

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 3, Task ID: 10

Task ID:	10
Risk Level:	4
Date Processed:	2016-04-28 12:46:39 (UTC)
Processing Time:	61.69 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe"
Sample ID:	3
Type:	basic
Owner:	admin
Label:	70707b1474e1364c222b5738e7a5ebca
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	316928 bytes
MD5:	70707b1474e1364c222b5738e7a5ebca
SHA256:	f8e4da55708ab83851edcf19c766a83277939d0f486a1be82352f4da69ab61aa
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:	C:\WINDOWS\Temp\70707b1474e1364c222b5738e7a5ebca.exe
["c:\windows\temp\70707b1474e1364c222b5738e7a5ebca.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.IDH
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

## File System Events

Opens:	C:\WINDOWS\Prefetch\70707B1474E1364C222B5738E7A5E-2CC4C477.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\mf100.dll
Opens:	C:\WINDOWS\system32\msvcr100.dll
Opens:	C:\WINDOWS\system32\msimg32.dll
Opens:	C:\WINDOWS\system32\imm32.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\uxtheme.dll
Opens:	C:\WINDOWS\Fonts\SEGOEUI.TTF
Opens:	C:\WINDOWS\system32\mf100.dll.2.Manifest
Opens:	C:\WINDOWS\system32\mf100.dll.3.Manifest

Opens:	C:\WINDOWS\system32\mfc100.dll.Manifest
Opens:	C:\WINDOWS\system32\mfc100enu.dll
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe.2.Manifest
Opens:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe.3.Manifest
Opens:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe.Manifest
Opens:	C:\windows\temp\70707b1474e1364c222b5738e7a5ebca.exe.Config
Opens:	C:\WINDOWS\Fonts\sserife.fon
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\system32\ole32.dll

## Windows Registry Events

---

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\70707b1474e1364c222b5738e7a5ebca.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\msvcr100.dll
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\shlwapi.dll
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\msimg32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\mfc100.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\comdlg32.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\windows\currentversion\explorer\performance  
 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\uxtheme.dll  
 Opens key: HKCU\software\microsoft\windows\currentversion\thememanager  
 Opens key: HKCU\software\microsoft\windows nt\currentversion\windows  
 Opens key: HKLM\system\setup  
 Opens key:  
 HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\mfc100enu.dll  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\network  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\msctf.dll  
 Opens key:  
 HKLM\software\microsoft\ctf\compatibility\70707b1474e1364c222b5738e7a5ebca.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\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: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\ole32.dll  
 Opens key: HKLM\software\microsoft\ole  
 Opens key: HKCR\interface  
 Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}  
 Opens key: HKCU\software\microsoft\ctf  
 Opens key: HKLM\software\microsoft\ctf\systemshared  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes  
 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[70707b1474e1364c222b5738e7a5ebca]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime  
 compatibility[70707b1474e1364c222b5738e7a5ebca]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit\_dlls]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]  
 Queries value: HKCU\control panel\desktop[multiuilanguageid]  
 Queries value: HKCU\control panel\desktop[smoothscroll]  
 Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]  
 Queries value: HKCU\control panel\desktop[lamebuttontext]

Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]  
 Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]  
 Queries value: HKLM\system\setup[systemsetupinprogress]  
 Queries value:  
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]  
 Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norun]  
 Queries value:  
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nodrives]  
 Queries value:  
 HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]  
 Queries value:  
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetconnectdisconnect]  
 Queries value:  
 HKCU\software\microsoft\windows\currentversion\policies\explorer[norecentdocshistory]  
 Queries value:  
 HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose]  
 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\software\microsoft\windows nt\currentversion\imm[ime file]  
 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\software\microsoft\ctf[disable thread input manager]  
 Queries value:  
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\fontsubstitutes[tahoma]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms  
 sans serif]  
 Value changes: HKLM\software\microsoft\cryptography\rng[seed]