Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 221, Task ID: 883

Task ID:	883
Risk Level:	3
Date Processed:	2016-04-28 13:11:44 (UTC)
Processing Time:	3.82 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1aca077963eb842ac865c50dd866d52c.exe"

Sample ID:	221
Type:	basic
Owner:	admin
Label:	1aca077963eb842ac865c50dd866d52c
Date Added:	2016-04-28 12:45:13 (UTC)
File Type:	PE32:win32:gui
File Size:	989832 bytes
MD5:	1aca077963eb842ac865c50dd866d52c
SHA256:	aa67952a7266af5c575c7acf194ff30866fe5cf8ea7f09049dc94c1ee15b0850
Description:	None

Pattern Matching Results

3 Long sleep detected

1 YARA score 1

Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\1aca077963eb842ac865c50dd866d52c.exe ["c:\windows\temp\1aca077963eb842ac865c50dd866d52c.exe"]
Terminates process:	C:\WINDOWS\Temp\1aca077963eb842ac865c50dd866d52c.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?1ACA077963EB842AC865C50DD866D52C.EXE
Creates semaphore:	\BaseNamedObjects\OleDfRoot0000216CE

File System Events

Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\~DF16D1.tmp
Opens:	C:\WINDOWS\Prefetch\1ACA077963EB842AC865C50DD866D-0CB8335C.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\1aca077963eb842ac865c50dd866d52c.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\system32\comctl32.dll
  Opens:                 C:\WINDOWS\system32\comctl32.dll.124.Manifest
  Opens:                 C:\WINDOWS\system32\comctl32.dll.124.Config
  Opens:                 C:\WINDOWS\system32\psapi.dll
  Opens:                 C:\WINDOWS\Fonts\sserife.fon
  Opens:                 C:\WINDOWS\WINHELP.INI
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Temp\~DF16D1.tmp
  Opens:                 C:\WINDOWS\Temp\21d97c23-a2ab-4cc6-be33-aeec3107283d
  Reads from:            C:\WINDOWS\Temp\1aca077963eb842ac865c50dd866d52c.exe
  Reads from:            C:\WINDOWS\Registration\R000000000007.clb
  Deletes:               C:\Documents and Settings\Admin\Local Settings\Temp\~DF16D1.tmp
```

Windows Registry Events

```
  Creates key:           HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}
  Creates key:           HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5
  Creates key:           HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags
  Creates key:           HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0
  Creates key:           HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32
  Creates key:           HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir
  Creates key:           HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}
  Creates key:           HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid
  Creates key:           HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32
  Creates key:           HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib
  Creates key:           HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}
  Creates key:           HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\progid
  Creates key:           HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\localserver32
  Creates key:           HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\typelib
  Creates key:           HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\version
  Creates key:           HKCR\pdfsaver.remotecontrol
  Creates key:           HKCR\pdfsaver.remotecontrol\clsid
  Creates key:           HKCR\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}
  Creates key:           HKCR\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid
  Creates key:           HKCR\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid32
  Creates key:           HKCR\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\forward
  Creates key:           HKCR\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}
  Creates key:           HKCR\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid
  Creates key:           HKCR\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid32
  Creates key:           HKCR\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\forward
  Creates key:           HKCR\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}
  Creates key:           HKCR\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid
  Creates key:           HKCR\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid32
  Creates key:           HKCR\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\forward
  Creates key:           HKCR\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}
  Creates key:           HKCR\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid
  Creates key:           HKCR\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid32
  Creates key:           HKCR\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\forward
  Creates key:           HKCR\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}
  Creates key:           HKCR\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid
  Creates key:           HKCR\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid32
  Creates key:           HKCR\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\forward
  Creates key:           HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\implemented categories
  Creates key:           HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\programmable
  Creates key:           HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\implemented
categories\{40fc6ed5-2438-11cf-a3db-080036f12502}
```

