Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 618, Task ID: 2419

Task ID: 2419 Risk Level: 2

Date Processed: 2016-02-22 05:28:13 (UTC)

Processing Time: 61.37 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:2240

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_2212

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\System32

 Opens:
 C:\Windows\System32\mscoree.dll

 Opens:
 C:\Windows\System32\sechost.dll

 Opens:
 C:\Windows\SYSTEM32\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\System32\imm32.dll

Opens:

 $\hbox{C:} \verb|\windows| temp| 476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.config Opens: \\$

C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll Opens:

C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.Local\Opens:

 $\hbox{C:$\windows\\winsxs\\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc Opens: } \\$

Opens: C:\Windows
Cpens: C:\Windows

 Opens:
 C:\Windows\Microsoft.NET\Framework\v2.0.50727\C0NFIG\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

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config

Opens:

Opens: C:\windows\temp\profapi.dll
Opens: C:\windows\system32\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\index145.dat

Opens:

Opens:

```
C: \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly a
                                        C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089
  Opens:
   Opens:
                                        C:\Windows\Temp
  Opens:
                                        C:\Windows\System32\l_intl.nls
  Opens:
                                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
  Opens:
                                        C:\Windows\System32\rpcss.dll
  Opens:
                                        C:\windows\temp\CRYPTBASE.dll
  Opens:
                                        C:\Windows\System32\cryptbase.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
                                         C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a
  Opens:
  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
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
C:\Windows\assembly\GAC_32\System.EnterpriseServices\2.0.0.0_b03f5f7f11d50a3a
  Opens:
                                        C:\Windows\System32\apphelp.dll
  Opens:
\label{lem:config} C: \windows \wicrosoft. NET \end{config} Security. config. cch. 2212.59936
  Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2212.59936
                                        C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config.cch.2212.59946
                                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
  Reads from:
  Reads from:
{\tt C:Windows Temp 476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe}
Windows Registry Events
  Creates key
                                        HKLM\software\microsoft\fusion\gacchangenotification\default
  Opens key:
                                        HKLM\system\currentcontrolset\control\session manager
  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\policies\microsoft\windows\safer\codeidentifiers
  Opens key:
                                        HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:
                                        HKCU\
  Opens key:
                                        HKCU\control panel\desktop\muicached\machinelanguageconfiguration
                                        HKLM\software\policies\microsoft\mui\settings
  Opens key:
  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\microsoft\windows\currentversion\sidebyside
  Opens key:
                                        HKLM\
  Opens key:
                                        \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows nt + current version + diagnostics \\
   Opens key:
                                        HKLM\software\microsoft\.netframework\policy\
  Opens key:
                                        HKLM\software\microsoft\.netframework\policy\v2.0
                                        HKLM\software\microsoft\.netframework
  Opens kev:
  Opens key:
                                        HKLM\software\microsoft\.netframework\policy\upgrades
  Opens key:
                                        HKLM\software\microsoft\.netframework\policy\standards
  Opens key:
                                        HKLM\software\microsoft\.netframework\policy\apppatch
  Opens key:
                                        HKLM\system\currentcontrolset\control\error message instrument\
                                        HKLM\system\currentcontrolset\control\error message instrument
  Opens key:
   Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\gre initialize
  Opens key:
                                        \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\- current version\+ compatibility 32
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\windows
   Opens key:
                                        \label{lem:hkcu} \verb+KCU\+ software\+ microsoft\+ .net framework\+ policy\+ standards
  Opens key:
                                        HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727
  Opens key:
```

HKLM\software\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\microsoft\windows nt\currentversion\image file execution

options Opens key:

HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets

Opens key

 $\label{thm:local_hammon} HKLM \software \microsoft \. net framework \security \policy \extensions \named permission sets \cite{local_hammon_$

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus profile list \setminus s-1-5-21-1000 + (-1) \cdot (-1)$ 2160590473-689474908-1361669368-1002

Opens key:

