Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 93, Task ID: 371

Task ID:	371
Risk Level:	1
Date Processed:	2016-04-28 12:57:14 (UTC)
Processing Time:	2.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\2d227eb0d416daad9b011fcc9a9062e9.exe"
Sample ID:	93
Type:	basic
Owner:	admin
Label:	2d227eb0d416daad9b011fcc9a9062e9
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	61440 bytes
MD5:	2d227eb0d416daad9b011fcc9a9062e9
SHA256:	f61090e9f71976a5043a7a7cfec8a577c8555d997727548d7595b162a10c5ae4
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\WINDOWS\Temp\2d227eb0d416daad9b011fcc9a9062e9.exe ["c:\windows\temp\2d227eb0d416daad9b011fcc9a9062e9.exe"]
Terminates process: C:\WINDOWS\Temp\2d227eb0d416daad9b011fcc9a9062e9.exe

File System Events

Opens: C:\WINDOWS\Prefetch\2D227EB0D416DAAD9B011FCC9A906-289B0323.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\2d227eb0d416daad9b011fcc9a9062e9.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]