Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 618, Task ID: 2417

Task ID:	2417
Risk Level:	6
Date Processed:	2016-02-22 05:28:11 (UTC)
Processing Time:	61.07 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
3 Writes to a log file [Info]
6 Creates executable in application data folder

Process/Thread Events

Creates process:
```
C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
["C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe" ]
```
Writes to process: PID:2796
```
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_2740

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0_32
Creates:	C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs
Creates:	

```
C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.log
```

Opens:	C:\Windows\Prefetch\476FC456C66CBEC138E3DAB72A0F0-C3D55795.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\mscoree.dll
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	

```
C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
```

Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v4.0.30319
Opens:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
Opens:	C:\Windows\Microsoft.NET\Framework
Opens:	C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	

C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.config
Opens:
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6910_none_d089c358442de345
Opens:
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6910_none_d089c358442de345\msvcr80.dll
Opens: C:\
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Opens:
C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.log
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\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\Windows\SysWOW64\SHCore.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\profapi.dll
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\index21.dat
Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\452f06494f05cb9d89325460550d1d62\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\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\6124280f8365d6683e54dd997421c0f6\System.ni.dll
Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\b8f373895aa19304a2cb6b888e298529\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\5ba5657c270bdd2fde78ecda4c2ad910\System.Windows.Forms.ni.dll
Opens:
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089
Opens:
C:\Windows\assembly\GAC_32\System.EnterpriseServices\2.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.dll
Opens:
C:\Windows\assembly\GAC_32\System.EnterpriseServices\2.0.0.0__b03f5f7f11d50a3a
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2740.10903796
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2740.10903796
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config.cch.2740.10903812
Opens: C:\Windows\SysWOW64\nsi.dll
Opens: C:\Windows\SysWOW64\ws2_32.dll
Writes to:
C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.log
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\wow64
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\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\v4.0
Opens key: HKLM\software\wow6432node\microsoft\.netframework
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKCU\software\microsoft\.netframework
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\.netframework\policy\standards
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\standards\v2.0.50727
Opens key: HKLM\software\wow6432node\microsoft\fusion
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch\v4.0.30319.00000
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch\v4.0.30319.00000\mscorwks.dll
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\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\software\wow6432node\microsoft\.netframework\ngen\policy\v2.0
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-1-5-21-1923240461-1905901954-2556564120-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
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\system\currentcontrolset\control\session manager
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
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\index21
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\1

Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1
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\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\153b7f91\9
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\210819fb\6
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\5206cfdb\7
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6ff8cf57\8
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\aptca
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\10
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\6604efc\3
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\6bbd663d\4
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7a981124\1f
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\bd38540\f
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\34e16fb6\20
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df
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: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
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\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: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[installroot]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[clrloadlogdir]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
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[uselegacyv2runtimeactivationpolicydefaultvalue]
Queries value: HKLM\software\wow6432node\microsoft\.netframework[onlyuselatestclr]
Queries value: HKLM\software\wow6432node\microsoft\fusion[noclientchecks]
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\wow6432node\microsoft\.netframework\ngen\policy\v2.0[optimizeusedbinaries]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
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\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index21[niusagemask]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index21[ilusagemask]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[displayname]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[configmask]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[configstring]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[mvid]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[evalationdata]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[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\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[configstring]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\153b7f91\9[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\153b7f91\9[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\153b7f91\9[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\153b7f91\9[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\153b7f91\9[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\210819fb\6[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\210819fb\6[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\210819fb\6[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\210819fb\6[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\210819fb\6[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\5206cfdb\7[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\5206cfdb\7[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\5206cfdb\7[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\5206cfdb\7[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\5206cfdb\7[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6ff8cf57\8[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6ff8cf57\8[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6ff8cf57\8[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6ff8cf57\8[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6ff8cf57\8[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\10[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[evalationdata]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\6604efc\3[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\6604efc\3[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\6604efc\3[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\6604efc\3[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\6604efc\3[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\6bbd663d\4[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\6bbd663d\4[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\6bbd663d\4[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\6bbd663d\4[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\6bbd663d\4[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7a981124\1f[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7a981124\1f[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7a981124\1f[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7a981124\1f[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7a981124\1f[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\bd38540\f[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\bd38540\f[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\bd38540\f[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\bd38540\f[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\bd38540\f[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\34e16fb6\20[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\34e16fb6\20[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\34e16fb6\20[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\34e16fb6\20[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\34e16fb6\20[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\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe]