Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	859
Risk Level:	1
Date Processed:	2016-04-28 13:11:14 (UTC)
Processing Time:	2.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\af4ef1956ff0b59e9849a57d9fe16ec8.exe"
Sample ID:	215
Type:	basic
Owner:	admin
Label:	af4ef1956ff0b59e9849a57d9fe16ec8
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	69632 bytes
MD5:	af4ef1956ff0b59e9849a57d9fe16ec8
SHA256:	0c14ec6b8c51805eb948466868ffada2a0b25d9681032c257b5844d0b34f883c
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\af4ef1956ff0b59e9849a57d9fe16ec8.exe ["c:\windows\temp\af4ef1956ff0b59e9849a57d9fe16ec8.exe"]
Terminates process:	C:\WINDOWS\Temp\af4ef1956ff0b59e9849a57d9fe16ec8.exe

File System Events

Opens:	C:\WINDOWS\Prefetch\AF4EF1956FF0B59E9849A57D9FE16-2EAF39C2.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\af4ef1956ff0b59e9849a57d9fe16ec8.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]