Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 61, Task ID: 243

Task ID:	243
Risk Level:	6
Date Processed:	2016-04-28 12:53:54 (UTC)
Processing Time:	61.15 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\967842de2c778fe74c96b778671a51c7.exe"
Sample ID:	61
Type:	basic
Owner:	admin
Label:	967842de2c778fe74c96b778671a51c7
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	623616 bytes
MD5:	967842de2c778fe74c96b778671a51c7
SHA256:	d395ec62cac671ce4eb25c90632db84e477c0c840f2e26fcad953d1ccd0f6293
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\967842de2c778fe74c96b778671a51c7.exe ["c:\windows\temp\967842de2c778fe74c96b778671a51c7.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\967842DE2C778FE74C96B778671A5-32FA18A9.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\967842de2c778fe74c96b778671a51c7.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]