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
        Opens key:
                                                                                                                HKLM\software\microsoft\ole
         Opens key:
                                                                                                                 HKLM\software\microsoft\ole\tracing
       Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
 a03a-e3ef65729f3d}
         Opens key:
a03a-e3ef65729f3d}\propertybag
                                                                                                                HKCU\software\microsoft\windows\currentversion\explorer
        Opens kev:
        Opens key:
                                                                                                                HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
        Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follown folders
        Opens key:
                                                                                                                HKCU\software\microsoft\windows\currentversion\explorer\user shell
  folders
        Opens key:
                                                                                                                HKLM\system\currentcontrolset\control\nls\customlocale
        Opens key:
                                                                                                                HKLM\system\currentcontrolset\control\nls\extendedlocale
        Opens key:
                                                                                                                HKLM\software\policies\microsoft\windows\explorer
        Opens key:
                                                                                                                HKCU\software\policies\microsoft\windows\explorer
        Opens key:
9afe-ea3317b67173}
        Opens key:
9afe-ea3317b67173}\propertybag
        Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
        Opens key:
                                                                                                                HKLM\software\microsoft\.netframework\v2.0.50727\security\policy
        Opens key:
                                                                                                                HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32
        Opens key:
                                                                                                                HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index145
         Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus ni \setminus 181938c6 \setminus 7950e2c5
       Opens kev:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 181938c6 \ 7950e2c5 \ 890 \ next \ ne
        Opens key:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ il\ 7950e2c5 \ 183e33de \ 189e3de \ 
        Opens key:
ba85-6007caedcf9d}
       Opens kev:
ba85-6007caedcf9d}\propertybag
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\4846a846\3ed6137e
                                                                                                                HKLM\software\microsoft\net framework setup\dotnetclient\v3.5
       Opens key:
                                                                                                                 HKLM\software\microsoft\strongname
        Opens key:
        Opens key:
                                                                                                                HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus 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 \ native images in dex \ v2.0.50727\_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 83 \ new \ ne
        Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ i1 \ 6dc7d4c0 \ a5cd4db \ 86dc7d4c0 \ a5cd4db \
        Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 8f60fe4f \ 1000fe4f \ 1000
       Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d
         Opens key:
Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 3f50fe4f \ 6f1da7aa \ 8f1da7aa \ 8f1da7aa \ 8f2da7aa \ 8f2da7aaa \ 8f2da7aa \ 8f2d
        Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. system \underline{\quad b77a5c561934e089}
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. system. \ xml\_b77a5c561934e089
       Opens key:
HKLM \label{likelihood} No ftware \mbox{\tt icrosoft} fusion \mbox{\tt ublisherpolicy} \mbox{\tt default} \mbox{\tt policy}. 2.0. system. configuration\_b03f5f7f11d50a3a
        Opens key:
                                                                                                                HKLM\software\microsoft\.netframework\policy\aptca
        Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.windows.forms__b77a5c561934e089
        Opens key:
Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i \setminus 61e7e666 \setminus c991064 \setminus 82e82 \setminus 61e7e666 \setminus c991064 \setminus 61e7e6666 \setminus c991064 \setminus 61e7e666 \setminus c991064 \setminus 61e7e6666 \setminus c991064 \setminus 61e7e666 \setminus c991066 \setminus c991
        Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c
       Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\il\2dd6ac50\163e1f5e\88
       Opens key:
Opens key:
 Opens key:
Opens key:
```

 $HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. system. deployment \underline{\quad b03f5f7f11d50a3a}$

