Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	2418
Risk Level:	2
Date Processed:	2016-02-22 05:28:12 (UTC)
Processing Time:	61.13 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe"

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

Pattern Matching Results

2 .NET compiled executable

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe ["c:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe"]
Writes to process:	PID:2044 C:\WINDOWS\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Terminates process:	C:\WINDOWS\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe

Named Object Events

Creates event:	\BaseNamedObjects\CorDBIPCSetupSyncEvent_2028
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Opens:	C:\WINDOWS\Prefetch\476FC456C66CBEC138E3DAB72A0F0-0385EC13.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\mscoree.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.config
Opens:	C:\WINDOWS\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Manifest
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca\msvcr80.dll
Opens:	C:\
Opens:	C:\WINDOWS
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\shell32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\shell32.dll.124.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Config
Opens:	C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security Config\v2.0.50727.42\security.config
Opens:	C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security Config\v2.0.50727.42\security.config.cch

```
  Opens:                  C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\index9c.dat
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\mscorlib\9adb89fa22fd5b4ce433b5aca7fb1b07\mscorlib.ni.dll
  Opens:                  C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089
  Opens:                  C:\WINDOWS\Temp
  Opens:                  C:\WINDOWS\system32\l_intl.nls
  Opens:                  C:\WINDOWS\system32\rpcss.dll
  Opens:                  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
  Opens:                  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll.2.Manifest
  Opens:                  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll.2.Config
  Opens:                  C:\WINDOWS\assembly\pubpol1.dat
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System\aa7926460a336408c8041330ad90929d\System.ni.dll
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Drawing\6978f2e90f13bc720d57fa6895c911e2\System.Drawing.ni.dll
  Opens:                  C:\WINDOWS\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a
  Opens:                  C:\WINDOWS\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\9a254c455892c02355ab0ab0f0727c5b\System.Windows.Forms.ni.dll
  Opens:
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.EnterpriseSe#\5f9cd5bfebcb94175d440ebab3aa412f\System.EnterpriseServices.ni.dll
  Opens:
C:\WINDOWS\WinSxS\x86_System.EnterpriseServices_b03f5f7f11d50a3a_2.0.0.0_x-ww_7d5f3790
  Opens:                  C:\WINDOWS\system32\apphelp.dll
  Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:
C:\windows\temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe.Manifest
  Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2028.57322
  Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2028.57322
  Opens:                  C:\WINDOWS\system32\ws2_32.dll
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
Config\v2.0.50727.42\security.config.cch.2028.57342
  Opens:                  C:\WINDOWS\system32\ws2help.dll
  Reads from:             C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
  Reads from:
C:\WINDOWS\Temp\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
```

