Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

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

Task ID: 2417 Risk Level: 6

Date Processed: 2016-02-22 05:28:11 (UTC)

61.07 seconds Processing Time: 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:

Pattern Matching Results

2 .NET compiled executable

Writes to a log file [Info] 6 Creates executable in application data folder

Process/Thread Events

Creates process:

 ${\tt C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe}$ $["C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe"]$

Writes to process: PTD: 2796

C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe Terminates process:

C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex Creates event: \BaseNamedObjects\CorDBIPCSetupSyncEvent_2740

File System Events

Creates: C:\Users\Admin

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

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

Creates:

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

Opens:

C:\Windows\System32\wow64.dll Opens:

C:\Windows\SysWOW64 Opens:

C:\Windows\SysWOW64\mscoree.dll Opens: Opens: C:\Windows\SysWOW64\apphelp.dll Opens:

C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe

C:\Windows\SysWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll Opens: C:\Windows\SysWOW64\KernelBase.dll Opens: Opens: C:\Windows\apppatch\sysmain.sdb C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\msvcrt.dll Opens:

C:\Windows\SysWOW64\bcryptprimitives.dll Opens: C:\Windows\SysWOW64\cryptbase.dll Opens: C:\Windows\SysWOW64\sspicli.dll Opens: Opens: C:\Windows\SysWOW64\rpcrt4.dll C:\Windows\SysWOW64\advapi32.dll Opens:

C:\Windows\Microsoft.NET\Framework\v4.0.30319 Opens:

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll Opens:

Opens: C:\Windows\Microsoft.NET\Framework

Opens: C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll Opens: $C: \verb|\windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll|$ C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll Opens: Opens: C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll Opens: C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll

Opens: C:\Windows\SysWOW64\gdi32.dll C:\Windows\SysWOW64\user32.dll Opens: Opens: C:\Windows\SysWOW64\shlwapi.dll C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\SysWOW64\msctf.dll Opens: Opens:

```
C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.config
     Opens:
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6910_none_d089c358442de345
     Opens:
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6910_none_d089c358442de345\msvcr80.dll
     Opens:
                                                                       C:\
                                                                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
     Opens:
     Opens:
C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.log
                                                                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config
     Opens:
     Opens:
                                                                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
     Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
     Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
                                                                        C:\Windows\SysWOW64\combase.dll
     Opens:
                                                                       C:\Windows\SysWOW64\shell32.dll
     Opens:
     Opens:
                                                                       C:\Windows\SysWOW64\SHCore.dll
     Opens:
                                                                        C:\Windows\Globalization\Sorting\SortDefault.nls
     Opens:
                                                                       C:\Windows\SysWOW64\profapi.dll
                                                                       C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
     Opens:
Config\v2.0.50727.312\security.config
     Opens:
                                                                       C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config.cch
                                                                       C:\Windows\assembly\NativeImages_v2.0.50727_32\index21.dat
     Opens:
C: \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\windows| assembly asse
                                                                       C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0_b77a5c561934e089
     Opens:
     Opens:
                                                                       C:\Windows\Temp
     Opens:
                                                                       C:\Windows\SysWOW64\l_intl.nls
                                                                        C:\Windows\SysWOW64\ole32.dll
     Opens:
                                                                        C:\Windows\SysWOW64\oleaut32.dll
     Opens:
     Opens:
                                                                       C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
     Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\6124280f8365d6683e54dd99742100f6\System.ni.dll
C: \verb|\windows| assembly \verb|\NativeImages_v2.0.50727_32 \verb|\System.Drawing| b8f373895aa19304a2cb6b888e298529 \verb|\System.Drawing.ni.dll| basembly \verb|\NativeImages_v2.0.50727_32 \verb|\System.Drawing| b8f373895aa19304a2cb6b888e298529 \verb|\System.Drawing.ni.dll| basembly \verb|\NativeImages_v2.0.50727_32 \verb|\System.Drawing| b8f373895aa19304a2cb6b888e298529 \verb|\System.Drawing.ni.dll| basembly \verb|\NativeImages_v2.0.50727_32 \verb|\System.Drawing| b8f373895aa19304a2cb6b888e298529 \verb|\System.Drawing.ni.dll| b8f373895aa19304a2cb6b888e2
     Opens:
                                                                        C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0_b03f5f7f11d50a3a
                                                                        C:\Windows\assembly\GAC_MSIL\System\2.0.0.0_b77a5c561934e089
     Opens:
    Opens:
C: \verb|Windows| assembly \verb|NativeImages_v2.0.50727_32 \verb|System.Windows.Forms|| 5ba5657c270bdd2fde78ecda4c2ad910 \verb|System.Windows.Forms.ni.dll|| 5ba5657c270bd2fde78ecda4c2ad910 \verb|System.Windows.forms.ni.dll|| 5ba567c270bd2fde78ecda4c2ad910 \verb|Syst
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0_b77a5c561934e089
     Opens:
C:\Windows\assembly\GAC_32\System.EnterpriseServices\2.0.0.0_b03f5f7f11d50a3a\System.EnterpriseServices.dll
     Opens:
\label{lem:c:windows} $$C: \widetilde{AC_32\S} = EnterpriseServices $$2.0.0.0\_b03f5f7f11d50a3a$$
     Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2740.10903796
    Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2740.10903796
                                                                       C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
     Opens:
Config\v2.0.50727.312\security.config.cch.2740.10903812
     Opens:
                                                                       C:\Windows\SysWOW64\nsi.dll
                                                                        C:\Windows\SysWOW64\ws2_32.dll
     Opens:
    Writes to:
C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.log
     Reads from:
                                                                       \label{lem:config} C: \verb|\windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config| | C: \verb|\windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config| | C: \verb|\windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config| | C: \verb|\windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config| | C: \verb|\windows\Microsoft.NET\Framework\w2.0.50727\CONFIG\machine.config| | C: \verb|\windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\Windows\W
     Reads from:
C:\Windows\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Windows Registry Events
     Creates key:
                                                                        \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ fusion\+ gacchangenotification\+ default
     Opens key:
                                                                        HKLM\software\microsoft\wow64
     Opens key:
                                                                       HKLM\svstem\currentcontrolset\control\nls\sorting\versions
     Opens key:
                                                                        HKLM\system\currentcontrolset\control\safeboot\option
     Opens key:
                                                                       HKLM\system\currentcontrolset\control\srp\gp\dll
     Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
                                                                       HKLM\software\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
                                                                        HKCU\software\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
                                                                       Opens key:
                                                                        HKLM\system\currentcontrolset\control\nls\language
     Opens key:
                                                                        HKLM\system\currentcontrolset\control\mui\uilanguages
     Opens key:
                                                                        HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
     Opens key:
                                                                        HKLM \verb|\system| current controlset \verb|\control| mui \verb|\uilanguages| pending delete
     Opens key:
                                                                       HKLM\software\wow6432node\policies\microsoft\mui\settings
     Opens key:
                                                                        HKLM\software\policies\microsoft\mui\settings
     Opens key:
                                                                       HKCU\
                                                                        HKCU\control panel\desktop\muicached\machinelanguageconfiguration
     Opens key:
     Opens key:
                                                                        HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
     Opens key:
                                                                        HKCU\software\policies\microsoft\control panel\desktop
```

 ${\tt HKCU \backslash control\ panel \backslash desktop \backslash language configuration}$

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside

HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

HKCU\control panel\desktop

HKCU\control panel\desktop\muicached

Opens key:

Opens key:

Opens key:

Opens key: Opens key:

```
\label{lem:hkcu} \mbox{HKCU\software\mbox{$\backslash$ microsoft\windows nt\currentversion\appcompatflags}} \label{lem:hkcu}
       Opens key:
       Opens key:
                                                                                                    HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
                                                                                                   HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
       Opens kev:
       Opens key:
                                                                                                    HKLM\system\currentcontrolset\control\lsa
       Opens key:
HKLM \verb|\system| current controlset| policies \verb|\microsoft| cryptography| configuration
       Opens key:
       Opens key:
                                                                                                    HKLM\software\wow6432node\microsoft\.netframework\policy\
       Opens key:
                                                                                                    HKLM\software\wow6432node\microsoft\.netframework\policv\v4.0
       Opens key:
                                                                                                    HKLM\software\wow6432node\microsoft\.netframework
       Opens key:
                                                                                                    HKLM\software\policies\microsoft\sqmclient\windows
       Opens key:
                                                                                                    HKLM\software\microsoft\sqmclient\windows
       Opens key:
                                                                                                    HKCU\software\microsoft\.netframework
                                                                                                    HKLM\software\wow6432node\microsoft\windows
       Opens key:
nt\currentversion\gre_initialize
                                                                                                    HKLM\software\wow6432node\microsoft\windows
       Opens key:
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:
                                                                                                    HKLM\software\wow6432node\microsoft\.netframework\policy\standards
       Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\standards\v2.0.50727
       Opens key:
                                                                                                   HKLM\software\wow6432node\microsoft\fusion
       Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebvside\assemblvstorageroots
       Opens key:
                                                                                                   HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch
       Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch\v4.0.30319.00000
       Opens key:
Opens kev:
                                                                                                   HKLM\software\microsoft\fusion
                                                                                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
       Opens kev:
options\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
                                                                                                    HKCU\software\microsoft\fusion
       Opens key:
       Opens key:
                                                                                                    \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
options
       Opens kev:
                                                                                                    HKLM\software\wow6432node\microsoft\.netframework\ngen\policv\v2.0
       Opens kev:
HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem
       Opens key:
HKLM \label{lem:hklm} Which is the second of the second 
      Opens key:
HKLM \ software \ wow 6432 node \ icrosoft \ . net framework \ security \ policy \ extensions \ named permission sets \ local intranet
       Opens key:
                                                                                                    HKLM\software\wow6432node\microsoft\windows
nt \verb|\currentversion| profile list \verb|\s-1-5-21-1923240461-1905901954-2556564120-1001| | terrentversion| | terrentversi
       Opens key:
                                                                                                    HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 1923240461-1905901954-2556564120-1001
       Opens key:
                                                                                                   HKLM\software\wow6432node\microsoft\ole
       Opens key:
                                                                                                    HKLM\software\wow6432node\microsoft\ole\tracing
       Opens key:
                                                                                                    HKLM\software\microsoft\ole\tracing
       Opens key:
                                                                                                    HKLM\system\currentcontrolset\control\session manager
       Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
       Opens kev:
65f9-4cf6-a03a-e3ef65729f3d}
      Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10ex, 10ex, 1
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
       Opens key:
                                                                                                   HKCU\software\microsoft\windows\currentversion\explorer
       Opens kev:
                                                                                                    HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
       Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follown folders
                                                                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
       Opens key:
 folders
       Opens key:
                                                                                                    HKLM\system\currentcontrolset\control\nls\extendedlocale
       Opens key:
                                                                                                    HKLM\system\currentcontrolset\control\nls\sorting\ids
       Opens key:
                                                                                                    HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus explorer
       Opens key:
                                                                                                    HKLM\software\policies\microsoft\windows\explorer
                                                                                                    HKCU\software\policies\microsoft\windows\explorer
       Opens key:
       Opens key:
HKLM \label{lem:hklm} Which is the large statement of the large st
0e22-4760-9afe-ea3317b67173}
       Opens kev:
0e22-4760-9afe-ea3317b67173}\propertybag
       Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
       Opens key:
\label{lem:hklm} \begin{tabular}{ll} HKLM \software \wow 6432 node \microsoft \. net framework \v2.0.50727 \security \policy \end{tabular} \label{lem:hklm}
       Opens key:
                                                                                                    HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32
       Opens key:
                                                                                                    HKLM \ software \ microsoft \ fusion \ native images in dex \ v2.0.50727\_32 \ in dex 21.0.50727\_32 \ in dex 21.0.507207\_32 \ in dex 21.0.50727\_32 \ in dex 21.0.50727\_32 \ in dex 21.
       Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 181938c6 \setminus 7950e2c5
       Opens key:
```

Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1 Opens key: 33be-4251-ba85-6007caedcf9d} Opens key: 33be-4251-ba85-6007caedcf9d}\propertybag Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\ni\4846a846\3ed6137e Opens key: HKLM\software\wow6432node\microsoft\strongname Opens key: HKLM\software\microsoft\fusion\publisherpolicy\default Opens key: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni\ 3cca06a0\ 6dc7d4c0$ Opens key HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9 Opens key: Opens key: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 30bc7c4f \ 3f50fe4f \ 8f50fe4f \ New \ New$ Opens key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i1 \setminus 424bd4d8 \setminus 210819fb \setminus 60.50727_32 \setminus i1 \setminus 424bd4d8 \setminus 210819fb \setminus 60.50727-32 \setminus$ Opens key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 5206cfdb \setminus 7abb \mid v2.0.50727_32 \setminus i1 \setminus 19ab8d57 \setminus 19ab8d5$ Opens key: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3f50fe4f\ 6ff8cf57\ 8ex \ for the control of the control o$ Opens kev: HKLM\software\wow6432node\microsoft\.netframework\policy\aptca Opens key: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 61e7e666 \ c991064$ Opens key: Opens key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.0.50727_32 \setminus i1 \setminus 475 dce 40 \setminus 6604 efc \setminus 3.000 + index \setminus v2.000 + index \setminus v2.000$ Opens kev HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\i1\2dd6ac50\6bbd663d\4 Opens key: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 41c04c7e \setminus 7a981124 \setminus 1f$ Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\bd38540\f Opens kev $HKLM \verb|\software\microsoft| fusion \verb|\nativeimagesindex| v2.0.50727_32 \verb|\since| 1 \end{to} 1 \en$ Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat Opens key: HKLM\software\policies\microsoft\windows\appcompat Opens key: HKCU\software\microsoft\windows nt\currentversion Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\appcompatflags HKLM\software\wow6432node\microsoft\windows Opens key: $\verb|nt\currentversion|| approx|| approx$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens kev HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers Opens key: HKLM\software\microsoft\windows $\verb|nt\currentversion| app compatflags \verb|custom|| 476 fc 456 c66 cbec 138e 3 dab 72 a 0 f0 e54 f2 0 3 db f27 ce 8873 6b 1893 b 668 b ce 63 c4 . executive for the first of the first of the following statement of the first of th$ Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions Oueries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[] Oueries value: $HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]|$ HKLM\system\currentcontrolset\control\nls\customlocale[empty] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback] HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\mui\uilanguages\enus[alternatecodepage] Queries value: HKCU\control panel\desktop[preferreduilanguages] Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]$ Oueries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo] HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Queries value: Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] HKLM\software\wow6432node\microsoft\.netframework[installroot] Queries value: Oueries value: HKLM\software\wow6432node\microsoft\.netframework[clrloadlogdir]

nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]

HKLM\software\microsoft\windows

HKLM\software\microsoft\sqmclient\windows[ceipenable]

Oueries value:

Oueries value:

Queries value:

HKLM\software\wow6432node\microsoft\.netframework[uselegacyv2runtimeactivationpolicydefaultvalue]

HKLM\software\wow6432node\microsoft\.netframework[onlyuselatestclr] Queries value:

HKLM\software\wow6432node\microsoft\fusion[noclientchecks] Oueries value: Oueries value: HKLM\software\wow6432node\microsoft\.netframework[gcstressstart] Queries value: HKLM\software\wow6432node\microsoft\.netframework[gcstressstartatjit] Queries value: HKLM\software\wow6432node\microsoft\.netframework[disableconfigcache] Queries value: HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-

931b-d9cc2eee27e41

Oueries value: HKLM\system\currentcontrolset\control\wmi\security[cc2bcbba-16b6-4cf3-

8990-d74c2e8af5001

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

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

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

HKLM\software\microsoft\fusion[noclientchecks] Queries value: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$

options[devoverrideenable]

Queries value:

Oueries value:

HKLM\software\wow6432node\microsoft\.netframework\ngen\policy\v2.0[optimizeusedbinaries]

Oueries value: HKLM\software\microsoft\ole[pageallocatorusesvstemheap] ${\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocator system heap is private]}$ Oueries value:

Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ version \ explorer \ folder descriptions \ (3eb685 db-microsoft) \ windows \ version \ ver$ 65f9-4cf6-a03a-e3ef65729f3d}[category]

Oueries value:

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

Queries value:

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

Oueries value:

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

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

Queries value:

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

Oueries value:

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:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

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}[localredirectonly]

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ version \ explorer \ folder descriptions \ (3eb685 db-microsoft) \ windows \ version \ ver$ 65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]

Oueries value:

 $HKLM \label{lem:hklm} \\ HKLM \label{lem:hklm} HKLM \label{lem:hklm} \\ Software \label{lem:hklm} \\ Wigner \label{lem:hklm} \\ HKLM \label{lem:hklm} \\ Software \label{lem:hklm} \\ Wigner \label{lem:hkklm} \\ Wigner \label$ 65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

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

folders[appdata]

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx] Queries value:

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us] $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ ls \+ sorting \+ ids \+ [en]$ Queries value:

Oueries value:

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

0e22-4760-9afe-ea3317b67173}[name]

Oueries value:

0e22-4760-9afe-ea3317b67173}[parentfolder]

0e22-4760-9afe-ea3317b67173}[description]

Oueries value:

0e22-4760-9afe-ea3317b67173}[relativepath]

0e22-4760-9afe-ea3317b67173}[parsingname]

Oueries value:

0e22-4760-9afe-ea3317b67173}[infotip]

Queries value:

0e22-4760-9afe-ea3317b67173}[localizedname]

Oueries value:

0e22-4760-9afe-ea3317b67173}[icon]

Queries value:

0e22-4760-9afe-ea3317b67173}[security]

Oueries value:

0e22-4760-9afe-ea3317b67173}[streamresource]

0e22-4760-9afe-ea3317b67173}[streamresourcetype]

Queries value:

0e22-4760-9afe-ea3317b67173}[localredirectonly] Oueries value:

Queries value:

0e22-4760-9afe-ea3317b67173}[roamable]

0e22-4760-9afe-ea3317b67173}[precreate]

Oueries value:

0e22-4760-9afe-ea3317b67173}[stream] Queries value:

0e22-4760-9afe-ea3317b67173}[publishexpandedpath]

0e22-4760-9afe-ea3317b67173}[attributes]

Oueries value:

0e22-4760-9afe-ea3317b67173}[foldertypeid]

Queries value:

0e22-4760-9afe-ea3317b67173}[initfolderhandler]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001[profileimagepath]

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

Queries value:

 $HKLM \verb|\software\microsoft| fusion \verb|\nativeimagesindex| v2.0.50727_32 \verb|\index21[niusagemask]| \\$

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus index 21 [ilusage mask]$

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727_32 \setminus i181938c6 \setminus 7950e2c5 \setminus 1[display name]$ Queries value:

 $HKLM \ software \ |\ microsoft \ fusion \ |\ magesindex \ |\ v2.0.50727_32 \ |\ 181938c6 \ |\ 7950e2c5 \ |\ [configmask]$ Oueries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[configstring]

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 1 \ [mvid]$ Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 181938c6 \ 7950e2c5 \ 1[evalation data]$ Queries value:

```
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ ni \ 181938c6 \ 7950e2c5 \ 1[status]
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727\_32 \setminus ni \setminus 181938c6 \setminus 7950e2c5 \setminus 1[ildependencies]
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus mi \setminus 181938c6 \setminus 7950e2c5 \setminus 1[nidependencies]
  Queries value:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus mative images index \setminus v2.0.50727\_32 \setminus i181938c6 \setminus 7950e2c5 \setminus 1[missing dependencies]
  Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 7950e2c5 \ 27a18466 \ 1 \ [display name]
  Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[status]
  Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 7950e2c5 \ 27a18466 \ l[modules]
  Queries value:
HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727\_32 \ il\ 7950e2c5 \ v27a18466 \ v1[sig]
  Oueries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[lastmodtime]
  Oueries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
```

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM \label{lem:hklm} Which is the latest and the$ 33be-4251-ba85-6007caedcf9d}[streamresource]

