Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 55, Task ID: 219

Task ID:	219
Risk Level:	3
Date Processed:	2016-04-28 12:53:12 (UTC)
Processing Time:	2.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\602bcc42064dbb0bcb1933b4247937fe.exe"

Sample ID:	55
Type:	basic
Owner:	admin
Label:	602bcc42064dbb0bcb1933b4247937fe
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	335872 bytes
MD5:	602bcc42064dbb0bcb1933b4247937fe
SHA256:	1cba995b5874702639b780fe754cb9d1f3f86238dbf00af062a1777221bb2a9c
Description:	None

Pattern Matching Results

3 Long sleep detected

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\602bcc42064dbb0bcb1933b4247937fe.exe ["c:\windows\temp\602bcc42064dbb0bcb1933b4247937fe.exe"]
Terminates process:	C:\WINDOWS\Temp\602bcc42064dbb0bcb1933b4247937fe.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates semaphore:	\BaseNamedObjects\C:?WINDOWS?TEMP?602BCC42064DBB0BCB1933B4247937FE.EXE

File System Events

Opens:	C:\WINDOWS\Prefetch\602BCC42064DBB0BCB1933B424793-03D776B9.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\msvbvm60.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\rpcss.dll
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\Temp\602bcc42064dbb0bcb1933b4247937fe.exe
Opens:	C:\WINDOWS\system32\sxs.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\system32\clbcatq.dll
Opens:	C:\WINDOWS\system32\comres.dll
Opens:	C:\WINDOWS\Registration\R000000000007.clb
Opens:	C:\WINDOWS\system32\winlogon.exe

```
  Opens:                  C:\WINDOWS\system32\xpsp2res.dll
  Opens:                  C:\WINDOWS\WINHELP.INI
  Reads from:             C:\WINDOWS\Temp\602bcc42064dbb0bcb1933b4247937fe.exe
  Reads from:             C:\WINDOWS\Registration\R000000000007.clb
```

