Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 237, Task ID: 948

Task ID:	948
Risk Level:	4
Date Processed:	2016-04-28 13:13:35 (UTC)
Processing Time:	2.43 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\f6042a643d6c886966d9416258fc77d1.exe"
Sample ID:	237
Type:	basic
Owner:	admin
Label:	f6042a643d6c886966d9416258fc77d1
Date Added:	2016-04-28 12:45:14 (UTC)
File Type:	PE32:win32:gui
File Size:	32736 bytes
MD5:	f6042a643d6c886966d9416258fc77d1
SHA256:	63f0e5b6489fc11f018f691bf94a1c186b6e551a680a658b9eeb6b3235163d4d
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\f6042a643d6c886966d9416258fc77d1.exe
["C:\windows\temp\f6042a643d6c886966d9416258fc77d1.exe"]

File System Events

Opens: C:\Windows\Prefetch\F6042A643D6C886966D9416258FC7-4E1BDD7B.pf