc1.exe
Opens key: HKLM\software\microsoft\windows\currentversion\app_paths\protocolpc1.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\protocolpc1.exe
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\protocolpc1.exe
Opens key:
HKCU\software\classes\appid\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe
Opens key:
HKCR\appid\007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.exe
Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
Opens key: HKLM\system\currentcontrolset\control\lsa\fpisalgorithmpolicy
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-
0000000000046}
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
0000000000046}\proxystubclsid32
Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-
0000000000046}\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: HKLM\software\microsoft\windows\currentversion\installer\managed\5-1-5-
21-2469590586-531574596-741558139-
1004\installer\assemblies\c:\users\admin\appdata\roaming\protocolpc1.exe
Opens key:
HKCU\software\microsoft\installer\assemblies\c:\users\admin\appdata\roaming\protocolpc1.exe
Opens key: HKCR\installer\assemblies\c:\users\admin\appdata\roaming\protocolpc1.exe
Opens key: HKCU\environment
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netsh.exe
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\netsh.exe
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\software\wow6432node\microsoft\netsh
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\0ff928cb-17719a24
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\0ff928cb
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\000000028
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\ipsec\policy\local
Opens key: HKLM\software\policies\microsoft\windows\ipsec\policy\local
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\software\wow6432node\microsoft\bidinterface\loader
Opens key: HKCU\software\odbc\odbc.ini\odbc
Opens key: HKLM\software\wow6432node\odbc\odbc.ini\odbc
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters
Opens key: HKLM\system\currentcontrolset\services\iphlpvc\config
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\policyprovider
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\system
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKLM\software\policies\microsoft\peerdist
Opens key: HKLM\software\policies\microsoft\peerdist\service
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\service
Opens key: HKLM\software\policies\microsoft\peerdist\downloadmanager
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager
Opens key: HKLM\software\policies\microsoft\peerdist\downloadmanager\protocol
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager\protocol
Opens key: HKLM\software\policies\microsoft\peerdist\downloadmanager\download
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager\download
Opens key: HKLM\software\policies\microsoft\peerdist\downloadmanager\discovery
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager\discovery
Opens key: HKLM\software\policies\microsoft\peerdist\downloadmanager\upload
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager\upload
Opens key: HKLM\software\policies\microsoft\peerdist\downloadmanager\utilityindex
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager\utilityindex
Opens key:
HKLM\software\policies\microsoft\peerdist\downloadmanager\peers\connection
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager\peers\connection
Opens key: HKLM\software\policies\microsoft\peerdist\securitymanager
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\securitymanager
Opens key: HKLM\software\policies\microsoft\peerdist\securitymanager\restricted
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\securitymanager\restricted
Opens key: HKLM\software\policies\microsoft\peerdist\cachemgr\republication
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\cachemgr\republication
Opens key: HKLM\software\policies\microsoft\peerdist\cachemgr\publication
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\cachemgr\publication
Opens key: HKLM\software\policies\microsoft\peerdist\handlemgr
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\handlemgr
Opens key: HKLM\software\policies\microsoft\peerdist\hostedcache\connection
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache\connection
Opens key: HKLM\software\policies\microsoft\peerdist\hostedcache
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\hostedcache
Opens key: HKLM\software\policies\microsoft\peerdist\cooperativecaching
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\cooperativecaching
Opens key: HKLM\software\policies\microsoft\peerdist\discoverymanager
Opens key: HKLM\software\microsoft\windows
nt\currentversion\peerdist\discoverymanager
Opens key: HKLM\software\policies\microsoft\peerdist\publisher
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\publisher
Opens key: HKLM\software\policies\microsoft\peerdist\roaming
Opens key: HKLM\software\microsoft\windows nt\currentversion\peerdist\roaming
Opens key: HKLM\system\currentcontrolset\control\cryptography\providers
Opens key: HKLM\system\currentcontrolset\control\cryptography\configuration
Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid
Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32
Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-

```
b913c40c9cd4}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
  Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
  Opens key: HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
  Opens key: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
  Opens key: HKLM\software\wow6432node\microsoft\rpc\securityservice
  Opens key: HKLM\software\microsoft\rpc\securityservice
  Opens key: HKCU\software\microsoft\windows\currentversion\run
  Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\run
  Opens key: HKCU\software\d0b7ff2d863d1a546f17291f4911b563
  Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8
  Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5
  Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57
  Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4
  Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\7566cac\2
  Opens key: HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.data.sqlxml1_b77a5c561934e089
  Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\043d2a44
  Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip
  Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6
  Opens key: HKLM\system\currentcontrolset\control\computername
  Opens key: HKLM\system\currentcontrolset\services\.net clr networking\performance
  Opens key: HKCU\control panel\international
  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\software\microsoft\wow64\wow64executeflags]
  Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  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[alternatetcodepage]
  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\software\wow6432node\microsoft\.netframework[installroot]
  Queries value: HKLM\software\wow6432node\microsoft\.netframework[clrloadlogdir]
  Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
  Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33]
  Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
  Queries value: HKLM\software\wow6432node\microsoft\.netframework[uselegacyv2runtimeactivationpolicydefaultvalue]
  Queries value: HKLM\software\wow6432node\microsoft\.netframework[onlyuselatestclr]
  Queries value: HKLM\software\wow6432node\microsoft\fusion[noclientchecks]
  Queries value: HKLM\software\wow6432node\microsoft\.netframework[gcteststartatjit]
  Queries value: HKLM\software\wow6432node\microsoft\.netframework[gcteststartatjit]
  Queries value: HKLM\software\wow6432node\microsoft\fusion[noclientchecks]
  Queries value: HKLM\software\microsoft\fusion[cacheolocation]
  Queries value: HKLM\software\microsoft\fusion[downloadcachequotainkb]
  Queries value: HKLM\software\microsoft\fusion[enablelog]
  Queries value: HKLM\software\microsoft\fusion[logginglevel]
  Queries value: HKLM\software\microsoft\fusion[forcelog]
  Queries value: HKLM\software\microsoft\fusion[logfailures]
  Queries value: HKLM\software\microsoft\fusion[versioninglog]
  Queries value: HKLM\software\microsoft\fusion[logresourcebinds]
  Queries value: HKLM\software\microsoft\fusion[uselegacyidentityformat]
  Queries value: HKLM\software\microsoft\fusion[disablesipeek]
  Queries value: HKLM\software\microsoft\fusion[noclientchecks]
  Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[devoverrideenable]
  Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapprivate]
  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: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-

0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2469590586-531574596-741558139-1004[profileimagepath]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\indexf8[niusagemask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\indexf8[ilusagemask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[evaluationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\1[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\1[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\1[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\1[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\1[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnsoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnsoptions[mscorlib.ni.dll]
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}[parsingname]
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\microsoft\windows nt\currentversion\image file execution
options\dlloptions[mscorjit.dll]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[index38]
Queries value:
HKLM\software\microsoft\fusion\publisherpolicy\default[legacypolicytimestamp]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions[culture.dll]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[evaluationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\5[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\5[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\5[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\5[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\5[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\6[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\6[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\6[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\6[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\6[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\7[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\7[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\7[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\7[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\7[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.configuration,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[evaluationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\73[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\16[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\16[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\16[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\16[sig]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\c991064\2bd33e1c\16[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6dc7d4c0\5cd4db\1e[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6dc7d4c0\5cd4db\1e[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6dc7d4c0\5cd4db\1e\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6dc7d4c0\5cd4db\1e[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6dc7d4c0\5cd4db\1e[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\3ced59c5\1b2590b1\1a[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\3ced59c5\1b2590b1\1a[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\3ced59c5\1b2590b1\1a\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\3ced59c5\1b2590b1\1a[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\3ced59c5\1b2590b1\1a[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6e8397\46ad0879\1f[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6e8397\46ad0879\1f[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6e8397\46ad0879\1f\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6e8397\46ad0879\1f[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\6e8397\46ad0879\1f[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\2b1a4e4\38a3212c\2a[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\2b1a4e4\38a3212c\2a[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\2b1a4e4\38a3212c\2a\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\2b1a4e4\38a3212c\2a[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\2b1a4e4\38a3212c\2a[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\24bf93f6\455bab30\1b[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\24bf93f6\455bab30\1b[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\24bf93f6\455bab30\1b\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\24bf93f6\455bab30\1b[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\24bf93f6\455bab30\1b[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\4f99a7c9\53bea2b0\73[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\4f99a7c9\53bea2b0\73[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\4f99a7c9\53bea2b0\73\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\4f99a7c9\53bea2b0\73[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\4f99a7c9\53bea2b0\73[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[microsoft.visualbasic,8.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[System.Web,2.0.0.0,,b03f5f7f11d50a3a,x86]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[System.Management,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[System.Runtime.Remoting,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[System.Deployment,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[System.Drawing,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[System.Windows.Forms,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[evaluationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\61e7e666\c991064\13[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\475dce40\2d382ce6\3[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\475dce40\2d382ce6\3[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\475dce40\2d382ce6\3\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\475dce40\2d382ce6\3[sig]


