# Malware Analysis Appliance by Blue Coat Systems, Inc.

### Task Details

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

Task ID: 2420 Risk Level:

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: 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

476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4 SHA256

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

\KernelObjects\LowMemoryCondition Creates event:

## File System Events

C:\Users\Admin

Creates: C:\Users\Admin\AppData\Roaming

C:\Windows\Prefetch\476FC456C66CBEC138E3DAB72A0F0-C3D55795.pf Opens:

Opens: C:\Windows

C:\Windows\System32\wow64.dll Opens: C:\Windows\System32\wow64win.dll Opens: Opens: C:\Windows\System32\wow64cpu.dll Opens: C:\Windows\system32\wow64log.dll

C:\Windows\SysWOW64 Opens:

Opens: C:\Windows\SysWOW64\mscoree.dll C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\MSCOREE.DLL.local Opens:

Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727 C:\Windows\Microsoft.NET\Framework\Upgrades.2.0.50727\ Opens:

C:\Windows\SysWOW64\imm32.dll

Opens:

Opens:

C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.config

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

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

C:\Windows\winsxs\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.4940\_none\_d08cc06a442b34fc

C:\Windows\winsxs\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.4940\_none\_d08cc06a442b34fc\msvcr80.dll Opens:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac Opens: Opens:  $\label{lem:c:windows} $$ 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:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch Opens:  ${\tt C:\Windows\Globalization\Sorting\SortDefault.nls}$ 

C:\windows\temp\profapi.dll Opens: C:\Windows\SysWOW64\profapi.dll Opens:

Opens: C:\Users\Admin

C:\Users\Admin\AppData\Roaming Opens:

 ${\tt C:\Users\Admin\AppData\Roaming\Microsoft\CLR\ Security}$ Opens:

Config\v2.0.50727.312\security.config

```
C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
   Opens:
Config\v2.0.50727.312\security.config.cch
                                             C:\Windows\assembly\NativeImages_v2.0.50727_32\index127.dat
   Opens:
   Opens:
Opens:
                                             C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089
   Opens:
                                             C:\Windows\Temp
                                             C:\Windows\SysWOW64\l_intl.nls
   Opens:
   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: \verb|Windows \assembly \ative Images_v2.0.50727_32 \system \ 9e0a3b9b9f457233a335d7fba8f95419 \system.ni.dll \ ative Images_v2.0.50727_32 \system \ ative Ima
   Opens:
C: \verb|Windows| assembly \verb|NativeImages_v2.0.50727_32| System.Drawing \verb|\dbfe8642a8ed7b2b103ad28e0c96418a| System.Drawing.ni.dll | System.Drawing.ni.d
                                              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 \Native Images\_v2.0.50727\_32 \system. \windows. Forms \afcd 5168c7a6cb02eab99d7fd71e102 \system. \windows. Forms. \ni.dll
   Opens:
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089
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
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2812.72359
                                             C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
  Opens:
Config\v2.0.50727.312\security.config.cch.2812.72359
   Reads from:
                                             C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Windows Registry Events
   Creates key:
                                             HKLM \backslash software \backslash microsoft \backslash fusion \backslash gacchange notification \backslash 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:
                                             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
                                             HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
   Opens kev:
   Opens kev:
                                             HKLM\svstem\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\svstem\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
                                             HKLM\
   Opens key:
                                             HKLM\software\wow6432node\microsoft\windows
   Opens key:
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\policv\upgrades
                                             HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| .netframework\\| policy\\| standards
   Opens key:
   Opens key:
                                             Opens key:
                                             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens kev:
                                             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
                                             HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
   Opens key:
compatibility
                                             HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
   Opens key:
   Opens key:
                                             HKCU\software\microsoft\.netframework\policy\standards
```

Opens key:

```
\label{local-condition} HKLM \software \wow 6432 node \microsoft \. net framework \policy \standards \v2.0.50727 \end{tikzpicture}
            Opens key:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus side \\ by side \setminus assembly \\ storage \\ roots
                                                                                                                                                                                  HKCU\software\microsoft\.netframework
            Opens kev:
            Opens key:
                                                                                                                                                                                  HKLM\software\microsoft\fusion
           Opens key:
                                                                                                                                                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
 options\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
            Opens key:
                                                                                                                                                                                  HKCU\software\microsoft\fusion
            Opens key:
HKLM \label{lem:hklm} Wow 6432 node \verb|\microsoft|.net framework \| security \verb|\policy| extensions \| named permission sets \| security \
           Opens key:
HKLM \ software \ wow 6432 node \ internet \ curity \ policy \ extensions \ named permission sets \ internet \ named \ permission \ n
             Opens kev
 HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus .net framework \setminus security \setminus policy \setminus extensions \setminus nemed permission sets \setminus local intranet \setminus policy \setminus extensions \setminus nemed permission sets \setminus local intranet \setminus policy \setminus extension sets \setminus policy \setminus p
                                                                                                                                                                                  HKLM\software\wow6432node\microsoft\windows
           Opens key:
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
            Opens key:
                                                                                                                                                                                  980053277-1733835069-2361817685-1001
             Opens key:
 HKLM\software\wow6432node\microsoft\ole
            Opens key:
            Opens key:
                                                                                                                                                                                  HKLM\software\wow6432node\microsoft\ole\tracing
            Opens key:
                                                                                                                                                                                  HKLM\software\microsoft\ole\tracing
            Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde
 65f9-4cf6-a03a-e3ef65729f3d}
            Opens kev
HKLM \label{lem:hklm} Software \label{lem:hklm} Which is the last of the las
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
            Opens key:
                                                                                                                                                                                  HKCU\software\microsoft\windows\currentversion\explorer
             Opens key:
                                                                                                                                                                                   HKCU \ software \ `microsoft\ `windows\ `current version\ `explorer\ `session info\ `1" \ info\ `1" 
            Opens key:
 HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
                                                                                                                                                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
            Opens key:
  folders
            Opens key:
                                                                                                                                                                                  HKLM \verb|\system| current controlset \verb|\control| nls \verb|\extended| locale
                                                                                                                                                                                  \label{local-bound} \mbox{HKLM} \mbox{$\mbox{$N$} irrosoft\windows} \mbox{$\mbox{$\mbox{$explorer$}$} \mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$explorer$}$}$} \mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$c$}$} irrosoft\windows} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbo
            Opens key:
            Opens key:
                                                                                                                                                                                  HKLM\software\policies\microsoft\windows\explorer
            Opens kev:
                                                                                                                                                                                  HKCU\software\policies\microsoft\windows\explorer
            Opens key:
0e22-4760-9afe-ea3317b67173}
             Opens key:
0e22-4760-9afe-ea3317b67173}\propertybag
            Opens key
HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| \verb|\windows| current version \verb|\explorer| known folders ettings | leaves to the second of th
             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 \ native images index \ 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 \ native images index \ v2.0.50727\_32 \ il\ 7950e2c5 \ 183e33de \ 183e3de \ 1
           Opens key:
 HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}
            Opens key:
33be-4251-ba85-6007caedcf9d}\propertybag
            Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 4846a846 \ 3ed6137ed \ normalised \ no
                                                                                                                                                                                  HKLM\software\wow6432node\microsoft\strongname
             Opens key:
            Opens key:
                                                                                                                                                                                  HKLM\software\microsoft\fusion\publisherpolicy\default
            Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. system. drawing \underline{\quad} b03f5f7f11d50a3a
            Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus ni \setminus 3cca06a0 \setminus 6dc7d4c0
            Opens key:
 HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ ii \ 3cca06a0 \ 6dc7d4c0 \ 7bca06a0 \ decaded 
           Opens key:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 6dc7d4c0\ a5cd4db\ 7ee
            Opens kev
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 88ex \ new \ n
            Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\86
           Opens key:
HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ i1 \ 19ab8d57 \ 1bd7b0d8 \ 87abb \ 10bb \
           Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\88
             Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default \setminus policy. 2.0. system \underline{\quad b77a5c561934e089}
```

HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.xml\_\_b77a5c561934e089

Opens kev:

Opens key:

```
HKLM \label{lem:hklm} Which is a full that the limit of the limit of
          Opens key:
                                                                                                                                            HKLM\software\wow6432node\microsoft\.netframework\policy\aptca
           Opens key:
 HKLM \backslash software \backslash microsoft \backslash fusion \backslash publisher policy \backslash default \backslash policy. 2.0. system. \\ windows. forms \underline{\ \ \ } b77a5c561934e089
         Opens key:
  HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064
           Opens key:
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\85
         Opens key:
 HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i1 \setminus 2dd6ac50 \setminus 163e1f5e \setminus 80.0126 \setminus 1000 \setminus 10000 \setminus 1000 \setminus 1000
  HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i1 \setminus 41c04c7e \setminus 753b6ac4 \setminus 783b6ac4 \setminus 783b
         Opens key:
  HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\7c
          Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il \ c991064 \ 2bd33e1c \ 7991064 \ 2bd34e1c \ 7991064 \
           Opens key:
 HKLM \backslash software \backslash microsoft \backslash fusion \backslash publisher policy \backslash default \backslash policy. 2.0. system. deployment \underline{~~}b03f5f7f11d50a3a
         Opens key:
 HKLM \label{lem:hklm} Which is the policy \label{lem:hklm} Which is the policy \label{lem:hklm} Which is the policy \label{lem:hklm}. So it is the policy \label{lem:hklm} Which is the policy \label{lem:hklm} Which is the policy \label{lem:hklm}. Which is the policy \label{lem:hklm} Which is the policy \label{lem:hklm} Which is the policy \label{lem:hklm}. Which is the policy \label{lem:hklm} Which is the policy \label{lem:hklm}. Which is the policy \label{lem:hklm} Which is the policy \label{lem:hkklm} Which is the policy 
          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 kev
 Opens key:
  HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df
          Opens key:
 HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 57d4b1bf \ 85e83df \ 70d4b1bf \ 70d4b1bf \ 85e83df \ 70d4b1bf \ 85e83df \ 70d4b1bf \ 70d4b1bf
         Opens kev:
 Opens key:
 HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ il\ 3a6a696d \ 52d7076e \ 72d10 \ and \ 
          Opens key:
 HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i1 \setminus f6e8397 \setminus 46ad0879 \setminus f6e8397 \setminus f
         Opens kev
  HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\59f3b67b\82
          Opens key:
 HKLM \ software \ microsoft. fusion \ publisher policy \ default \ policy. 8.0. microsoft. visual \ c\_b03f5f7f11d50a3a
         Opens key:
 HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 2.0. system. runtime. remoting \underline{\ \ } 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
                                                                                                                                            HKLM\system\currentcontrolset\control\session manager\appcertdlls
          Opens key:
          Opens key:
                                                                                                                                            HKLM\system\currentcontrolset\control\session manager\appcompatibility
          Opens key:
                                                                                                                                              HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| windows\\| appcompat
          Opens key:
                                                                                                                                            HKLM\software\policies\microsoft\windows\appcompat
          Opens kev:
                                                                                                                                              HKCU\software\microsoft\windows nt\currentversion
          Opens key:
                                                                                                                                            HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
         Opens kev:
                                                                                                                                           HKLM\software\wow6432node\microsoft\windows
  nt\currentversion\appcompatflags
          Opens key:
                                                                                                                                           HKLM\software\wow6432node\microsoft\windows
 \verb|nt\currentversion| appcompatflags \land 476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe| application of the first 
          Opens key:
                                                                                                                                            HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
  execution options\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
                                                                                                                                           HKLM\svstem\currentcontrolset\control\terminal server
          Opens kev:
          Oueries value:
                                                                                                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
  options[disableusermodecallbackfilter]
                                                                                                                                            HKLM\system\currentcontrolset\control\session
           Queries value:
 manager[cwdillegalindllsearch]
                                                                                                                                           HKLM\system\currentcontrolset\control\nls\sorting\versions[]
           Queries value:
           Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
           Oueries value:
                                                                                                                                            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                                                                                                                            HKLM\system\currentcontrolset\control\nls\customlocale[empty]
           Queries value:
           Queries value:
 Oueries value:
                                                                                                                                            HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
          Oueries 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 \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]
           Queries value:
                                                                                                                                            HKLM\software\wow6432node\microsoft\.netframework[installroot]
           Oueries value:
                                                                                                                                            HKLM\software\wow6432node\microsoft\.netframework[clrloadlogdir]
           Queries value:
                                                                                                                                            HKLM\software\wow6432node\microsoft\.netframework[onlyuselatestclr]
           Oueries value:
                                                                                                                                            HKLM\software\microsoft\windows
 \verb|nt\currentversion\gre_initialize[disablemetafiles]|\\
                                                                                                                                            HKLM\software\wow6432node\microsoft\windows
          Oueries value:
```