```
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\78
```

Opens key:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\35249b34\531d6b08\78

HKLM\SOTTWare\microsoft\tusion\nativeimagesindex\v2.0.50/2/_32\ii\3b249b34\531d6b08\/8 Opens key:

 $\label{thm:hklm:software} $$HKLM \circ ftware \end{thm:} A $$HkLM \circ ftware \end{thm:} A $$1.3a6a696d \end{thm:} A $$0.50727_32 \end{thm:} A $$0.50727_$

 $\label{lem:hklm} $HKLM \sim \max_{i=1}^{10} \frac{1}{6e8397} 46ad0879 \\ \ Opens \ key:$

 $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727_32 \sinladd 590 c3f \sion \native images in dex \normalized 2.0.50727_32 \sinladd 590 c3f \sion \native images in dex \normalized 2.0.50727_32 \sinladd 590 c3f \sion \normalized 596 c3f \sion \normalized 2.0.50727_32 \sinladd 590 c3f \sion \normalized 596 c3f \sion \normalized 596 c3f \sion \normalized 2.0.50727_32 \sion \normalized 1.0.50727_32 \sion \normali$

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\4c239d82\79

Opens key:

 $\label{lem:hklmsoftware} HKLM \software \mbox{\m

 $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} in $\mathbb{Z}_0.$ system. runtime. remoting $\underline{\mbox{$\mathbb{Z}_0.$} b77a5c561934e089}$ Opens key:$

HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.directoryservices__b03f5f7f11d50a3a
 Opens key:

Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility

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\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKLM\software\microsoft\windows

 $\verb|nt| urrentversion| appcompatflags | ustom| 476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe| exemple | usersion| exemple |$

Opens key: HKLM\system\currentcontrolset\control\terminal server

Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

Queries value:

 $\label{lem:hklm} \verb+KLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]$

Queries value: HKLM\system\currentcontrol\session manager[safedllsearchmode]

Queries value: HKCU\control panel\desktop[preferreduilanguages]

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Queries value:

Queries value: HKLM\software\microsoft\.netframework[onlyuselatestclr]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\.netframework[gcstressstart]
Queries value: HKLM\software\microsoft\.netframework[gcstressstartatjit]
Queries value: HKLM\software\microsoft\.netframework[disableconfigcache]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-

931b-d9cc2eee27e41

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]
Oueries 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:

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[name]$

Queries value:

a03a-e3ef65729f3d}[parentfolder]

Queries value:

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \footnote{Action} \cal{lem:hklmsoftware} \cal{lem:$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} a03a-e3ef65729f3d \cal{lem:hklmsoftware} [parsing name]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\mbox{\mbox{1}} eb685db-65f9-4cf6-a03a-e3ef65729f3d} [infotip]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \called 3eb685db-65f9-4cf6-a03a-e3ef65729f3d \called [localized name]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\[icon]$

Queries value:

Oueries value:

 $\label{lem:hklm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklm} a03a-e3ef65729f3d \footnote{a03a-e3ef65729f3d} \cal{lem:hklm} [stream resource]$

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \ensuremath{\mbox{\mbox{1}} eb685db-65f9-4cf6-a03a-e3ef65729f3d} \label{localredirectonly} I coalredirectonly \ensuremath{\mbox{2}} eb685db-65f9-4cf6-a03a-e3ef65729f3d \ensuremath{\mbox{2}} eb685db-$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [roamable]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \cal{lem:hklmsoftware} \ a03a-e3ef65729f3d \cal{lem:hklmsoftware} \cal{lem:hklmsoftware} \label{lem:hklmsoftware}$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]$

Queries value:

 $\label{lem:hklmsoftware} HkLM \software \ensuremath{\sc Number \sc Number \$

Queries value:

Queries value:

 $\label{thm:hklm} HKL^{M} software \ensuremath{\mbox{\mbox{1}} eb685db-65f9-4cf6-a03a-e3ef65729f3d} [foldertypeid]$

Oueries value:

