Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 179, Task ID: 715

Task ID:	715
Risk Level:	6
Date Processed:	2016-04-28 13:07:12 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\5acd7389a405704ba061180af3f390b0.exe"
Sample ID:	179
Type:	basic
Owner:	admin
Label:	5acd7389a405704ba061180af3f390b0
Date Added:	2016-04-28 12:45:08 (UTC)
File Type:	PE32:win32:gui
File Size:	72704 bytes
MD5:	5acd7389a405704ba061180af3f390b0
SHA256:	337e1a93c00d1b50839d37958e2c046ea506b5bfab20fa95b21e9da2427d3cd0
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\5acd7389a405704ba061180af3f390b0.exe ["c:\windows\temp\5acd7389a405704ba061180af3f390b0.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\5ACD7389A405704BA061180AF3F39-2B6CD3CB.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\5acd7389a405704ba061180af3f390b0.exe

Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]