Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 53, Task ID: 211

Task ID:	211
Risk Level:	3
Date Processed:	2016-04-28 12:53:09 (UTC)
Processing Time:	3.72 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\602364a4b81740b1e02627127600088a.exe"

Sample ID:	53
Type:	basic
Owner:	admin
Label:	602364a4b81740b1e02627127600088a
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	350856 bytes
MD5:	602364a4b81740b1e02627127600088a
SHA256:	acee4163520723c05718fe63d26f581c80503a1a54f7e70c340517a912b86665
Description:	None

Pattern Matching Results

3 Long sleep detected

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\602364a4b81740b1e02627127600088a.exe ["c:\windows\temp\602364a4b81740b1e02627127600088a.exe"]
Terminates process:	C:\WINDOWS\Temp\602364a4b81740b1e02627127600088a.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?602364A4B81740B1E02627127600088A.EXE

File System Events

Opens:	C:\WINDOWS\Prefetch\602364A4B81740B1E026271276000-220AE6D2.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\602364a4b81740b1e02627127600088a.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\602364a4b81740b1e02627127600088a.exe
  Reads from:                 C:\WINDOWS\Registration\R000000000007.clb
```

Windows Registry Events

```
  Creates key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}
  Creates key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2
  Creates key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags
  Creates key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0
  Creates key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32
  Creates key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir
  Creates key:                HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
  Creates key:                HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid
  Creates key:                HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32
  Creates key:                HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib
  Creates key:                HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}
  Creates key:                HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid
  Creates key:                HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32
  Creates key:                HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib
  Creates key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}
  Creates key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\progid
  Creates key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\localserver32
  Creates key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\typelib
  Creates key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\version
  Creates key:                HKCR\aloahaprintercontrol.control
  Creates key:                HKCR\aloahaprintercontrol.control\clsid
  Creates key:                HKCR\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}
  Creates key:                HKCR\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\proxystubclsid
  Creates key:                HKCR\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\proxystubclsid32
  Creates key:                HKCR\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\forward
  Creates key:                HKCR\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}
  Creates key:                HKCR\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\proxystubclsid
  Creates key:                HKCR\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\proxystubclsid32
  Creates key:                HKCR\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\forward
  Creates key:                HKCR\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}
  Creates key:                HKCR\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\proxystubclsid
  Creates key:                HKCR\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\proxystubclsid32
  Creates key:                HKCR\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\forward
  Creates key:                HKCR\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}
  Creates key:                HKCR\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid
  Creates key:                HKCR\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid32
  Creates key:                HKCR\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\forward
  Creates key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\implemented categories
  Creates key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\programmable
  Creates key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\implemented
categories\{40fc6ed5-2438-11cf-a3db-080036f12502}
  Deletes value:              HKCR\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\localserver32[threadingmodel]
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\602364a4b81740b1e02627127600088a.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\602364a4b81740b1e02627127600088a.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\{86234880-05f2-4242-b9b4-
ef95b0ac62f3}\1.2\0
  Opens key:              HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0
  Opens key:              HKCU\software\classes\typelib
  Opens key:              HKCR\typelib
  Opens key:              HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}
  Opens key:              HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}
  Opens key:              HKLM\software\classes
  Opens key:              HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2
  Opens key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2
  Opens key:                HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-
ef95b0ac62f3}\1.2\flags
  Opens key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags
  Opens key:                HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-
ef95b0ac62f3}\1.2\0\win32
  Opens key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32
  Opens key:                HKCU\software\classes\typelib\{86234880-05f2-4242-b9b4-
ef95b0ac62f3}\1.2\helpdir
  Opens key:                HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir
  Opens key:                HKCU\software\classes\interface
  Opens key:                HKCU\software\classes\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
  Opens key:                HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}
  Opens key:                HKCU\software\classes\interface\{590b6fce-d67f-4955-b9b9-
7c2e07745dd6}\proxystubclsid
  Opens key:                HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{590b6fce-d67f-4955-b9b9-
7c2e07745dd6}\proxystubclsid32
  Opens key:                HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{590b6fce-d67f-4955-b9b9-
7c2e07745dd6}\typelib
  Opens key:                HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib
  Opens key:                HKCU\software\classes\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}
  Opens key:                HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}
  Opens key:                HKCU\software\classes\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\proxystubclsid
  Opens key:                HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\proxystubclsid32
  Opens key:                HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{355155d6-3981-473b-9fec-
c81c43f77f1f}\typelib
  Opens key:                HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\progid
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\localserver32
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\typelib
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\version
  Opens key:                HKCU\software\classes\aloahaprintercontrol.control
  Opens key:                HKCR\aloahaprintercontrol.control
  Opens key:                HKCU\software\classes\aloahaprintercontrol.control\clsid
  Opens key:                HKCU\software\classes\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}
  Opens key:                HKCU\software\classes\interface\{e8455db1-67d2-425f-80b9-
d6e4ed2304b2}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{e8455db1-67d2-425f-80b9-
