Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 618, Task ID: 2420

Task ID:	2420
Risk Level:	2
Date Processed:	2016-02-22 05:28:13 (UTC)
Processing Time:	62.85 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	

```
"c:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe"
```

Sample ID:	618
Type:	basic
Owner:	admin
Label:	476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4
Date Added:	2016-02-22 05:26:49 (UTC)
File Type:	PE32:win32:gui:.net
File Size:	90112 bytes
MD5:	758d4de025b7b396dc7211c457520776
SHA256:	476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4
Description:	None

Pattern Matching Results

2 .NET compiled executable

Process/Thread Events

Creates process:
C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
["C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe"]
Writes to process: PID:2864
C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Terminates process:
C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \BaseNamedObjects\CorDBIPCSetupSyncEvent_2812
Creates event: \KernelObjects\LowMemoryCondition

File System Events

Creates: C:\Users\Admin
Creates: C:\Users\Admin\AppData\Roaming
Opens: C:\Windows\Prefetch\476FC456C66CBEC138E3DAB72A0F0-C3D55795.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\mscoree.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\MSCOREE.DLL.local
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727
Opens: C:\Windows\Microsoft.NET\Framework\Upgrades.2.0.50727\
Opens: C:\Windows\SysWOW64\imm32.dll
Opens:
C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.config
Opens:
C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
Opens:
C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.Local\
Opens:
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
Opens:
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
Opens: C:\
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\index127.dat
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
Opens: C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089
Opens: C:\Windows\Temp
Opens: C:\Windows\SysWOW64\l_intl.nls
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
Opens: C:\Windows\assembly\pubpol4.dat
Opens: C:\Windows\assembly\GAC\PublisherPolicy.tme
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
Opens: C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a
Opens: C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll
Opens: C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System.EnterpriseSe#\887ef2648686aad19feff405eddbffd2\System.EnterpriseServices.ni.dll
Opens: C:\Windows\assembly\GAC_32\System.EnterpriseServices\2.0.0.0__b03f5f7f11d50a3a
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2812.72359
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2812.72359
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2812.72359
Reads from: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Reads from: C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe

Windows Registry Events

Creates key: HKLM\software\microsoft\fusion\gacchangenotification\default
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\nls\sorting\versions
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\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\v2.0
Opens key: HKLM\software\wow6432node\microsoft\.netframework
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\upgrades
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\standards
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch
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: HKCU\software\microsoft\.netframework\policy\standards
Opens key:

HKLM\software\wow6432node\microsoft\.netframework\policy\standards\v2.0.50727
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\microsoft\.netframework
Opens key: HKLM\software\microsoft\fusion
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Opens key: HKCU\software\microsoft\fusion
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets\localintranet
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key:
HKLM\software\wow6432node\microsoft\windows\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\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\explorer
Opens key: HKLM\software\policies\microsoft\windows\explorer
Opens key: HKCU\software\policies\microsoft\windows\explorer
Opens key:
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\currentversion\explorer\knownfoldersettings
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\v2.0.50727\security\policy
Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32
Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index127
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}\propertybag
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\4846a846\3ed6137e
Opens key: HKLM\software\wow6432node\microsoft\strongname
Opens key: HKLM\software\microsoft\fusion\publisherpolicy\default
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.drawing__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\7e
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\86
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\87
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\88
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system__b77a5c561934e089
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.xml__b77a5c561934e089
Opens key:

HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.configuration__b03f5f7f11d50a3a
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\aptca
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.windows.forms__b77a5c561934e089
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\85
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\80
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\78
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\7c
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\79
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.deployment__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.runtime.serialization.formatters.soap__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.accessibility__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.security__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.enterpriseservices__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\70
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\52d7076e\72
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\46ad0879\6f
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\59f3b67b\82
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\4c239d82\71
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.8.0.microsoft.visualc__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.runtime.remoting__b77a5c561934e089
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.directoryservices__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.transactions__b77a5c561934e089
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\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
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\system\currentcontrolset\control\nls\sorting\versions[]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
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\software\wow6432node\microsoft\.netframework[installroot]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[clrloadlogdir]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[onlyuselatestclr]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[gcstressstart]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[gcstressstartatjit]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[disableconfigcache]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-931b-d9cc2eee27e4]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[cc2bcbba-16b6-4cf3-8990-d74c2e8af500]
Queries value: HKLM\software\microsoft\fusion[cachelocation]
Queries value: HKLM\software\microsoft\fusion[downloadcachequotainkb]
Queries value: HKLM\software\microsoft\fusion[enablelog]
Queries value: HKLM\software\microsoft\fusion[logginglevel]
Queries value: HKLM\software\microsoft\fusion[forcelog]
Queries value: HKLM\software\microsoft\fusion[logfailures]
Queries value: HKLM\software\microsoft\fusion[versioninglog]
Queries value: HKLM\software\microsoft\fusion[logresourcebinds]
Queries value: HKLM\software\microsoft\fusion[uselegacyidentityformat]
Queries value: HKLM\software\microsoft\fusion[disablemsipeek]
Queries value: HKLM\software\microsoft\fusion[noclientchecks]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[devoverrideenable]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
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\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]

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-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index127[niusagemask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index127[ilusagemask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[displayname]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[index4]
Queries value:
HKLM\software\microsoft\fusion\publisherpolicy\default[legacypolicytimestamp]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[status]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\7b[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\7e[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\7e[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\7e[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\7e[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\7e[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\88[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\86[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\86[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\86[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\86[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\86[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\87[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\87[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\87[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\87[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\87[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\88[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\88[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\88[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\88[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\88[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.drawing,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.configuration,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[nidependencies]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\7a[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\85[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\85[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\85[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\85[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\85[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\80[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\80[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\80[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\80[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\80[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\78[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\78[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\78[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\78[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\78[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\7c[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\7c[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\7c[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\7c[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\7c[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\79[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\79[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\79[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\79[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\79[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.deployment,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.serialization.formatters.soap,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[accessibility,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\70[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\70[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\70[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\70[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\70[sig]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\70[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\52d7076e\72[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\52d7076e\72[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\52d7076e\72[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\52d7076e\72[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\52d7076e\72[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\46ad0879\6f[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\46ad0879\6f[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\46ad0879\6f[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\46ad0879\6f[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\46ad0879\6f[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\59f3b67b\82[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\59f3b67b\82[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\59f3b67b\82[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\59f3b67b\82[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\59f3b67b\82[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\4c239d82\71[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\4c239d82\71[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\4c239d82\71[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\4c239d82\71[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\4c239d82\71[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.enterpriseservices,2.0.0.0,,b03f5f7f11d50a3a,x86]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[microsoft.visualc,8.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.remoting,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.directoryservices,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.transactions,2.0.0.0,,b77a5c561934e089,x86]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]