Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 72, Task ID: 287

Task ID:	287
Risk Level:	6
Date Processed:	2016-04-28 12:55:22 (UTC)
Processing Time:	61.13 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1e5ef6a6d5a102f3d81459d04866cc96.exe"
Sample ID:	72
Type:	basic
Owner:	admin
Label:	1e5ef6a6d5a102f3d81459d04866cc96
Date Added:	2016-04-28 12:44:57 (UTC)
File Type:	PE32:win32:gui
File Size:	233984 bytes
MD5:	1e5ef6a6d5a102f3d81459d04866cc96
SHA256:	279e9eedd1e2ff5273edd2eb4695fa0dcaf1c8678f87fe34f763b6024c0c7166
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\1e5ef6a6d5a102f3d81459d04866cc96.exe ["c:\windows\temp\1e5ef6a6d5a102f3d81459d04866cc96.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\1E5EF6A6D5A102F3D81459D04866C-15EB96C1.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\1e5ef6a6d5a102f3d81459d04866cc96.exe

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