Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	141
Risk Level:	1
Date Processed:	2016-04-28 12:50:41 (UTC)
Processing Time:	61.46 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\42c3a976e0e61290cc95bb51c2d1be2f.exe"
Sample ID:	36
Type:	basic
Owner:	admin
Label:	42c3a976e0e61290cc95bb51c2d1be2f
Date Added:	2016-04-28 12:44:53 (UTC)
File Type:	PE32:win32:gui
File Size:	358968 bytes
MD5:	42c3a976e0e61290cc95bb51c2d1be2f
SHA256:	4ba0f73492c9a830986d1a7af9dd0a36d04ee06bf97a65c5e35da151b5bfd6a4
Description:	None

Pattern Matching Results

`1` YARA score 1

Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable
Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\windows\temp\42c3a976e0e61290cc95bb51c2d1be2f.exe

["C:\windows\temp\42c3a976e0e61290cc95bb51c2d1be2f.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\Sessions\1\BaseNamedObjects\OleDfRoot597ED553826A2792
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?

42C3A976E0E61290CC95BB51C2D1BE2F.EXE

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\~DF55B1640207681207.TMP
Opens:	C:\Windows\Prefetch\42C3A976E0E61290CC95BB51C2D1B-32C377A2.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\42c3a976e0e61290cc95bb51c2d1be2f.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\msvbvm60.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll

Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\iertutil.dll
Opens:	C:\Windows\SysWOW64\wininet.dll
Opens:	C:\Windows\SysWOW64\urlmon.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\sxs.dll
Opens:	C:\Windows\SysWOW64\shell32.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\shfolder.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\SysWOW64\clbcatq.dll
Opens:	C:\Windows\SysWOW64\scrrun.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\
Opens:	C:\Users
Opens:	C:\Users\Admin
Opens:	C:\Users\Admin\AppData
Opens:	C:\Users\Admin\AppData\Local
Opens:	C:\Windows\Fonts\sserife.fon
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\Windows\SysWOW64\dwmapi.dll
Opens:	C:\Windows\Fonts\tahoma.ttf
Opens:	C:\Windows\Fonts\tahomabd.ttf
Opens:	C:\Windows\SysWOW64\asycfilt.dll
Opens:	C:\Users\Admin\AppData\Roaming\Jumping Bytes\ClipboardMaster\settings.ini
Opens:	C:\windows\temp\languages\English.lng
Opens:	C:\Windows\Fonts\StaticCache.dat
Reads from:	C:\Windows\SysWOW64\scrrun.dll
Reads from:	C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

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

```
Opens key:                  HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key:                  HKCU\software\policies\microsoft\control panel\desktop
Opens key:                  HKCU\control panel\desktop\languageconfiguration
Opens key:                  HKCU\control panel\desktop
Opens key:                  HKCU\control panel\desktop\muicached
Opens key:                  HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:                  HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:                  HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key:                  HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:                  HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key:                  HKLM\system\currentcontrolset\control\session manager
Opens key:                  HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key:                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options
Opens key:                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
Opens key:                  HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key:                  HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key:                  HKLM\
Opens key:                  HKLM\software\wow6432node\microsoft\ole
Opens key:                  HKLM\software\microsoft\ole
Opens key:                  HKLM\software\wow6432node\microsoft\ole\tracing
Opens key:                  HKLM\software\microsoft\ole\tracing
Opens key:                  HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
Opens key:                  HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
Opens key:                  HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
Opens key:                  HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key:                  HKLM\software\wow6432node\microsoft\oleaut
Opens key:                  HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:                  HKLM\system\currentcontrolset\control\nls\sorting\ids
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\windows\windows error reporting\wmr
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\codepage
Opens key:                  HKLM\software\wow6432node\microsoft\vba\monitors
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:                  HKCU\software\jumping bytes\clipboard master
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key:                  HKCU\software\microsoft\windows\currentversion\explorer
Opens key:                  HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key:                  HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
```

Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion
  Opens key: HKCU\software\classes\
  Opens key: HKLM\software\microsoft\com3
  Opens key: HKCU\software\classes\scripting.filesystemobject
  Opens key: HKCR\scripting.filesystemobject
  Opens key: HKCU\software\classes\scripting.filesystemobject\clsid
  Opens key: HKCR\scripting.filesystemobject\clsid
  Opens key: HKLM\software\microsoft\windowsruntime\clsid
  Opens key: HKLM\software\microsoft\windowsruntime\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
  Opens key: HKCR\activatableclasses\clsid
  Opens key: HKCR\activatableclasses\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
  Opens key: HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
  Opens key: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
  Opens key: HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas
  Opens key: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas
  Opens key: HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32
  Opens key: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32
  Opens key: HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler32
  Opens key: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler32
  Opens key: HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler
  Opens key: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler
  Opens key: HKCU\software\classes\typelib
  Opens key: HKCR\typelib
  Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}
  Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}
  Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0
  Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0
  Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0
  Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0
  Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32
  Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32
  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\control panel\international
  Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\42c3a976e0e61290cc95bb51c2d1be2f.exe
  Opens key: HKLM\software\wow6432node\microsoft\ctf\
  Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
  Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0
  Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback
  Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\tahoma
  Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]

```
Queries value:              HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value:              HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value:              HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
Queries value:              HKCU\control panel\desktop[preferreduilanguages]
Queries value:              HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value:              HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
Queries value:              HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
Queries value:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[msvbvm60.dll]
Queries value:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[42c3a976e0e61290cc95bb51c2d1be2f.exe]
Queries value:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value:              HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value:              HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value:              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[42c3a976e0e61290cc95bb51c2d1be2f]
Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value:              HKLM\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\system\currentcontrolset\control\nls\locale[00000409]
Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value:              HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
    Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
    Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion[currentversion]
    Queries value:              HKLM\software\microsoft\com3[com+enabled]
    Queries value:              HKCR\scripting.filesystemobject\clsid[]
    Queries value:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[]
    Queries value:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32[inprocserver32]
    Queries value:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32[]
    Queries value:              HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32[threadingmodel]
    Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
    Queries value:              HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[]
    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:              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\sorting\ids[de-de]
    Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[de]
    Queries value:              HKCU\control panel\international[slanguage]
    Queries value:              HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
    Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
```