

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 201, Task ID: 803

Task ID:	803
Risk Level:	6
Date Processed:	2016-04-28 13:09:42 (UTC)
Processing Time:	61.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\c0d7007dfdc093732bcae8144bab71d5.exe"
Sample ID:	201
Type:	basic
Owner:	admin
Label:	c0d7007dfdc093732bcae8144bab71d5
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	79360 bytes
MD5:	c0d7007dfdc093732bcae8144bab71d5
SHA256:	3f42f77aa67f34c41b46d17de28ca58f7ff3061e198f1cba2fcd08e351f67b92
Description:	None

## Pattern Matching Results

6	PE: File has TLS callbacks
2	PE: Nonstandard section

## Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: File contain TLS callbacks

## Process/Thread Events

Creates process:	C:\WINDOWS\Temp\c0d7007dfdc093732bcae8144bab71d5.exe
["c:\windows\temp\c0d7007dfdc093732bcae8144bab71d5.exe" ]	

## File System Events

Opens:	C:\WINDOWS\Prefetch\C0D7007DFDC093732BCAE8144BAB7-31907440.pf
Opens:	C:\Documents and Settings\Admin

## Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\c0d7007dfdc093732bcae8144bab71d5.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]