# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 615, Task ID: 2405

Task ID: 2405

Risk Level:

Date Processed: 2016-02-22 05:26:52 (UTC)

Processing Time: 34.8 seconds IntelliVM Virtual Environment:

**Execution Arguments:** 

c:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe"

Sample ID: Type: basic admin Owner:

Label: 8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96

2016-02-22 05:26:48 (UTC) Date Added: File Type: PE32:win32:gui:.net

50688 bytes File Size:

MD5: d3109c83e07dd5d7fe032dc80c581d08

SHA256: 8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96

Description:

## Pattern Matching Results

2 .NET compiled executable

3 Long sleep detected

5 Abnormal sleep detected

Creates executable in application data folder

3 Writes to a log file [Info]

#### Process/Thread Events

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

Opens: C:\Windows\Prefetch\8995535721EBEAF6983C6CECF3182-53289CA2.pf

Opens: C:\Windows

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

C:\Windows\SysWOW64 Opens:

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

C:\Windows\Temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe

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

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

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

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

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

 $\label{lem:c:windows} $$C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll $$$ Opens: 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 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: Opens: C:\Windows\SysWOW64\user32.dll Opens: C:\Windows\SysWOW64\shlwapi.dll C:\Windows\SysWOW64\imm32.dll Opens: Opens: C:\Windows\SysWOW64\msctf.dll

Opens:

C:\windows\temp\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe.config

C:\Windows\SysWOW64\msvcr110\_clr0400.dll Opens:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
        Opens:
       Opens:
                                                                                                     C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.log
                                                                                                     C:\Windows\SysWOW64\combase.dll
       Opens:
        Opens:
 C:\Users\Admin\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe.log
                                                                                                     C:\Windows\Globalization\Sorting\SortDefault.nls
       Opens:
                                                                                                     C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib
       Opens:
        Opens:
 C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\51e2934144ba15628ba5a31be2dae7dc\mscorlib.ni.dll.aux
 C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\51e2934144ba15628ba5a31be2dae7dc\mscorlib.ni.dll
        Opens:
        Opens:
                                                                                                     C:\Windows\Temp
       Opens:
                                                                                                     C:\Windows\SysWOW64\ole32.dll
                                                                                                     C:\Windows\SvsWOW64\oleaut32.dll
       Opens:
        Opens:
                                                                                                     C:\Windows\assembly\NativeImages_v4.0.30319_32\tDiscoverer\
       Opens:
                                                                                                     C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
                                                                                                    C: \verb|\windows\assembly\NativeImages_v4.0.30319_32\System.Core| \\
       Opens:
        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 \Native Images\_v4.0.30319\_32 \System \eqda7a49f8c3f0108e7c835b342f382 \System.ni.dll.aux \assembly \As
C: \verb|\windows| assembly \verb|\NativeImages| v4.0.30319\_32 \\ System | e40 \\ da7a49 \\ f8c3 \\ f010 \\ 8e7c835 \\ b342 \\ f382 \\ System.ni.dll \\ and all \\ and \\ a
       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: \verb|\windows| Microsoft.NET| assembly GAC_MSIL \verb|\windows| Microsoft.CSharp| v4.0\_4.0.0.0\_b03f5f7f11d50a3a \verb|\windows| Microsoft.CSharp.dll| Microsoft.
        Opens:
                                                                                                     C:\Windows\SysWOW64\version.dll
                                                                                                     C:\Windows\SysWOW64\tzres.dll
        Opens:
       Opens:
                                                                                                     C:\Windows\SysWOW64\en-US\tzres.dll.mui
                                                                                                     C:\Windows\SysWOW64\sxs.dll
       Opens:
        Opens:
                                                                                                     C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
        Opens:
                                                                                                     C:\Windows\SysWOW64\clbcatq.dll
                                                                                                    C:\Windows\SysWOW64\cryptsp.dll
       Opens:
                                                                                                     C:\Windows\SysWOW64\rsaenh.dll
        Opens:
        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
                                                                                                     C:\Windows\SysWOW64\mshtml.tlb
        Opens:
                                                                                                     C:\Windows\SysWOW64\stdole2.tlb
       Opens:
        Opens:
                                                                                                     C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers
        Opens:
 Opens:
 Opens:
Opens:
 C:\Windows\Microsoft.Net\assembly\GAC_32\CustomMarshalers\v4.0_4.0.0.0_b03f5f7f11d50a3a\CustomMarshalers.dll.config
       Writes to:
 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 \Native Images\_v4.0.30319\_32 \mbox{\sc} 151e2934144ba15628ba5a31be2dae7dc\mbox{\sc} 1b.ni.dll.aux \assembly \ass
        Reads from:
 C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\b9f7adbc90a2bcbe8eb9e6e8d2bb975b\System.Core.ni.dll.aux
        Reads from:
 C: \windows \assembly \Native Images\_v4.0.30319\_32 \System \eqda7a49f8c3f0108e7c835b342f382 \System.ni.dll.aux \assembly \As
        Reads from:
                                                                                                     C:\Windows\SysWOW64\mshtml.tlb
                                                                                                     C:\Windows\SysWOW64\stdole2.tlb
        Reads from:
        Reads from:
C: \verb|\windows| assembly \verb|\NativeImages_v4.0.30319_32 \verb|\CustomMarshalers| 8a37b97ce8d5b322c455be3dd440e5f2 \verb|\CustomMarshalers.ni.dll.aux| aux to the following the fol
 Windows Registry Events
        Opens key:
                                                                                                      HKLM\software\microsoft\wow64
Н
```

Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\sorting\versions</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\safeboot\option</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\srp\gp\dll</pre>
Opens key:	
HKLM\software\wow	5432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:	<pre>HKLM\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKCU\software\policies\microsoft\windows\safer\codeidentifiers</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\customlocale</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\nls\language</pre>
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages\en-us</pre>
Opens key:	<pre>HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete</pre>
Opens key:	<pre>HKLM\software\wow6432node\policies\microsoft\mui\settings</pre>