Queries value:

33be-4251-ba85-6007caedcf9d}[streamresourcetype] Oueries value:

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

Queries value:

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

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}[precreate]

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}[stream]

Queries value:

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{lkklm} White \label{l$ 33be-4251-ba85-6007caedcf9d}[publishexpandedpath]

Oueries value:

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

Queries value:

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

Oueries value:

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

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

folders[cache]

Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[latest]

Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 9[displayname]$ Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[configmask] Oueries value:

 $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 3cca06a0 \ 6dc7d4c0 \ 9[configstring]$

```
Queries value:
```

- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[mvid]
 Queries value:
- $\label{localization} $HKLM\software\microsoft\fusion\native images in dex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9 [evalation data] $$Oueries value:$
- $\label{thm:hklm} HKLM\software\microsoft\fusion\native images index \v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[status] \\ Oueries\ value:$
- $\label{lem:hklm} \begin{tabular}{ll} HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\acca06a0\6dc7d4c0\9[ildependencies] \\ Oueries\value: \begin{tabular}{ll} Color of the color of$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\9[missingdependencies] Oueries value:
- $\label{thm:local-bound} HKLM\software\mbox{\setminus hKLM\software\mbox{\setminus il\software\mbox{\setminus il\software\mbox{$\setminus$$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\153b7f91\9[status]
 Oueries value:
- $\label{lem:hklmsoftware} HkLM \software \microsoft \size on \native images in dex \v2.0.50727_32 \size of \native images in dex \size of \native images in$
- $\label{local-equation} HKLM \software \mbox{$\mbox{$\mathbb{N}$} $$ in \adverses and ex. $\mbox{$\mathbb{N}$} $$ in \adverses a local decoration of the second of the$
- $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[display name] Queries value:$
- $\label{local-equation} HKLM \software \end{array} WKLM \software \end{array} 1.50727_32 \end{array} 1.30bc7c4f \array \software \end{array} 1.50bc7c4f \array \software \array \array \software \software \array \software \array \software \array \software \array \software \software \array \software \array \software \software \array \software \soft$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[configstring] Oueries value:
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8[mvid]
 Oueries value:
- $\label{local-bound} HKLM \software \microsoft \sion \native images in dex \v2.0.50727_32 \ni\30bc7c4f\3f50fe4f\8 \ [evalation data] Queries value:$
- $\label{lem:hklm} $HKLM \setminus software \end{array} $HKLM \setminus software \end{array} $1.0.50727_32 \in 30bc7c4f \end{array} $1.0.507$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{lem:hklmsoftware} HKLM \software \since \s$
- $\label{local-bound} HKLM\software\microsoft\fusion\native\mbox{images index $$\nu 2.0.50727_32\il\424bd\4d8\210819fb\6[displayname]$$ Oueries value:$
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{lem:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_32 \il\424 bd4d8 \calebox{210819fb} \end{6modules} Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \end{array} HKLM \software \end{array} 1.0.50727_32 \end{array} 1.424 \bd \end{array} black \software \end{array} 1.0.50727_32 \end{array} 1.424 \bd \end{array} black \software \end{array} 1.0.50727_32 \e$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\210819fb\6[lastmodtime] Queries value:
- $\label{lem:hklmsoftware} HkLM \software \since \s$
- $\label{local-equation} HKLM\software\microsoft\fusion\native images in dex \v2.0.50727_32\il\19ab8d57\5206cfdb\7[status] Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727_32 \normalized 19ab8d57 \sion \normalized 19ab8d57 \s$
- $\label{thm:hkm} \begin{tabular}{ll} HKLM\software\microsoft\fusion\native images in dex\v2.0.50727_32\il\19ab8d57\5206cfdb\7[sig] \\ Oueries\ value: \begin{tabular}{ll} Ouer$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\5206cfdb\7[lastmodtime]
 Oueries value:
- $\label{lem:hklmsoftware} HKLM \software \slight \sli$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6ff8cf57\8[status] Queries value:
- $\label{lem:hklmsoftware} HKLM \software \microsoft \sion \native images in dex \normalized 2.0.50727_32 \sinled 13f50 fe4f \sion \native images in dex \normalized 2.0.50727_32 \sinled 13f50 fe4f \sion \native images in dex \normalized 2.0.50727_32 \sinled 13f50 fe4f \sion \normalized 13f50 fe4f \sion \n$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6ff8cf57\8[sig] Oueries value:
- $\label{local-prop} HKLM \software \mbox{$\mbox{$\mathbb{N}$} irrosoft \subseted in a tive images in dex $\mbox{$\mathbb{N}$} 2.0.50727_32 \subseted in \mathbb{N} in a tive image sindex \subseted in \mathbb{N} in \mathbb
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \$
- $\label{lem:hklm} HKLM \software \mbox{$\mbox{}\mbox{$\mb$
- $\label{lem:hklmsoftware} HKLM \software \mbox{\mathbb{N} in \mathbb{R}^2.} Which is the sum of the sum of$
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} which is a configuration, 2.0.0.0, , b03f5f7f11d50a3a, msil] Queries value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[displayname]
 Oueries value:
- $\label{lem:hklm} HKLM \software \microsoft \fusion \native images in dex \v2.0.50727_32 \ni\61e7e666 \c991064 \10 \configmask] Queries value:$
- $\label{local-equation} HKLM\software\microsoft\fusion\native\mbox{imagesindex}\v2.0.50727_32\ni\61e7e666\c991064\10\configstring\] Queries\ value:$
- HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[mvid]
 Oueries value:

Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\10[status] Queries value: Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 61e7e666 \ c991064 \ 10[nide pendencies]$ $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ ni \ 61e7e666 \ c991064 \ 10 \ [missing dependencies]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ 475 dce 40 \ 6604 efc \ 3[display name]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ i1 \ 475 dce 40 \ 6604 efc \ 3[status]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\6604efc\3[sig] Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ 475 dce 40 \ 6604 efc \ 3[last mod time]$ $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ 2dd6ac50 \ 6bbd663d \ 4[displayname]$ Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727 32\il\2dd6ac50\6bbd663d\4[status] Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ 2dd6ac50 \ 6bbd663d \ 4[modules]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 2dd6ac50 \setminus 6bbd663d \setminus 4[sig]$ Oueries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 2dd6ac50 \setminus 6bbd663d \setminus 4[last modtime]$ Oueries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7a981124\1f[displayname] Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ 41c04c7e \ 7a981124 \ 1f[status]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 41c04c7e\ 7a981124 \ 1f[modules]$ Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 41c04c7e\ 7a981124 \ 1f[sig]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus fusion \setminus native images index \setminus v2.0.50727_32 \setminus i1 \setminus 41c04c7e \setminus 7a981124 \setminus 1f[last modtime]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5 \ bd38540 \ f[displayname]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ i1\ 3ced59c5 \ bd38540 \ f[status]$ $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5 \ bd38540 \ f[modules]$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5 \ bd38540 \ f[sig] \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5 \ bd38540 \ f[sig] \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5 \ bd38540 \ f[sig] \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5 \ bd38540 \ f[sig] \ microsoft \ fusion \ native images \ n$ Oueries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ 3ced59c5 \ bd38540 \ f[last mod time]$ Oueries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\34e16fb6\20[displayname] Queries value: $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il\ c991064 \ 34e16fb6 \ 20[status]$ $HKLM \ software \ microsoft \ fusion \ native images index \ v2.0.50727_32 \ il \ c991064 \ 34e16fb6 \ 20 \ [modules]$ Oueries value: $HKLM\software\microsoft\subseteq$ HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\34e16fb6\20[sig] Oueries value:

 $\label{local-equation} HKLM \software \mbox{$\mbox{$\mathbb{N}$} $$ in \adverses in dex \scales. } 20.50727_32 \scales. \\ Queries value:$

HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
Queries value:

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

HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.serialization.formatters.soap,2.0.0.0,,b03f5f7f11d50a3a,msil] Queries value:

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

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Security, 2.0.0.0, , b03f5f7f11d50a3a, msilly \label{lem:hklm} White \label{lem:hkklm} White \label{$

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe]