Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	739
Risk Level:	7
Date Processed:	2016-05-18 10:32:31 (UTC)
Processing Time:	62.05 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe"

Sample ID:	3308
Type:	basic
Owner:	admin
Label:	6bb534e6c0348b33b54c16dff868e84d
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui:.net
File Size:	53760 bytes
MD5:	6bb534e6c0348b33b54c16dff868e84d
SHA256:	b2b97a02e614803454ab41f62b1d21e177f742cdc9d280c1712f0c0d7d89394c
Description:	None

Pattern Matching Results

2 .NET compiled executable
7 YARA score 7
4 Reads process memory

Static Events

YARA rule hit:	NET_Obfuscation

Process/Thread Events

Creates process:	C:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe ["C:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe"]
Creates process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe [dw20.exe -x -s 456]
Reads from process:	PID:1236 C:\Windows\Temp\6bb534e6c0348b33b54c16dff868e84d.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\dc11b8a9-1ce3-11e6-be80-080027fac36d
Creates event:	\BaseNamedObjects\CorDBIPCSetupSyncEvent_1236

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Roaming
Opens:	C:\Windows\Prefetch\6BB534E6C0348B33B54C16DFF868E-6CD0992B.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\mscoree.dll
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\6bb534e6c0348b33b54c16dff868e84d.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\Microsoft.NET\Framework\v4.0.30319
Opens:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll

```
  Opens:                        C:\Windows\Microsoft.NET\Framework
  Opens:                        C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
  Opens:                        C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
  Opens:                        C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
  Opens:                        C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
  Opens:                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
  Opens:                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
  Opens:                        C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
  Opens:                        C:\Windows\SysWOW64\gdi32.dll
  Opens:                        C:\Windows\SysWOW64\user32.dll
  Opens:                        C:\Windows\SysWOW64\shlwapi.dll
  Opens:                        C:\Windows\SysWOW64\imm32.dll
  Opens:                        C:\Windows\SysWOW64\msctf.dll
  Opens:                        C:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe.config
  Opens:
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6910_none_d089c358442de345
  Opens:
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6910_none_d089c358442de345\msvcr80.dll
  Opens:                        C:\
  Opens:                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\6bb534e6c0348b33b54c16dff868e84d.exe.log
  Opens:                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config
  Opens:                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
  Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
  Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
  Opens:                        C:\Windows\SysWOW64\combase.dll
  Opens:                        C:\Windows\SysWOW64\shell32.dll
  Opens:                        C:\Windows\SysWOW64\SHCore.dll
  Opens:                        C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                        C:\Windows\SysWOW64\profapi.dll
  Opens:                        C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config
  Opens:                        C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\security.config.cch
  Opens:                        C:\Windows\assembly\NativeImages_v2.0.50727_32\index21.dat
  Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\452f06494f05cb9d89325460550d1d62\mscorlib.ni.dll
  Opens:                        C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089
  Opens:                        C:\Windows\Temp
  Opens:                        C:\Windows\SysWOW64\ole32.dll
  Opens:                        C:\Windows\SysWOW64\oleaut32.dll
  Opens:                        C:\Windows\SysWOW64\uxtheme.dll
  Opens:                        C:\Windows\SysWOW64\l_intl.nls
  Opens:                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
  Opens:                        C:\Windows\SysWOW64\tzres.dll
  Opens:                        C:\Windows\SysWOW64\en-US\tzres.dll.mui
  Opens:                        C:\Windows\SysWOW64\version.dll
  Opens:                        C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
  Opens:                        C:\Windows\Microsoft.NET\Framework\v2.0.50727
  Opens:                        C:\Windows\Prefetch\DW20.EXE-1EFBE0F9.pf
  Opens:                        C:\Windows\SysWOW64\psapi.dll
  Opens:                        C:\Windows\SysWOW64\wer.dll
  Opens:                        C:\Windows\SysWOW64\en-US\wer.dll.mui
  Opens:                        C:\Windows\SysWOW64\werui.dll
  Opens:                        C:\Windows\SysWOW64\SensApi.dll
  Opens:                        C:\Windows\SysWOW64\clbcatq.dll
  Opens:                        C:\Windows\SysWOW64\netprofm.dll
  Opens:                        C:\Windows\SysWOW64\slc.dll
  Opens:                        C:\Windows\SysWOW64\cryptsp.dll
  Opens:                        C:\Windows\SysWOW64\rsaenh.dll
  Opens:                        C:\Windows\SysWOW64\npmproxy.dll
  Opens:                        C:\Windows\SysWOW64\en-US\werui.dll.mui
  Opens:                        C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
  Opens:                        C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
  Opens:                        C:\Windows\WindowsShell.Manifest
  Opens:                        C:\Windows\SysWOW64\dui70.dll
  Opens:                   C:\Windows\SysWOW64\duser.dll
  Opens:                   C:\Windows\SysWOW64\riched20.dll
  Opens:                   C:\Windows\SysWOW64\usp10.dll
  Opens:                   C:\Windows\SysWOW64\msls31.dll
  Opens:                   C:\Windows\SysWOW64\dwmapi.dll
  Opens:                   C:\Windows\SysWOW64\xmllite.dll
  Opens:                   C:\Windows\SysWOW64\en-US\duser.dll.mui
  Opens:                   C:\Windows\WinSxS\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.9200.16384_en-us_9f44aa25b2ac1b72
  Opens:                   C:\Windows\WinSxS\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.9200.16384_en-us_9f44aa25b2ac1b72\comctl32.dll.mui
  Opens:                   C:\Windows\win.ini
  Opens:                   C:\Windows\SysWOW64\uxtheme.dll.Config
  Opens:                   C:\Windows\Fonts\StaticCache.dat
  Opens:                   C:\Windows\Fonts\segoeuib.ttf
  Opens:                   C:\Windows\SysWOW64\en-US\erofflps.txt
  Reads from:              C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
  Reads from:              C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
  Reads from:              C:\Windows\win.ini
  Reads from:              C:\Windows\Fonts\StaticCache.dat
```