```
Opens key:
                                                                  HKLM\software\policies\microsoft\mui\settings
    Opens key:
    Opens key:
                                                                  HKCU\control panel\desktop\muicached\machinelanguageconfiguration
    Opens key:
                                                                  HKLM \verb|\system| current controlset| control \verb|\mui| settings \verb|\language| configuration
                                                                  HKCU\software\policies\microsoft\control panel\desktop
    Opens key:
    Opens kev:
                                                                  HKCU\control panel\desktop\languageconfiguration
    Opens kev:
                                                                  HKCU\control panel\desktop
    Opens key:
                                                                  HKCU\control panel\desktop\muicached
    Opens key:
                                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
    Opens key:
                                                                  \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\software\mbox{\sc microsoft\windows} & nt\current\version\app\compatflags\dbglog \\ \end{tabular}
    Opens key:
                                                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows nt\+ current version\+ app compatflags
    Opens key:
                                                                  HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
                                                                  HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
    Opens key:
    Opens key:
                                                                  HKLM\system\currentcontrolset\control\lsa
    Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
                                                                 HKLM\
    Opens key:
    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 kev:
                                                                  HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
                                                                  HKLM\software\wow6432node\microsoft\windows
    Opens key:
nt\currentversion\compatibility32
    Opens kev:
                                                                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
                                                                  HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
    Opens key:
    Opens key:
                                                                 HKLM\software\wow6432node\microsoft\.netframework\policy\standards
    Opens key:
HKLM\software\wow6432node\microsoft\.netframework\policy\standards\v4.0.30319
                                                                  HKLM\software\wow6432node\microsoft\fusion
    Opens key:
    Opens key:
                                                                  HKLM\software\wow6432node\microsoft\.netframework\v4.0.30319\skus\
    Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ .net framework \ v4.0.30319 \ skus \ default
    Opens key:
                                                                  HKLM\svstem\currentcontrolset\control\session manager
    Opens key:
                                                                  HKLM\software\microsoft\fusion
    Opens key:
                                                                  \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
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 kev:
                                                                  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 kev:
                                                                  HKLM\software\microsoft\fusion\publisherpolicy\default
    Opens key:
HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lem:hkklm} White \label{lkklm} White \labe
    Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.core__b77a5c561934e089
    Opens kev:
HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} HKLM \label{limits} LA \label{limits} 
    Opens key:
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.configuration__b03f5f7f11d50a3a
    Opens key:
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.system.xml_b77a5c561934e089
    Opens kev:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.system.numerics__b77a5c561934e089
    Opens key:
HKLM \label{lem:hkkm} Which is not soft further one of the limit of 
    Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ v4.0\_policy. 4.0. \ system. security\_b03f5f7f11d50a3a
Opens key:
                                                                  HKLM\software\wow6432node\microsoft\.netframework\policy\aptca
    Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ v4.0\_policy. 4.0.microsoft.csharp\_b03f5f7f11d50a3a
```

Opens key: HKLM\software\microsoft\fusion\publisherpolicy\default\policy.4.0.microsoft.csharp\_\_b03f5f7f11d50a3a Opens kev: 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 HKLM\system\currentcontrolset\control\nls\language groups Opens kev: Opens key: HKCU\software\microsoft\internet explorer\main Opens key: HKCU\software\classes\ Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-00000000046}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-00000000046}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32 HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-Opens key: 000000000046}\localserver32 Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-000000000046}\localserver32 Opens key: HKCR\clsid\{0002df01-0000-0000-c000-00000000046}\localserver32 Opens key: HKLM\software\microsoft\com3 Opens key: HKLM\software\microsoft\windowsruntime\clsid Opens key: 00000000046} Opens key: HKCR\activatableclasses\clsid HKCR\activatableclasses\clsid\{0002df01-0000-0000-c000-00000000046} Opens kev: Opens key: HKLM\software\wow6432node\microsoft\oleaut Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-00000000046} HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-00000000046} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-000000000046}\treatas HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-0000000046}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-00000000046}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-00000000046}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{0002df01-0000-0000-c000-Opens key: 00000000046}\inprochandler Opens key: HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-00000000046}\inprochandler Opens key:  $HKCU \setminus software \setminus classes \setminus appid \setminus 8995535721 \\ ebeaf 6983c6 \\ cecf 3182 \\ d756 \\ ca5b3911607452 \\ dd4ba2ad8 \\ ec86cf 96. \\ exeappid \setminus 8995535721 \\ ebeaf 6983c6 \\ cecf 3182 \\ d756 \\ ca5b3911607452 \\ dd4ba2ad8 \\ ec86cf 96. \\ exeappid \setminus 8995535721 \\ ebeaf 6983c6 \\ eccf 3182 \\ d756 \\ exappid \setminus 8995535721 \\ ebeaf 6983c6 \\ eccf 3182 \\ d756 \\ exappid \setminus 8995535721 \\ ebeaf 6983c6 \\ eccf 3182 \\ eccf 3182$ Opens kev: HKCR\appid\8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat HKLM\software\microsoft\ole\appcompat Opens key: Opens kev: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider Opens key: HKLM\software\policies\microsoft\cryptography HKLM\software\microsoft\cryptography Opens key: Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{00000134-0000-0000-c000-c000-c000-c000-c00-c00-c000-c000-c$ 00000000046} HKCR\wow6432node\interface\{00000134-0000-0000-c000-00000000046} Opens key: Opens key: 00000000046}\proxystubclsid32 HKCR\wow6432node\interface\{00000134-0000-0000-c000-Opens key: 00000000046}\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-c000-0000000000463 Opens key: HKCR\activatableclasses\clsid\{0000032a-0000-0000-c000-00000000046} HKCU\software\classes\wow6432node\clsid\{0000032a-0000-0000-c000-Opens key: 00000000046} Opens key:  $HKCR \setminus wow 6432 node \\ clsid \setminus \{0000032a-0000-0000-c000-0000000000046\}$ Opens key: HKCU\software\classes\clsid\{0000032a-0000-0000-c000-00000000046} HKCR\clsid\{0000032a-0000-0000-c000-00000000046} Opens key: Opens kev: HKCU\software\classes\activatableclasses\clsid HKCU\software\classes\activatableclasses\clsid\{0000032a-0000-0000-c000-Opens key: 00000000046} Opens key: HKLM\software\microsoft\windowsruntime\clsid\{00000339-0000-0000-c000-00000000000463 HKCR\activatableclasses\clsid\{00000339-0000-0000-c000-000000000046} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00000339-0000-0000-c000-00000000046} HKCR\wow6432node\clsid\{00000339-0000-0000-c000-00000000046} Opens key: Opens key: HKCU\software\classes\clsid\{00000339-0000-0000-c000-00000000046}

HKCR\clsid\{00000339-0000-0000-c000-00000000046} Opens key: Opens key: HKCU\software\classes\activatableclasses\clsid\{00000339-0000-0000-c000-000000000046} Opens key: 2878998f69a2}

HKCR\activatableclasses\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2} Opens key: HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-Opens kev: 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 HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-Opens key: 2878998f69a2}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-Opens key: 2878998f69a2}\inprochandler32 HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-Opens kev: 2878998f69a2}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-Opens key: 2878998f69a2}\inprochandler HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-Opens key: 2878998f69a2}\inprochandler Opens kev: 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 HKCR\wow6432node\interface\{5f568e3e-317c-402e-a883-Opens kev: 546b0f7673a4}\proxystubclsid32  $HKLM \setminus software \setminus microsoft \setminus windows runtime \setminus clsid \setminus \{a4a1a128-768f-41e0-bf75-41e$ Opens key: e4fddd701cba} HKCR\activatableclasses\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75e4fddd701cba} Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba} Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75e4fddd701cba}\treatas  $HKCR \setminus wow6432 node \\ clsid \\ \{a4a1a128-768f-41e0-bf75-e4fddd701cba\} \\ \\ treatas$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75e4fddd701cba}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75e4fddd701cba}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-Opens key: e4fddd701cba}\inprochandler32 HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-Opens key: e4fddd701cba}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-Opens kev: e4fddd701cba}\inprochandler HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-Opens key: e4fddd701cba}\inprochandler Opens kev: 000000000046} Opens key: HKCR\wow6432node\interface\{00020400-0000-0000-c000-000000000046} Opens key: HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: HKCR\wow6432node\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: 0000000000463 Opens key: HKCR\activatableclasses\clsid\{00020420-0000-0000-c000-00000000046} HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-Opens kev: 000000000046} HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046} Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00020420-0000-0000-c000-c000-c000-c00-c00-c000-c000-c000-c000-c00$ 000000000046}\treatas HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}\treatas Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32 Opens key: 00000000046}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler HKCR\wow6432node\clsid\{00020420-0000-0000-c000-Opens key: 00000000046}\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}
                                                                                       HKCR\activatableclasses\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
      Opens kev:
      Opens kev:
                                                                                       HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}
                                                                                       HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
      Opens key:
                                                                                       HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
     Opens kev:
00aa00341d07}\treatas
      Opens key:
                                                                                       \label{lem:hkcrwow6432} HKCR\wow6432 node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\\\ \treat as
      Opens key:
