Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 115, Task ID: 459

Task ID:	459
Risk Level:	8
Date Processed:	2016-04-28 12:59:30 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\71ee06c836c06dc9070744db6a072a1e.exe"
Sample ID:	115
Type:	basic
Owner:	admin
Label:	71ee06c836c06dc9070744db6a072a1e
Date Added:	2016-04-28 12:45:02 (UTC)
File Type:	PE32:win32:gui
File Size:	175880 bytes
MD5:	71ee06c836c06dc9070744db6a072a1e
SHA256:	765a50799e74731fef1ad77366e68ff8efdef348a35934fa0ecf94b2c0a3f2b3
Description:	None

Pattern Matching Results

8 Contains suspicious Microsoft certificate

Process/Thread Events

Creates process: C:\WINDOWS\Temp\71ee06c836c06dc9070744db6a072a1e.exe ["c:\windows\temp\71ee06c836c06dc9070744db6a072a1e.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\71EE06C836C06DC9070744DB6A072-16DAAA29.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\71ee06c836c06dc9070744db6a072a1e.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]