 $\label{thm:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\ex$

 $Queries \ value: \\ HKCU \ software \ microsoft \ windows \ current version \ (explorer \ shell) \\$

folders[appdata]

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Oueries value:

Queries value:

 $\label{lem:hkkm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \folder$

Queries value:

Queries value

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]

Queries value:

 $\label{thm:local-condition} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{5}e6c858f-0e22-4760-9afe-ea3317b67173\footnote{1}{7}[relative path]$

Queries value

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \ensuremath{\mbox{\currentversion}\explorer \folder descriptions} \ensuremath{\mbox{\currentversion}\explorer \folder descriptions} \ensuremath{\mbox{\currentversion}\explorer \folder descriptions} \ensuremath{\mbox{\currentversion}\explorer \folder descriptions} \ensuremath{\mbox{\currentversion}\explorer \folder \folder\folder \folder \folder \folder \folder \folder \folder \folder \$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [localized name]$

Queries value:

Queries value:

 $\label{thm:microsoftwindows} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \folder \fol$

Oueries value:

 $HKLM \label{lem:hklm} Which is the latest and the$

9afe-ea3317b67173}[streamresource] Oueries value: 9afe-ea3317b67173}[streamresourcetype] Oueries value: $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-164e7descriptions\} \ for the software \ microsoft \ windows \ for the software \ microsoft \ micr$ 9afe-ea3317b67173}[localredirectonly] Queries value: 9afe-ea3317b67173}[roamable] Oueries value: 9afe-ea3317b67173}[precreate] Queries value: 9afe-ea3317b67173}[stream] Oueries value: 9afe-ea3317b67173}[publishexpandedpath] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes] Oueries value: 9afe-ea3317b67173}[foldertypeid] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler] Oueries value: $\label{lem:hklm} \mbox{ HKLM} \mbox{ hicrosoft} \mbox{ windows nt} \mbox{ currentversion} \mbox{ profilelist} \mbox{ s-1-5-21-1} \mbox{ of tware} \mbox{ windows nt} \mbox{ currentversion} \mbox{ profilelist} \mbox{ software} \mbox{ of tware} \mbox{ of tware}$ 2160590473-689474908-1361669368-1002[profileimagepath] Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex] Oueries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus index 145 [nius agemask]$ Queries value: $HKLM \verb|\software\microsoft\fusion\native images index \verb|\v2.0.50727_32\ndex 145[ilus age mask]| \\$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus 89[displayname]$ Oueries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[configmask] Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 89[configstring]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 89[mvid]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 89 \ [evalation data]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 89[status]$ Oueries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[ildependencies] Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[nidependencies] $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i181938c6 \setminus 7950e2c5 \setminus 89[missing dependencies]$ Oueries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\89[displayname] Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 7950e2c5 \ 183e33de \ 89[status]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i1 \setminus 7950e2c5 \setminus 183e33 de \setminus 89[modules]$ Oueries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\89[sig] Oueries value: $\label{local-hamma} HKLM \setminus software \setminus introsoft \setminus fusion \setminus introsoft \setminus introsoft \setminus fusion \setminus introsoft \setminus introsoft \setminus fusion \setminus introsoft \setminus$ Queries value: Queries value: ba85-6007caedcf9d}[category] Oueries value: ba85-6007caedcf9d}[name] Queries value: ba85-6007caedcf9d}[parentfolder] Oueries value: ba85-6007caedcf9d}[description] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251ba85-6007caedcf9d}[relativepath] Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]
Queries value:

ba85-6007caedcf9d}[parsingname]

Oueries value:

```
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localizedname]
  Queries value:
ba85-6007caedcf9d}[icon]
  Queries value:
ba85-6007caedcf9d}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[streamresource]
  Oueries value:
ba85-6007caedcf9d}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localredirectonly]
  Oueries value:
ba85-6007caedcf9d}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[stream]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[publishexpandedpath]
ba85-6007caedcf9d}[attributes]
  Oueries value:
ba85-6007caedcf9d}[foldertypeid]
  Queries value:
ba85-6007 caedcf9d \} [init folder handler] \\
                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[cache]
  Queries value:
                                   HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default[latest]
  Queries value:
                                   HKLM\software\microsoft\fusion\publisherpolicy\default[index4]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default[legacypolicy timestamp]
  Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca 06a0 \ 6dc 7d4c0 \ 83 \ [display name]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[configmask]
  Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[mvid]
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[evalationdata]
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus mi \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 83[status]
  Oueries value:
HKLM \label{lem:hklm} Software \mbox{\sc a06a0\6dc7d4c0\83[ildependencies]} \\
  Queries value:
\label{localization} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \ni\3cca06a0 \6dc7d4c0 \83[nidependencies]
  Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 83 \ [missing dependencies]
  Oueries value:
Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ i1 \ 6dc7d4c0 \ a5cd4db \ 86[status]
  Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 6dc7d4c0\ a5cd4db\ 86[modules]
  Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ i1\ 6dc7d4c0\ a5cd4db \ 86 \ [sig] \ microsoft 
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i1 \setminus 6dc7d4c0 \setminus a5cd4db \setminus 86[last modtime]
  Queries value:
Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[configmask]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i \setminus 30bc7c4f \setminus 3f50fe4f \setminus 8f[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\ni\30bc7c4f\3f50fe4f\8f[mvid]
  Oueries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 8f[evalation data]
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 30bc7c4f \setminus 3f50fe4f \setminus 8f[status]
  Queries value:
```

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 30bc7c4f \ 8f[ildependencies]$

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 8f[nidependencies]$

Oueries value:

Queries value:

- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[missingdependencies]
 Queries value:
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-equation} HKLM \software \end{array} HKLM \software \end{array} All \end{array}$
- $\label{lem:hklmsoftware} HkLM \software \end{array} Hklm \software \end{array} 1 \software \end{arra$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d[sig]
 Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d[lastmodtime]
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\8e[displayname]
 Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\19ab8d57\1bd7b0d8\8e[status]
 Oueries value:
- $\label{local-observation} HKLM \software \since \$
- $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} in a tive images in dex.} $$2.0.50727_32 \il\19ab8d57\1bd7b0d8\8e[sig] $$Oueries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\8e[lastmodtime]
 Oueries value:
- $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f[displayname] Queries\ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f[status]
 Oueries value:
- $\label{local-operator} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_32\label{local-operator} 13750 fe4f\6f1 da7aa\8f[modules] Queries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f[sig]
 Oueries value:
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- 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]
 Oueries value:
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
 Oueries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Significant \label{lem:hklm} White \label{lem:hkklm} White$
- $\label{lem:hklmsoftware} HkLM \software \slices value: 0.50727_32 \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[configmask]
 Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \mbox{$\mbox{$\mbox{\sim}} 1.50727_32 \mbox{$\mbox{$\sim$}} 1.61e7e666 \c991064 \sold 2[configstring] } Queries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[mvid]
 Oueries value:
- $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727_32\ni\61e7e666\c991064\82\end{2} [evalation data] Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \v2.0.50727_32 \ni\61e7e666 \c991064 \82[status] \\ Queries \value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[ildependencies]
 Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[nidependencies]
 Oueries value:
- $\label{lem:hklm} \begin{tabular}{ll} HKLM\software\microsoft\fusion\native images in dex\v2.0.50727_32\ni\61e7e666\c991064\82[missing dependencies] \\ Oueries\ value: \begin{tabular}{ll} Color of the color of the$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\475dce40\2d382ce6\8c[displayname]
 Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c[status]
- $Queries\ value: \\ HKLM\ voftware\ microsoft\ fusion\ native\ images in dex\ v2.0.50727_32\ il\ 475dce 40\ 2d382ce 6\ 8c[modules]$
- Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c[sig] Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c[lastmodtime]
 Oueries value:
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\slash\sla$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727_32 \normalized 163e1f5e \normalized 88[status] Oueries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\88[modules]
 Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\88[sig]
 Oueries value:
- $\label{thm:local_ham} HKLM \software \mbox{\sim 1.50727_32\il\2dd6ac50\163e1f5e\88[last mod time] } Queries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\80[displayname]
 Queries value:
- $\label{local-prop} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_32 \il\41c04c7e\7f3b6ac4\80[status] \\ Queries \value:$
- $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex $$v2.0.50727_32\il\41c04c7e\7f3b6ac4\80[modules]$$ Queries value:$
- $\label{lem:hklm} HKLM \software \microsoft \subseted in the lambda subseted in the lambda$

