Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 66, Task ID: 263

Task ID:	263
Risk Level:	6
Date Processed:	2016-04-28 12:54:08 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1e1ec93bb4f5555fb4d45b0472a6171b.exe"

Sample ID:	66
Type:	basic
Owner:	admin
Label:	1e1ec93bb4f5555fb4d45b0472a6171b
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	206336 bytes
MD5:	1e1ec93bb4f5555fb4d45b0472a6171b
SHA256:	d7f4fef158bf433b7bf7e8ea796be29e555b7991e7a6659af6fcec53fc444280
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\1e1ec93bb4f5555fb4d45b0472a6171b.exe ["c:\windows\temp\1e1ec93bb4f5555fb4d45b0472a6171b.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\1E1EC93BB4F5555FB4D45B0472A61-22AFF047.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\1e1ec93bb4f5555fb4d45b0472a6171b.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]