 $nt \verb| current version \verb| compatibility 32[476fc 456c 66c bec 138e 3dab 72a0f0 e 54f2 0 3db f27ce 88736b 1893b 668b ce 63c4]|$ 

HKLM\software\wow6432node\microsoft\windows Queries value:

nt\currentversion\windows[loadappinit\_dlls]

HKLM\software\wow6432node\microsoft\.netframework[gcstressstart] Queries value: HKLM\software\wow6432node\microsoft\.netframework[gcstressstartatiit] Oueries value: Oueries 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]

Oueries value: HKLM\software\microsoft\fusion[cachelocation]

Oueries value: HKLM\software\microsoft\fusion[downloadcachequotainkb]

Oueries value: HKLM\software\microsoft\fusion[enablelog] HKLM\software\microsoft\fusion[logginglevel] Oueries value: Queries value: HKLM\software\microsoft\fusion[forcelog] Queries value: HKLM\software\microsoft\fusion[logfailures] Oueries value: HKLM\software\microsoft\fusion[versioninglog] Oueries value: HKLM\software\microsoft\fusion[logresourcebinds] Oueries value: HKLM\software\microsoft\fusion[uselegacyidentityformat] HKLM\software\microsoft\fusion[disablemsipeek] Queries value: HKLM\software\microsoft\fusion[noclientchecks] Queries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[devoverrideenable]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$ 

65f9-4cf6-a03a-e3ef65729f3d}[category] Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[name] Queries value: 

65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]

Oueries value: 

65f9-4cf6-a03a-e3ef65729f3d}[description]

65f9-4cf6-a03a-e3ef65729f3d}[relativepath]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$ 65f9-4cf6-a03a-e3ef65729f3d}[parsingname]

65f9-4cf6-a03a-e3ef65729f3d}[infotip]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$ 65f9-4cf6-a03a-e3ef65729f3d}[localizedname]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10ex, 10ex, 1$ 65f9-4cf6-a03a-e3ef65729f3d}[icon]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$ 65f9-4cf6-a03a-e3ef65729f3d}[security]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[streamresource]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[roamable]

Queries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-16422 \\ node \setminus \{3eb68$ 65f9-4cf6-a03a-e3ef65729f3d}[precreate]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[stream]

Queries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-16422 \\ node \setminus \{3eb68$ 65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]

Oueries value:

65f9-4cf6-a03a-e3ef65729f3d}[attributes]

Queries value:

65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

HKCU\software\microsoft\windows\currentversion\explorer\user shell Queries value:

folders[appdata]

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

Oueries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$ 

Queries value:

Oueries value:

 $\label{thm:local-problem} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \cite{thm:local-particle} folder \cite{thm:local-particle} folde$ 

Oueries value

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [parsing name]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [infotip]$ 

Oueries value:

 $\label{localized-microsoft-windows} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folde$ 

Oueries value

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \cite{thm:local-particle} folder \$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [stream resource]$ 

Oueries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \f$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdesc$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \colone \co$ 

Queries value:

 $\label{thm:local-problem} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \current \folder \$ 

Queries value:

 $\label{thm:local-problem} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folder$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [folder type id]$ 

Queries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$ 

 $\label{lem:profile} Queries \ value: \\ HKLM\ software \ microsoft\ windows \ nt\ current version\ profile list\ s-1-5-21-980053277-1733835069-2361817685-1001 [profile image path]$ 

Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32[latestindex]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus index 127 [nius agemask]$ 

Queries value:

 $\label{lem:hklm} \begin{tabular}{ll} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \index 127 [ilus age mask] \end{tabular}$ 

Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\181938c6\7950e2c5\83[displayname]
Queries value:

 $\label{local-bound} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \ni\181938c6 \7950e2c5 \83 [configmask] Queries value:$ 

 $\label{lem:hklm} HkLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \ni\181938c6 \7950e2c5 \83 \mbox{[mvid]} \\ Oueries \value:$ 

 $\label{lem:hklmsoftware} HKLM \software \since \s$ 

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\181938c6\7950e2c5\83[status]
Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \mbox{$\le$ 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]
Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\7950e2c5\183e33de\83[status] Queries value:

Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\7950e2c5\183e33de\83[sig]

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus i1 \setminus 7950e2c5 \setminus 183e33de \setminus 83[last modtime]$ Queries value:

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

33be-4251-ba85-6007caedcf9d}[category]

Queries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{352481e8-1641e1\} \\ note that the first of the$ 33be-4251-ba85-6007caedcf9d}[name]

Oueries value:

33be-4251-ba85-6007caedcf9d}[parentfolder]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8- $33 be-4251-ba85-6007 caedcf9d \} \texttt{[description]}$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-1644444 \ explorer \ folder \ explorer \ \ \}$ 33be-4251-ba85-6007caedcf9d}[relativepath]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-164444944, \ node \ node \ node \ \ \}$ 33be-4251-ba85-6007caedcf9d}[parsingname]

Queries value:

33be-4251-ba85-6007caedcf9d}[infotip]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]

Queries value:

33be-4251-ba85-6007caedcf9d}[icon]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-164444944, \ node \ node \ node \ \ \}$ 33be-4251-ba85-6007caedcf9d}[streamresource]

Queries value:

33be-4251-ba85-6007caedcf9d}[streamresourcetype]

Oueries value:

33be-4251-ba85-6007caedcf9d}[localredirectonly] Queries value:

33be-4251-ba85-6007caedcf9d}[roamable]

Queries value:

33be-4251-ba85-6007caedcf9d}[precreate]

Oueries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{352481e8-1641e1\} \\ note that the first index of t$ 33be-4251-ba85-6007caedcf9d}[stream]

Queries value:

33be-4251-ba85-6007caedcf9d}[publishexpandedpath]

Queries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{352481e8-1641e1\} \\ note that the first index of t$ 33be-4251-ba85-6007caedcf9d}[attributes]

Queries value:

 $HKLM \label{lem:hklm} \\ HKLM \label{lem:hklm} HKLM \label{lem:hklm} \\ Software \label{lem:hklm} \\ Wigner \label{lem:hklm} \\ HKLM \label{lem:hklm} \\ Software \label{lem:hklm} \\ Wigner \label{lem:hkklm} \\ Wigner \label{$ 33be-4251-ba85-6007caedcf9d}[foldertypeid]

Queries value:

33be-4251-ba85-6007caedcf9d}[initfolderhandler]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cache] Queries value:  $HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default[latest]$  $HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default[index 4]$ Queries value: Oueries value:

HKLM\software\microsoft\fusion\publisherpolicy\default[legacypolicytimestamp]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i \setminus 3cca06a0 \setminus 6dc7d4c0 \setminus 7b[display name]$ Queries value:

 $HKLM \ software \ |\ microsoft \ fusion \ |\ massindex \ |\ v2.0.50727\_32 \ |\ mi\ account \ |\ massindex \ |\ mi\ account \ |\ mi\ account \ |\ mi\ account \ |\ mi\ account \ |\ mi\ account\ |\ mi\ accou$ Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni\ 3cca06a0\ 6dc7d4c0\ 7b[configstring]$ Queries value:

 $\label{localization} HKLM \software \microsoft \fusion \native images in dex \normalization \n$ Queries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 7b[evalation data]$ Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni\ 3cca06a0\ 6dc7d4c0\ 7b[status]$ 

