Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 259, Task ID: 1035

Task ID:	1035
Risk Level:	5
Date Processed:	2016-04-28 13:16:01 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\be7b825c3b803daeccdcca38f3ed964f.exe"
Sample ID:	259
Type:	basic
Owner:	admin
Label:	be7b825c3b803daeccdcca38f3ed964f
Date Added:	2016-04-28 12:45:16 (UTC)
File Type:	PE32:win32:gui
File Size:	446464 bytes
MD5:	be7b825c3b803daeccdcca38f3ed964f
SHA256:	d29cbcb8df6bc4844d4b2ef56ed88b305525c116a647f5802a4e3ed1336efaf4
Description:	None

Pattern Matching Results

5 Possible injector

Process/Thread Events

Creates process: C:\WINDOWS\Temp\be7b825c3b803daeccdcca38f3ed964f.exe ["c:\windows\temp\be7b825c3b803daeccdcca38f3ed964f.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\BE7B825C3B803DAECCDCCA38F3ED9-0ECA26B5.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\be7b825c3b803daeccdcca38f3ed964f.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]