

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 100, Task ID: 399

Task ID:	399
Risk Level:	1
Date Processed:	2016-04-28 12:57:47 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\006bfb7286f8b1511346975a4ec7d3d4.exe"
Sample ID:	100
Type:	basic
Owner:	admin
Label:	006bfb7286f8b1511346975a4ec7d3d4
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	114688 bytes
MD5:	006bfb7286f8b1511346975a4ec7d3d4
SHA256:	bbd9d3e1421fede3b6dc485ef528181204dfa5959105875782b0f79978d847b9
Description:	None

## Pattern Matching Results

1 YARA score 1

## Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable

## Process/Thread Events

Creates process:	C:\WINDOWS\Temp\006bfb7286f8b1511346975a4ec7d3d4.exe
["c:\windows\temp\006bfb7286f8b1511346975a4ec7d3d4.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-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.AOG
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.IN
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.IN.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.IN.IC
Creates semaphore:	\BaseNamedObjects\C:\?WINDOWS?TEMP?006BFB7286F8B1511346975A4EC7D3D4.EXE
Creates semaphore:	\BaseNamedObjects\OleDfRoot000021553

## File System Events

Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\~DF1556.tmp
Opens:	C:\WINDOWS\Prefetch\006BFB7286F8B1511346975A4EC7D-256B433C.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\Fonts\sserife.fon
Opens:	C:\WINDOWS\system32\asycfilt.dll
Opens:	C:\
Opens:	C:\WINDOWS\system32\clbcatq.dll
Opens:	C:\WINDOWS\system32\comres.dll
Opens:	C:\WINDOWS\Registration\R0000000000007.clb
Reads from:	C:\WINDOWS\Registration\R0000000000007.clb

## Windows Registry Events

---

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\006bfb7286f8b1511346975a4ec7d3d4.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\006bfb7286f8b1511346975a4ec7d3d4.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\windows nt\currentversion\image file execution

options\asycfilt.dll  
 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\{f9043c85-f6f2-101a-a3c9-08002b2f49fb}  
 Opens key: HKCR\clsid\{f9043c85-f6f2-101a-a3c9-08002b2f49fb}  
 Opens key: HKCU\software\policies\microsoft\windows\app management  
 Opens key: HKLM\software\policies\microsoft\windows\app management  
 Opens key: HKCU\software\microsoft\ctf\langbaraddin\  
 Opens key: HKLM\software\microsoft\ctf\langbaraddin\  
 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[006bfb7286f8b1511346975a4ec7d3d4]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime  
 compatibility[006bfb7286f8b1511346975a4ec7d3d4]  
 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[minimumfreemempercentagecreateprocess]  
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagecreateobject]  
Queries value: HKLM\software\microsoft\com3[regdbversion]  
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]  
Value changes: HKLM\software\microsoft\cryptography\rng[seed]