

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 186, Task ID: 743

Task ID:	743
Risk Level:	4
Date Processed:	2016-04-28 13:08:00 (UTC)
Processing Time:	2.5 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\253635f7a1de05ca2b150731c2473fbc.exe"
Sample ID:	186
Type:	basic
Owner:	admin
Label:	253635f7a1de05ca2b150731c2473fbc
Date Added:	2016-04-28 12:45:09 (UTC)
File Type:	PE32:win32:gui
File Size:	929280 bytes
MD5:	253635f7a1de05ca2b150731c2473fbc
SHA256:	7f6d85e11a306b88b0f8ef0d1c83df643defd9bd03402bd9e057a594e0912347
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:	C:\WINDOWS\Temp\253635f7a1de05ca2b150731c2473fbc.exe
["c:\windows\temp\253635f7a1de05ca2b150731c2473fbc.exe" ]	
Terminates process:	C:\WINDOWS\Temp\253635f7a1de05ca2b150731c2473fbc.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 semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

## File System Events

Opens:	C:\WINDOWS\Prefetch\253635F7A1DE05CA2B150731C2473-2DAE72EC.pf
Opens:	C:\Documents and Settings\Admin
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\system32\winmm.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
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\system32\rpcss.dll  
Opens: C:\WINDOWS\system32\MSCTF.dll

## Windows Registry Events

---

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\253635f7a1de05ca2b150731c2473fbc.exe	
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots	
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\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\winmm.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.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:	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: HKCU\software\microsoft\windows\currentversion\explorer\advanced  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32  
 Opens key:  
 HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm  
 Opens key: HKLM\system\setup  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\msctf.dll  
 Opens key:  
 HKLM\software\microsoft\ctf\compatibility\253635f7a1de05ca2b150731c2473fbc.exe  
 Opens key: HKLM\software\microsoft\ctf\systemshared\  
 Opens key: HKCU\keyboard layout\toggle  
 Opens key: HKLM\software\microsoft\ctf\  
 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[253635f7a1de05ca2b150731c2473fbc]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime  
 compatibility[253635f7a1de05ca2b150731c2473fbc]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit\_dlls]  
 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: HKCU\control panel\desktop[smoothscroll]  
 Queries value:  
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]  
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]  
Queries value: HKLM\system\setup[systemsetupinprogress]  
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]  
Value changes: HKLM\software\microsoft\cryptography\rng[seed]