

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 253, Task ID: 1011

Task ID:	1011
Risk Level:	1
Date Processed:	2016-04-28 13:15:12 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d88c28f5c7d0a561b5245d8aff35ebd3.exe"
Sample ID:	253
Type:	basic
Owner:	admin
Label:	d88c28f5c7d0a561b5245d8aff35ebd3
Date Added:	2016-04-28 12:45:16 (UTC)
File Type:	PE32:win32:gui
File Size:	30208 bytes
MD5:	d88c28f5c7d0a561b5245d8aff35ebd3
SHA256:	18df2634933f140d8a44e634d58c207761730910a72ecdae44ee2e8e23fd5766
Description:	None

## Pattern Matching Results

## Process/Thread Events

Creates process:	C:\WINDOWS\Temp\d88c28f5c7d0a561b5245d8aff35ebd3.exe
["c:\windows\temp\d88c28f5c7d0a561b5245d8aff35ebd3.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:	MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.AEH
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.MOF
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.MOF.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.MOF.IC

## File System Events

Opens:	C:\WINDOWS\Prefetch\D88C28F5C7D0A561B5245D8AFF35E-3A007D90.pf
Opens:	C:\Documents and Settings\Admin
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\riched32.dll
Opens:	C:\WINDOWS\system32\riched20.dll
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\system32\ole32.dll
Opens:	C:\WINDOWS\win.ini

Opens: C:\WINDOWS\system32\MSIMTF.dll  
Reads from: C:\WINDOWS\win.ini

## Windows Registry Events

---

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\d88c28f5c7d0a561b5245d8aff35ebd3.exe	
Opens key:	HKLM\system\currentcontrolset\control\terminal server
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\winlogon
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
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\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\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\gdi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.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:	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\msvcrt.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\riched20.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\riched32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll	
Opens key:	HKLM\software\microsoft\ctf\compatibility\d88c28f5c7d0a561b5245d8aff35ebd3.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\msctftime.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: HKCU\software\microsoft\windows nt\currentversion\windows  
 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\system\currentcontrolset\control\terminal server[tsuserenabled]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]  
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
 Queries value:  
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\gre\_initialize[disablemetafiles]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\compatibility32[d88c28f5c7d0a561b5245d8aff35ebd3]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime  
 compatibility[d88c28f5c7d0a561b5245d8aff35ebd3]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit\_dlls]  
 Queries value: HKCU\control panel\desktop[multiuilanguageid]  
 Queries value: HKCU\control panel\desktop[smoothscroll]  
 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 nt\currentversion\windows[scrollinset]  
 Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]  
 Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]  
 Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollldelay]  
 Queries value: HKCU\software\microsoft\windows  
 nt\currentversion\windows[scrollinterval]  
 Value changes: HKLM\software\microsoft\cryptography\rng[seed]