Windows Registry Events

```
  Creates key:             HKLM\software\microsoft\fusion\gacchangenotification\default
  Opens key:               HKLM\software\microsoft\wow64
  Opens key:               HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:               HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:               HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:               HKLM\system\currentcontrolset\control\nls\language
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:               HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:               HKLM\software\policies\microsoft\mui\settings
  Opens key:               HKCU\
  Opens key:               HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:               HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key:               HKCU\software\policies\microsoft\control panel\desktop
  Opens key:               HKCU\control panel\desktop\languageconfiguration
  Opens key:               HKCU\control panel\desktop
  Opens key:               HKCU\control panel\desktop\muicached
  Opens key:               HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:               HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:               HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:               HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:               HKLM\
  Opens key:               HKLM\software\wow6432node\microsoft\.netframework\policy\
  Opens key:               HKLM\software\wow6432node\microsoft\.netframework\policy\v4.0
  Opens key:               HKLM\software\wow6432node\microsoft\.netframework
  Opens key:               HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:               HKLM\software\microsoft\sqmclient\windows
  Opens key:               HKCU\software\microsoft\.netframework
  Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:               HKLM\software\wow6432node\microsoft\.netframework\policy\standards
  Opens key:
```

```
HKLM\software\wow6432node\microsoft\.netframework\policy\standards\v2.0.50727
  Opens key:                 HKLM\software\wow6432node\microsoft\fusion
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                 HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch
  Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch\v4.0.30319.00000
  Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch\v4.0.30319.00000\mscorwks.dll
  Opens key:                 HKLM\software\microsoft\fusion
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\6bb534e6c0348b33b54c16dff868e84d.exe
  Opens key:                 HKCU\software\microsoft\fusion
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:                 HKLM\software\wow6432node\microsoft\.netframework\ngen\policy\v2.0
  Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets
  Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet
  Opens key:
HKLM\software\wow6432node\microsoft\.netframework\security\policy\extensions\namedpermissionsets\localintranet
  Opens key:                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001
  Opens key:                 HKLM\software\wow6432node\microsoft\ole
  Opens key:                 HKLM\software\microsoft\ole
  Opens key:                 HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                 HKLM\software\microsoft\ole\tracing
  Opens key:                 HKLM\system\currentcontrolset\control\session manager
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                 HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                 HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\windows\explorer
  Opens key:                 HKLM\software\policies\microsoft\windows\explorer
  Opens key:                 HKCU\software\policies\microsoft\windows\explorer
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}\propertybag
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key:
HKLM\software\wow6432node\microsoft\.netframework\v2.0.50727\security\policy
  Opens key:                 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32
  Opens key:                 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index21
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1
  Opens key:                 HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}\propertybag
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\34ba5e84\3aaa9883
  Opens key:                HKLM\software\wow6432node\microsoft\strongname
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                HKCU\software\policies\microsoft\pchealth\errorreporting
  Opens key:                HKLM\software\wow6432node\policies\microsoft\pchealth\errorreporting
  Opens key:                HKLM\software\policies\microsoft\pchealth\errorreporting
  Opens key:                HKCU\software\microsoft\pchealth\errorreporting
  Opens key:                HKLM\software\wow6432node\microsoft\pchealth\errorreporting
  Opens key:                HKCU\software\policies\microsoft\pchealth\errorreporting\exclusionlist
  Opens key:
HKLM\software\wow6432node\policies\microsoft\pchealth\errorreporting\exclusionlist
  Opens key:                HKLM\software\policies\microsoft\pchealth\errorreporting\exclusionlist
  Opens key:                HKCU\software\microsoft\pchealth\errorreporting\exclusionlist
  Opens key:
HKLM\software\wow6432node\microsoft\pchealth\errorreporting\exclusionlist
  Opens key:                HKCU\software\policies\microsoft\pchealth\errorreporting\inclusionlist
  Opens key:
HKLM\software\wow6432node\policies\microsoft\pchealth\errorreporting\inclusionlist
  Opens key:                HKLM\software\policies\microsoft\pchealth\errorreporting\inclusionlist
  Opens key:                HKCU\software\microsoft\pchealth\errorreporting\inclusionlist
  Opens key:
HKLM\software\wow6432node\microsoft\pchealth\errorreporting\inclusionlist
