

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 160, Task ID: 641

Task ID:	641
Risk Level:	4
Date Processed:	2016-04-28 13:04:47 (UTC)
Processing Time:	61.2 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\85d91c1c1b1aebdf1ceb74a7ef0bed54.exe"
Sample ID:	160
Type:	basic
Owner:	admin
Label:	85d91c1c1b1aebdf1ceb74a7ef0bed54
Date Added:	2016-04-28 12:45:06 (UTC)
File Type:	PE32:win32:gui
File Size:	778752 bytes
MD5:	85d91c1c1b1aebdf1ceb74a7ef0bed54
SHA256:	ded6339bd07478fcdf9950a21e232ae040f90a6370e3bb30c50dfb3f8a5b2669
Description:	None

Pattern Matching Results

- 2 PE: Nonstandard section
- 3 Long sleep detected
- 4 Checks whether debugger is present

Static Events

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

Process/Thread Events

Creates process:	C:\windows\temp\85d91c1c1b1aebdf1ceb74a7ef0bed54.exe
["C:\windows\temp\85d91c1c1b1aebdf1ceb74a7ef0bed54.exe"]	

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtftMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtftActivated.Default1
Creates event:	\KernelObjects\MaximumCommitCondition

File System Events

Opens:	C:\Windows\Prefetch\85D91C1C1B1AEBDF1CEB74A7EF0BE-0F39EB65.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\85d91c1c1b1aebdf1ceb74a7ef0bed54.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens:	C:\windows\temp\WINHTTP.dll
Opens:	C:\Windows\SysWOW64\winhttp.dll
Opens:	C:\windows\temp\webio.dll
Opens:	C:\Windows\SysWOW64\webio.dll
Opens:	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
Opens:	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\SysWOW64\rpcss.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll

```

Opens:                C:\Windows\Fonts\tahoma.ttf
Opens:                C:\windows\temp\dwmapi.dll
Opens:                C:\Windows\SysWOW64\dwmapi.dll
Opens:                C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens:                C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:                C:\Windows\Fonts\StaticCache.dat
Opens:                C:\windows\temp\WindowsCodecs.dll
Opens:                C:\Windows\SysWOW64\WindowsCodecs.dll
Opens:                C:\Windows\SysWOW64\ole32.dll
Opens:                C:\Windows\winsxs\x86_microsoft.windows.c...-
controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9
Opens:                C:\Windows\winsxs\x86_microsoft.windows.c...-
controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui
Opens:                C:\Windows\SysWOW64\uxtheme.dll.Config
Opens:                C:\Windows\Temp\85d91c1c1b1aebdf1ceb74a7ef0bed54.exe
Opens:                C:\
Opens:                C:\windows\temp\CRYPTSP.dll
Opens:                C:\Windows\SysWOW64\cryptsp.dll
Opens:                C:\Windows\SysWOW64\rsaenh.dll
Opens:                C:\windows\temp\RpcRtRemote.dll
Opens:                C:\Windows\SysWOW64\RpcRtRemote.dll
Opens:                C:\windows\temp\imageres.dll
Opens:                C:\Windows\SysWOW64\imageres.dll
Opens:                C:\Windows\SysWOW64\en-US\imageres.dll.mui
Reads from:           C:\Windows\Fonts\StaticCache.dat

```

Windows Registry Events

```

Opens key:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options
Opens key:            HKLM\system\currentcontrolset\control\session manager
Opens key:            HKLM\software\microsoft\wow64
Opens key:            HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:            HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:            HKLM\
Opens key:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
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\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:            HKLM\software\wow6432node\microsoft\rpc

```

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\sqlclient\windows
Opens key: HKLM\software\microsoft\sqlclient\windows
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\appid\85d91c1c1b1aebdf1ceb74a7ef0bed54.exe
Opens key: HKCR\appid\85d91c1c1b1aebdf1ceb74a7ef0bed54.exe
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
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\system\currentcontrolset\control\cmf\config
Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\85d91c1c1b1aebdf1ceb74a7ef0bed54.exe
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\datastore_v1.0
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-1e1a187c13e9}\0000
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
Opens key: HKCU\software\classes\wow6432node\clsid\{fae3d380-fea4-4623-8c75-c6b61110b681}\instance
Opens key: HKCR\wow6432node\clsid\{fae3d380-fea4-4623-8c75-c6b61110b681}\instance
Opens key: HKCU\software\classes\wow6432node\clsid\{fae3d380-fea4-4623-8c75-c6b61110b681}\instance\disabled
Opens key: HKCR\wow6432node\clsid\{fae3d380-fea4-4623-8c75-c6b61110b681}\instance\disabled
Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\wow6432node\microsoft\ctf\
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\system
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\microsoft sans serif
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\ctf\knownclasses
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{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\microsoft\com3
  Opens key: HKCU\software\classes\wow6432node\clsid\{f7fe4993-2936-4685-aed1-
6429dcb88d64}
  Opens key: HKCR\wow6432node\clsid\{f7fe4993-2936-4685-aed1-6429dcb88d64}
  Opens key: HKCU\software\classes\clsid\{f7fe4993-2936-4685-aed1-6429dcb88d64}
  Opens key: HKCR\clsid\{f7fe4993-2936-4685-aed1-6429dcb88d64}
  Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
  Opens key: HKLM\system\currentcontrolset\control\lsa\lipsalgorithmpolicy
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key: HKLM\software\policies\microsoft\cryptography
  Opens key: HKLM\software\microsoft\cryptography
  Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
  Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
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\system\currentcontrolset\services\bfe
  Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Opens key: HKCU\software\policies\microsoft\windows\app management
  Opens key: HKLM\software\wow6432node\policies\microsoft\windows\app management
  Opens key: HKLM\software\policies\microsoft\windows\app management
  Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
  Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value: HKLM\system\currentcontrolset\control\ls\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\ls\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\ls\sorting\versions[]
  Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[85d91c1c1b1aebdf1ceb74a7ef0bed54]
  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\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\sqmclient\windows[ceipenable]
  Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value: HKLM\system\currentcontrolset\control\ls\customlocale[en-us]
  Queries value: HKLM\system\currentcontrolset\control\ls\extendedlocale[en-us]
  Queries value: HKLM\system\currentcontrolset\control\ls\locale[00000409]
  Queries value: HKLM\system\currentcontrolset\control\ls\language groups[1]
  Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]

```

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell_dlg_2]

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\hardware\devicemap\video[maxobjectnumber]

Queries value: HKLM\hardware\devicemap\video[\device\video3]

Queries value: HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-
1e1a187c13e9}\0000[pruningmode]

Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]

Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]

Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]

Queries value: HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[microsoft sans serif]

Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsiname]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-

b2f1-4857-a4ce-a8e7c6ea7d27}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27}[initfolderhandler]
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\microsoft\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[6bad60e5]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]