Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 96, Task ID: 383

Task ID:	383
Risk Level:	1
Date Processed:	2016-04-28 12:57:33 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\e5cd011aa053b4d825844332db22f1b2.exe"
Sample ID:	96
Type:	basic
Owner:	admin
Label:	e5cd011aa053b4d825844332db22f1b2
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	840344 bytes
MD5:	e5cd011aa053b4d825844332db22f1b2
SHA256:	c2b2644c913407ba97a06fc852d7319359bf0b3c0e6155fac53c91b33c13f634
Description:	None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\WINDOWS\Temp\e5cd011aa053b4d825844332db22f1b2.exe ["c:\windows\temp\e5cd011aa053b4d825844332db22f1b2.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\E5CD011AA053B4D825844332DB22F-10AC6424.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\winspool.drv

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\e5cd011aa053b4d825844332db22f1b2.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]