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dw20.exe
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows\appcompat
  Opens key:                HKLM\software\policies\microsoft\windows\appcompat
  Opens key:                HKCU\software\microsoft\windows nt\currentversion
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\dw20.exe
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\dw20.exe
  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
  Opens key:                HKLM\software\wow6432node\microsoft\rpc
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\debug
  Opens key:                HKLM\software\microsoft\windows\windows error reporting
  Opens key:                HKCU\software\microsoft\windows\windows error reporting\consent
  Opens key:                HKLM\software\policies\microsoft\windows\windows error reporting
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\consent
  Opens key:                HKLM\software\microsoft\windows\windows error
reporting\excludedapplications
  Opens key:                HKLM\software\microsoft\windows\windows error
reporting\debugapplications
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\brokerup
  Opens key:                HKCU\software\policies\microsoft\windows\windows error reporting
  Opens key:                HKCU\software\microsoft\windows\windows error reporting
  Opens key:                HKCU\software\microsoft\windows\windows error
reporting\excludedapplications
  Opens key:                HKCU\software\microsoft\windows\windows error
reporting\debugapplications
  Opens key:                HKCU\software\microsoft\windows\windows error reporting\brokerup
  Opens key:                HKLM\software\microsoft\reliability analysis\rac
  Opens key:                HKCU\software\microsoft\telemetryclient\throttlestore
  Opens key:                HKLM\software\microsoft\telemetryclient\samplestore
  Opens key:                HKLM\software\microsoft\telemetryclient\samplestore\watson
  Opens key:                HKCU\software\microsoft\windows\windows error
reporting\throttling\clr20r3
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\syspreplock
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}
  Opens key:                HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\treatas
  Opens key:                HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler
  Opens key:                HKLM\software\wow6432node\microsoft\rpc\extensions
  Opens key:                HKLM\software\microsoft\rpc\extensions
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}
  Opens key:                HKCR\activatableclasses\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}
  Opens key:                HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\treatas
  Opens key:                HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler
  Opens key:                HKCU\software\classes\appid\dw20.exe
  Opens key:                HKCR\appid\dw20.exe
  Opens key:                HKLM\software\wow6432node\microsoft\ole\appcompat
  Opens key:                HKLM\software\microsoft\ole\appcompat
  Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\wow6432node\microsoft\cryptography\offload
  Opens key:                HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
```

```
  Opens key:                HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKCU\software\classes\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-
199fdba5723b}
  Opens key:                HKCR\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
  Opens key:                HKCU\software\classes\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-
199fdba5723b}\proxystubclsid32
  Opens key:                HKCR\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-
199fdba5723b}\proxystubclsid32
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}
  Opens key:                HKCR\activatableclasses\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}
  Opens key:                HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\treatas
  Opens key:                HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler
  Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8
  Opens key:                HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows
  Opens key:                HKLM\software\microsoft\telemetryclient\throttlestore\sqm
  Opens key:                HKLM\software\microsoft\telemetryclient\throttlestore
  Opens key:                HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
  Opens key:                HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows
  Opens key:                HKLM\software\microsoft\telemetryclient\samplestore\sqm
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238528
  Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784
  Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
  Opens key:                HKLM\software\wow6432node\microsoft\directui
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:                HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\compatibility\dw20.exe
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\knownclasses
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}
  Opens key:                HKCR\activatableclasses\clsid\{713aacc8-3b71-435c-a3a1-be4e53621ab1}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}
  Opens key:                HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-be4e53621ab1}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\treatas
  Opens key:                HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-be4e53621ab1}\treatas
```

```
 Opens key:                HKCU\software\classes\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprocserver32
 Opens key:                HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprocserver32
