Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	2405
Risk Level:	6
Date Processed:	2016-02-22 05:26:52 (UTC)
Processing Time:	34.8 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe"

Sample ID:	615
Type:	basic
Owner:	admin
Label:	8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96
Date Added:	2016-02-22 05:26:48 (UTC)
File Type:	PE32:win32:gui:.net
File Size:	50688 bytes
MD5:	d3109c83e07dd5d7fe032dc80c581d08
SHA256:	8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96
Description:	None

Pattern Matching Results

2 .NET compiled executable
3 Long sleep detected
5 Abnormal sleep detected
6 Creates executable in application data folder
3 Writes to a log file [Info]

Process/Thread Events

Creates process:
C:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
["C:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe"]
Terminates process:
C:\Windows\Temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\CPFATE_2832_v4.0.30319

File System Events

Creates:	C:\Users\Admin\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe.log
Opens:	C:\Windows\Prefetch\8995535721EBEAF6983C6CECF3182-53289CA2.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\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.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\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe.config
Opens:	C:\Windows\SysWOW64\msvcr110_clr0400.dll

```
  Opens:                 C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
  Opens:                 C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.log
  Opens:                 C:\Windows\SysWOW64\combase.dll
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe.log
  Opens:                 C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                 C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib
  Opens:
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\51e2934144ba15628ba5a31be2dae7dc\mscorlib.ni.dll.aux
  Opens:
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\51e2934144ba15628ba5a31be2dae7dc\mscorlib.ni.dll
  Opens:                 C:\
  Opens:                 C:\Windows\Temp
  Opens:                 C:\Windows\SysWOW64\ole32.dll
  Opens:                 C:\Windows\SysWOW64\oleaut32.dll
  Opens:                 C:\Windows\assembly\NativeImages_v4.0.30319_32\tDiscoverer\
  Opens:                 C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
  Opens:                 C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core
  Opens:
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\b9f7adbc90a2bcbe8eb9e6e8d2bb975b\System.Core.ni.dll.aux
  Opens:                 C:\Windows\assembly\NativeImages_v4.0.30319_32\System
  Opens:
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\e40da7a49f8c3f0108e7c835b342f382\System.ni.dll.aux
  Opens:
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\e40da7a49f8c3f0108e7c835b342f382\System.ni.dll
  Opens:
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\b9f7adbc90a2bcbe8eb9e6e8d2bb975b\System.Core.ni.dll
  Opens:                 C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.CSharp\
  Opens:
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.CSharp\v4.0_4.0.0.0__b03f5f7f11d50a3a\Microsoft.CSharp.dll
  Opens:                 C:\Windows\SysWOW64\version.dll
  Opens:                 C:\Windows\SysWOW64\tzres.dll
  Opens:                 C:\Windows\SysWOW64\en-US\tzres.dll.mui
  Opens:                 C:\Windows\SysWOW64\sxs.dll
  Opens:                 C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
  Opens:                 C:\Windows\SysWOW64\clbcatq.dll
  Opens:                 C:\Windows\SysWOW64\cryptsp.dll
  Opens:                 C:\Windows\SysWOW64\rsaenh.dll
  Opens:                 C:\Program Files (x86)\Internet Explorer\ieproxy.dll
  Opens:                 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll
  Opens:                 C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dynamic\
  Opens:
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Dynamic\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Dynamic.dll
  Opens:                 C:\Windows\SysWOW64\mshtml.tlb
  Opens:                 C:\Windows\SysWOW64\stdole2.tlb
  Opens:                 C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers
  Opens:
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\8a37b97ce8d5b322c455be3dd440e5f2\CustomMarshalers.ni.dll.aux
  Opens:
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\8a37b97ce8d5b322c455be3dd440e5f2\CustomMarshalers.ni.dll
  Opens:
C:\Windows\Microsoft.NET\assembly\GAC_32\CustomMarshalers\v4.0_4.0.0.0__b03f5f7f11d50a3a\CustomMarshalers.dll
  Opens:
C:\Windows\Microsoft.Net\assembly\GAC_32\CustomMarshalers\v4.0_4.0.0.0__b03f5f7f11d50a3a\CustomMarshalers.dll.config
  Writes to:
C:\Users\Admin\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe.log
  Reads from:            C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
  Reads from:            C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.log
  Reads from:
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\51e2934144ba15628ba5a31be2dae7dc\mscorlib.ni.dll.aux
  Reads from:
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\b9f7adbc90a2bcbe8eb9e6e8d2bb975b\System.Core.ni.dll.aux
  Reads from:
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\e40da7a49f8c3f0108e7c835b342f382\System.ni.dll.aux
  Reads from:            C:\Windows\SysWOW64\mshtml.tlb
  Reads from:            C:\Windows\SysWOW64\stdole2.tlb
  Reads from:
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\8a37b97ce8d5b322c455be3dd440e5f2\CustomMarshalers.ni.dll.aux
```

