

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 256, Task ID: 1024

Task ID:	1024
Risk Level:	1
Date Processed:	2016-04-28 13:15:44 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\beca4042a2b7c3c30a3f0cf16a9f3541.exe"
Sample ID:	256
Type:	basic
Owner:	admin
Label:	beca4042a2b7c3c30a3f0cf16a9f3541
Date Added:	2016-04-28 12:45:16 (UTC)
File Type:	PE32:win32:gui
File Size:	701456 bytes
MD5:	beca4042a2b7c3c30a3f0cf16a9f3541
SHA256:	2fc6f301036b7c6cda33cd19577d4bd72585c8defa21c91ec68dd5d3810118a3
Description:	None

## Pattern Matching Results

## Process/Thread Events

Creates process:	C:\windows\temp\beca4042a2b7c3c30a3f0cf16a9f3541.exe
["C:\windows\temp\beca4042a2b7c3c30a3f0cf16a9f3541.exe" ]	

## File System Events

Opens:	C:\Windows\Prefetch\BECA4042A2B7C3C30A3F0CF16A9F3-F63F7308.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\vc1100.bpl
Opens:	C:\Windows\system32\vc1100.bpl
Opens:	C:\Windows\system\vc1100.bpl
Opens:	C:\Windows\vc1100.bpl
Opens:	C:\Windows\System32\Wbem\vc1100.bpl
Opens:	C:\Windows\System32\WindowsPowerShell\v1.0\vc1100.bpl

## Windows Registry Events

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\terminal server
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
Queries value:	HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]