 Opens key:                HKCU\software\classes\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprochandler32
 Opens key:                HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprochandler32
 Opens key:                HKCU\software\classes\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprochandler
 Opens key:                HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprochandler
 Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
 Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
 Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
 Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
 Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
 Queries value:            HKCU\control panel\desktop[preferreduilanguages]
 Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
 Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
 Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
 Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
 Queries value:            HKLM\software\wow6432node\microsoft\.netframework[installroot]
 Queries value:            HKLM\software\wow6432node\microsoft\.netframework[clrloadlogdir]
 Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
 Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[6bb534e6c0348b33b54c16dff868e84d]
 Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
 Queries value:
HKLM\software\wow6432node\microsoft\.netframework[uselegacyv2runtimeactivationpolicydefaultvalue]
 Queries value:            HKLM\software\wow6432node\microsoft\.netframework[onlyuselatestclr]
 Queries value:            HKLM\software\wow6432node\microsoft\fusion[noclientchecks]
 Queries value:            HKLM\software\wow6432node\microsoft\.netframework[gcstressstart]
 Queries value:            HKLM\software\wow6432node\microsoft\.netframework[gcstressstartatjit]
 Queries value:            HKLM\software\wow6432node\microsoft\.netframework[disableconfigcache]
 Queries value:            HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-
931b-d9cc2eee27e4]
 Queries value:            HKLM\system\currentcontrolset\control\wmi\security[cc2bcbba-16b6-4cf3-
8990-d74c2e8af500]
 Queries value:            HKLM\software\microsoft\fusion[cachelocation]
 Queries value:            HKLM\software\microsoft\fusion[downloadcachequotainkb]
 Queries value:            HKLM\software\microsoft\fusion[enablelog]
 Queries value:            HKLM\software\microsoft\fusion[logginglevel]
 Queries value:            HKLM\software\microsoft\fusion[forcelog]
 Queries value:            HKLM\software\microsoft\fusion[logfailures]
 Queries value:            HKLM\software\microsoft\fusion[versioninglog]
 Queries value:            HKLM\software\microsoft\fusion[logresourcebinds]
 Queries value:            HKLM\software\microsoft\fusion[uselegacyidentityformat]
 Queries value:            HKLM\software\microsoft\fusion[disablemsipeek]
 Queries value:            HKLM\software\microsoft\fusion[noclientchecks]
 Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options[devoverrideenable]
 Queries value:
HKLM\software\wow6432node\microsoft\.netframework\ngen\policy\v2.0[optimizeusedbinaries]
 Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
 Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
 Queries value:              HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[category]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[name]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[description]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[infotip]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[icon]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[security]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[roamable]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[precreate]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[stream]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[attributes]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
 Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
 Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
 Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
 Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[category]
```

```
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001[profileimagepath]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index21[niusagemask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index21[ilusagemask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[configmask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[configstring]
```

```
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[mvid]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[evalationdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[ildependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[nidependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\1[missingdependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\27a18466\1[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[stream]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[attributes]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[foldertypeid]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
 Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
 Queries value:            HKLM\system\currentcontrolset\control\cmf\config[system]
 Queries value:            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
 Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
 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[dw20.exe]
 Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[dw20]
 Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value:            HKLM\system\setup[oobeinprogress]
 Queries value:            HKLM\system\setup[systemsetupinprogress]
 Queries value:            HKLM\software\microsoft\rpc[idletimerwindow]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[machineid]
