Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 216, Task ID: 863

Task ID:	863
Risk Level:	3
Date Processed:	2016-04-28 13:11:32 (UTC)
Processing Time:	2.45 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\af08d8af6efe2bd3a801df9206306c08.exe"

Sample ID:	216
Type:	basic
Owner:	admin
Label:	af08d8af6efe2bd3a801df9206306c08
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	36864 bytes
MD5:	af08d8af6efe2bd3a801df9206306c08
SHA256:	4dd56d2ea589054858a876456ad1cb490c077fcd82590bbe72bf88ccf9885417
Description:	None

Pattern Matching Results

3 Long sleep detected

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\af08d8af6efe2bd3a801df9206306c08.exe ["c:\windows\temp\af08d8af6efe2bd3a801df9206306c08.exe"]
Terminates process:	C:\WINDOWS\Temp\af08d8af6efe2bd3a801df9206306c08.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?AF08D8AF6EFE2BD3A801DF9206306C08.EXE

File System Events

Opens:	C:\WINDOWS\Prefetch\AF08D8AF6EFE2BD3A801DF9206306-0C3A7EE4.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\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\Registration\R000000000007.clb
```

Windows Registry Events

```
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\af08d8af6efe2bd3a801df9206306c08.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\af08d8af6efe2bd3a801df9206306c08.exe
  Opens key:                HKLM\software\microsoft\ctf\systemshared\
  Opens key:                HKCU\keyboard layout\toggle
  Opens key:                HKLM\software\microsoft\ctf\
  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:                HKCU\software\classes\
  Opens key:                HKLM\software\classes
  Opens key:                HKU\
  Opens key:                HKCR\clsid
  Opens key:                HKCU\software\classes\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
  Opens key:                HKCR\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
  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\af08d8af6efe2bd3a801df9206306c08.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKCU\software\classes\appid\af08d8af6efe2bd3a801df9206306c08.exe
  Opens key:                HKCR\appid\af08d8af6efe2bd3a801df9206306c08.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:                HKCU\software\policies\microsoft\windows\app management
  Opens key:                HKLM\software\policies\microsoft\windows\app management
  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[af08d8af6efe2bd3a801df9206306c08]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[af08d8af6efe2bd3a801df9206306c08]
  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:          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:          HKLM\software\microsoft\rpc[maxrpcsize]
  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]
  Value changes:          HKLM\software\microsoft\cryptography\rng[seed]
```