

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 134, Task ID: 534

Task ID:	534
Risk Level:	5
Date Processed:	2016-04-28 13:01:37 (UTC)
Processing Time:	61.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\2a331c13d2c596ffd675768823c8930d.exe"
Sample ID:	134
Type:	basic
Owner:	admin
Label:	2a331c13d2c596ffd675768823c8930d
Date Added:	2016-04-28 12:45:04 (UTC)
File Type:	PE32:win32:gui
File Size:	896000 bytes
MD5:	2a331c13d2c596ffd675768823c8930d
SHA256:	0cc7c6045521da5ecf43219c120eda04ff5e7c8727659f863d3894dcf203b7b7
Description:	None

## Pattern Matching Results

- 2 PE: Nonstandard section
- 5 Packer: UPX
- 5 PE: Contains compressed section

## Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

## Process/Thread Events

Creates process:	C:\windows\temp\2a331c13d2c596ffd675768823c8930d.exe
["C:\windows\temp\2a331c13d2c596ffd675768823c8930d.exe" ]	

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
----------------	---

## File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\ic#0
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#1
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#2
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#3
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#4
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#5
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#6
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#7
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#8
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#9
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#10
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#11
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#12
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#13
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#14
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#15
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#16
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#17
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#18
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#19
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#20
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#21
Creates:	C:\Users\Admin\AppData\Local\Temp\ic#22
Opens:	C:\Windows\Prefetch\2A331C13D2C596FFD675768823C89-3E55A9B5.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\2a331c13d2c596ffd675768823c8930d.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\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\version.dll  
Opens: C:\Windows\SysWOW64\sechost.dll  
Opens: C:\Windows\SysWOW64\combase.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\advapi32.dll  
Opens: C:\Windows\SysWOW64\user32.dll  
Opens: C:\Windows\SysWOW64\gdi32.dll  
Opens: C:\Windows\SysWOW64\ole32.dll  
Opens: C:\Windows\SysWOW64\oleaut32.dll  
Opens: C:\Windows\SysWOW64\shlwapi.dll  
Opens: C:\Windows\SysWOW64\shell32.dll  
Opens: C:\Windows\SysWOW64\imm32.dll  
Opens: C:\Windows\SysWOW64\msctf.dll  
Opens: C:\Windows\SysWOW64\uxtheme.dll  
Opens: C:\Windows\SysWOW64\dwmapl.dll  
Opens: C:\Windows\SysWOW64\msimg32.dll  
Opens: C:\Windows\WinSxS\x86\_microsoft.windows.c..-  
controls\_resources\_6595b64144ccf1df\_5.82.9200.16384\_en-us\_d51b55b9729b0b41  
Opens: C:\Windows\WinSxS\x86\_microsoft.windows.c..-  
controls\_resources\_6595b64144ccf1df\_5.82.9200.16384\_en-us\_d51b55b9729b0b41\comctl32.dll.mui  
Opens: C:\Windows\SysWOW64\SHCore.dll  
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls  
Opens: C:\Windows\Fonts\tahoma.ttf  
Opens: C:\Windows\SysWOW64\uxtheme.dll.Config  
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\Fonts\arial.ttf  
Opens: C:\Windows\Fonts\StaticCache.dat  
Opens: C:\Windows\Fonts\arialbd.ttf  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#0  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#1  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#2  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#3  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#4  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#5  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#6  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#7  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#8  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#9  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#10  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#11  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#12  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#13  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#14  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#15  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#16  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#17  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#18  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#19  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#20  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#21  
Opens: C:\Users\Admin\AppData\Local\Temp\ic#22  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#0  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#1  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#2  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#3  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#4  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#5  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#6  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#7  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#8  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#9  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#10  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#11  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#12  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#13  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#14  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#15  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#16  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#17  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#18  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#19  
Writes to: C:\Users\Admin\AppData\Local\Temp\ic#20

Writes to:	C:\Users\Admin\AppData\Local\Temp\ic#21
Writes to:	C:\Users\Admin\AppData\Local\Temp\ic#22
Reads from:	C:\Windows\Fonts\StaticCache.dat
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#0
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#1
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#2
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#3
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#4
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#5
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#6
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#7
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#8
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#9
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#10
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#11
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#12
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#13
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#14
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#15
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#16
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#17
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#18
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#19
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#20
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#21
Reads from:	C:\Users\Admin\AppData\Local\Temp\ic#22
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#0
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#1
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#2
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#3
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#4
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#5
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#6
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#7
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#8
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#9
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#10
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#11
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#12
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#13
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#14
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#15
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#16
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#17
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#18
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#19
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#20
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#21
Deletes:	C:\Users\Admin\AppData\Local\Temp\ic#22

## 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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots	

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\dlloptions  
 Opens key: HKLM\system\currentcontrolset\control\lsa\lspolicy  
 Opens key: HKLM\system\currentcontrolset\control\lsa  
 Opens key:  
 HKLM\system\currentcontrolset\policies\microsoft\cryptology\configuration  
 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\software\wow6432node\microsoft\ole  
 Opens key: HKLM\software\wow6432node\microsoft\ole\tracing  
 Opens key: HKLM\software\microsoft\ole\tracing  
 Opens key: HKLM\software\wow6432node\microsoft\oleaut  
 Opens key: HKCU\software\borland\locales  
 Opens key: HKLM\software\wow6432node\borland\locales  
 Opens key: HKCU\software\borland\delphi\locales  
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
 Opens key: HKLM\software\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\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\system\currentcontrolset\control\nls\sorting\ids  
 Opens key:  
 HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfolderssettings  
 Opens key:  
 HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer  
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer  
 Opens key:  
 HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\2a331c13d2c596ffd675768823c8930d.exe  
 Opens key: HKCU\software\exejoiner\_dem  
 Opens key: HKLM\system\currentcontrolset\control\nls\locale  
 Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts  
 Opens key: HKLM\system\currentcontrolset\control\nls\language groups  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\datastore\_v1.0  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback\arial  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback\system  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced  
 Opens key: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\fontsubstitutes  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback\tahoma  
 Opens key:  
 HKLM\software\wow6432node\microsoft\ctf\compatibility\2a331c13d2c596ffd675768823c8930d.exe  
 Opens key: HKLM\software\wow6432node\microsoft\ctf\  
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]  
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]  
 Queries value:  
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]  
 Queries value:  
 HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]  
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatencodepage]  
Queries value: HKCU\control panel\desktop[preferreduilanguages]  
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]  
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]  
Queries value: 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\dllexportoptions[usefilter]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllexportoptions[2a331c13d2c596ffd675768823c8930d.exe]  
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]  
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles]  
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[2a331c13d2c596ffd675768823c8930d]  
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]  
Queries value: HKLM\software\microsoft\ole[aggressivemtesting]  
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]  
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable]  
Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]  
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\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\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]  
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]  
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\datastore\_v1.0[disable]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\datastore\_v1.0[datafilepath]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane1]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane2]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane3]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane4]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane5]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane6]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane7]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane8]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane9]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane10]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane11]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane12]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane13]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane14]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane15]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback[plane16]  
Queries value: HKLM\system\currentcontrolset\control\session  
manager[safeprocesssearchmode]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe  
ui]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial]  
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]