                                                                                       HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32
                                                                                       HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
     Opens key:
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
                                                                                       HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-
     Opens key:
00aa00341d07}\inprochandler
      Opens key:
                                                                                       HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler
     Opens kev:
                                                                                       HKCU\software\classes\wow6432node\interface\{00020401-0000-0000-c000-
000000000046}
      Opens key:
                                                                                       HKCR\wow6432node\interface\{00020401-0000-0000-c000-000000000046}
      Opens key:
                                                                                       00000000046}\proxystubclsid32
                                                                                       HKCR\wow6432node\interface\{00020401-0000-0000-c000-
     Opens kev:
00000000046}\proxystubclsid32
     Opens key:
                                                                                       HKLM\software\microsoft\windowsruntime\clsid\{00020422-0000-0000-c000-
000000000046}
      Opens key:
                                                                                       Opens key:
                                                                                       HKCU\software\classes\wow6432node\clsid\{00020422-0000-0000-c000-
00000000046}
                                                                                       HKCR\wow6432node\clsid\{00020422-0000-0000-c000-000000000046}
      Opens key:
      Opens key:
                                                                                       HKCU\software\classes\wow6432node\clsid\{00020422-0000-0000-c000-
000000000046}\treatas
                                                                                       HKCR\wow6432node\clsid\{00020422-0000-0000-c000-00000000046}\treatas
      Opens key:
                                                                                       HKCU\software\classes\wow6432node\clsid\{00020422-0000-0000-c000-
     Opens key:
00000000046}\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-
00000000046}\inprochandler32
     Opens key:
                                                                                       00000000046}\inprochandler
      Opens key:
                                                                                       HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
00000000046}\inprochandler
     Opens key:
                                                                                       HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
                                                                                       HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
     Opens key:
00aa00686f13}\inprocserver32
     Opens key:
                                                                                       HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0
                                                                                       HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
     Opens key:
00aa00686f13}\inprocserver32\7.0.3300.0
      Opens key:
HKLM \setminus software \setminus microsoft \setminus fusion \setminus publisher policy \setminus default \setminus v4.0\_policy.7.0.microsoft.mshtml\_b03f5f7f11d50a3a
     Opens key:
HKLM \ software \ microsoft \ fusion \ publisher policy \ default \ policy. 7.0. microsoft. mshtml\_b03f5f7f11d50a3a
                                                                                       HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus installer \setminus managed \setminus s-1-5-managed \setminus s-1-5-manage
     Opens key:
 21-1923240461-1905901954-2556564120-
1001\installer\assemblies\c:|windows|temp|8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
     Opens key:
HKCU \setminus software \setminus microsoft \setminus installer \setminus assemblies \setminus c: | windows | temp | 8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe | windows | temp | tem
     Opens key:
HKCR \ installer \ assemblies \ \ \ \ |\ windows\ |\ temp\ |\ 8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96.exe
      Opens key:
                                                                                       HKLM \ software \ microsoft \ windows \ current version \ installer \ managed \ s-1-5-1000 \ managed \ m
21-1923240461-1905901954-2556564120-1001\installer\assemblies\global
     Opens key:
                                                                                       HKCU\software\microsoft\installer\assemblies\global
     Opens key:
                                                                                       HKCR\installer\assemblies\global
     Opens key:
Opens key:
Opens key:
                                                                                       HKCU\software\classes\wow6432node\interface\{3050f55f-98b5-11cf-bb82-
00aa00bdce0b}
                                                                                       HKCR\wow6432node\interface\{3050f55f-98b5-11cf-bb82-00aa00bdce0b}
      Opens key:
      Opens key:
                                                                                       HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{3050 \\ f55 \\ f-98 \\ b5-11 \\ cf-bb82-10 \\ f-10 
{\tt 00aa00bdce0b} \verb|\proxystubclsid32| \\
     Opens key:
                                                                                       HKCR\wow6432 node\interface \ \{3050f55f-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82
00aa00bdce0b}\proxystubclsid32
     Opens key:
                                                                                       HKCU\software\classes\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
```

 $HKCR \setminus wow 6432 \\ node \setminus interface \setminus \{3050f21f-98b5-11cf-bb82-00aa00bdce0b\}$ 

00aa00bdce0b} Opens key:

```
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}
                                                HKCR\activatableclasses\clsid\{00020424-0000-0000-c000-00000000046}
   Opens key:
   Opens key:
                                                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}
   Opens key:
                                                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}
                                                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
   Opens key:
000000000046}\treatas
   Opens key:
                                                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}\treatas
   Opens key:
                                                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32
                                                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
   Opens key:
00000000046}\inprocserver32
                                                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
   Opens key:
00000000046}\inprochandler32
                                                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
   Opens kev:
00000000046}\inprochandler32
   Opens key:
                                                HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprochandler
   Opens key:
                                                HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprochandler
                                                HKCU\software\classes\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
   Opens key:
00aa00bdce0b}\forward
   Opens key:
                                                HKCR \setminus 6432 \\ node \setminus interface \setminus \{3050f21f-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-b
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
                                                HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
   Opens key:
00aa00bdce0b}\typelib
                                                \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \typelib \{3050f1c5-98b5-11cf-bb82-00aa00bdce0b\} \end{tabular}
   Opens key:
   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
                                                HKCR\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}\4.0\0
   Opens key:
                                                HKCU\software\classes\typelib\{3050f1c5-98b5-11cf-bb82-
   Opens kev:
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\tvpelib
                                                HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
   Opens key:
   Opens key:
                                                HKCR\typelib\{00020430-0000-0000-c000-00000000046}
   Opens key:
                                                HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}\2.0
                                                HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0
   Opens key:
   Opens key:
                                                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
                                                HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
   Opens key:
   Opens key:
                                                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
00000000046}\2.0\0\win32
                                                HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
   Opens kev:
   Opens key:
                                                HKLM\software\microsoft\rpc
   Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\v4.0_policy.4.0.custommarshalers__b03f5f7f11d50a3a
   Opens kev:
HKLM\software\microsoft\fusion\publisherpolicv\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}
                                                \label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \wow 6432 node \interface \classes \classes
   Opens kev:
00000000046}\proxystubclsid32
                                                HKCR\wow6432node\interface\{00020404-0000-0000-c000-
000000000046}\proxystubclsid32
                                                HKLM\software\microsoft\windowsruntime\clsid\{00020421-0000-0000-c000-
   Opens kev:
000000000046}
   Opens key:
                                                HKCR\activatableclasses\clsid\{00020421-0000-0000-c000-00000000046}
   Opens key:
                                                HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
00000000046}
   Opens key:
                                                HKCR\wow6432node\clsid\{00020421-0000-0000-c000-000000000046}
                                                HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
   Opens key:
000000000046}\treatas
                                                Opens key:
                                                HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-
   Opens key:
000000000046}\inprocserver32
                                                HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
   Opens key:
```