```
  Deletes value:          HKCR\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\localserver32[threadingmodel]
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\1aca077963eb842ac865c50dd866d52c.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\1aca077963eb842ac865c50dd866d52c.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\{7428f527-bc34-4911-b2a3-
41a5861b6aa3}\1.5\0
  Opens key:                HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0
  Opens key:                HKCU\software\classes\typelib
  Opens key:                HKCR\typelib
  Opens key:                HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}
  Opens key:                HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}
  Opens key:                HKLM\software\classes
  Opens key:                HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5
  Opens key:                HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5
  Opens key:                HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-
41a5861b6aa3}\1.5\flags
  Opens key:                HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags
  Opens key:                HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-
41a5861b6aa3}\1.5\0\win32
  Opens key:                HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32
  Opens key:                HKCU\software\classes\typelib\{7428f527-bc34-4911-b2a3-
41a5861b6aa3}\1.5\helpdir
  Opens key:                HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir
  Opens key:                HKCU\software\classes\interface
  Opens key:                HKCU\software\classes\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}
  Opens key:                HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}
  Opens key:                HKCU\software\classes\interface\{e194c84a-c2c5-4be2-a499-
7b32bb445d93}\proxystubclsid
  Opens key:                HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{e194c84a-c2c5-4be2-a499-
7b32bb445d93}\proxystubclsid32
  Opens key:                HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{e194c84a-c2c5-4be2-a499-
7b32bb445d93}\typelib
  Opens key:                HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\progid
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\localserver32
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\typelib
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\version
  Opens key:                HKCU\software\classes\pdfsaver.remotecontrol
  Opens key:                HKCR\pdfsaver.remotecontrol
  Opens key:                HKCU\software\classes\pdfsaver.remotecontrol\clsid
  Opens key:                HKCU\software\classes\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}
  Opens key:                HKCU\software\classes\interface\{ed353f97-de5c-49fd-9b0a-
b42282ece401}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{ed353f97-de5c-49fd-9b0a-
b42282ece401}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{ed353f97-de5c-49fd-9b0a-
b42282ece401}\forward
  Opens key:                HKCU\software\classes\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}
  Opens key:                HKCU\software\classes\interface\{0d2a9439-05f3-49ff-870c-
81398464fe59}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{0d2a9439-05f3-49ff-870c-
81398464fe59}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{0d2a9439-05f3-49ff-870c-
81398464fe59}\forward
  Opens key:                HKCU\software\classes\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}
  Opens key:                HKCU\software\classes\interface\{00ca193a-1486-4fe6-bab1-
9bc676a2f229}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{00ca193a-1486-4fe6-bab1-
9bc676a2f229}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{00ca193a-1486-4fe6-bab1-
9bc676a2f229}\forward
  Opens key:                HKCU\software\classes\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}
  Opens key:                HKCU\software\classes\interface\{9c8c339e-b96f-48a4-9e24-
a660704d23e4}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{9c8c339e-b96f-48a4-9e24-
a660704d23e4}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{9c8c339e-b96f-48a4-9e24-
a660704d23e4}\forward
  Opens key:                HKCU\software\classes\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}
  Opens key:                HKCU\software\classes\interface\{6c116783-ac8c-4590-be5c-
4360bf89ecc6}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{6c116783-ac8c-4590-be5c-
4360bf89ecc6}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{6c116783-ac8c-4590-be5c-
4360bf89ecc6}\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\1aca077963eb842ac865c50dd866d52c.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\implemented categories
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\programmable
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\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\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\treatas
  Opens key:                HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\treatas
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\inprocserver32
  Opens key:                HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\inprocserverx86
```

