Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 130, Task ID: 519

Task ID:	519
Risk Level:	4
Date Processed:	2016-04-28 13:01:22 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ada3f051bedc650553af52d9321bec2c.exe"
Sample ID:	130
Type:	basic
Owner:	admin
Label:	ada3f051bedc650553af52d9321bec2c
Date Added:	2016-04-28 12:45:03 (UTC)
File Type:	PE32:win32:gui
File Size:	245248 bytes
MD5:	ada3f051bedc650553af52d9321bec2c
SHA256:	ec0425791646e77dcaa471392c2d53da3c0ba4fd1523c305d38189cd42c692be
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\ada3f051bedc650553af52d9321bec2c.exe ["c:\windows\temp\ada3f051bedc650553af52d9321bec2c.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\ADA3F051BEDC650553AF52D9321BE-27AEEE34.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ada3f051bedc650553af52d9321bec2c.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]