Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	70
Risk Level:	1
Date Processed:	2016-04-28 12:48:29 (UTC)
Processing Time:	61.29 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	`"c:\windows\temp\7a81151e615b04638ac056c428c42423.exe"`

Sample ID:	18
Type:	basic
Owner:	admin
Label:	7a81151e615b04638ac056c428c42423
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	915472 bytes
MD5:	7a81151e615b04638ac056c428c42423
SHA256:	a07c92d0dc9a27a149cc905ba41160b8d8550b19934e181a082e8a1118e5dcc3
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	`C:\WINDOWS\Temp\7a81151e615b04638ac056c428c42423.exe ["c:\windows\temp\7a81151e615b04638ac056c428c42423.exe" ]`

File System Events

Opens:	`C:\WINDOWS\Prefetch\7A81151E615B04638AC056C428C42-2983E66E.pf`
Opens:	`C:\Documents and Settings\Admin`

Windows Registry Events

Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\7a81151e615b04638ac056c428c42423.exe`
Opens key:	`HKLM\system\currentcontrolset\control\terminal server`
Queries value:	`HKLM\system\currentcontrolset\control\terminal server[tsappcompat]`