

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 127, Task ID: 509

Task ID:	509
Risk Level:	5
Date Processed:	2016-04-28 13:01:20 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6b113eace91be7de836c25f1584b0e1c.exe"
Sample ID:	127
Type:	basic
Owner:	admin
Label:	6b113eace91be7de836c25f1584b0e1c
Date Added:	2016-04-28 12:45:03 (UTC)
File Type:	PE32:win32:gui
File Size:	248832 bytes
MD5:	6b113eace91be7de836c25f1584b0e1c
SHA256:	6ed034e5a6c704ee960848642a8942497bef1c0cef8634aa0769513814bc624b
Description:	None

## Pattern Matching Results

5	Packer: Asprotect
2	PE: Nonstandard section
5	PE: Contains compressed section

## Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	ASProtect

## Process/Thread Events

Creates process:	C:\windows\temp\6b113eace91be7de836c25f1584b0e1c.exe
["C:\windows\temp\6b113eace91be7de836c25f1584b0e1c.exe" ]	

## File System Events

Opens:	C:\Windows\Prefetch\6B113EACE91BE7DE836C25F1584B0-73C0173E.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\windows\temp\efpmres.dll
Opens:	C:\Windows\SysWOW64\efpmres.dll
Opens:	C:\Windows\system\efpmres.dll
Opens:	C:\Windows\efpmres.dll
Opens:	C:\Windows\SysWOW64\Wbem\efpmres.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\efpmres.dll

## Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options

Opens key: HKLM\system\currentcontrolset\control\safeboot\option  
Opens key: HKLM\system\currentcontrolset\control\srp\gp\ddl  
Opens key:  
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers  
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers  
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options[disableusermodecallbackfilter]  
Queries value: HKLM\system\currentcontrolset\control\session  
manager[cwdillegalindllsearch]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]