- $\label{thm:locality} HKLM\software\microsoft\fusion\native images in dex\v2.0.50727\_32\ni\3cca06a0\6dc7d4c0\7b[ildependencies] Queries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\3cca06a0\6dc7d4c0\7b[nidependencies]
  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\3cca06a0\6dc7d4c0\7b[missingdependencies]
   Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\6dc7d4c0\a5cd4db\7e[modules]
- $\label{thm:hative} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl v2.0.50727\_32\mbox{\sl}\sl (6dc7d4c0\a5cd4db\7e[sig]\ Oueries\ value:$
- $\label{local-equation} HKLM \software \mbox{$\mbox{$\mathbb{N}$} = \mbox{$\mathbb{N}$} = \mbox{$\mathbb{N}$} \mbox{$\mathbb{N}$} = \mbox{$\mathbb{N}$} = \mbox{$\mathbb{N}$} \mbox{$\mathbb{N}$} = \mbox{$\mathbb{N}$} \mbox{$\mathbb{N}$} = \mbox{$\mathbb{N}$} -$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\30bc7c4f\3f50fe4f\88[displayname]
   Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{lem:hklmsoftware} HkLM \software \end{subarray} HkLM \software \end{subarray} Note \software \end{subarray} Not \software \end{subarray} Note \software \end{subarray} Note \software \end{subarray} Note \software \end{subarray} Not \software \software \end{subarray} Not \software \$
- $HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 88[evalation data] \\ Oueries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\30bc7c4f\3f50fe4f\88[status]
  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\30bc7c4f\3f50fe4f\88[ildependencies]
   Oueries value:
- $\label{local-observation} HKLM \software \end{align*} HKLM \software \end{align*} Nucreal \software \end{align*} Nucreal \software \end{align*} Nucreal \software \end{align*} Nucreal \software \software \software \end{align*} Nucreal \software \software$
- $\label{lem:hklmsoftware} HKLM \software \mbox{$\mathbb{N}$ in sing dependencies} Queries \ value:$
- $\label{lem:hklmsoftware} HkLM \software \subseted in the limit of th$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727\_32 \sinled 424 \bd 4d8 \normalized 1c83327 \bd 86 \sinled 5 \normalized 2.0.50727\_32 \sinled 6 \norma$
- $\label{local-prop} HKLM \software \microsoft \sion \native images in dex \sindex \sindex \sion \native images in dex \sion \$

- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\19ab8d57\1bd7b0d8\87[status]$  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\19ab8d57\1bd7b0d8\87[sig]
  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\19ab8d57\1bd7b0d8\87[lastmodtime]
  Oueries value:
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{lem:hklm} HKLM \software \microsoft \sion \native images in dex \noindex \n$
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\3f50fe4f\6f1da7aa\88[sig]
  Oueries value:
- $\label{local-bound} HKLM \software \mbox{$\mbox{$\mathbb{N}$} irrosoft \subseted in a tive images in dex $\mbox{$\mathbb{N}$} 2.0.50727\_32 \subseted in \subse$
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.drawing,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Oueries 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]
  Queries value:
- $HKLM \ software \ microsoft \ fusion \ default [system.configuration, 2.0.0.0, ,b03f5f7f11d50a3a, msil] \\ Oueries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\61e7e666\c991064\7a[displayname]
  Oueries value:
- $\label{lem:hklm} HKLM \software \microsoft \sin \native images in dex \v2.0.50727\_32 \ni \61e7e666 \c991064 \7a[configmask] \noindent \noindent$
- $\label{lem:hklmsoftware} HKLM \software \mbox{$\sim 1.50727\_32\ni\61e7e666\c991064\7a[configstring]$} Queries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\61e7e666\c991064\7a[mvid]
   Oueries value:
- $\label{lem:hklmlsoftware} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\sl 2.0.50727\_32\mbox{ni}\end{6}167e666\c991064\argument{7}a\end{6}evalationdata\graysuments.}$  Queries value:
- $\label{local-observation} HKLM\software\microsoft\fusion\native\mbox{images} index\v2.0.50727\_32\ni\61e7e666\c991064\7a[status] Queries\value:$
- $\label{local-equation} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \ni\61e7e666 \c991064 \7a[ildependencies] \noindent \noinden$

```
Queries value:
```

