# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 624, Task ID: 2441

| | |
|---|---|
| Task ID: | 2441 |
| Risk Level: | 7 |
| Date Processed: | 2016-02-22 05:30:57 (UTC) |
| Processing Time: | 61.96 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe" |

| | |
|---|---|
| Sample ID: | 624 |
| Type: | basic |
| Owner: | admin |
| Label: | 2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d |
| Date Added: | 2016-02-22 05:26:49 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 506404 bytes |
| MD5: | 6c6ee4868e04ff41ebe0c6312de19368 |
| SHA256: | 2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d |
| Description: | None |

## Pattern Matching Results

| | |
|---|---|
| 7 | Writes to memory of system processes |
| 4 | Reads process memory |
| 5 | Abnormal sleep detected |
| 4 | Register or unregister a DLL from command line |
| 6 | Modifies registry autorun entries |
| 2 | PE: Nonstandard section |
| 6 | Tries to detect VM environment |
| 5 | Adds autostart object |
| 4 | Checks whether debugger is present |
| 4 | Terminates process under Windows subfolder |
| 5 | PE: Contains compressed section |

## Static Events

| | |
|---|---|
| Anomaly: | PE: Contains one or more non-standard sections |

## Process/Thread Events

| | |
|---|---|
| Creates process: | C:\windows\temp\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe ["C:\windows\temp\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe" ] |
| Creates process: | C:\Windows\SysWOW64\regsvr32.exe [regsvr32.exe] |
| Creates process: | C:\Windows\SysWOW64\regsvr32.exe ["C:\Windows\SysWOW64\regsvr32.exe"] |
| Reads from process: | PID:2152 C:\Windows\SysWOW64\regsvr32.exe |
| Reads from process: | PID:3064 C:\Windows\SysWOW64\regsvr32.exe |
| Reads from process: | PID:2272 C:\Windows\SysWOW64\regsvr32.exe |
| Reads from process: | PID:2008 C:\Windows\System32\taskhostex.exe |
| Reads from process: | PID:1080 C:\Windows\explorer.exe |
| Reads from process: | PID:1272 C:\Windows\System32\dllhost.exe |
| Reads from process: | PID:2340 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe |
| Reads from process: | PID:2616 C:\Windows\System32\conhost.exe |
| Reads from process: | PID:1296 C:\Windows\System32\mshta.exe |
| Reads from process: | PID:2996 C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| Reads from process: | PID:3032 C:\Windows\System32\conhost.exe |
| Writes to process: | PID:2152 C:\Windows\SysWOW64\regsvr32.exe |
| Writes to process: | PID:3064 C:\Windows\SysWOW64\regsvr32.exe |
| Writes to process: | PID:2272 C:\Windows\SysWOW64\regsvr32.exe |
| Terminates process: | C:\Windows\Temp\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe |
| Terminates process: | C:\Windows\SysWOW64\regsvr32.exe |

## Named Object Events

| | |
|---|---|
| Creates mutex: | \Sessions\1\BaseNamedObjects\DBWinMutex |
| Creates mutex: | \BaseNamedObjects\8D4974EE93029E3A |
| Creates mutex: | \Sessions\1\BaseNamedObjects\705F1AE2597CEF07 |
| Creates mutex: | \Sessions\1\BaseNamedObjects\91EA448AF6528EAD |
| Creates event: | \Sessions\1\BaseNamedObjects\C1A6472D10724C7FF5F9381DA85D8A4F |

