Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 113, Task ID: 451

Task ID:	451
Risk Level:	1
Date Processed:	2016-04-28 12:59:27 (UTC)
Processing Time:	61.17 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\71cfa0de4981df28171710cf03332a99.exe"
Sample ID:	113
Type:	basic
Owner:	admin
Label:	71cfa0de4981df28171710cf03332a99
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	176128 bytes
MD5:	71cfa0de4981df28171710cf03332a99
SHA256:	50a5c41e0987d687a7cb83e8ae06d7f84489b8df0ea4c856add2a3fbcae8f246
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\WINDOWS\Temp\71cfa0de4981df28171710cf03332a99.exe ["c:\windows\temp\71cfa0de4981df28171710cf03332a99.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\71CFA0DE4981DF28171710CF03332-04D20AB6.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\71cfa0de4981df28171710cf03332a99.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]