- $\label{lem:hklmsoftware} HkLM \software \subseted in the limit of th$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\475dce40\2d382ce6\85[status]
- $\label{lem:hklmsoftware} HkLM \software \end{area} Hklm \software \end{area} Nuclear \software \end{area} A single \end{area} Oueries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\475dce40\2d382ce6\85[sig]
  Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\475dce40\2d382ce6\85[lastmodtime]
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\2dd6ac50\163e1f5e\80[displayname]
   Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\2dd6ac50\163e1f5e\80[status]
  Oueries value:
- $\label{local-prop} HKLM \software \microsoft \sion \native images in dex \sin 2.0.50727\_32 \sin 2dd 6ac 50 \sin 63e 1f 5e \sion \sin 2dd 6ac 50 \sin 63e 1f 5e \sion \sin 2dd 6ac 50 \sion \sin 2dd 6ac 50 \sion \sion$
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\2dd6ac50\163e1f5e\80[lastmodtime]
   Oueries value:
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727\_32\il\41c04c7e\7f3b6ac4\78[displayname] Queries value:$
- $\label{local-prop} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \label{local-prop} 1 \label{local-prop} All \cite{Local-prop} All \cite{Local-prop}$
- $\label{lem:hklmsoftware} HkLM \software \mbox{$\mathbb{N}$ in a tive images in dex.} $$2.0.50727\_32 \il\41c04c7e\7f3b6ac4\78[sig] $$Oueries value:$
- $\label{local-prop} HKLM \software \mbox{$\$
- $\label{local-prop} HKLM \software \microsoft \sion \native images in dex \v2.0.50727\_32 \il\aced 59c5 \label{local-prop} 1b2590b1 \slash \sl$
- $\label{lem:hklmsoftware} HkLM \software \end{area} Hklm \software \end{area} In $$ 1.3ced 59c5 \1b2590b1 \7c[modules] Oueries value: $$ 2.0.50727_32 \13ced 59c5 \1b2590b1 \7c[modules] $$ 2.0.50727_32 \1b2590b1 \2ced 59c5 \1b2590b1 \2ced 59c5 \2ced 59c$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\3ced59c5\1b2590b1\7c[sig]
  Queries value:
- $\label{local-prop} HKLM \software \end{align*} HKLM \software \end{align*} With \software \end{align*} 10.50727\_32 \end$
- $\label{local-prop} \begin{tabular}{ll} HKLM\software\microsoft\fusion\native\mbox{images} index\v2.0.50727\_32\il\c991064\2bd33e1c\79[modules] \\ Oueries\ value: \begin{tabular}{ll} Color of the color$
- $\label{local-equation} HKLM\software\microsoft\fusion\native\midgesindex\v2.0.50727\_32\ll\c991064\2bd33e1c\79[sig] Queries\ value:$
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
  Oueries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Significant \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Significant \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{lem:hkklm}$
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.serialization.formatters.soap,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Oueries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Simply \label{lem:hklm} White \label{lem:hkklm} Whi$
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Oueries value:
- $\label{lem:hklm} HKLM \software \mbox{$\mbox{}\mbox{$\mb$
- $\label{lem:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727\_32 \ni \57d4b1bf \85e83df \70 [configmask] Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \mbox{$\mbox{$\mbox{$\sim$}} 1.57d4b1bf\sbe83df\sbe83df\sbeen{lem:hklmsoftware} Together \mbox{$\mbox{$\sim$}} 2.0.50727\_32\mbox{$\mbox{$\sim$}} 1.57d4b1bf\sbeen{lem:hklmsoftware} 1.57d4b1bf\sb$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\57d4b1bf\85e83df\70[mvid]
   Oueries value:
- $\label{lem:hklmsoftware} HkLM \software \end{array} With the label{lem:hklmsoftware} With the lab$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\ni\57d4b1bf\85e83df\70[status]
  Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{thm:local-bound} HKLM \software \mbox{$\sim 1.57d4b1bf.85e83df.70[nidependencies]} \\ Queries \ value:$
- $\label{local-bound} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727\_32\ni\57d4b1bf\85e83df\70\mbox{[missing dependencies]} \\ Queries\ value:$
- $\label{lem:hklmsoftware} HKLM \software \mbox{$\le$ index$ $\le$ 0.50727\_32$ in $\le$ 49b34$ $\le$ 10b08$ $\le$ 0.50727\_32$ in $\le$ 49b34$ $\le$ 10b08$ $\le$ 0.50727\_32$ in $\le$ 10b08$ $\le$ 1$
- $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727\_32\il\3b249b34\531d6b08\70[status] Queries\ value:$
- $\label{local-bound} HKLM\software\microsoft\fusion\native\midgesindex\v2.0.50727\_32\lil\ab249b34\531d6b08\70\mathcharmoniand \cite{Ab249b34}. Queries value:$
- $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i1 \setminus 3b249b34 \setminus 531d6b08 \setminus 70[sig]$

