Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	751
Risk Level:	10
Date Processed:	2016-05-18 10:33:56 (UTC)
Processing Time:	62.2 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe"
Sample ID:	3311
Type:	basic
Owner:	admin
Label:	2a29e3a5d469fbc803a504464393f98e
Date Added:	2016-05-18 10:30:49 (UTC)
File Type:	PE32:win32:gui
File Size:	1127085 bytes
MD5:	2a29e3a5d469fbc803a504464393f98e
SHA256:	c16b99b6dd2073d18c21dc2a0a24ba4b99355ab89405e9abf1d902d7f841f5cd
Description:	None

Pattern Matching Results

`10` Creates malicious mutex: DarkComet [APT, RAT]
`7` Writes to memory of system processes
`7` YARA score 7
`5` Possible injector
`4` Connects to local IP
`7` Injects thread into Windows process

Static Events

YARA rule hit:	KeyLoggerStrings
Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe
["C:\windows\temp\2a29e3a5d469fbc803a504464393f98e.exe"]	
Creates process:	C:\Windows\SysWOW64\notepad.exe [notepad]
Writes to process:	PID:2912 C:\Windows\SysWOW64\notepad.exe
Creates remote thread:	C:\Windows\SysWOW64\notepad.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\DC_MUTEX-F5B0MXB
Creates mutex:	\Sessions\1\BaseNamedObjects\DCPERSFWBP

File System Events

Creates:	C:\Users\Admin\AppData\Roaming\dclogs
Creates:	C:\Users\Admin\AppData\Roaming\dclogs\2016-05-18-4.dc
Opens:	C:\Windows\Prefetch\2A29E3A5D469FBC803A504464393F-7BFA99C0.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\2a29e3a5d469fbc803a504464393f98e.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\wsock32.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\Windows\SysWOW64\netapi32.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_ba245425e0986353
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_ba245425e0986353\GdiPlus.dll
Opens:	C:\Windows\SysWOW64\msacm32.dll
Opens:	C:\Windows\SysWOW64\shfolder.dll
Opens:	C:\Windows\SysWOW64\avicap32.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\winmmbase.dll
Opens:	C:\Windows\SysWOW64\netutils.dll
Opens:	C:\Windows\SysWOW64\srvcli.dll

```
Opens:                    C:\Windows\SysWOW64\wkscli.dll
Opens:                    C:\Windows\SysWOW64\msvfw32.dll
Opens:                    C:\Windows\SysWOW64\msvcrt.dll
Opens:                    C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:                    C:\Windows\SysWOW64\cryptbase.dll
Opens:                    C:\Windows\SysWOW64\sspicli.dll
Opens:                    C:\Windows\SysWOW64\rpcrt4.dll
Opens:                    C:\Windows\SysWOW64\combase.dll
Opens:                    C:\Windows\SysWOW64\oleaut32.dll
Opens:                    C:\Windows\SysWOW64\advapi32.dll
Opens:                    C:\Windows\SysWOW64\gdi32.dll
Opens:                    C:\Windows\SysWOW64\user32.dll
Opens:                    C:\Windows\SysWOW64\nsi.dll
Opens:                    C:\Windows\SysWOW64\ws2_32.dll
Opens:                    C:\Windows\SysWOW64\ole32.dll
Opens:                    C:\Windows\SysWOW64\shlwapi.dll
Opens:                    C:\Windows\SysWOW64\shell32.dll
Opens:                    C:\Windows\SysWOW64\iertutil.dll
Opens:                    C:\Windows\SysWOW64\wininet.dll
Opens:                    C:\Windows\SysWOW64\urlmon.dll
Opens:                    C:\Windows\SysWOW64\imm32.dll
Opens:                    C:\Windows\SysWOW64\msctf.dll
Opens:                    C:\Windows\SysWOW64\en-US\msvfw32.dll.mui
Opens:                    C:\Windows\SysWOW64\en-US\avicap32.dll.mui
Opens:                    C:\Windows\SysWOW64\uxtheme.dll
Opens:                    C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:                    C:\Windows\SysWOW64\dwmapi.dll
Opens:                    C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens:                    C:\
Opens:                    C:\Windows\SysWOW64\SHCore.dll
Opens:                    C:\Windows\SysWOW64\notepad.exe
Opens:                    C:\Windows\Prefetch\NOTEPAD.EXE-1605FA5B.pf
Opens:                    C:\Windows\SysWOW64\clbcatq.dll
Opens:                    C:\Windows\SysWOW64\propsys.dll
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db
Opens:                    C:\Users\desktop.ini
Opens:                    C:\Windows\SysWOW64\cfgmgr32.dll
Opens:                    C:\Windows\SysWOW64\devobj.dll
Opens:                    C:\Windows\SysWOW64\setupapi.dll
Opens:                    C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens:                    C:\Users
Opens:                    C:\Users\Admin
Opens:                    C:\Users\Admin\AppData
Opens:                    C:\Users\Admin\Desktop\desktop.ini
Opens:                    C:\Windows\SysWOW64\winspool.drv
Opens:                    C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens:                    C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
Opens:                    C:\Windows\SysWOW64\comdlg32.dll
Opens:                    C:\Windows\SysWOW64\en-US\notepad.exe.mui
Opens:                    C:\Windows\SysWOW64\mswsock.dll
Opens:                    C:\Windows\WindowsShell.Manifest
Opens:                    C:\Windows\Fonts\StaticCache.dat
Opens:                    C:\Windows\SysWOW64\uxtheme.dll.Config
Opens:                    C:\Windows\Fonts\consola.ttf
Writes to:                C:\Users\Admin\AppData\Roaming\dclogs\2016-05-18-4.dc
Reads from:               C:\Windows\SysWOW64\notepad.exe
Reads from:               C:\Users\desktop.ini
Reads from:               C:\Users\Admin\Desktop\desktop.ini
Reads from:               C:\Windows\Fonts\StaticCache.dat
```