Windows Registry Events

```
  Creates key:            HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}
  Creates key:            HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5
  Creates key:            HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags
  Creates key:            HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0
  Creates key:            HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32
  Creates key:            HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir
  Creates key:            HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}
  Creates key:            HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid
  Creates key:            HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32
  Creates key:            HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib
  Creates key:            HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}
  Creates key:            HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\progid
  Creates key:            HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\localserver32
  Creates key:            HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\typelib
  Creates key:            HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\version
  Creates key:            HKCR\aloahaflowchart64.engine64
  Creates key:            HKCR\aloahaflowchart64.engine64\clsid
  Creates key:            HKCR\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}
  Creates key:            HKCR\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid
  Creates key:            HKCR\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid32
  Creates key:            HKCR\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\forward
  Creates key:            HKCR\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}
  Creates key:            HKCR\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid
  Creates key:            HKCR\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid32
  Creates key:            HKCR\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\forward
  Creates key:            HKCR\interface\{55af540b-13af-4de5-a975-5600b0589e59}
  Creates key:            HKCR\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid
  Creates key:            HKCR\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid32
  Creates key:            HKCR\interface\{55af540b-13af-4de5-a975-5600b0589e59}\forward
  Creates key:            HKCR\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}
  Creates key:            HKCR\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid
  Creates key:            HKCR\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid32
  Creates key:            HKCR\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\forward
  Creates key:            HKCR\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}
  Creates key:            HKCR\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid
  Creates key:            HKCR\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid32
  Creates key:            HKCR\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\forward
  Creates key:            HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\implemented categories
  Creates key:            HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\programmable
  Creates key:            HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\implemented
categories\{40fc6ed5-2438-11cf-a3db-080036f12502}
  Deletes value:          HKCR\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\localserver32[threadingmodel]
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\602bcc42064dbb0bcb1933b4247937fe.exe
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\ntdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvbvm60.dll
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:                HKLM\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\602bcc42064dbb0bcb1933b4247937fe.exe
  Opens key:                HKLM\software\microsoft\ctf\systemshared\
  Opens key:                HKCU\keyboard layout\toggle
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\typelib\{000204ef-0000-0000-c000-
000000000046}\6.0\9
  Opens key:                HKCR\typelib\{000204ef-0000-0000-c000-000000000046}\6.0\9
  Opens key:                HKCU\software\classes\typelib\{000204ef-0000-0000-c000-
000000000046}\6.0\9\win32
  Opens key:                HKCR\typelib\{000204ef-0000-0000-c000-000000000046}\6.0\9\win32
  Opens key:                HKCU\software\classes\typelib\{ea544a21-c82d-11d1-a3e4-
00a0c90aea82}\6.0\9
  Opens key:                HKCR\typelib\{ea544a21-c82d-11d1-a3e4-00a0c90aea82}\6.0\9
  Opens key:                HKCU\software\classes\typelib\{ea544a21-c82d-11d1-a3e4-
00a0c90aea82}\6.0\9\win32
  Opens key:                HKCR\typelib\{ea544a21-c82d-11d1-a3e4-00a0c90aea82}\6.0\9\win32
  Opens key:                HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-
418274d25ba9}\1.5\0
  Opens key:                HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0
  Opens key:                HKCU\software\classes\typelib
  Opens key:                HKCR\typelib
  Opens key:                HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}
  Opens key:                HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}
  Opens key:                HKLM\software\classes
  Opens key:                HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5
  Opens key:                HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5
  Opens key:                HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-
418274d25ba9}\1.5\flags
  Opens key:                HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags
  Opens key:                HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-
418274d25ba9}\1.5\0\win32
  Opens key:                HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32
  Opens key:                HKCU\software\classes\typelib\{f1713e8f-3698-497d-873c-
418274d25ba9}\1.5\helpdir
  Opens key:                HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir
  Opens key:                HKCU\software\classes\interface
  Opens key:                HKCU\software\classes\interface\{d7a6a14f-7947-4899-be20-a019be861538}
  Opens key:                HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}
  Opens key:                HKCU\software\classes\interface\{d7a6a14f-7947-4899-be20-
a019be861538}\proxystubclsid
  Opens key:                HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{d7a6a14f-7947-4899-be20-
a019be861538}\proxystubclsid32
  Opens key:                HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{d7a6a14f-7947-4899-be20-
a019be861538}\typelib
  Opens key:                HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\progid
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\localserver32
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\typelib
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\version
  Opens key:                HKCU\software\classes\aloahaflowchart64.engine64
  Opens key:                HKCR\aloahaflowchart64.engine64
  Opens key:                HKCU\software\classes\aloahaflowchart64.engine64\clsid
  Opens key:                HKCU\software\classes\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}
  Opens key:                HKCU\software\classes\interface\{18af9e71-cb41-42ee-8abc-
9ecae5c39561}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{18af9e71-cb41-42ee-8abc-
9ecae5c39561}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{18af9e71-cb41-42ee-8abc-
9ecae5c39561}\forward
  Opens key:                HKCU\software\classes\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}
  Opens key:                HKCU\software\classes\interface\{86aaf6a6-261a-4d96-b8ac-
90dad4b42a80}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{86aaf6a6-261a-4d96-b8ac-
90dad4b42a80}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{86aaf6a6-261a-4d96-b8ac-
90dad4b42a80}\forward
  Opens key:                HKCU\software\classes\interface\{55af540b-13af-4de5-a975-5600b0589e59}
  Opens key:                HKCU\software\classes\interface\{55af540b-13af-4de5-a975-
5600b0589e59}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{55af540b-13af-4de5-a975-
5600b0589e59}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{55af540b-13af-4de5-a975-
5600b0589e59}\forward
  Opens key:                HKCU\software\classes\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}
  Opens key:                HKCU\software\classes\interface\{e3c69a39-8de3-4f6c-b9ec-
1eb1c1b2539e}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{e3c69a39-8de3-4f6c-b9ec-
1eb1c1b2539e}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{e3c69a39-8de3-4f6c-b9ec-
1eb1c1b2539e}\forward
  Opens key:                HKCU\software\classes\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}
  Opens key:                HKCU\software\classes\interface\{b8a7b45c-0890-4a01-b191-
