

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 256, Task ID: 1023

Task ID:	1023
Risk Level:	1
Date Processed:	2016-04-28 13:15:43 (UTC)
Processing Time:	61.41 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\BECA4042A2B7C3C30A3F0CF16A9F3-03AA66F4.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\beca4042a2b7c3c30a3f0cf16a9f3541.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]