Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 127, Task ID: 507

Task ID:	507
Risk Level:	5
Date Processed:	2016-04-28 13:01:18 (UTC)
Processing Time:	61.33 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6b113eace91be7de836c25f1584b0e1c.exe"

Sample ID:	127
Type:	basic
Owner:	admin
Label:	6b113eace91be7de836c25f1584b0e1c
Date Added:	2016-04-28 12:45:03 (UTC)
File Type:	PE32:win32:gui
File Size:	248832 bytes
MD5:	6b113eace91be7de836c25f1584b0e1c
SHA256:	6ed034e5a6c704ee960848642a8942497bef1c0cef8634aa0769513814bc624b
Description:	None

Pattern Matching Results

5 Packer: Asprotect

2 PE: Nonstandard section

5 PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	ASProtect

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\6b113eace91be7de836c25f1584b0e1c.exe ["c:\windows\temp\6b113eace91be7de836c25f1584b0e1c.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\6B113EACE91BE7DE836C25F1584B0-37D57026.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\6b113eace91be7de836c25f1584b0e1c.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]