Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 181, Task ID: 723

Task ID:	723
Risk Level:	5
Date Processed:	2016-04-28 13:07:37 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\25f424cb9894dd2808f2c387eac9ccc3.exe"

Sample ID:	181
Type:	basic
Owner:	admin
Label:	25f424cb9894dd2808f2c387eac9ccc3
Date Added:	2016-04-28 12:45:08 (UTC)
File Type:	PE32:win32:gui
File Size:	851264 bytes
MD5:	25f424cb9894dd2808f2c387eac9ccc3
SHA256:	eb1d325f1225109b2873593b8d21ca300bd8a58209442c998d26abef3fce00ac
Description:	None

Pattern Matching Results

5 PE: Contains compressed section

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

```
   Creates process:          C:\WINDOWS\Temp\25f424cb9894dd2808f2c387eac9ccc3.exe
["c:\windows\temp\25f424cb9894dd2808f2c387eac9ccc3.exe" ]
```

File System Events

```
   Opens:                    C:\WINDOWS\Prefetch\25F424CB9894DD2808F2C387EAC9C-348F62D2.pf
   Opens:                    C:\Documents and Settings\Admin
```

Windows Registry Events

```
   Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\25f424cb9894dd2808f2c387eac9ccc3.exe
   Opens key:                HKLM\system\currentcontrolset\control\terminal server
   Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
```