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00020421-0000-0000-c000-c000-c000-c0000-c00-c00-c000-c000-c000-c00-$ 

000000000046}\inprocserver32 00000000046}\inprochandler32

Opens key:

HKCR\wow6432node\clsid\{00020421-0000-0000-c000-Opens key: 00000000046}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{00020421-0000-0000-c000-Opens kev: 00000000046}\inprochandler HKCR\wow6432node\clsid\{00020421-0000-0000-c000-Opens key: 00000000046}\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 HKCR\wow6432node\clsid\{3050f27e-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\localserver32 Opens key: HKCU\software\classes\clsid\{3050f27e-98b5-11cf-bb82-00aa00bdce0b}\localserver32  $HKCR\clsid\{3050f27e-98b5-11cf-bb82-00aa00bdce0b}\localserver32$ Opens key: HKCU\software\classes\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-Opens key: 00aa00bdce0b} HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-00aa00bdce0b} Opens kev: Opens kev: HKCU\software\classes\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-00aa00bdce0b}\proxystubclsid32 Opens key:  $HKCR \land wow 6432 node \land interface \land \{3050f1ff-98b5-11cf-bb82-11cf$ 00aa00bdce0b}\proxystubclsid32 Opens key: HKCU\software\classes\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-00aa00bdce0b}\forward HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\forward HKCU\software\classes\interface\{3050f1ff-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\forward Opens key: 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 HKCU\software\classes\wow6432node\clsid\{3050f491-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\localserver32 HKCR\wow6432node\clsid\{3050f491-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\localserver32 HKCU\software\classes\clsid\{3050f491-98b5-11cf-bb82-Opens kev: 00aa00bdce0b}\localserver32 HKCR\clsid\{3050f491-98b5-11cf-bb82-00aa00bdce0b}\localserver32 Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{3050f248-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{3050f248-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{3050f248-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\localserver32 Opens key: HKCR\wow6432node\clsid\{3050f248-98b5-11cf-bb82-00aa00bdce0b}\localserver32 HKCU\software\classes\clsid\{3050f248-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\localserver32 Opens key: HKCR\clsid\{3050f248-98b5-11cf-bb82-00aa00bdce0b}\localserver32 Opens kev: 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] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty] Oueries 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\enus[alternatecodepage] Queries value: HKCU\control panel\desktop[preferreduilanguages] HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]] \ detailed by the side of the sid$ Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo] HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled] Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy] Oueries value: Queries value: HKLM\software\wow6432node\microsoft\.netframework[installroot] Queries value: HKLM\software\wow6432node\microsoft\.netframework[clrloadlogdir] HKLM\software\microsoft\sqmclient\windows[ceipenable] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles]

Oueries value:

HKLM\software\wow6432node\microsoft\windows

 $nt \verb|\currentversion| compatibility 32[8995535721ebeaf6983c6cecf3182d756ca5b3911607452dd4ba2ad8ec86cf96]|$ 