- $\label{thm:local-bound} HKLM \software \mbox{$\le$ index$ $\le$ 0.50727\_32$ il \sb249b34$ $\le$ 1d6b08$ $\le$ 0.50727\_32$. Il \sb249b34$ $\le$ 1d6b08$ $\le$ 0.50727\_32$ il \sb249b34$ $\le$ 1d6b08$ $\le$ 0.50727\_32$. Il \sb249b34$ $\le$ 1d6b08$ $\le$ 1d$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\3a6a696d\52d7076e\72[status] Oueries value:
- $\label{lem:hklmsoftware} HkLM \software \end{area} Hklm \software \end{area} In \some \software \end{area} A \some \so$
- $\label{thm:local-bound} $HKLM \sim \max_{n=0} \frac{1}{3a6a696d} \frac{13a6a696d}{2d7076e} \ Queries \ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\3a6a696d\52d7076e\72[lastmodtime]
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\f6e8397\46ad0879\6f[status]
  Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sinon \native images in dex \native images \native images in dex \native images \nativ$
- $\label{lem:hklmsoftware} HkLM \software \microsoft \sizes on \native images in dex \sizes 2.0.50727\_32 \sizes 1 \sizes 66 \sizes 1 \size$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\il\f6e8397\46ad0879\6f[lastmodtime]
  Oueries value:
- $\label{lem:hklmsoftware} HkLM \software \sinces of this ion \native images in dex \v2.0.50727\_32 \sinces 11 \add 590 \c3f \b82[display name] Oueries value:$
- $\label{local-prop} HKLM \software \microsoft \micros$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727\_32\i1\3d590c3f\59f3b67b\82[sig]
  Oueries value:
- $\label{lem:hklmsoftware} HkLM \software \sinces of this ion \sinces will be a single single with the last single single$
- $\label{lem:hklm} HKLM \software \sin dex \v2.0.50727\_32 \il\85e83 \df \4c239 \d82 \71 \[display name] Queries value:$
- $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727\_32\il\85e83df\4c239d82\71[status] \\ Oueries\ value:$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727\_32 \normalized 185e83 \normalized 4c239 \normalized 4c239 \normalized 4c239 \normalized 8c239 \normalized 4c239 \normalized 8c239 \normalized 8$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-bound} HKLM \software \since \since$
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.enterpriseservices,2.0.0.0,,b03f5f7f11d50a3a,x86] Oueries value:
- HKLM\software\microsoft\fusion\gacchangenotification\default[microsoft.visualc,8.0.0.0,,b03f5f7f11d50a3a,msil]
   Oueries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Sitter \label{lem:hklm} White \label{lem:hkklm} White \$
- $HKLM \ software \ microsoft \ fusion \ gacchange notification \ default [system. directory services, 2.0.0.0, , b03f5f7f11d50a3a, msil] \\ Queries value:$
- HKLM\software\microsoft\fusion\gacchangenotification\default[system.transactions,2.0.0.0,,b77a5c561934e089,x86] Oueries 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]