 Queries value:            HKCU\software\microsoft\windows\windows error
reporting\consent[defaultconsent]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting[dontsendadditionaldata]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[disabled]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting\consent[defaultconsent]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting\consent[defaultoverridebehavior]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting\consent[clr20r3]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[loggingdisabled]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[dontshowui]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[disablearchive]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting[configurearchive]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[disablequeue]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[maxqueuecount]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[maxarchivecount]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[forcequeue]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting[queuepesterinterval]
 Queries value:            HKLM\software\microsoft\windows\windows error reporting[sendefsfiles]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting[bypassdatathrottling]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting[forceusermodecabcollection]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting\brokerup[clr20r3]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting[bypasspowerthrottling]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting[bypassnetworkcostthrottling]
 Queries value:            HKLM\software\microsoft\windows\windows error
reporting[queuenopesterinterval]
 Queries value:            HKCU\software\microsoft\windows\windows error
reporting[dontsendadditionaldata]
```

```
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[disabled]
  Queries value:            HKCU\software\microsoft\windows\windows error
reporting\consent[defaultoverridebehavior]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting\consent[clr20r3]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[loggingdisabled]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[dontshowui]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[disablearchive]
  Queries value:            HKCU\software\microsoft\windows\windows error
reporting[configurearchive]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[disablequeue]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[maxqueuecount]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[maxarchivecount]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[forcequeue]
  Queries value:            HKCU\software\microsoft\windows\windows error
reporting[queuepesterinterval]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[sendefsfiles]
  Queries value:            HKCU\software\microsoft\windows\windows error
reporting[bypassdatathrottling]
  Queries value:            HKCU\software\microsoft\windows\windows error
reporting[forceusermodecabcollection]
  Queries value:            HKCU\software\microsoft\windows\windows error
reporting[bypasspowerthrottling]
  Queries value:            HKCU\software\microsoft\windows\windows error
reporting[bypassnetworkcostthrottling]
  Queries value:            HKCU\software\microsoft\windows\windows error
reporting[queuenopesterinterval]
  Queries value:            HKLM\software\microsoft\windows\windows error
reporting[corporatewerserver]
  Queries value:            HKLM\software\microsoft\windows\windows error
reporting[corporatewerusessl]
  Queries value:            HKLM\software\microsoft\windows\windows error
reporting[corporatewerportnumber]
  Queries value:            HKLM\software\microsoft\windows\windows error
reporting[corporateweruseauthentication]
  Queries value:            HKLM\software\microsoft\reliability analysis\rac[racwersampletime]
  Queries value:            HKLM\software\microsoft\windows\windows error reporting[restartruntime]
  Queries value:            HKCU\software\microsoft\windows\windows error reporting[restartruntime]
  Queries value:            HKLM\software\microsoft\telemetryclient\samplestore[sampledout]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[fcd00fef-04fa-41c0-
889e-ae613d97602b]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}[]
  Queries value:            HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:            HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:            HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]
  Queries value:            HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:            HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
  Queries value:            HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:            HKCR\wow6432node\interface\{d0074ffd-570f-4a9b-8d69-
199fdba5723b}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
  Queries value:              HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses[44d72c57]
  Queries value:              HKLM\software\microsoft\sqmclient\windows[studyid]
  Queries value:              HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:              HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
  Queries value:              HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:              HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
  Queries value:              HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
  Queries value:              HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:              HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:              HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-be4e53621ab1}[]
  Queries value:              HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-
be4e53621ab1}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
```