Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 103, Task ID: 411

Task ID:	411
Risk Level:	6
Date Processed:	2016-04-28 12:58:14 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\00fb23764cfbd971977575f9ac3df234.exe"

Sample ID:	103
Type:	basic
Owner:	admin
Label:	00fb23764cfbd971977575f9ac3df234
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	150016 bytes
MD5:	00fb23764cfbd971977575f9ac3df234
SHA256:	3ef040cf800ba46d2b275465ac3838a11419d25033ba80f7304f30eb621202ea
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\00fb23764cfbd971977575f9ac3df234.exe ["c:\windows\temp\00fb23764cfbd971977575f9ac3df234.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\00FB23764CFBD971977575F9AC3DF-01EDFEC7.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\00fb23764cfbd971977575f9ac3df234.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]