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

Oueries value:

```
HKLM \ software \ wow 6432 node \ microsoft \ .net framework [uselegacyv2runtime activation policy default value] \ and \ software \ wow 6432 node \ microsoft \ .net framework [uselegacyv2runtime activation policy default \ value] \ and \ software \ wow 6432 node \ microsoft \ .net framework \ [uselegacyv2runtime activation policy default \ value] \ and \ software \ wow 6432 node \ microsoft \ .net framework \ [uselegacyv2runtime activation policy default \ value] \ and \ software \ wow 6432 node \ microsoft \ .net framework \ [uselegacyv2runtime activation policy \ default \ node 
                                              HKLM\software\wow6432node\microsoft\.netframework[onlyuselatestclr]
   Oueries value:
                                              HKLM\software\wow6432node\microsoft\fusion[noclientchecks]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                              HKLM\software\wow6432node\microsoft\.netframework[disableconfigcache]
   Queries value:
   Oueries value:
                                              HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-
931b-d9cc2eee27e41
   Queries value:
                                              HKLM\system\currentcontrolset\control\wmi\security[763fd754-7086-4dfe-
95eb-c01a46faf4ca1
   Queries value:
                                              HKLM\system\currentcontrolset\control\wmi\security[a669021c-c450-4609-
a035-5af59af4df181
   Queries value:
                                              HKLM\system\currentcontrolset\control\wmi\security[cc2bcbba-16b6-4cf3-
8990-d74c2e8af500]
   Oueries value:
                                              HKLM\software\microsoft\fusion[cachelocation]
   Oueries value:
                                              HKLM\software\microsoft\fusion[downloadcacheguotainkb]
   Queries value:
                                              HKLM\software\microsoft\fusion[enablelog]
   Queries value:
                                              HKLM\software\microsoft\fusion[logginglevel]
   Oueries value:
                                              HKLM\software\microsoft\fusion[forcelog]
   Queries value:
                                              HKLM\software\microsoft\fusion[logfailures]
                                              HKLM\software\microsoft\fusion[logresourcebinds]
   Oueries value:
   Queries value:
                                              HKLM\software\microsoft\fusion[fileinuseretryattempts]
                                              HKLM\software\microsoft\fusion[fileinusemillisecondsbetweenretries]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\fusion[uselegacyidentityformat]
   Queries value:
                                              HKLM\software\microsoft\fusion[disablemsipeek]
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
   Oueries value:
options[devoverrideenable]
   Queries value:
                                              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Queries value:
                                              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                                              HKLM\software\microsoft\ole[aggressivemtatesting]
   Oueries value:
   Queries value:
HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft|.netframework \verb|\ngen| policy \verb|\v4.0[| optimize used binaries]| \\
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
                                              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-usl
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
                                              HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
   Queries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
   Oueries value:
                                              HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                              HKLM\system\setup[oobeinprogress]
   Queries value:
   Queries value:
                                              HKLM\system\setup[systemsetupinprogress]
   Queries value:
                                              HKLM\software\microsoft\rpc[idletimerwindow]
   Queries value:
                                              HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
   Oueries value:
                                              HKLM\svstem\currentcontrolset\control\cmf\config[svstem]
   Queries value:
                                              HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus windows \cdot error
reporting\wmr[disable]
   Queries value:
                                              HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Oueries value:
                                              HKLM\system\currentcontrolset\control\nls\language groups[1]
   Oueries value:
                                              HKCU\software\microsoft\internet explorer\main[disablefirstruncustomize]
   Queries value:
                                              HKCU\software\microsoft\internet explorer\main[check_associations]
                                              HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-
   Queries value:
00000000046}\localserver32[class]
                                              \label{localserver32[class]} HKCR \ clsid \ \{0002df01-0000-0000-c000-00000000046\} \ localserver \ 32[class]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\com3[com+enabled]
   Queries value:
                                              HKCR\wow6432node\clsid\{0002df01-0000-0000-c000-00000000046}[]
   Oueries value:
                                              HKLM\software\microsoft\ole[maxsxshashcount]
   Oueries value:
                                              HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
                                              HKLM\software\microsoft\ole[defaultaccesspermission]
   Oueries value:
   Queries value:
                                              \label{lem:hklm} \verb+kklm \system \current control \lsa[everyone includes an onymous]
   Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
   Oueries value:
HKLM \label{lem:hklm} Which was expressed in the strong control of the strong control 
provider[image path]
   Queries value:
                                              HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
   Oueries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
                                              HKLM \verb|\software\policies\m| icrosoft \verb|\cryptography[privatekeylifetimeseconds]| \\
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\cryptography[machineguid]