8e104a921919}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{b8a7b45c-0890-4a01-b191-
8e104a921919}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{b8a7b45c-0890-4a01-b191-
8e104a921919}\forward
  Opens key:                HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\602bcc42064dbb0bcb1933b4247937fe.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\implemented categories
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\programmable
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\implemented categories\{40fc6ed5-2438-11cf-a3db-080036f12502}
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\imm
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
  Opens key:                HKCU\software\microsoft\ctf
  Opens key:                HKLM\software\microsoft\ctf\systemshared
  Opens key:                HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:                HKLM\software\microsoft\vba\monitors
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
  Opens key:                HKLM\software\microsoft\com3\debug
  Opens key:                HKU\
  Opens key:                HKCR\clsid
  Opens key:                HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\treatas
  Opens key:                HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\treatas
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\inprocserver32
  Opens key:                HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\inprocserverx86
  Opens key:                HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprocserverx86
  Opens key:                HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\localserver32
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\inprochandler32
  Opens key:                HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\inprochandlerx86
  Opens key:                HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\inprochandlerx86
  Opens key:                HKCU\software\classes\appid\602bcc42064dbb0bcb1933b4247937fe.exe
  Opens key:                HKCR\appid\602bcc42064dbb0bcb1933b4247937fe.exe
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKLM\software\microsoft\windows
  Opens key:                HKLM\software\microsoft\windows\html help
  Opens key:                HKLM\software\microsoft\windows\help
  Queries value:              HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:              HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[602bcc42064dbb0bcb1933b4247937fe]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[602bcc42064dbb0bcb1933b4247937fe]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:              HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:              HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:              HKCR\interface[interfacehelperdisableall]
  Queries value:              HKCR\interface[interfacehelperdisableallforole32]
  Queries value:              HKCR\interface[interfacehelperdisabletypelib]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:              HKCU\control panel\desktop[multiuilanguageid]
  Queries value:              HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:              HKCU\keyboard layout\toggle[language hotkey]
  Queries value:              HKCU\keyboard layout\toggle[hotkey]
  Queries value:              HKCU\keyboard layout\toggle[layout hotkey]
  Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:              HKCR\typelib\{000204ef-0000-0000-c000-000000000046}\6.0\9\win32[]
  Queries value:              HKCR\typelib\{ea544a21-c82d-11d1-a3e4-00a0c90aea82}\6.0\9\win32[]
  Queries value:              HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5[]
  Queries value:              HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags[]
  Queries value:              HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32[]
  Queries value:              HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir[]
  Queries value:              HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}[]
  Queries value:              HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid[]
  Queries value:              HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32[]
  Queries value:              HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[]
  Queries value:              HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[version]
  Queries value:              HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:              HKCU\software\microsoft\ctf[disable thread input manager]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[932]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[950]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:              HKLM\software\microsoft\com3[com+enabled]
  Queries value:              HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
  Queries value:              HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
  Queries value:              HKLM\software\microsoft\com3[regdbversion]
  Queries value:              HKCR\clsid\{7a54054e-098c-460e-a45d-
64f80a1b9754}\localserver32[localserver32]
  Queries value:              HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\localserver32[]
  Queries value:              HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:              HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:              HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Sets/Creates value:         HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5[]
  Sets/Creates value:         HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\flags[]
```

```
Sets/Creates value:      HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\0\win32[]
Sets/Creates value:      HKCR\typelib\{f1713e8f-3698-497d-873c-418274d25ba9}\1.5\helpdir[]
Sets/Creates value:      HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}[]
Sets/Creates value:      HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid[]
Sets/Creates value:      HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32[]
Sets/Creates value:      HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[]
Sets/Creates value:      HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\typelib[version]
Sets/Creates value:      HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}[]
Sets/Creates value:      HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\progid[]
Sets/Creates value:      HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\localserver32[]
Sets/Creates value:      HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\typelib[]
Sets/Creates value:      HKCR\clsid\{7a54054e-098c-460e-a45d-64f80a1b9754}\version[]
Sets/Creates value:      HKCR\aloahaflowchart64.engine64[]
Sets/Creates value:      HKCR\aloahaflowchart64.engine64\clsid[]
Sets/Creates value:      HKCR\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}[]
Sets/Creates value:      HKCR\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid[]
Sets/Creates value:      HKCR\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\proxystubclsid32[]
Sets/Creates value:      HKCR\interface\{18af9e71-cb41-42ee-8abc-9ecae5c39561}\forward[]
Sets/Creates value:      HKCR\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}[]
Sets/Creates value:      HKCR\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid[]
Sets/Creates value:      HKCR\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\proxystubclsid32[]
Sets/Creates value:      HKCR\interface\{86aaf6a6-261a-4d96-b8ac-90dad4b42a80}\forward[]
Sets/Creates value:      HKCR\interface\{55af540b-13af-4de5-a975-5600b0589e59}[]
Sets/Creates value:      HKCR\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid[]
Sets/Creates value:      HKCR\interface\{55af540b-13af-4de5-a975-5600b0589e59}\proxystubclsid32[]
Sets/Creates value:      HKCR\interface\{55af540b-13af-4de5-a975-5600b0589e59}\forward[]
Sets/Creates value:      HKCR\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}[]
Sets/Creates value:      HKCR\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid[]
Sets/Creates value:      HKCR\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\proxystubclsid32[]
Sets/Creates value:      HKCR\interface\{e3c69a39-8de3-4f6c-b9ec-1eb1c1b2539e}\forward[]
Sets/Creates value:      HKCR\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}[]
Sets/Creates value:      HKCR\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid[]
Sets/Creates value:      HKCR\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\proxystubclsid32[]
Sets/Creates value:      HKCR\interface\{b8a7b45c-0890-4a01-b191-8e104a921919}\forward[]
Value changes:           HKLM\software\microsoft\cryptography\rng[seed]
Value changes:           HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}[]
Value changes:           HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid[]
Value changes:           HKCR\interface\{d7a6a14f-7947-4899-be20-a019be861538}\proxystubclsid32[]
```