## File System Events

| | |
|---|---|
| Opens: | C:\Windows\Prefetch\2B8AD717E0F5509CFAFBA2D0B0D83-22CFBA5B.pf |
| Opens: | C:\Windows |
| Opens: | C:\Windows\System32\wow64.dll |
| Opens: | C:\Windows\SysWOW64 |
| Opens: | C:\Windows\SysWOW64\apphelp.dll |
| Opens: | C:\Windows\Temp\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.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\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\combase.dll
  Opens:                        C:\Windows\SysWOW64\sechost.dll
  Opens:                        C:\Windows\SysWOW64\SHCore.dll
  Opens:                        C:\Windows\SysWOW64\gdi32.dll
  Opens:                        C:\Windows\SysWOW64\user32.dll
  Opens:                        C:\Windows\SysWOW64\msvcrt.dll
  Opens:                        C:\Windows\SysWOW64\shlwapi.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\advapi32.dll
  Opens:                        C:\Windows\SysWOW64\shell32.dll
  Opens:                        C:\Windows\SysWOW64\comdlg32.dll
  Opens:                        C:\Windows\SysWOW64\imm32.dll
  Opens:                        C:\Windows\SysWOW64\msctf.dll
  Opens:                        C:\Windows\SysWOW64\uxtheme.dll
  Opens:                        C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                        C:\Windows\SysWOW64\dwmapi.dll
  Opens:                        C:\Windows\System32\C_1256.NLS
  Opens:                        C:\Windows\System32\C_1251.NLS
  Opens:                        C:\Windows\System32\C_950.NLS
  Opens:                        C:\Windows\System32\C_1250.NLS
  Opens:                        C:\Windows\System32\C_1253.NLS
  Opens:                        C:\Windows\System32\C_932.NLS
  Opens:                        C:\Windows\System32\C_949.NLS
  Opens:                        C:\Windows\System32\C_874.NLS
  Opens:                        C:\Windows\System32\C_1254.NLS
  Opens:                        C:\Windows\System32\C_1257.NLS
  Opens:                        C:\Windows\System32\C_1258.NLS
  Opens:                        C:\Windows\System32\C_936.NLS
  Opens:                        C:\Windows\SysWOW64\oleaut32.dll
  Opens:                        C:\Windows\SysWOW64\ole32.dll
  Opens:                        C:\Windows\SysWOW64\iertutil.dll
  Opens:                        C:\Windows\SysWOW64\wininet.dll
  Opens:                        C:\Windows\SysWOW64\wsock32.dll
  Opens:                        C:\Windows\SysWOW64\nsi.dll
  Opens:                        C:\Windows\SysWOW64\ws2_32.dll
  Opens:                        C:\Windows\SysWOW64\winmm.dll
  Opens:                        C:\Windows\SysWOW64\winmmbase.dll
  Opens:                        C:\Windows\SysWOW64\atl.dll
  Opens:                        C:\Windows\SysWOW64\wtsapi32.dll
  Opens:                        C:\Windows\SysWOW64\psapi.dll
  Opens:                        C:\Windows\SysWOW64\urlmon.dll
  Opens:                        C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
  Opens:                        C:\Windows\SysWOW64\mshta.exe
  Opens:                        C:\Windows\SysWOW64\clbcatq.dll
  Opens:                        C:\Windows\SysWOW64\wbem\wbemprox.dll
  Opens:                        C:\Windows\SysWOW64\wbemcomn.dll
  Opens:                        C:\Windows\SysWOW64\cryptsp.dll
  Opens:                        C:\Windows\SysWOW64\rsaenh.dll
  Opens:                        C:\Windows\SysWOW64\wbem\wbemsvc.dll
  Opens:                        C:\Windows\SysWOW64\wbem\fastprox.dll
  Opens:                        C:\Windows\SysWOW64\regsvr32.exe
  Opens:                        C:\Windows\apppatch\apppatch64\sysmain.sdb
  Opens:                        C:\
  Opens:                        C:\Windows\Prefetch\REGSVR32.EXE-D5170E12.pf
  Opens:                        C:\Windows\apppatch\AcLayers.dll
  Opens:                        C:\Windows\SysWOW64\mpr.dll
  Opens:                        C:\Windows\SysWOW64\sfc.dll
  Opens:                        C:\Windows\SysWOW64\winspool.drv
  Opens:                        C:\Windows\SysWOW64\sfc_os.dll
  Opens:                        C:\Windows\SysWOW64\cfgmgr32.dll
  Opens:                        C:\Windows\SysWOW64\devobj.dll
  Opens:                        C:\Windows\SysWOW64\setupapi.dll
  Opens:                        C:\Windows\SysWOW64\en-US\regsvr32.exe.mui
  Opens:                        C:\Windows\SysWOW64\en-US\setupapi.dll.mui
  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\WindowsShell.Manifest
  Opens:                        C:\WINDOWS\SysWOW64\drivers\VBoxMouse.sys
  Opens:                        C:\Windows\SysWOW64\mswsock.dll
  Opens:                 C:\Windows\SysWOW64\profapi.dll
  Reads from:            C:\Windows\SysWOW64\regsvr32.exe
  Reads from:
C:\Windows\Temp\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe
  Deletes:
C:\Windows\Temp\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe
```

# Network Events

```
  Connects to:           31.166.62.60:80
  Connects to:           129.167.94.233:80
  Connects to:           154.158.141.154:80
  Connects to:           241.254.164.46:80
  Connects to:           186.255.76.229:80
  Connects to:           254.118.40.142:80
  Connects to:           169.33.53.165:80
  Connects to:           158.32.182.151:80
  Connects to:           71.168.140.148:80
  Connects to:           162.15.172.142:80
  Connects to:           2.29.149.149:80
```

# Windows Registry Events

