Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 202, Task ID: 807

Task ID:	807
Risk Level:	4
Date Processed:	2016-04-28 13:09:46 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9af75510bac6aa983165d40392917512.exe"
Sample ID:	202
Type:	basic
Owner:	admin
Label:	9af75510bac6aa983165d40392917512
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	443416 bytes
MD5:	9af75510bac6aa983165d40392917512
SHA256:	776b9b4fac717c342ab35fb19f65ac6b4c311ca206fdc844cec2ef84826cc274
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\9af75510bac6aa983165d40392917512.exe ["c:\windows\temp\9af75510bac6aa983165d40392917512.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\9AF75510BAC6AA983165D40392917-071DD3D1.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\9af75510bac6aa983165d40392917512.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]