Network Events

```
Connects to:              192.168.0.149:100
```

Windows Registry Events

```
Creates key:              HKCU\software
Creates key:              HKCU\software\dc3_fexec
Opens key:                HKLM\software\microsoft\wow64
Opens key:                HKLM\system\currentcontrolset\control\terminal server
Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
Opens key:                HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:                HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:                HKLM\system\currentcontrolset\control\nls\language
Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key:                HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
```

```
Opens key:                HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key:                HKLM\software\policies\microsoft\mui\settings
Opens key:                HKCU\
Opens key:                HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:                HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key:                HKCU\software\policies\microsoft\control panel\desktop
Opens key:                HKCU\control panel\desktop\languageconfiguration
Opens key:                HKCU\control panel\desktop
Opens key:                HKCU\control panel\desktop\muicached
Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key:                HKLM\system\currentcontrolset\control\session manager
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
Opens key:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key:                HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key:                HKLM\
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
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\oleaut
Opens key:                HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
Opens key:                HKLM\system\currentcontrolset\control\cmf\config
Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\vfw
Opens key:                HKCU\software\borland\locales
Opens key:                HKLM\software\wow6432node\borland\locales
Opens key:                HKCU\software\borland\delphi\locales
Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
Opens key:                HKLM\software\microsoft\sqmclient\windows
Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
Opens key:                HKLM\hardware\devicemap\video
Opens key:                HKLM\system\currentcontrolset\control\video\{bf735b18-1b5a-4e14-b64c-
f2223c917d28}\0000
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
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\086496d7
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
    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\software\wow6432node\microsoft\rpc
    Opens key:                   HKLM\system\currentcontrolset\control\computername\activecomputername
    Opens key:                   HKLM\system\setup
    Opens key:                   HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
    Opens key:                   HKLM\software\policies\microsoft\windows nt\rpc
    Opens key:                   HKLM\system\currentcontrolset\control\idconfigdb
    Opens key:                   HKLM\system\currentcontrolset\control\idconfigdb\hardware profiles\0001
    Opens key:                   HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}\propertybag
    Opens key:                   HKLM\software\wow6432node\microsoft\windows\currentversion
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
    Opens key:                   HKCU\software\dc3_fexec
    Opens key:                   HKCU\software\dc2_users
    Opens key:                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\notepad.exe
    Opens key:                   HKLM\system\currentcontrolset\control\session manager\appcertdlls
    Opens key:                   HKLM\system\currentcontrolset\control\session manager\appcompatibility
    Opens key:                   HKLM\software\wow6432node\policies\microsoft\windows\appcompat
    Opens key:                   HKLM\software\policies\microsoft\windows\appcompat
    Opens key:                   HKCU\software\microsoft\windows nt\currentversion
    Opens key:                   HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
    Opens key:                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
    Opens key:                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\notepad.exe
    Opens key:                   HKCU\software\microsoft\windows\currentversion\explorer\shell folders
    Opens key:                   HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
    Opens key:                   HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\notepad.exe
    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\software\wow6432node\microsoft\windows\currentversion\policies\explorer
    Opens key:                   HKLM\software\microsoft\windows\currentversion\policies\explorer
    Opens key:                   HKCU\software\microsoft\windows\currentversion\policies\explorer
    Opens key:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\2a29e3a5d469fbc803a504464393f98e.exe
   Opens key:              HKCU\software\classes\
   Opens key:              HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
   Opens key:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder
   Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-
a2d8-08002b30309d}\shellfolder
   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:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}\
   Opens key:              HKCU\software\classes\drive\shellex\folderextensions
   Opens key:              HKCR\drive\shellex\folderextensions