```
  Creates key:           HKLM\software\wow6432node\076d08883c3fd02b
  Creates key:           HKLM\software\wow6432node\5sacgv8hb0
  Creates key:           HKLM\software\wow6432node\microsoft\wbem\cimom
  Creates key:           HKCU\software\microsoft\internet explorer\main\featurecontrol
  Creates key:           HKCU\software\microsoft\internet explorer\international
  Creates key:           HKCU\software\d514d55fab
  Creates key:           HKLM\software\wow6432node\d514d55fab
  Creates key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer\run
  Creates key:           HKLM\software\microsoft\windows\currentversion\policies\explorer\run
  Deletes value:         HKLM\software\wow6432node\076d08883c3fd02b[4313902a5ea0ce0c1123]
  Deletes value:         HKLM\software\wow6432node\5sacgv8hb0[5cd3fsxgz8]
  Deletes value:         HKLM\software\wow6432node\5sacgv8hb0[xulz75]
  Opens key:             HKLM\software\microsoft\wow64
  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\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\
  Opens key:             HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  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\software\wow6432node\microsoft\ole
  Opens key:             HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}\propertybag
  Opens key:                HKCU\software\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\explorer\knownfoldersettings
  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\wow6432node\microsoft\oleaut
  Opens key:                HKCU\software\borland\locales
  Opens key:                HKCU\software\borland\delphi\locales
  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\31632ce2
  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\microsoft\windows nt\currentversion
  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\
  Opens key:                 HKLM\software\wow6432node\076d08883c3fd02b\
  Opens key:                 HKLM\software\wow6432node\076d08883c3fd02b
  Opens key:                 HKLM\software\wow6432node\5sacgv8hb0
  Opens key:                 HKLM\software\wow6432node\5sacgv8hb0\
  Opens key:                 HKLM\software\wow6432node\microsoft\rpc
  Opens key:                 HKLM\software\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:                 HKCU\software\classes\
  Opens key:
HKCU\software\classes\appid\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe
  Opens key:
HKCR\appid\2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe
  Opens key:                 HKLM\software\microsoft\com3
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}
  Opens key:                 HKCR\activatableclasses\clsid
  Opens key:                 HKCR\activatableclasses\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}
  Opens key:                 HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler
  Opens key:                 HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\system\dnsclient
  Opens key:                 HKLM\software\policies\microsoft\system\dnsclient
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}
  Opens key:                 HKCR\activatableclasses\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}
  Opens key:                 HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler
  Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
  Opens key:                 HKLM\software\policies\microsoft\cryptography
  Opens key:                 HKLM\software\microsoft\cryptography
  Opens key:                 HKLM\software\wow6432node\microsoft\cryptography\offload
  Opens key:                 HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKLM\software\wow6432node\microsoft\rpc\extensions
  Opens key:                 HKLM\software\microsoft\rpc\extensions
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\activatableclasses\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                  HKCR\wow6432node\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                  HKCR\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\activatableclasses\clsid
  Opens key:                  HKCU\software\classes\activatableclasses\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                  HKLM\software\microsoft\windowsruntime\clsid\{00000339-0000-0000-c000-
000000000046}
  Opens key:                  HKCR\activatableclasses\clsid\{00000339-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{00000339-0000-0000-c000-
000000000046}
  Opens key:                  HKCR\wow6432node\clsid\{00000339-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\clsid\{00000339-0000-0000-c000-000000000046}
  Opens key:                  HKCR\clsid\{00000339-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\activatableclasses\clsid\{00000339-0000-0000-c000-
000000000046}
  Opens key:                  HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}
  Opens key:                  HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
  Opens key:                  HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
  Opens key:                  HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
  Opens key:                  HKLM\software\microsoft\windowsruntime\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}
  Opens key:                  HKCR\activatableclasses\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\treatas
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler32
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler
  Opens key:                  HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}
  Opens key:                  HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
  Opens key:                  HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32
  Opens key:                  HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32
  Opens key:                  HKLM\software\microsoft\windowsruntime\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}
  Opens key:                  HKCR\activatableclasses\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\treatas
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler32
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler
  Opens key:                  HKLM\software\wow6432node\microsoft\wbem\cimom
  Opens key:                  HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}
  Opens key:                  HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
  Opens key:                  HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32
  Opens key:                  HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32
  Opens key:                  HKLM\software\microsoft\windowsruntime\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}
```

