Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 142, Task ID: 566

Task ID:	566
Risk Level:	4
Date Processed:	2016-04-28 13:02:38 (UTC)
Processing Time:	2.38 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0922c62f848a2fbb3ea159a0ee95241c.exe"
Sample ID:	142
Type:	basic
Owner:	admin
Label:	0922c62f848a2fbb3ea159a0ee95241c
Date Added:	2016-04-28 12:45:04 (UTC)
File Type:	PE32:win32:gui
File Size:	95312 bytes
MD5:	0922c62f848a2fbb3ea159a0ee95241c
SHA256:	b132021658d5e4bc90b1ce03da4a6960335b7f5c0c70bf203de14fddb2a2ea5a
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\0922c62f848a2fbb3ea159a0ee95241c.exe
["C:\windows\temp\0922c62f848a2fbb3ea159a0ee95241c.exe"]

File System Events

Opens: C:\Windows\Prefetch\0922C62F848A2FBB3EA159A0EE952-222731DE.pf