Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	74
Risk Level:	8
Date Processed:	2016-04-28 12:48:42 (UTC)
Processing Time:	61.39 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	`"c:\windows\temp\80d07266dc2fc193805e1291c3f1ea4c.exe"`

Sample ID:	19
Type:	basic
Owner:	admin
Label:	80d07266dc2fc193805e1291c3f1ea4c
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	89864 bytes
MD5:	80d07266dc2fc193805e1291c3f1ea4c
SHA256:	8b4800e2ef8d81b0e23ccb8a0fb6a57a812fde04b4cfbce0537658caa4cbfb0f
Description:	None

Pattern Matching Results

8 Contains suspicious Microsoft certificate

Process/Thread Events

Creates process:	`C:\WINDOWS\Temp\80d07266dc2fc193805e1291c3f1ea4c.exe ["c:\windows\temp\80d07266dc2fc193805e1291c3f1ea4c.exe" ]`

File System Events

Opens:	`C:\WINDOWS\Prefetch\80D07266DC2FC193805E1291C3F1E-20C4A011.pf`
Opens:	`C:\Documents and Settings\Admin`

Windows Registry Events

Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\80d07266dc2fc193805e1291c3f1ea4c.exe`
Opens key:	`HKLM\system\currentcontrolset\control\terminal server`
Queries value:	`HKLM\system\currentcontrolset\control\terminal server[tsappcompat]`