Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	82
Risk Level:	1
Date Processed:	2016-04-28 12:48:47 (UTC)
Processing Time:	61.17 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\19006d7d9c79190a3fb3032a97874a36.exe"

Sample ID:	21
Type:	basic
Owner:	admin
Label:	19006d7d9c79190a3fb3032a97874a36
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	886168 bytes
MD5:	19006d7d9c79190a3fb3032a97874a36
SHA256:	0562a8ed75e8d1d36e4a342cf37f1281fbffb375c958d9f91638ab65fb975edb
Description:	None

Pattern Matching Results

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\19006d7d9c79190a3fb3032a97874a36.exe ["c:\windows\temp\19006d7d9c79190a3fb3032a97874a36.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\19006D7D9C79190A3FB3032A97874-2FF0A288.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\19006d7d9c79190a3fb3032a97874a36.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]