```
  Opens key:                 HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprocserverx86
  Opens key:                 HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\localserver32
  Opens key:                 HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\inprochandler32
  Opens key:                 HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprochandler32
  Opens key:                 HKCU\software\classes\clsid\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\inprochandlerx86
  Opens key:                 HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\inprochandlerx86
  Opens key:                 HKCU\software\classes\appid\1aca077963eb842ac865c50dd866d52c.exe
  Opens key:                 HKCR\appid\1aca077963eb842ac865c50dd866d52c.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 nt\currentversion\image file execution
options\comctl32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
  Opens key:                 HKCU\software\classes\aloahapopup.dialogs
  Opens key:                 HKCR\aloahapopup.dialogs
  Opens key:                 HKCU\software\policies\microsoft\windows\app management
  Opens key:                 HKLM\software\policies\microsoft\windows\app management
  Opens key:                 HKCU\software\classes\clsid\{acfb11f9-16bb-4fd7-9371-271f607c13d9}
  Opens key:                 HKCR\clsid\{acfb11f9-16bb-4fd7-9371-271f607c13d9}
  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[1aca077963eb842ac865c50dd866d52c]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[1aca077963eb842ac865c50dd866d52c]
  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\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5[]
  Queries value:             HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags[]
  Queries value:             HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32[]
  Queries value:             HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir[]
  Queries value:            HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}[]
  Queries value:            HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid[]
  Queries value:            HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32[]
  Queries value:            HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[]
  Queries value:            HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\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\{3e7af308-6ae1-49a0-bc92-
47fbe4b9d920}\localserver32[localserver32]
  Queries value:            HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\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]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Sets/Creates value:       HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5[]
  Sets/Creates value:       HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\flags[]
  Sets/Creates value:       HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\0\win32[]
  Sets/Creates value:       HKCR\typelib\{7428f527-bc34-4911-b2a3-41a5861b6aa3}\1.5\helpdir[]
  Sets/Creates value:       HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}[]
  Sets/Creates value:       HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid[]
  Sets/Creates value:       HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32[]
  Sets/Creates value:       HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[]
  Sets/Creates value:       HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\typelib[version]
  Sets/Creates value:       HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}[]
  Sets/Creates value:       HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\progid[]
  Sets/Creates value:       HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\localserver32[]
  Sets/Creates value:       HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\typelib[]
  Sets/Creates value:       HKCR\clsid\{3e7af308-6ae1-49a0-bc92-47fbe4b9d920}\version[]
  Sets/Creates value:       HKCR\pdfsaver.remotecontrol[]
  Sets/Creates value:       HKCR\pdfsaver.remotecontrol\clsid[]
  Sets/Creates value:       HKCR\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}[]
  Sets/Creates value:       HKCR\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid[]
  Sets/Creates value:       HKCR\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\proxystubclsid32[]
  Sets/Creates value:       HKCR\interface\{ed353f97-de5c-49fd-9b0a-b42282ece401}\forward[]
  Sets/Creates value:       HKCR\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}[]
  Sets/Creates value:       HKCR\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid[]
  Sets/Creates value:       HKCR\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\proxystubclsid32[]
  Sets/Creates value:       HKCR\interface\{0d2a9439-05f3-49ff-870c-81398464fe59}\forward[]
  Sets/Creates value:       HKCR\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}[]
  Sets/Creates value:       HKCR\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid[]
  Sets/Creates value:       HKCR\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\proxystubclsid32[]
  Sets/Creates value:       HKCR\interface\{00ca193a-1486-4fe6-bab1-9bc676a2f229}\forward[]
  Sets/Creates value:       HKCR\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}[]
  Sets/Creates value:       HKCR\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid[]
  Sets/Creates value:       HKCR\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\proxystubclsid32[]
  Sets/Creates value:       HKCR\interface\{9c8c339e-b96f-48a4-9e24-a660704d23e4}\forward[]
  Sets/Creates value:       HKCR\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}[]
  Sets/Creates value:       HKCR\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid[]
  Sets/Creates value:       HKCR\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\proxystubclsid32[]
  Sets/Creates value:       HKCR\interface\{6c116783-ac8c-4590-be5c-4360bf89ecc6}\forward[]
```

Value changes:	`HKLM\software\microsoft\cryptography\rng[seed]`
Value changes:	`HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}[]`
Value changes:	`HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid[]`
Value changes:	`HKCR\interface\{e194c84a-c2c5-4be2-a499-7b32bb445d93}\proxystubclsid32[]`