```
  Opens key:                 HKCR\activatableclasses\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}
  Opens key:                 HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}
  Opens key:                 HKCR\activatableclasses\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}
  Opens key:                 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprochandler
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}
  Opens key:                 HKCR\activatableclasses\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}
  Opens key:                 HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprochandler
  Opens key:                 HKCU\software\classes\wow6432node\interface\{44aca675-e8fc-11d0-a07c-
00c04fb68820}
  Opens key:                 HKCR\wow6432node\interface\{44aca675-e8fc-11d0-a07c-00c04fb68820}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{44aca675-e8fc-11d0-a07c-
00c04fb68820}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{44aca675-e8fc-11d0-a07c-
00c04fb68820}\proxystubclsid32
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\regsvr32.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\regsvr32.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\regsvr32.exe
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:             HKLM\system\currentcontrolset\control\cmf\config
  Opens key:             HKLM\system\currentcontrolset\control\networkprovider\hworder
  Opens key:             HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:             HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:             HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\21b9e6fd
  Opens key:             HKLM\software\wow6432node\d514d55fab\
  Opens key:             HKCU\software\d514d55fab\
  Opens key:             HKU\
  Opens key:             HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:             HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:             HKCU\software\
  Opens key:             HKLM\system\currentcontrolset\control\computername
  Opens key:             HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\wireshark.exe
  Opens key:             HKLM\software\microsoft\windows\currentversion\app paths\wireshark.exe
  Opens key:             HKCU\software\microsoft\windows\currentversion\app paths\wireshark.exe
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wireshark
  Opens key:             HKCU\software\microsoft\windows\currentversion\uninstall\wireshark
  Opens key:             HKLM\software\wow6432node\wireshark
  Opens key:             HKCU\software\wireshark
  Opens key:             HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\fiddler.exe
  Opens key:             HKLM\software\microsoft\windows\currentversion\app paths\fiddler.exe
  Opens key:             HKCU\software\microsoft\windows\currentversion\app paths\fiddler.exe
  Opens key:             HKLM\hardware\devicemap\scsi\scsi port 0\scsi bus 0\target id 0\logical
unit id 0
  Opens key:             HKLM\hardware\description\system
  Opens key:             HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\fiddler2.exe
  Opens key:             HKLM\software\microsoft\windows\currentversion\app paths\fiddler2.exe
  Opens key:             HKCU\software\microsoft\windows\currentversion\app paths\fiddler2.exe
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\fiddler2
  Opens key:             HKCU\software\microsoft\windows\currentversion\uninstall\fiddler2
  Opens key:             HKLM\software\wow6432node\microsoft\fiddler2
  Opens key:             HKCU\software\microsoft\fiddler2
  Opens key:             HKCR\software\ieinspectorsoft\httpanalyzeraddon
  Opens key:             HKCU\software\classes\software\ieinspectorsoft\httpanalyzeraddon
  Opens key:             HKLM\system\currentcontrolset\services\disk\enum
  Opens key:             HKLM\software\wow6432node\oracle\virtualbox guest additions
  Opens key:             HKCR\iehttpanalyzer.httpanalyzeraddon
  Opens key:             HKCU\software\classes\iehttpanalyzer.httpanalyzeraddon
  Opens key:             HKCR\httpanalyzerstd.httpanalyzerstandalone
  Opens key:             HKCU\software\classes\httpanalyzerstd.httpanalyzerstandalone
  Opens key:             HKCR\charles.amf.document
  Opens key:             HKCU\software\classes\charles.amf.document
  Opens key:             HKCR\charles.document
  Opens key:             HKCU\software\classes\charles.document
  Opens key:             HKLM\software\wow6432node\xk72 ltd folder
  Opens key:             HKCU\software\xk72 ltd folder
  Opens key:             HKLM\software\wow6432node\vmware, inc.\vmware tools
  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:
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:             HKCU\software\d514d55fab
  Opens key:             HKLM\software\wow6432node\d514d55fab
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}\propertybag
  Opens key:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}
```