```

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\3[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\1b[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\1b[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\1b\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\1b[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\1b[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\1e[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\1e[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\1e\modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\1e[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\1e[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[evaluationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\d[missingdependencies]
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\Policies\Microsoft\SQMClient\Windows[CeipEnabled]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[System.Runtime.Serialization.Formatters.Soap,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[Accessibility,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[System.Security,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKCU[dll]
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:
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer[EnableShellExecuteHooks]
Queries value:
HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnsoptions[System.NI.dll]
Queries value:
HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnsoptions[Microsoft.VisualBasic.NI.dll]
Queries value:
HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnsoptions[System.Drawing.NI.dll]
Queries value:
HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnsoptions[System.Windows.Forms.NI.dll]
Queries value:
HKLM\software\microsoft\windows\currentversion\Policies\Explorer[NoPropertiesMyComputer]
Queries value:
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer[NoPropertiesMyComputer]
Queries value:
HKLM\software\microsoft\windows\currentversion\Policies\Explorer[NoPropertiesRecycleBin]
Queries value:
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer[NoPropertiesRecycleBin]
Queries value:
HKLM\software\microsoft\windows\currentversion\Policies\Explorer[NoControlPanel]
Queries value:
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer[NoControlPanel]
Queries value:
HKLM\software\microsoft\windows\currentversion\Policies\Explorer[NoSetFolders]
Queries value:
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer[NoSetFolders]
Queries value:
HKLM\software\microsoft\windows\currentversion\Policies\Explorer[NoInternetIcon]
Queries value:
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer[NoInternetIcon]
Queries value:
HKLM\software\microsoft\windows\currentversion\Policies\Explorer[NoCommonGroups]
Queries value:
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer[NoCommonGroups]
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[hideondesktopperuser]
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[pintonamespacetree]
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\drive\shell\folderextensions\{fbcb8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKCU\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: HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
Queries value: 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: 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}[streamresource]
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: HKLM\software\microsoft\com3[com+enabled]
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\microsoft\ole[maxsxshashcount]
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: HKCR\directory[docobject]
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\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]

[illegible]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f3ce0f7c-4901-4acc-8648-d5d44b04ef8f}[initfolderhandler]
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\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}[]
Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[inprocserver32]
Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[threadingmodel]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[streamresource]type
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7d1d3a04-debb-4115-95cf-2f29da2920da}[publishexpandedpath]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```
4e1e-4676-835a-98395c3bc3bb}{stream}
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{33e28130-4e1e-4676-835a-98395c3bc3bb}[initfolderhandler]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my pictures]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[parsingsname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{8ad10c31-2adb-4296-a8f7-e4701232c972}[initfolderhandler]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[parsingsname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{82a5ea35-d9cd-47c5-9629-e15d2f714e6e}[icon]
```


[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

6d19-48d3-be97-42220080e43}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4bd8d571-6d19-48d3-be97-42220080e43}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user_shell
folders[my music]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[parsiname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{de61d971-5ebc-4f02-a3a9-6c82895e5c04}[initfolderhandler]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{0762d272-c50a-4bb0-a382-697dcd729b80}[relativepath]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```
c6a9-404c-b2b2-aee6db6af4968}{initfolderhandler]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user_shell_folders[{bf9d5e0f-c6a9-404c-b2b2-ae6db6af4968}]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[parsingsname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[streamresourcetypetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5cd7aee2-2219-4a67-b85d-6c9ce15660cb}[initfolderhandler]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[parsingsname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b94237e7-57ac-4347-9151-b08c6c32d1f7}[streamresourcetypetype]
