

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3308, Task ID: 742

Task ID:	742
Risk Level:	7
Date Processed:	2016-05-18 10:32:37 (UTC)
Processing Time:	65.36 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 396]
Reads from process:	PID: 2200 C:\Windows\Temp\6bb534e6c0348b33b54c16dff868e84d.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\17757556-1ce4-11e6-ba45-080027b54693
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\BaseNamedObjects\CorDBIPCSyncSetupSyncEvent_2200
Creates event:	\KernelObjects\LowMemoryCondition
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
Creates event:	\KernelObjects\MaximumCommitCondition

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\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\mscoree.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\MSCOREEE.DLL.local
Opens:	C:\Windows\Microsoft.NET\Framework\v2.0.50727
Opens:	C:\Windows\Microsoft.NET\Framework\Upgrades.2.0.50727\
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe.config
Opens:	C:\Windows\Temp\6bb534e6c0348b33b54c16dff868e84d.exe

Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
 Opens: C:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.exe.Local\
 Opens:
 C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
 Opens:
 C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
 Opens: C:\
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localalgac
 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\Globalization\Sorting\SortDefault.nls
 Opens: C:\windows\temp\profapi.dll
 Opens: C:\Windows\SysWOW64\profapi.dll
 Opens: C:\Users\Admin
 Opens: C:\Users\Admin\AppData\Roaming
 Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
 Config\v2.0.50727.312\security.config
 Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
 Config\v2.0.50727.312\security.config.cch
 Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\index127.dat
 Opens:
 C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
 Opens: C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089
 Opens: C:\Windows\Temp
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
 Opens: C:\Windows\SysWOW64\rpcss.dll
 Opens: C:\Windows\SysWOW64\uxtheme.dll
 Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens: C:\windows\temp\6bb534e6c0348b33b54c16dff868e84d.config
 Opens: C:\Windows\SysWOW64\l_intl.nls
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
 Opens: C:\Windows\SysWOW64\tzres.dll
 Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\VERSION.dll
 Opens: C:\windows\temp\VERSION.dll
 Opens: C:\Windows\SysWOW64\version.dll
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
 Opens: C:\Windows\SysWOW64\apphelp.dll
 Opens: C:\Windows\AppPatch\sysmain.sdb
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\ui\SwDRM.dll
 Opens: C:\Windows\Prefetch\DW20.EXE-1EFBE0F9.pf
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe.Local\
 Opens: C:\Windows\SysWOW64\wer.dll
 Opens: C:\Windows\SysWOW64\en-US\wer.dll.mui
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\SensApi.dll
 Opens: C:\Windows\SysWOW64\SensApi.dll
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\werui.dll
 Opens: C:\Windows\SysWOW64\werui.dll
 Opens: C:\Windows\SysWOW64\en-US\werui.dll.mui
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\DUI70.dll
 Opens: C:\Windows\SysWOW64\dui70.dll
 Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
 controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
 Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
 controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
 Opens: C:\Windows\WindowsShell.Manifest
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\DUser.dll
 Opens: C:\Windows\SysWOW64\duser.dll
 Opens: C:\Windows\SysWOW64\riched20.dll
 Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\dwmapapi.dll
 Opens: C:\Windows\SysWOW64\dwmapapi.dll
 Opens: C:\Windows\SysWOW64\xmlite.dll
 Opens: C:\Windows\SysWOW64\en-US\duser.dll.mui
 Opens: C:\Windows\winsxs\x86_microsoft.windows.c.-
 controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9
 Opens: C:\Windows\winsxs\x86_microsoft.windows.c.-

controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\win.ini
Opens: C:\Windows\SysWOW64\uxtheme.dll.Config
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\Windows\Fonts\segoeui.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\Fonts\StaticCache.dat
Reads from: C:\Windows\win.ini

Windows Registry Events

Creates key: HKLM\software\microsoft\fusion\gacchangenotification\default
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\ddl
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\
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\v2.0
Opens key: HKLM\software\wow6432node\microsoft\.netframework
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\upgrades
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\standards
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\apppatch
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: HKCU\software\microsoft\.netframework\policy\standards
Opens key: HKLM\software\wow6432node\microsoft\windows
Opens key: HKLM\software\wow6432node\microsoft\.netframework\policy\standards\v2.0.50727
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\microsoft\.netframework
Opens key: HKLM\software\microsoft\fusion
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\6bb534e6c0348b33b54c16dff868e84d.exe
Opens key: HKCU\software\microsoft\fusion
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-1-5-21-980053277-1733835069-2361817685-1001
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\wow6432node\microsoft\ole
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\ole\tracing
Opens key:
HKLM\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\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\knownfolderssettings
Opens key:
HKLM\software\wow6432node\microsoft\.netframework\v2.0.50727\security\policy
Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32
Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index127
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83
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\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\currentversion\explorer\shell folders
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
 Opens key: HKCU\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\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\policies\microsoft\sqlclient\windows
 Opens key: HKLM\software\microsoft\sqlclient\windows
 Opens key: HKLM\software\microsoft\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: 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: HKLM\software\microsoft\reliability analysis\rac
 Opens key: HKCU\software\microsoft\windows\windows error
 reporting\throttling\clr20r3
 Opens key: HKLM\software\wow6432node\microsoft\directui
 Opens key: HKLM\software\wow6432node\microsoft\oleaut
 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: HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key: HKLM\software\wow6432node\microsoft\ctf\compatibility\dw20.exe
 Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\wow6432node\microsoft\ctf\
 Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
 Opens key: HKCU\software\classes\
 Opens key: HKLM\software\microsoft\com3
 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}\progid
 Opens key: HKCR\wow6432node\clsid\{713aacc8-3b71-435c-a3a1-be4e53621ab1}\progid
 Opens key: HKCU\software\classes\clsid\{713aacc8-3b71-435c-a3a1-be4e53621ab1}
 Opens key: HKCR\clsid\{713aacc8-3b71-435c-a3a1-be4e53621ab1}
 Opens key: HKCU\software\classes\clsid\{713aacc8-3b71-435c-a3a1-be4e53621ab1}\progid
 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\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]
 Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
 Queries value: HKLM\system\currentcontrolset\control\cls\sorting\versions[]
 Queries value: HKLM\system\currentcontrolset\control\cls\session manager[safedllsearchmode]
 Queries value: HKLM\system\currentcontrolset\control\cls\customlocale[empty]
 Queries value: HKLM\system\currentcontrolset\control\cls\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: HKLM\software\wow6432node\microsoft\framework[installroot]
 Queries value: HKLM\software\wow6432node\microsoft\framework[clrloadlogdir]
 Queries value: HKLM\software\wow6432node\microsoft\framework[onlyuselatestclr]
 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\framework[gcstressstart]
 Queries value: HKLM\software\wow6432node\microsoft\framework[gcstressstartatjit]
 Queries value: HKLM\software\wow6432node\microsoft\framework[disableconfigcache]
 Queries value: HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-931b-d9cc2eee27e4]
 Queries value: HKLM\system\currentcontrolset\control\wmi\security[cc2bcbbba-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\microsoft\ole[pageallocatorusesystemheap]
  Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
  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}[parsiname]
  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\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}[parsiname]
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-1-5-21-980053277-1733835069-2361817685-1001[profileimagepath]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index127[niusagemask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index127[ilusagemask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[configstring]
Queries value:

HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[evaluationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\83[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\83[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[disablelocaloverride]

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\sqmclient\windows[ceipenable]

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[senddfsfiles]

Queries value: HKLM\software\microsoft\windows\windows error
reporting[bypassdatathrottling]

Queries value: HKLM\software\microsoft\windows\windows error
reporting[forceusermodecabcollection]

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[senddfsfiles]
 Queries value: HKCU\software\microsoft\windows\windows error
 reporting[bypassdatathrottling]
 Queries value: HKCU\software\microsoft\windows\windows error
 reporting[forceusermodecabcollection]
 Queries value: HKLM\software\microsoft\windows\windows error
 reporting[corporatewserver]
 Queries value: HKLM\software\microsoft\windows\windows error
 reporting[corporatewusessl]
 Queries value: HKLM\software\microsoft\windows\windows error
 reporting[corporatewserverportnumber]
 Queries value: HKLM\software\microsoft\windows\windows error
 reporting[corporatewserveruseauthentication]
 Queries value: HKLM\software\microsoft\reliability analysis\rac[racwrsampletime]
 Queries value: HKLM\software\microsoft\windows\windows error reporting[restartruntime]
 Queries value: HKCU\software\microsoft\windows\windows error reporting[restartruntime]
 Queries value: HKLM\system\currentcontrolset\control\wmi\security[fcd00fef-04fa-41c0-
 889e-ae613d97602b]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[safeprocesssearchmode]
 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: 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[scrollldelay]
 Queries value: HKCU\software\microsoft\windows
 nt\currentversion\windows[scrollinterval]
 Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
 Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]

Queries value: HKLM\software\microsoft\com3[com+enabled]
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\ole[maxsxshashcount]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
Value changes: HKLM\software\microsoft\rpc[uuidsequencenumber]