```
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}\propertybag
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001
  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:                HKLM\software\wow6432node\microsoft\windows\currentversion\run
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer\run
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer\run
  Opens key:                HKCU\software\microsoft\windows\currentversion\run
  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[2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d.exe]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[2b8ad717e0f5509cfafba2d0b0d83108b6e290525c0a1cd583580d31f7c5237d]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  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\sqmclient\windows[ceipenable]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\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\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\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ar]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ar]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ar-sa]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-sa]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[bg]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[bg]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[bg-bg]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[bg-bg]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ca]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ca]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ca-es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ca-es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[zh-hans]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hans]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-cn]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[cs]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[cs]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[cs-cz]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[cs-cz]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[da]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[da]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[da-dk]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[da-dk]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[de]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[de]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[de-de]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[de-de]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[el]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[el]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[el-gr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[el-gr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[es-es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[es-es]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[fi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[fi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[fi-fi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[fi-fi]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[fr-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-fr]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[he]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[he]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[he-il]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[he-il]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hu-hu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hu-hu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[is]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[is]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[is-is]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[is-is]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[it]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[it]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[it-it]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[it-it]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ja]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ja]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ja-jp]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ja-jp]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ko]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ko]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ko-kr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ko-kr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[nl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[nl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[nl-nl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[nl-nl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[no]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[no]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[nb-no]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[nb-no]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[pl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[pl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[pl-pl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[pl-pl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[pt]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[pt]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[pt-br]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[pt-br]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[rm]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[rm]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[rm-ch]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[rm-ch]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ro]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ro]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ro-ro]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ro-ro]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ru-ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ru-ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hr-hr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hr-hr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sk-sk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sk-sk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sq]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sq]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sq-al]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sq-al]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sv]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sv]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sv-se]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sv-se]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[th]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[th]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[th-th]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[th-th]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tr-tr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tr-tr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ur]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ur]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ur-pk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ur-pk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[id]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[id]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[id-id]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[id-id]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[uk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[uk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[uk-ua]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[uk-ua]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[be]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[be]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[be-by]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[be-by]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sl-si]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sl-si]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[et]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[et]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[et-ee]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[et-ee]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lv]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lv]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lv-lv]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lv-lv]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lt]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lt]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lt-lt]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lt-lt]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tg]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tg]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tg-cyrl-tj]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tg-cyrl-tj]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fa]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fa]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fa-ir]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fa-ir]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[vi]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[vi]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[vi-vn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[vi-vn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hy]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hy]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hy-am]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hy-am]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[az]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[az]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[az-latn-az]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[az-latn-az]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[eu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[eu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[eu-es]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[eu-es]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hsb]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hsb]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hsb-de]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hsb-de]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mk-mk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mk-mk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tn-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tn-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[xh]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[xh]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[xh-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[xh-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[zu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[zu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[zu-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[zu-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[af]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[af]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[af-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[af-za]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ka]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ka]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ka-ge]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ka-ge]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fo-fo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fo-fo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hi]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hi]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[hi-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[hi-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mt]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mt]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mt-mt]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mt-mt]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[se]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[se]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[se-no]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[se-no]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ga]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ga]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ga-ie]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ga-ie]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ms]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ms]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ms-my]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ms-my]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kk-kz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kk-kz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ky]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ky]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ky-kg]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ky-kg]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sw]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sw]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sw-ke]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sw-ke]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tk-tm]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tk-tm]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[uz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[uz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[uz-latn-uz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-latn-uz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tt]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tt]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tt-ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tt-ru]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bn-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bn-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[pa]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[pa]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[pa-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[pa-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gu-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gu-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[or]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[or]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[or-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[or-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ta]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ta]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ta-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ta-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[te]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[te]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[te-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[te-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kn-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kn-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ml]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ml]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ml-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ml-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[as]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[as]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[as-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[as-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mr-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mr-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sa]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sa]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sa-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sa-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[mn-mn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-mn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bo-cn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bo-cn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[cy]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[cy]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[cy-gb]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[cy-gb]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[km]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[km]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[km-kh]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[km-kh]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[lo-la]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[lo-la]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gl-es]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gl-es]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kok]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kok]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[kok-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[kok-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sd]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sd]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sd-arab-pk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sd-arab-pk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[syr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[syr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[syr-sy]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[syr-sy]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[si]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[si]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[si-lk]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[si-lk]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[chr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[chr]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[chr-cher-us]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[chr-cher-us]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[iu]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[iu]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[iu-latn-ca]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-latn-ca]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[am]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[am]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[am-et]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[am-et]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tzm]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[tzm-latn-dz]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm-latn-dz]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ne]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ne]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ne-np]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ne-np]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fy]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fy]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fy-nl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fy-nl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ps]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ps]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ps-af]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ps-af]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fil]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fil]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[fil-ph]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[fil-ph]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[dv]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[dv]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[dv-mv]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[dv-mv]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ff]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ff]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ff-latn-sn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ff-latn-sn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ha]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ha]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ha-latn-ng]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ha-latn-ng]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[yo]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[yo]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[yo-ng]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[yo-ng]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[quz]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[quz]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[quz-bo]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[quz-bo]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[nso]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[nso]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[nso-za]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[nso-za]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ba]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ba]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ba-ru]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ba-ru]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[lb]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[lb]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[lb-lu]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[lb-lu]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[kl]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[kl]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[kl-gl]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[kl-gl]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ig]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ig]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ig-ng]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ig-ng]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ti]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ti]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ti-er]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ti-er]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[haw]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[haw]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[haw-us]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[haw-us]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ii]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ii]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ii-cn]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ii-cn]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[arn]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[arn]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[arn-cl]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[arn-cl]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[moh]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[moh]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[moh-ca]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[moh-ca]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[br]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[br]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[br-fr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[br-fr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ug]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ug]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[ug-cn]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[ug-cn]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[mi]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[mi]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[mi-nz]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[mi-nz]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[oc]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[oc]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[oc-fr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[oc-fr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[co]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[co]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[co-fr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[co-fr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[gsw]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[gsw]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[gsw-fr]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[gsw-fr]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sah]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sah]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[sah-ru]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[sah-ru]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[qut]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[qut]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[qut-gt]
Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[qut-gt]
Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[rw]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[rw]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[rw-rw]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[rw-rw]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[wo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[wo]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[wo-sn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[wo-sn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[prs]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[prs]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[prs-af]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[prs-af]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gd]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gd]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[gd-gb]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[gd-gb]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ku]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ku]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ku-arab-iq]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ku-arab-iq]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000401]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[d]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000402]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[5]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000403]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[zh-tw]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-tw]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000404]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[9]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000405]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[2]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000406]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000407]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000408]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[4]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-es_tradnl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-es_tradnl]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000040a]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000040b]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000040c]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000040d]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[c]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000040e]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000040f]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000410]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000411]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[7]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000412]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[8]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000413]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000414]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000415]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000416]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000417]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000418]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000419]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000041a]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000041b]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000041c]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000041d]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000041e]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[b]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000041f]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[6]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000420]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000421]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000422]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000423]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000424]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000425]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[3]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000426]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000427]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000428]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000429]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000042a]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[e]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000042b]
Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[11]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000042c]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000042d]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000042e]
```

