

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 80, Task ID: 320

Task ID:	320
Risk Level:	4
Date Processed:	2016-04-28 12:56:03 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\8fd748a6f18e76796d0e274593740b83.exe"
Sample ID:	80
Type:	basic
Owner:	admin
Label:	8fd748a6f18e76796d0e274593740b83
Date Added:	2016-04-28 12:44:58 (UTC)
File Type:	PE32:win32:gui
File Size:	668160 bytes
MD5:	8fd748a6f18e76796d0e274593740b83
SHA256:	9dc17f9f85a9bc308a385c41400b31e6f7a60ad9bafdaa64c994a652bf2f0046
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:	C:\windows\temp\8fd748a6f18e76796d0e274593740b83.exe
["C:\windows\temp\8fd748a6f18e76796d0e274593740b83.exe" ]	

## File System Events

Opens:	C:\Windows\Prefetch\8FD748A6F18E76796D0E274593740-C5E440FE.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\WSOCK32.dll
Opens:	C:\Windows\System32\wsock32.dll
Opens:	C:\windows\temp\8fd748a6f18e76796d0e274593740b83.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens:	C:\windows\temp\WINMM.dll
Opens:	C:\Windows\System32\winmm.dll
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\windows\temp\zlib.dll
Opens:	C:\Windows\system32\zlib.dll
Opens:	C:\Windows\system\zlib.dll
Opens:	C:\Windows\zlib.dll
Opens:	C:\Windows\System32\Wbem\zlib.dll
Opens:	C:\Windows\System32\WindowsPowerShell\v1.0\zlib.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  
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
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]