Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 171, Task ID: 683

Task ID:	683
Risk Level:	4
Date Processed:	2016-04-28 13:05:39 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\c1e80ac15b65d55244d768ca6cda77c3.exe"
Sample ID:	171
Type:	basic
Owner:	admin
Label:	c1e80ac15b65d55244d768ca6cda77c3
Date Added:	2016-04-28 12:45:07 (UTC)
File Type:	PE32:win32:gui
File Size:	103200 bytes
MD5:	c1e80ac15b65d55244d768ca6cda77c3
SHA256:	6020c7ba41a20040ad6e5d247aa647c6f58b817b05f3934b8cf26e8605552a90
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\c1e80ac15b65d55244d768ca6cda77c3.exe
["c:\windows\temp\c1e80ac15b65d55244d768ca6cda77c3.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\C1E80AC15B65D55244D768CA6CDA7-2F914762.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53\mfc90u.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e\msvcr90.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\system32\msimg32.dll

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\c1e80ac15b65d55244d768ca6cda77c3.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]