   Opens key:              HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
   Opens key:              HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
   Opens key:              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:              HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32
   Opens key:              HKLM\software\microsoft\com3
   Opens key:              HKLM\software\microsoft\windowsruntime\clsid
   Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
   Opens key:              HKCR\activatableclasses\clsid
   Opens key:              HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
   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}\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:              HKCU\software\microsoft\windows\currentversion\explorer\
   Opens key:              HKLM\software\wow6432node\microsoft\windows\currentversion\setup
   Opens key:              HKLM\software\microsoft\windows\currentversion\setup
   Opens key:              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}
   Opens key:              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\properties
   Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\advanced
   Opens key:              HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32
   Opens key:              HKCU\software\classes\directory
   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\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}\
   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\{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\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\rpc\extensions
   Opens key:              HKLM\software\microsoft\rpc\extensions
   Opens key:              HKLM\system\currentcontrolset\services\winsock\parameters
   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:              HKCU\software\microsoft\notepad
   Opens key:              HKLM\software\wow6432node\microsoft\notepad\defaultfonts
   Opens key:              HKLM\software\microsoft\notepad\defaultfonts
   Opens key:              HKLM\system\currentcontrolset\control\nls\locale
   Opens key:              HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
   Opens key:              HKLM\system\currentcontrolset\control\nls\language groups
   Opens key:              HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
   Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
   Queries value:          HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
   Queries value:          HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
   Queries value:          HKCU\control panel\desktop[preferreduilanguages]
   Queries value:          HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
   Queries value:          HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Queries value:          HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
   Queries value:          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
   Queries value:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[2a29e3a5d469fbc803a504464393f98e.exe]
   Queries value:          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
   Queries value:          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
   Queries value:          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Queries value:          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:          HKLM\software\microsoft\ole[aggressivemtatesting]
   Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[2a29e3a5d469fbc803a504464393f98e]
   Queries value:          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
   Queries value:
```

```
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
   Queries value:           HKLM\system\currentcontrolset\control\cmf\config[system]
   Queries value:           HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
   Queries value:           HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Queries value:           HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:           HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:           HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
   Queries value:           HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
   Queries value:           HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
   Queries value:           HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
   Queries value:           HKLM\hardware\devicemap\video[maxobjectnumber]
   Queries value:           HKLM\hardware\devicemap\video[\device\video0]
   Queries value:           HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-
08002be10318}\0000[pruningmode]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
   Queries value:
HKLM\system\wm\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
   Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
   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\software\microsoft\rpc[maxrpcsize]
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Queries value:          HKLM\system\setup[oobeinprogress]
   Queries value:          HKLM\system\setup[systemsetupinprogress]
   Queries value:          HKLM\software\microsoft\rpc[idletimerwindow]
```

```
    Queries value:                 HKLM\system\currentcontrolset\control\idconfigdb[currentconfig]
    Queries value:
HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo[dockingstate]
    Queries value:                 HKLM\system\currentcontrolset\control\idconfigdb\hardware
profiles\0001[hwprofileguid]
    Queries value:                 HKLM\system\currentcontrolset\control\idconfigdb\hardware
profiles\0001[friendlyname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
```