Windows Registry Events

```
  Creates key:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:            HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:            HKLM\software\microsoft\fusion\gacchangenotification\default
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:              HKLM\
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscoree.dll
  Opens key:              HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:              HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:              HKLM\software\microsoft\.netframework
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:              HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:              HKLM\system\currentcontrolset\control\error message instrument
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKCU\
  Opens key:                HKCU\software\microsoft\.netframework\policy\standards
  Opens key:                HKLM\software\microsoft\.netframework\policy\standards
  Opens key:                HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcr80.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorwks.dll
  Opens key:                HKCU\software\microsoft\.netframework
  Opens key:                HKLM\software\microsoft\fusion
  Opens key:                HKCU\software\microsoft\fusion
  Opens key:
HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets
  Opens key:
HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet
  Opens key:
HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\localintranet
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:                HKLM\software\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\index9c
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorlib.ni.dll
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\4846a846\3ed6137e
  Opens key:                HKLM\software\microsoft\net framework setup\dotnetclient\v3.5
  Opens key:                HKLM\software\microsoft\strongname
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorjit.dll
  Opens key:                HKLM\software\microsoft\fusion\publisherpolicy\default
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7
  Opens key:                HKLM\software\microsoft\.netframework\policy\aptca
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49
```

```
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\2a2dcc42\1a
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\9876c30\1e
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\2503fe40\c
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\dfe0ed5\1b
  Opens key:                 HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.ni.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.drawing.ni.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.windows.forms.ni.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.enterpriseservices.ni.dll
  Opens key:                 HKLM\system\wpa\tabletpc
  Opens key:                 HKLM\system\wpa\mediacenter
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4.exe
  Opens key:                 HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key:                 HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}
  Opens key:                 HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:                 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
```

```
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscoree.dll[checkapphelp]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
  Queries value:            HKLM\software\microsoft\.netframework[installroot]
  Queries value:            HKLM\software\microsoft\.netframework[clrloadlogdir]
  Queries value:            HKLM\software\microsoft\.netframework[onlyuselatestclr]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[476fc456c66cbec138e3dab72a0f0e54f203dbf27ce88736b1893b668bce63c4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorwks.dll[checkapphelp]
  Queries value:            HKLM\software\microsoft\.netframework[gcstressstart]
  Queries value:            HKLM\software\microsoft\.netframework[gcstressstartatjit]
  Queries value:            HKLM\software\microsoft\.netframework[disableconfigcache]
  Queries value:            HKLM\software\microsoft\fusion[cachelocation]
  Queries value:            HKLM\software\microsoft\fusion[downloadcachequotainkb]
  Queries value:            HKLM\software\microsoft\fusion[enablelog]
  Queries value:            HKLM\software\microsoft\fusion[logginglevel]
  Queries value:            HKLM\software\microsoft\fusion[forcelog]
  Queries value:            HKLM\software\microsoft\fusion[logfailures]
  Queries value:            HKLM\software\microsoft\fusion[versioninglog]
  Queries value:            HKLM\software\microsoft\fusion[logresourcebinds]
  Queries value:            HKLM\software\microsoft\fusion[uselegacyidentityformat]
  Queries value:            HKLM\software\microsoft\fusion[disablemsipeek]
  Queries value:            HKLM\software\microsoft\fusion[noclientchecks]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c[niusagemask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c[ilusagemask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[configmask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[mvid]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[evalationdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[ildependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[nidependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[missingdependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[status]
```

```
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
   Queries value:              HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
   Queries value:              HKLM\software\microsoft\ole[rwlockresourcetimeout]
   Queries value:              HKCR\interface[interfacehelperdisableall]
   Queries value:              HKCR\interface[interfacehelperdisableallforole32]
   Queries value:              HKCR\interface[interfacehelperdisabletypelib]
   Queries value:              HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
   Queries value:              HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
   Queries value:              HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
   Queries value:              HKLM\software\microsoft\fusion\publisherpolicy\default[index1]
   Queries value:
HKLM\software\microsoft\fusion\publisherpolicy\default[legacypolicytimestamp]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[nidependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[nidependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[sig]
```

```
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.drawing,2.0.0.0,,b03f5f7f11d50a3a,msil]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system,2.0.0.0,,b77a5c561934e089,msil]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.configuration,2.0.0.0,,b03f5f7f11d50a3a,msil]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[nidependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[lastmodtime]
```

```
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.deployment,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.serialization.formatters.soap,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[accessibility,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[configmask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[mvid]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[evalationdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[ildependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[nidependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\57d4b1bf\85e83df\49[missingdependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\2a2dcc42\1a[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\2a2dcc42\1a[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\2a2dcc42\1a[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\2a2dcc42\1a[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3b249b34\2a2dcc42\1a[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\9876c30\1e[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\9876c30\1e[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\9876c30\1e[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\9876c30\1e[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3a6a696d\9876c30\1e[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\2503fe40\c[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\2503fe40\c[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\2503fe40\c[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\2503fe40\c[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3d590c3f\2503fe40\c[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\dfe0ed5\1b[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\dfe0ed5\1b[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\dfe0ed5\1b[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\dfe0ed5\1b[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\85e83df\dfe0ed5\1b[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.enterpriseservices,2.0.0.0,,b03f5f7f11d50a3a,x86]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[microsoft.visualc,8.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.remoting,2.0.0.0,,b77a5c561934e089,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.directoryservices,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.transactions,2.0.0.0,,b77a5c561934e089,x86]
```

```
   Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:              HKLM\system\wpa\mediacenter[installed]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
   Queries value:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
   Queries value:              HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Value changes:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
   Value changes:              HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
```