                                              HKCR\wow6432node\interface\{00000134-0000-0000-c000-
   Oueries value:
00000000046}\proxystubclsid32[]
   Queries value:
                                              HKLM\software\microsoft\rpc\extensions[ndroleextdll]
                                              HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-2878998f69a2}[]
   Queries value:
                                              HKCR\wow6432node\clsid\{3cb169b3-17d9-4e47-8b93-
   Oueries value:
2878998f69a2}\inprochandler32[]
                                              HKCR\wow6432node\interface\{5f568e3e-317c-402e-a883-
   Queries value:
546b0f7673a4}\proxystubclsid32[]
                                              HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba\}[]
   Queries value:
   Queries value:
                                              HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[inprocserver32]
                                             HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
   Oueries value:
e4fddd701cba}\inprocserver32[]
   Queries value:
                                              HKCR\wow6432node\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[threadingmodel]
```

```
HKCR\wow6432node\interface\{00020400-0000-0000-c000-
   Queries value:
00000000046}\proxystubclsid32[]
   Oueries value:
                                                    HKCR\wow6432node\clsid\{00020420-0000-0000-c000-00000000046}[]
   Queries value:
                                                    HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                                    HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
   Oueries value:
000000000046}\inprocserver32[]
   Queries value:
                                                    HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
   Queries value:
                                                    HKLM\software\wow6432node\microsoft\cryptography\defaults\provider
types\type 001[name]
                                                    HKCR\wow6432node\interface\{b196b283-bab4-101a-b69c-
   Queries value:
00aa00341d07}\proxystubclsid32[]
                                                    HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
   Oueries value:
   Oueries 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]
   Oueries value:
                                                    HKCR\wow6432node\interface\{00020401-0000-0000-c000-
00000000046}\proxystubclsid32[]
   Queries value:
                                                    \label{local-equation} \mbox{HKCR} $$ Wow6432 node \clsid{00020422-0000-0000-c000-00000000046}[] $$
   Queries value:
                                                    HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                                    HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
   Oueries value:
00000000046}\inprocserver32[]
   Queries value:
                                                    HKCR\wow6432node\clsid\{00020422-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
   Oueries 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]
                                                    HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Queries value:
00aa00686f13}\inprocserver32\7.0.3300.0[runtimeversion]
   Queries value:
                                                    HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32\7.0.3300.0[codebase]
                                                    HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
   Queries value:
00aa00686f13}\inprocserver32[]
   Queries value:
                                                    HKCR \land wow 6432 node \land interface \land \{3050f55f-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf
00aa00bdce0b}\proxystubclsid32[]
                                                    HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
   Oueries value:
00aa00bdce0b}\proxystubclsid32[]
                                                    HKCR\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}[]
   Queries value:
                                                    HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
   Queries value:
00000000046}\inprocserver32[inprocserver32]
   Queries value:
                                                    HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[]
                                                    HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
   Queries value:
00000000046}\inprocserver32[threadingmodel]
   Queries value:
                                                    HKCR\wow6432 node\interface \ \{3050f21f-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82
00aa00bdce0b}\typelib[]
                                                    HKCR\wow6432node\interface\{3050f21f-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\typelib[version]
   Queries value:
                                                    HKCR\typelib\{3050f1c5-98b5-11cf-bb82-00aa00bdce0b}\4.0\0\win32[]
                                                    HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
   Oueries value:
                                                    HKLM\software\microsoft\rpc[udtalignmentpolicy]
   Queries value:
                                                    HKCR\wow6432node\interface\{00020404-0000-0000-c000-
   Queries value:
00000000046}\proxystubclsid32[]
                                                    HKCR\wow6432node\clsid\{00020421-0000-0000-c000-00000000046}[]
   Queries value:
                                                    HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
   Oueries value:
00000000046}\inprocserver32[inprocserver32]
   Queries value:
                                                    HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
000000000046}\inprocserver32[]
                                                    HKCR\wow6432node\clsid\{00020421-0000-0000-c000-
   Oueries value:
00000000046}\inprocserver32[threadingmodel]
                                                    HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\proxystubclsid32[]
                                                    HKCR\wow6432node\interface\{3050f1ff-98b5-11cf-bb82-
   Oueries value:
```

 $HKCR \setminus wow6432 \\ node \setminus interface \setminus \{3050f1ff-98b5-11cf-bb82-11c$ 

 $\label{thm:local_explorer} \begin{tabular}{ll} HKCU \label{thm:local_explorer_main_e$ 

00aa00bdce0b}\typelib[]
 Queries value:

Sets/Creates value:

00aa00bdce0b}\typelib[version]