

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 4, Task ID: 15

Task ID:	15
Risk Level:	4
Date Processed:	2016-04-28 12:46:40 (UTC)
Processing Time:	9.6 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7069dc32ff70d12bc71cfb8ef87282fd.exe"
Sample ID:	4
Type:	basic
Owner:	admin
Label:	7069dc32ff70d12bc71cfb8ef87282fd
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	24544 bytes
MD5:	7069dc32ff70d12bc71cfb8ef87282fd
SHA256:	038b781a7822d8b09d29df350faddcd36f680afc467bb87fa13f2de440956d3d
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:	C:\windows\temp\7069dc32ff70d12bc71cfb8ef87282fd.exe
["C:\windows\temp\7069dc32ff70d12bc71cfb8ef87282fd.exe" ]	
Terminates process:	C:\Windows\Temp\7069dc32ff70d12bc71cfb8ef87282fd.exe

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
----------------	---

## File System Events

Opens:	C:\Windows\Prefetch\7069DC32FF70D12BC71CFB8EF8728-AA6DC018.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\MSVCP100.dll
Opens:	C:\Windows\System32\msvcp100.dll
Opens:	C:\windows\temp\MSVCR100.dll
Opens:	C:\Windows\System32\msvcr100.dll
Opens:	C:\Windows\System32\imm32.dll

## Windows Registry Events

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop\languageconfiguration
Opens key:	HKCU\control panel\desktop
Opens key:	HKCU\control panel\desktop\muicached
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions

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\  
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows  
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics  
Opens key: HKLM\software\microsoft\ole  
Opens key: HKLM\software\microsoft\ole\tracing  
Queries value: HKLM\system\currentcontrolset\control\session  
manager[cwdillegalindllsearch]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
Queries value: HKCU\control panel\desktop[preferreduilanguages]  
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]  
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[7069dc32ff70d12bc71cfb8ef87282fd]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]