Windows Registry Events

```
  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\v4.0.30319
  Opens key:                HKLM\software\wow6432node\microsoft\fusion
  Opens key:                HKLM\software\wow6432node\microsoft\.netframework\v4.0.30319\skus\
  Opens key:
HKLM\software\wow6432node\microsoft\.netframework\v4.0.30319\skus\default
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\fusion
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.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\ole
  Opens key:                HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\wow6432node\microsoft\.netframework\ngen\policy\v4.0
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  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\wow6432node\microsoft\strongname
  Opens key:                HKLM\software\microsoft\fusion\publisherpolicy\default
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.system.core__b77a5c561934e089
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.core__b77a5c561934e089
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.system__b77a5c561934e089
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system__b77a5c561934e089
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.system.configuration__b03f5f7f11d50a3a
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.configuration__b03f5f7f11d50a3a
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.system.xml__b77a5c561934e089
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.xml__b77a5c561934e089
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.system.numerics__b77a5c561934e089
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.numerics__b77a5c561934e089
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.system.security__b03f5f7f11d50a3a
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.security__b03f5f7f11d50a3a
  Opens key:                HKLM\software\wow6432node\microsoft\.netframework\policy\aptca
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.microsoft.csharp__b03f5f7f11d50a3a
```

```
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.microsoft.csharp__b03f5f7f11d50a3a
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  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:                HKCU\software\microsoft\internet explorer\main
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\localserver32
  Opens key:                HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\localserver32
  Opens key:                HKCU\software\classes\clsid\{0002df01-0000-0000-c000-
000000000046}\localserver32
  Opens key:                HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{0002df01-0000-0000-c000-
000000000046}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{0002df01-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\treatas
  Opens key:                HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\inprochandler
  Opens key:
HKCU\software\classes\appid\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
  Opens key:
HKCR\appid\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.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:                HKLM\software\wow6432node\microsoft\rpc\extensions
  Opens key:                HKLM\software\microsoft\rpc\extensions
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                HKCR\activatableclasses\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                HKCR\clsid\{0000032a-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\activatableclasses\clsid
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{0000032a-0000-0000-c000-
000000000046}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{00000339-0000-0000-c000-
000000000046}
  Opens key:                HKCR\activatableclasses\clsid\{00000339-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00000339-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\clsid\{00000339-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\clsid\{00000339-0000-0000-c000-000000000046}
  Opens key:                HKCR\clsid\{00000339-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{00000339-0000-0000-c000-
000000000046}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}
```

```
  Opens key:                 HKCR\activatableclasses\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}
  Opens key:                 HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}\inprochandler
  Opens key:                 HKCU\software\classes\wow6432node\interface\{5f568e3e-317c-402e-a883-
546b0f7673a4}
  Opens key:                 HKCR\wow6432node\interface\{5f568e3e-317c-402e-a883-546b0f7673a4}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{5f568e3e-317c-402e-a883-
546b0f7673a4}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{5f568e3e-317c-402e-a883-
546b0f7673a4}\proxystubclsid32
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}
  Opens key:                 HKCR\activatableclasses\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}
  Opens key:                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
  Opens key:                 HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\wow6432node\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{00020420-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\activatableclasses\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                 HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001
  Opens key:                 HKCU\software\classes\wow6432node\interface\{b196b283-bab4-101a-b69c-
00aa00341d07}
  Opens key:                 HKCR\wow6432node\interface\{b196b283-bab4-101a-b69c-00aa00341d07}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{b196b283-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{b196b283-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}
  Opens key:                    HKCR\activatableclasses\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}
  Opens key:                    HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\treatas
  Opens key:                    HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32
  Opens key:                    HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler32
  Opens key:                    HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler32
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler
  Opens key:                    HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler
  Opens key:                    HKCU\software\classes\wow6432node\interface\{00020401-0000-0000-c000-
000000000046}
  Opens key:                    HKCR\wow6432node\interface\{00020401-0000-0000-c000-000000000046}
  Opens key:                    HKCU\software\classes\wow6432node\interface\{00020401-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                    HKCR\wow6432node\interface\{00020401-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                    HKLM\software\microsoft\windowsruntime\clsid\{00020422-0000-0000-c000-
000000000046}
  Opens key:                    HKCR\activatableclasses\clsid\{00020422-0000-0000-c000-000000000046}
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}
  Opens key:                    HKCR\wow6432node\clsid\{00020422-0000-0000-c000-000000000046}
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\treatas
  Opens key:                    HKCR\wow6432node\clsid\{00020422-0000-0000-c000-000000000046}\treatas
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                    HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                    HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                    HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
  Opens key:                    HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
  Opens key:                    HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0
  Opens key:                    HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.7.0.microsoft.mshtml__b03f5f7f11d50a3a
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.7.0.microsoft.mshtml__b03f5f7f11d50a3a
  Opens key:                    HKLM\software\microsoft\windows\currentversion\installer\managed\s-1-5-
21-1923240461-1905901954-2556564120-
1001\installer\assemblies\c:|windows|temp|8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
  Opens key:
HKCU\software\microsoft\installer\assemblies\c:|windows|temp|8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
  Opens key:
HKCR\installer\assemblies\c:|windows|temp|8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
  Opens key:                    HKLM\software\microsoft\windows\currentversion\installer\managed\s-1-5-
21-1923240461-1905901954-2556564120-1001\installer\assemblies\global
  Opens key:                    HKCU\software\microsoft\installer\assemblies\global
  Opens key:                    HKCR\installer\assemblies\global
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.system.dynamic__b03f5f7f11d50a3a
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.dynamic__b03f5f7f11d50a3a
  Opens key:                    HKCU\software\classes\wow6432node\interface\{3050f55f-98b5-11cf-bb82-
00aa00bdce0b}
  Opens key:                    HKCR\wow6432node\interface\{3050f55f-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                    HKCU\software\classes\wow6432node\interface\{3050f55f-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32
  Opens key:                    HKCR\wow6432node\interface\{3050f55f-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32
  Opens key:                    HKCU\software\classes\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}
  Opens key:                    HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                HKCU\software\classes\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32
  Opens key:                HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{00020424-0000-0000-c000-
000000000046}
  Opens key:                HKCR\activatableclasses\clsid\{00020424-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
  Opens key:                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                HKCU\software\classes\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\forward
  Opens key:                HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\forward
  Opens key:                HKCU\software\classes\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\forward
  Opens key:                HKCR\interface\{3050f21f-98b5-11cf-bb82-00aa00bdce0b}\forward
  Opens key:                HKCU\software\classes\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\typelib
  Opens key:                HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\typelib
  Opens key:                HKCU\software\classes\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                HKCR\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                HKCU\software\classes\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}\4.0
  Opens key:                HKCR\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}\4.0
  Opens key:                HKCU\software\classes\typelib\{3050f1c5-98b5-11cf-bb82-
00aa00bdce0b}\4.0\0
  Opens key:                HKCR\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}\4.0\0
  Opens key:                HKCU\software\classes\typelib\{3050f1c5-98b5-11cf-bb82-
00aa00bdce0b}\4.0\0\win32
  Opens key:                HKCR\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}\4.0\0\win32
  Opens key:                HKCU\software\classes\typelib
  Opens key:                HKCR\typelib
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0\win32
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.custommarshalers__b03f5f7f11d50a3a
  Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.custommarshalers__b03f5f7f11d50a3a
  Opens key:                HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\interface\{00020404-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKCR\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{00020421-0000-0000-c000-
000000000046}
  Opens key:                HKCR\activatableclasses\clsid\{00020421-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\treatas
  Opens key:                HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler32
```

```
  Opens key:                HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                HKCU\software\classes\wow6432node\clsid\{3050f27e-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{3050f27e-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{3050f27e-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCR\wow6432node\clsid\{3050f27e-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCU\software\classes\clsid\{3050f27e-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCR\clsid\{3050f27e-98b5-11cf-bb82-00aa00bdce0b}\localserver32
  Opens key:                HKCU\software\classes\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}
  Opens key:                HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:                HKCU\software\classes\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32
  Opens key:                HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32
  Opens key:                HKCU\software\classes\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\forward
  Opens key:                HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\forward
  Opens key:                HKCU\software\classes\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\forward
  Opens key:                HKCR\interface\{3050f1ff-98b5-11cf-bb82-00aa00bdce0b}\forward
  Opens key:                HKCU\software\classes\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\typelib
  Opens key:                HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\typelib
  Opens key:                HKCU\software\classes\wow6432node\clsid\{3050f491-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{3050f491-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{3050f491-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCR\wow6432node\clsid\{3050f491-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCU\software\classes\clsid\{3050f491-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCR\clsid\{3050f491-98b5-11cf-bb82-00aa00bdce0b}\localserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{3050f248-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{3050f248-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{3050f248-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCR\wow6432node\clsid\{3050f248-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCU\software\classes\clsid\{3050f248-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:                HKCR\clsid\{3050f248-98b5-11cf-bb82-00aa00bdce0b}\localserver32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  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[8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96]
  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\system\currentcontrolset\control\session manager[safedllsearchmode]
  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[763fd754-7086-4dfe-
95eb-c01a46faf4ca]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[a669021c-c450-4609-
a035-5af59af4df18]
  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[logresourcebinds]
  Queries value:            HKLM\software\microsoft\fusion[fileinuseretryattempts]
  Queries value:            HKLM\software\microsoft\fusion[fileinusemillisecondsbetweenretries]
  Queries value:            HKLM\software\microsoft\fusion[uselegacyidentityformat]
  Queries value:            HKLM\software\microsoft\fusion[disablemsipeek]
  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[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
  Queries value:
HKLM\software\wow6432node\microsoft\.netframework\ngen\policy\v4.0[optimizeusedbinaries]
  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\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\fusion\publisherpolicy\default[latest]
  Queries value:            HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:            HKCU\software\microsoft\internet explorer\main[disablefirstruncustomize]
  Queries value:            HKCU\software\microsoft\internet explorer\main[check_associations]
  Queries value:            HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-
000000000046}\localserver32[class]
  Queries value:            HKCR\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32[class]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}[]
  Queries value:            HKLM\software\microsoft\ole[maxsxshashcount]
  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\rpc\extensions[ndroleextdll]
  Queries value:            HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}[]
  Queries value:            HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
2878998f69a2}\inprochandler32[]
  Queries value:            HKCR\wow6432node\interface\{5f568e3e-317c-402e-a883-
546b0f7673a4}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
  Queries value:            HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[threadingmodel]
```

```
  Queries value:            HKCR\wow6432node\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}[]
  Queries value:            HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001[name]
  Queries value:            HKCR\wow6432node\interface\{b196b283-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
  Queries value:            HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[threadingmodel]
  Queries value:            HKCR\wow6432node\interface\{00020401-0000-0000-c000-
000000000046}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{00020422-0000-0000-c000-000000000046}[]
  Queries value:            HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:            HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0[implementedinthisversion]
  Queries value:            HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0[assembly]
  Queries value:            HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0[class]
  Queries value:            HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0[runtimeversion]
  Queries value:            HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0[codebase]
  Queries value:            HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[]
  Queries value:            HKCR\wow6432node\interface\{3050f55f-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}[]
  Queries value:            HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:            HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\typelib[]
  Queries value:            HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
00aa00bdce0b}\typelib[version]
  Queries value:            HKCR\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}\4.0\0\win32[]
  Queries value:            HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
  Queries value:            HKLM\software\microsoft\rpc[udtalignmentpolicy]
  Queries value:            HKCR\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}[]
  Queries value:            HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:            HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\proxystubclsid32[]
  Queries value:            HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\typelib[]
  Queries value:            HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
00aa00bdce0b}\typelib[version]
  Sets/Creates value:       HKCU\software\microsoft\internet explorer\main[disablefirstruncustomize]
```