```
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000042f]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000432]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000434]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000435]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000436]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000437]
   Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[10]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000438]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000439]
   Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[f]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000043a]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000043b]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000043e]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000043f]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000440]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000441]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000442]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000443]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000444]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000445]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000446]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000447]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000448]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000449]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000044a]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000044b]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000044c]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000044d]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000044e]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000044f]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000450]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000451]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000452]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000453]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000454]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000456]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000457]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000045a]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000045b]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000045c]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[iu-cans-ca]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-cans-ca]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000045d]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000045e]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000461]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000462]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000463]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000464]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000465]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000468]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000046a]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000046b]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000046c]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000046d]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000046e]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000046f]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000470]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ti-et]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ti-et]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000473]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000475]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000478]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000047a]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000047c]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000047e]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000480]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000481]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000482]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000483]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000484]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000485]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000486]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000487]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000488]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000048c]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000491]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000492]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[qps-ploc]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[qps-ploc]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000501]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale\alternate
sorts[00000501]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[qps-ploca]
```

```
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[qps-ploca]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[000005fe]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale\alternate
sorts[000005fe]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-iq]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-iq]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000801]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ca-es-valencia]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ca-es-valencia]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000803]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000804]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[de-ch]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[de-ch]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000807]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-gb]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-gb]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000809]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-mx]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-mx]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000080a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fr-be]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-be]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000080c]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[it-ch]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[it-ch]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000810]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[nl-be]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[nl-be]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000813]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[nn-no]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[nn-no]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000814]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[pt-pt]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[pt-pt]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000816]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn-cs]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn-cs]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000081a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sv-fi]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sv-fi]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000081d]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[az-cyrl-az]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[az-cyrl-az]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000082c]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[dsb-de]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[dsb-de]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000082e]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tn-bw]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tn-bw]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000832]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[se-se]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[se-se]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000083b]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000083c]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ms-bn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ms-bn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000083e]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[uz-cyrl-uz]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-cyrl-uz]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000843]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[bn-bd]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[bn-bd]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000845]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[pa-arab-pk]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[pa-arab-pk]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000846]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ta-lk]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ta-lk]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000849]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[mn-mong-cn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-mong-cn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000850]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000859]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000085d]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000085f]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000867]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[quz-ec]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[quz-ec]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000086b]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000873]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[qps-plocm]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[qps-plocm]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[000009ff]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale\alternate
sorts[000009ff]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-eg]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-eg]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c01]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zh-hk]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hk]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c04]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[de-at]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[de-at]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c07]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-au]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-au]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c09]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c0a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fr-ca]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-ca]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c0c]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl-cs]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-cyrl-cs]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c1a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[se-fi]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[se-fi]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c3b]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[quz-pe]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[quz-pe]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000c6b]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-ly]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-ly]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001001]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zh-sg]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-sg]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001004]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[de-lu]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[de-lu]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001007]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-ca]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-ca]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001009]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-gt]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-gt]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000100a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fr-ch]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-ch]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000100c]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[hr-ba]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[hr-ba]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000101a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[smj-no]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[smj-no]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000103b]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tzm-tfng-ma]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm-tfng-ma]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000105f]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-dz]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-dz]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001401]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zh-mo]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-mo]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001404]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[de-li]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[de-li]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001407]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-nz]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-nz]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-cr]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-cr]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000140a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fr-lu]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-lu]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000140c]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[bs-latn-ba]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[bs-latn-ba]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000141a]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[smj-se]