Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 7, Task ID: 26

Task ID:	26
Risk Level:	1
Date Processed:	2016-04-28 12:46:44 (UTC)
Processing Time:	61.29 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\83aeb82d5c10754e84f518377a34999a.exe"
Sample ID:	7
Type:	basic
Owner:	admin
Label:	83aeb82d5c10754e84f518377a34999a
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	253952 bytes
MD5:	83aeb82d5c10754e84f518377a34999a
SHA256:	04ea191c4d621fd07c1c42cfdcf94d58685ff5458197b59d09cf72e1f097c058
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\WINDOWS\Temp\83aeb82d5c10754e84f518377a34999a.exe ["c:\windows\temp\83aeb82d5c10754e84f518377a34999a.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\83AEB82D5C10754E84F518377A349-27802B95.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\83aeb82d5c10754e84f518377a34999a.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]