```

[illegible]

[illegible]

[illegible]

[illegible]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4}]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{e2c3b244-9797-11e5-a31c-806e6f6e6963}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{e2c3b244-9797-11e5-a31c-806e6f6e6963}[generation]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{e2c3b243-9797-11e5-a31c-806e6f6e6963}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{e2c3b243-9797-11e5-a31c-806e6f6e6963}[generation]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders[suppressionpolicy]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders[]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\usersfiles\namespace\delegatefolders\{dffacd5-679f-4156-8947-c5c76bc0b67f}[suppressionpolicy]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[attributes]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[callforattributes]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[restrictedattributes]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[wantsfordisplay]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[hidefolderverbs]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[usedrophandler]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[wantsforparsing]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[queryforoverlay]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[queryforinfotip]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[hideinwebview]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[hideondesktopperuser]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[nofilefolderjunction]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[pintonamespacetree]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{dffacd5-679f-4156-8947-c5c76bc0b67f}]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\inprocserver32[]
Queries value: HKCR\wow6432node\clsid\{dffacd5-679f-4156-8947-c5c76bc0b67f}\inprocserver32[loadwithoutcom]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value: HKCU\software\microsoft\windows

```
nt\currentversion\appcompatflags\layers[c:\windows\system32\shdocvw.dll]
  Queries value: HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{dffacdc5-679f-4156-8947-c5c76bc0b67f} {add8ba80-002b-11d0-8f0f-00c04fd7d062}
0xffff]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-c5c76bc0b67f}[]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\inprocserver32[threadingmodel]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\instance[clsid]
  Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-
c66de400274e}\inprocserver32[]
  Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-
c66de400274e}\inprocserver32[loadwithoutcom]
  Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-c66de400274e}[]
  Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-
c66de400274e}\inprocserver32[inprocserver32]
  Queries value: HKCR\wow6432node\clsid\{0e5aae11-a475-4c5b-ab00-
c66de400274e}\inprocserver32[threadingmodel]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\instance\initpropertybag[attributes]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\instance\initpropertybag[descriptionid]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\instance\initpropertybag[helptopic]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\instance\initpropertybag[recursivesearch]
  Queries value: HKCR\wow6432node\clsid\{dffacdc5-679f-4156-8947-
c5c76bc0b67f}\instance\initpropertybag[targetknownfolder]
  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\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_hk1m_only]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33 .exe]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
  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\wow6432node\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: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33 .exe]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
  Queries value: HKCU\software\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value: HKLM\software\wow6432node\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[007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33 .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[007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33 .exe]
  Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  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: HKCU\software\microsoft\windows\currentversion\explorer\user_shell
folders[cookies]
Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[007c1a629ce11b8476753cc9195c1924894fb8100f2faae4e0e41de8c024bc33.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: HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
Queries value: HKCU\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
nt\currentversion\appcompatflags\layers[c:\users\admin\appdata\roaming\protocolpc1.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[protocolpc1]
Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
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\session
manager[safeprocesssearchmode]
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: HKCU\environment[see_mask_nozonechecks]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\windows\system32\netsh.exe]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32\netsh]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5a24fdb-1cf3-477b-
b422-ef4909d51223]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5855625e-4bd7-4b85-
b3a7-9307bab0b813]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[namespaces_callout]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:

[illegible]

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[storeserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value: HKLM\system\setup[upgrade]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[bc0a73a6-043e-432f-bded-3d18c2dbe320]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5f31090b-d990-4e91-b16d-46121d0255aa]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5b23f342-8421-42ef-87eb-3b686f5a1b2a]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[253f4cd1-9475-4642-88e0-6790d7a86cde]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[7076bf7a-db99-4a63-8afe-0bb2ab92997a]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[ab0d8ef9-866d-4d39-b83f-453f3b8f6325]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[94335eb3-79ea-44d5-8ea9-306f49b3a041]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[935f4ae6-845d-41c6-97fa-380dad429b72]
Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[94335eb3-79ea-44d5-8ea9-306f49b3a070]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e4ff10d8-8a88-4fc6-82c8-8c23e9462fe5]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion[currentbuildnumber]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters[disabledcomponents]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[c558cd2b-a861-454c-bb0b-3042ad795dff]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[28fcab19-3975-45cd-9e8c-5be612d60007]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[1f8b121d-45b3-4022-a9fb-3857177a65c1]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[28c9f48f-d244-45a8-842f-dc9fbc9b6e94]
Queries value:
HKLM\system\currentcontrolset\services\iphlpvc\config[connectivity_platform_enabled]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\policies\microsoft\windows\system\gpsvcdebuglevel]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\service[enable]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\service[policyrefreshinprogress]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager[transportdllpath]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\downloadmanager[cryptoalgo]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\securitymanager[blocksize]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\securitymanager[numblockspersegment]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\securitymanager\restricted[seed]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache[serverrole]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache[clientauth]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache[transportdllpath]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache[maxsimultaneousdownloads]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache[maxsimultaneousuploads]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache[maxpendingoffers]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache[maxpendingdownloads]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\hostedcache[donotusessl]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\discoverymanager[repubquorumsize]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\discoverymanager[minbackoffwindow]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\discoverymanager[discoveryproviderdllpath]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\roaming[forceroamingdetect]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\roaming[refreshdllname]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\peerdist\roaming[refreshprocname]
Queries value: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid[]
Queries value: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
Queries value: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]

Queries value: HKCU\software\microsoft\windows\currentversion\run[d0b7ff2d863d1a546f17291f4911b563]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\run[d0b7ff2d863d1a546f17291f4911b563]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user_shell_folders[startup]

Queries value: HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]

Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksizesize]

Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[displayname]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[configmask]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[configstring]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[mvid]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[evaluationdata]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[status]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[ildependencies]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[nidependencies]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\5[missingdependencies]

Queries value: HKLM\software\wow6432node\microsoft\framework[dbgjitdebuglaunchsetting]

Queries value: HKLM\software\wow6432node\microsoft\framework[dbgmanageddebugger]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[displayname]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[configmask]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[configstring]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[mvid]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[evaluationdata]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[status]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[ildependencies]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[nidependencies]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\4[missingdependencies]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\7566cac\2[displayname]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\7566cac\2[status]

Queries value: HKCU\software\microsoft\windows\currentversion\run[d0b7ff2d863d1a546f17291f4911b563]

Queries value: HKLM\software\microsoft\windows\currentversion\run[d0b7ff2d863d1a546f17291f4911b563]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\7566cac\2[modules]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\7566cac\2[sig]

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\7566cac\2[lastmodtime]

Queries value: HKLM\software\microsoft\fusion\gacchangenotification\default[system.data.sqlxml,2.0.0.0,b77a5c561934e089,msil]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloxoptions[system.configuration.ni.dll]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloxoptions[system.xml.ni.dll]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion[installationtype]

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\.net_clr networking\performance[library]

Queries value: HKLM\system\currentcontrolset\services\.net_clr
networking\performance[ismultiinstance]
Queries value: HKLM\system\currentcontrolset\services\.net_clr
networking\performance[first_counter]
Queries value: HKLM\system\currentcontrolset\services\.net_clr
networking\performance[categoryoptions]
Queries value: HKLM\system\currentcontrolset\services\.net_clr
networking\performance[filemappingsize]
Queries value: HKLM\system\currentcontrolset\services\.net_clr
networking\performance[counter_names]
Queries value: HKCU\control_panel\international[syearmonth]
Queries value: HKCU\software\d0b7ff2d863d1a546f17291f4911b563[[kl]]
Sets/Creates value: HKCU\[di]
Sets/Creates value: HKCU\environment[see_mask_nozonechecks]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[d0b7ff2d863d1a546f17291f4911b563]
Sets/Creates value:
HKLM\software\wow6432node\microsoft\windows\currentversion\run[d0b7ff2d863d1a546f17291f4911b563]
Sets/Creates value: HKCU\software\d0b7ff2d863d1a546f17291f4911b563[[kl]]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasinet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Value changes: HKCU\[di]
Value changes:
HKCU\software\microsoft\windows\currentversion\run[d0b7ff2d863d1a546f17291f4911b563]
Value changes:
HKLM\software\wow6432node\microsoft\windows\currentversion\run[d0b7ff2d863d1a546f17291f4911b563]
Value changes: HKCU\software\d0b7ff2d863d1a546f17291f4911b563[[kl]]