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[smj-se]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000143b]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-ma]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-ma]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001801]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-ie]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-ie]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001809]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-pa]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-pa]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000180a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[fr-mc]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-mc]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000180c]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn-ba]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn-ba]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000181a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sma-no]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sma-no]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000183b]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-tn]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-tn]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001c01]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-za]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001c09]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-do]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-do]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001c0a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl-ba]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-cyrl-ba]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001c1a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sma-se]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sma-se]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00001c3b]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-om]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-om]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002001]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-jm]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-jm]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002009]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-ve]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-ve]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000200a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[bs-cyrl-ba]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[bs-cyrl-ba]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000201a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sms-fi]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sms-fi]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000203b]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-ye]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-ye]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002401]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-029]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-029]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002409]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-co]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-co]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000240a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn-rs]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn-rs]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000241a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[smn-fi]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[smn-fi]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000243b]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-sy]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-sy]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002801]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-bz]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-bz]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002809]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-pe]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-pe]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000280a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl-rs]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-cyrl-rs]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[0000281a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ar-jo]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-jo]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002c01]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-tt]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-tt]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002c09]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[es-ar]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[es-ar]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002c0a]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn-me]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn-me]
Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00002c1a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ar-lb]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-lb]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00003001]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-zw]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-zw]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00003009]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-ec]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-ec]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000300a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl-me]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-cyrl-me]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000301a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ar-kw]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-kw]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00003401]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-ph]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-ph]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00003409]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-cl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-cl]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000340a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ar-ae]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-ae]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00003801]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-uy]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-uy]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000380a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ar-bh]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-bh]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00003c01]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-py]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-py]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00003c0a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[ar-qa]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-qa]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00004001]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-in]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00004009]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-bo]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-bo]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000400a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-my]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-my]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00004409]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-sv]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-sv]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000440a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-sg]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-sg]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00004809]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-hn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-hn]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000480a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-ni]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-ni]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00004c0a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-pr]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-pr]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000500a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[es-us]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[es-us]
Queries value:          HKLM\system\currentcontrolset\control\nls\locale[0000540a]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bs-cyrl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bs-cyrl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bs-latn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bs-latn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-cyrl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[smn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[smn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[az-cyrl]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[az-cyrl]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[sms]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[sms]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[zh]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[zh]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[nn]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[nn]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[bs]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[bs]
```

```
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[az-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[az-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sma]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sma]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[uz-cyrl]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-cyrl]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[mn-cyrl]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-cyrl]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[iu-cans]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-cans]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tzm-tfng]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm-tfng]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zh-hant]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hant]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[nb]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[nb]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sr]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sr]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tg-cyrl]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tg-cyrl]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[dsb]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[dsb]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[smj]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[smj]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[uz-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[pa-arab]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[pa-arab]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[mn-mong]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-mong]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[sd-arab]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[sd-arab]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[chr-cher]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[chr-cher]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[iu-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[tzm-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ff-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ff-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ha-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ha-latn]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ku-arab]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ku-arab]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[]
  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\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\windows nt\currentversion[installdate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[foldertypeid]
   Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-
1d43-42f2-9305-67de0b28fc23}[initfolderhandler]
  Queries value:            HKLM\software\wow6432node\076d08883c3fd02b[4313902a5ea0ce0c1123]
  Queries value:            HKLM\software\wow6432node\5sacgv8hb0[xulz75]
  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\lsa[everyoneincludesanonymous]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
  Queries value:            HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[logging directory]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[log file max size]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:            HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
  Queries value:            HKLM\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\ole[maximumallowedallocationsize]
  Queries value:            HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
  Queries value:            HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value:            HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[]
  Queries value:            HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[processid]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[enableprivateobjectheap]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[identifierlimit]
  Queries value:            HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
  Queries value:            HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
  Queries value:            HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}[]
  Queries value:            HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[threadingmodel]
  Queries value:            HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}[]
  Queries value:            HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
```

```
  Queries value:              HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[enableobjectvalidation]
  Queries value:              HKCR\wow6432node\interface\{44aca675-e8fc-11d0-a07c-
00c04fb68820}\proxystubclsid32[]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{c7a85eba-c2d1-41ec-c656-ca2c9221e354}]
  Queries value:              HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{c7a85eba-c2d1-41ec-c656-ca2c9221e354}]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[regsvr32]
  Queries value:              HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[regsvr32.exe]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion[digitalproductid]
  Queries value:              HKLM\hardware\description\system[systembiosversion]
  Queries value:              HKLM\hardware\description\system[videobiosversion]
  Queries value:              HKLM\system\currentcontrolset\services\disk\enum[0]
  Queries value:              HKLM\software\wow6432node\d514d55fab[8949c875]
  Queries value:              HKLM\software\wow6432node\d514d55fab[53a541f8]
  Queries value:              HKCU\software\d514d55fab[53a541f8]
  Queries value:              HKCU\software\d514d55fab[8949c875]
  Queries value:              HKLM\software\wow6432node\d514d55fab[d8c6d29b]
  Queries value:              HKCU\software\d514d55fab[d8c6d29b]
  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\d514d55fab[45b1ee63]
  Queries value:              HKCU\software\d514d55fab[45b1ee63]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
  Queries value:              HKLM\software\wow6432node\d514d55fab[f024c728]
  Queries value:              HKCU\software\d514d55fab[f024c728]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[category]
  Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{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-
1923240461-1905901954-2556564120-1001[profileimagepath]
   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:            HKLM\software\wow6432node\d514d55fab[1c8238d6]
   Queries value:            HKCU\software\d514d55fab[1c8238d6]
   Queries value:            HKLM\software\wow6432node\d514d55fab[a1c43031]
   Queries value:            HKCU\software\d514d55fab[a1c43031]
   Queries value:            HKLM\software\wow6432node\d514d55fab[8a0833d2]
   Queries value:            HKCU\software\d514d55fab[8a0833d2]
   Queries value:            HKLM\software\wow6432node\d514d55fab[ddcc1acd]
   Queries value:            HKCU\software\d514d55fab[ddcc1acd]
   Queries value:            HKLM\software\wow6432node\d514d55fab[59c4f52b]
   Queries value:            HKCU\software\d514d55fab[59c4f52b]
   Queries value:            HKLM\software\wow6432node\d514d55fab[6c6add07]
   Queries value:            HKCU\software\d514d55fab[6c6add07]
   Queries value:            HKLM\software\wow6432node\microsoft\windows\currentversion\run[]
   Queries value:            HKLM\software\microsoft\windows\currentversion\policies\explorer\run[]
   Queries value:            HKCU\software\microsoft\windows\currentversion\run[]
   Sets/Creates value:       HKLM\software\wow6432node\076d08883c3fd02b[4313902a5ea0ce0c1123]
   Sets/Creates value:       HKLM\software\wow6432node\5sacgv8hb0[5cd3fsxgz8]
   Sets/Creates value:       HKLM\software\wow6432node\5sacgv8hb0[xulz75]
   Sets/Creates value:       HKLM\software\wow6432node\d514d55fab[d8c6d29b]
   Sets/Creates value:       HKCU\software\d514d55fab[d8c6d29b]
   Sets/Creates value:       HKLM\software\wow6432node\d514d55fab[53a541f8]
   Sets/Creates value:       HKCU\software\d514d55fab[53a541f8]
   Sets/Creates value:       HKLM\software\wow6432node\d514d55fab[45b1ee63]
   Sets/Creates value:       HKCU\software\d514d55fab[45b1ee63]
   Sets/Creates value:       HKCU\software\d514d55fab[ddcc1acd]
   Sets/Creates value:       HKLM\software\wow6432node\d514d55fab[ddcc1acd]
   Sets/Creates value:       HKCU\software\d514d55fab[1c8238d6]
   Sets/Creates value:       HKLM\software\wow6432node\d514d55fab[1c8238d6]
   Sets/Creates value:       HKLM\software\wow6432node\microsoft\windows\currentversion\run[]
   Sets/Creates value:       HKLM\software\microsoft\windows\currentversion\policies\explorer\run[]
   Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\run[]
   Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1206]
   Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2300]
   Value changes:            HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\zones\3[1809]
  Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1206]
  Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[2300]
  Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1809]
```