d6e4ed2304b2}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{e8455db1-67d2-425f-80b9-
d6e4ed2304b2}\forward
  Opens key:                HKCU\software\classes\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}
  Opens key:                HKCU\software\classes\interface\{3782d58d-d973-4f9f-9820-
d4fb5a1dc4a3}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{3782d58d-d973-4f9f-9820-
d4fb5a1dc4a3}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{3782d58d-d973-4f9f-9820-
d4fb5a1dc4a3}\forward
  Opens key:                HKCU\software\classes\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}
  Opens key:                HKCU\software\classes\interface\{0777556d-bd1d-4200-b408-
3eee0fd115e0}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{0777556d-bd1d-4200-b408-
3eee0fd115e0}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{0777556d-bd1d-4200-b408-
3eee0fd115e0}\forward
  Opens key:                HKCU\software\classes\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}
  Opens key:                HKCU\software\classes\interface\{e35d9284-9319-44ca-8473-
8ce927f5e0b8}\proxystubclsid
  Opens key:                HKCU\software\classes\interface\{e35d9284-9319-44ca-8473-
8ce927f5e0b8}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{e35d9284-9319-44ca-8473-
8ce927f5e0b8}\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\602364a4b81740b1e02627127600088a.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\implemented categories
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\programmable
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\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\{df7530d2-2937-4e60-b644-2b7c067b6fdb}
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\treatas
  Opens key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\treatas
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\inprocserver32
  Opens key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\inprocserverx86
  Opens key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprocserverx86
  Opens key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\localserver32
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\inprochandler32
  Opens key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\inprochandlerx86
  Opens key:                HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\inprochandlerx86
  Opens key:                HKCU\software\classes\appid\602364a4b81740b1e02627127600088a.exe
  Opens key:                HKCR\appid\602364a4b81740b1e02627127600088a.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[602364a4b81740b1e02627127600088a]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[602364a4b81740b1e02627127600088a]
  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\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2[]
  Queries value:            HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags[]
  Queries value:            HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32[]
  Queries value:            HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir[]
  Queries value:            HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}[]
  Queries value:            HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid[]
  Queries value:            HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32[]
  Queries value:            HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[]
  Queries value:            HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[version]
  Queries value:            HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}[]
  Queries value:            HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid[]
  Queries value:            HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32[]
  Queries value:            HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[]
  Queries value:            HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\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\{df7530d2-2937-4e60-b644-
2b7c067b6fdb}\localserver32[localserver32]
  Queries value:              HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\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\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2[]
  Sets/Creates value:         HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\flags[]
  Sets/Creates value:         HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\0\win32[]
  Sets/Creates value:         HKCR\typelib\{86234880-05f2-4242-b9b4-ef95b0ac62f3}\1.2\helpdir[]
  Sets/Creates value:         HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}[]
  Sets/Creates value:         HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid[]
  Sets/Creates value:         HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32[]
  Sets/Creates value:         HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[]
  Sets/Creates value:         HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\typelib[version]
  Sets/Creates value:         HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}[]
  Sets/Creates value:         HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid[]
  Sets/Creates value:         HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32[]
  Sets/Creates value:         HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[]
  Sets/Creates value:         HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\typelib[version]
  Sets/Creates value:         HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}[]
  Sets/Creates value:         HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\progid[]
  Sets/Creates value:         HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\localserver32[]
  Sets/Creates value:         HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\typelib[]
  Sets/Creates value:         HKCR\clsid\{df7530d2-2937-4e60-b644-2b7c067b6fdb}\version[]
  Sets/Creates value:         HKCR\aloahaprintercontrol.control[]
  Sets/Creates value:         HKCR\aloahaprintercontrol.control\clsid[]
  Sets/Creates value:         HKCR\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}[]
  Sets/Creates value:         HKCR\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\proxystubclsid[]
  Sets/Creates value:         HKCR\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\proxystubclsid32[]
  Sets/Creates value:         HKCR\interface\{e8455db1-67d2-425f-80b9-d6e4ed2304b2}\forward[]
  Sets/Creates value:         HKCR\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}[]
  Sets/Creates value:         HKCR\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\proxystubclsid[]
  Sets/Creates value:         HKCR\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\proxystubclsid32[]
  Sets/Creates value:         HKCR\interface\{3782d58d-d973-4f9f-9820-d4fb5a1dc4a3}\forward[]
  Sets/Creates value:         HKCR\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}[]
  Sets/Creates value:         HKCR\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\proxystubclsid[]
  Sets/Creates value:         HKCR\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\proxystubclsid32[]
  Sets/Creates value:         HKCR\interface\{0777556d-bd1d-4200-b408-3eee0fd115e0}\forward[]
  Sets/Creates value:         HKCR\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}[]
  Sets/Creates value:         HKCR\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid[]
  Sets/Creates value:         HKCR\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\proxystubclsid32[]
  Sets/Creates value:         HKCR\interface\{e35d9284-9319-44ca-8473-8ce927f5e0b8}\forward[]
  Value changes:              HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:              HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}[]
  Value changes:              HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid[]
  Value changes:              HKCR\interface\{590b6fce-d67f-4955-b9b9-7c2e07745dd6}\proxystubclsid32[]
  Value changes:              HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}[]
  Value changes:              HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid[]
  Value changes:              HKCR\interface\{355155d6-3981-473b-9fec-c81c43f77f1f}\proxystubclsid32[]
```