```
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84[displayname]
 Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 3ced59c5 \ 1b2590b1 \ 84[status]
 Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84[sig]
```

- Queries value: $HKLM \ software \ |\ microsoft \ fusion \ |\ mative images in dex \ |\ v2.0.50727_32 \ |\ 11\ 3ced59c5 \ |\ 162590b1 \ |\ 84[last mod time]$
- Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ c991064 \ 2bd33e1c \ 81[displayname]$
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ c991064 \ 2bd33e1c \ 81[status]$ Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\81[modules] Oueries value:
- $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i1 \setminus c991064 \setminus 2bd33e1c \setminus 81[sig]$
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ c991064 \ 2bd33e1c \ 81[last mod time]$ Queries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} in \label{lem:hklm} Software \label{lem:hklm} his constant \label{lem:hklm} his constant \label{lem:hklm} Software \label{lem:hklm} his constant \label{lem:hklm} his constant \label{lem:hklm} Software \label{lem:hklm} his constant \label{lem:hkklm} his constant \label{lkklm} his consta$ Oueries value:
- $HKLM \setminus software \setminus microsoft \setminus fusion \setminus gacchange notification \setminus default [system.deployment, 2.0.0.0, , b03f5f7f11d50a3a, msil] + (2.0.0.0, b03f5f7f11d50a3a, msil) + (2.0.0.0, b03f5f11d50a3a, msil) + (2.0.0.0, b03f11d50a3a, msil) + (2.0.0.0, b03f1d50a3a, msil) + (2.0.0.0, b03f1d50aa, msil) + (2.0.0.0, b03f1d50aa, msil) + (2.0.0.0, b03f1d5$ Queries value:
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.serialization.formatters.soap,2.0.0.0,,b03f5f7f11d50a3a,msil] Oueries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lkklm} White \label{lkklm} White \label{lkklm} White \label{lkklm} White \label{lkklm} White$ Oueries value:
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil] Queries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 57d4b1bf \ 85e83df \ 78[display name]$ Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 57d4b1bf \ 85e83df \ 78[configmask]$ Queries value:
- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ ni \ 57d4b1bf \ 85e83df \ 78[configstring]$ Queries value:
- $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus mi \setminus 57d4b1bf \setminus 85e83df \setminus 78[mvid]$ Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 57d4b1bf \ 85e83df \ 78[evalation data]$ Queries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 57d4b1bf \ 85e83df \ 78[status]$ Queries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 57d4b1bf \ 85e83df \ 78[ildependencies]$ Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 57d4b1bf \ 85e83df \ 78[nidependencies]$ Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ ni \ 57d4b1bf \ 85e83df \ 78[missing dependencies]$ Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\78[displayname] Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\78[status] Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\78[modules] Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\531d6b08\78[sig] Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ il\ 3b249b34 \ 531d6b08 \ 78[last mod time]$ Queries value:
- Oueries value:
- $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i1 \setminus 3a6a696d \setminus 52d7076e \setminus 7a[status]$ Oueries value:
- $\label{local-hamilton} HKLM \software \mbox{\sc microsoft} fusion \native images index \norm{\sc v2.0.50727_32\ll} \ada6960 \sc v2760 \norm{\sc v2.0.50727_32\ll} \ada6960 \sc v2760 \norm{\sc v2.0.50727_32\ll} \ada6960 \norm{\sc v2.0.50727_32\ll} \norm{$ Queries value:
- $\label{local-prop} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_32\il\3a6a696d\52d7076e\7a[sig] \end{substrate}$ Queries value:
- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727_32 \ i1 \ 3a6a696d \ 52d7076e \ 7a[last mod time]$ Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ f6e8397 \ 46ad0879 \ 77 [display name]$ Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ f6e8397 \ 46ad0879 \ 77[status]$ Queries value:
- $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus f6e8397 \setminus 46ad0879 \setminus 7f[modules]$ Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\46ad0879\77[sig] Oueries value:
- $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i1 \setminus f6e8397 \setminus 46ad0879 \setminus 77[last mod time]$ Queries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\il\3d590c3f\59f3b67b\90[displayname] Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ i1\ 3d590c3f \ 59f3b67b \ 90[status]$ Oueries value:
- $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 3d590c3f \setminus 59f3b67b \setminus 90[modules]$ Queries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3d590c3f\ 59f3b67b\ 90[sig]$ Oueries value:
- $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3d590c3f\ 59f3b67b\ 90[last mod time]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \subseted in the lambda subseted and the lambda subseted and$

 $\label{thm:hkm} \begin{tabular}{ll} HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\4c239d82\79[status] \\ Oueries\value: \begin{tabular}{ll} Oueries\value: \begin{$

 $\label{local-bound} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727_32 \normalized 185e83 \normalized 4c239 \normalized 4c239 \normalized 85e83 \normalized 185e83 \normalized 4c239 \normalized 85e83 \normalized 185e83 \normalized$

 $\label{lem:hklmsoftware} HKLM \software \subseted in the linear law subseted and the linear law subseted and the linear law subseted as a linear$

HKLM\software\microsoft\fusion\gacchangenotification\default[system.enterpriseservices, 2.0.0.0, ,b03f5f7f11d50a3a, x86]
Oueries value:

 $\label{lem:hkm} \begin{tabular}{ll} HKLM\software\mbox{\setminusmicrosoft.visualc,8.0.0.0,$,b03f5f7f11d50a3a,msil]} \\ Oueries\ value: \begin{tabular}{ll} Oueries\ value: \begin{t$

HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.remoting,2.0.0.0,,b77a5c561934e089,msil]
Oueries value:

HKLM\software\microsoft\fusion\gacchangenotification\default[system.directoryservices,2.0.0.0,,b03f5f7f11d50a3a,msil] Oueries value:

HKLM\software\microsoft\fusion\gacchangenotification\default[system.transactions,2.0.0.0,,b77a5c561934e089,x86] Oueries value:

 $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]|$

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]