a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
    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\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
    Queries value:            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[foldervalueflags]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
    Queries value:            HKCU\software\dc3_fexec[{97e1de52-d6fa-11e1-be62-806e6f6e6963-
1783083262}]
    Queries value:            HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[data]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[generation]
    Queries value:            HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
    Queries value:            HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32[]
    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\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
    Queries value:            HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Queries value:
```

```
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   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:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
   Queries value:              HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
   Queries value:              HKCR\directory[docobject]
   Queries value:              HKCR\folder[docobject]
   Queries value:              HKCR\allfilesystemobjects[docobject]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[data]
   Queries value:              HKCR\directory[browseinplace]
   Queries value:              HKCR\folder[browseinplace]
   Queries value:              HKCR\allfilesystemobjects[browseinplace]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[generation]
   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\{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}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[icon]
```

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[desktop]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[stream]

    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]
    Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
    Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[notepad]
    Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    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: HKCU\software\microsoft\notepad[lfescapement]
    Queries value: HKCU\software\microsoft\notepad[lforientation]
    Queries value: HKCU\software\microsoft\notepad[lfweight]
    Queries value: HKCU\software\microsoft\notepad[lfitalic]
    Queries value: HKCU\software\microsoft\notepad[lfunderline]
    Queries value: HKCU\software\microsoft\notepad[lfstrikeout]
    Queries value: HKCU\software\microsoft\notepad[lfcharset]
    Queries value: HKCU\software\microsoft\notepad[lfoutprecision]
    Queries value: HKCU\software\microsoft\notepad[lfclipprecision]
    Queries value: HKCU\software\microsoft\notepad[lfquality]
    Queries value: HKCU\software\microsoft\notepad[lfpitchandfamily]
    Queries value: HKLM\software\microsoft\notepad\defaultfonts[lffacename]
    Queries value: HKLM\software\microsoft\notepad\defaultfonts[ipointsize]
    Queries value: HKCU\software\microsoft\notepad[lffacename]
    Queries value: HKCU\software\microsoft\notepad[ipointsize]
    Queries value: HKCU\software\microsoft\notepad[fwrap]
    Queries value: HKCU\software\microsoft\notepad[statusbar]
    Queries value: HKCU\software\microsoft\notepad[fsavewindowpositions]
    Queries value: HKCU\software\microsoft\notepad[szheader]
    Queries value: HKCU\software\microsoft\notepad[sztrailer]
    Queries value: HKCU\software\microsoft\notepad[imargintop]
    Queries value: HKCU\software\microsoft\notepad[imarginbottom]
    Queries value: HKCU\software\microsoft\notepad[imarginleft]
    Queries value: HKCU\software\microsoft\notepad[imarginright]
    Queries value: HKCU\software\microsoft\notepad[iwindowposy]
    Queries value: HKCU\software\microsoft\notepad[iwindowposx]
    Queries value: HKCU\software\microsoft\notepad[iwindowposdx]
    Queries value: HKCU\software\microsoft\notepad[iwindowposdy]
    Queries value: HKCU\software\microsoft\notepad[fmle_is_broken]
    Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
    Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
    Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]