Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 88, Task ID: 351

Task ID:	351
Risk Level:	5
Date Processed:	2016-04-28 12:56:42 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9003ab3119bca4c6bf6748d8cc07d9b7.exe"

Sample ID:	88
Type:	basic
Owner:	admin
Label:	9003ab3119bca4c6bf6748d8cc07d9b7
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	735648 bytes
MD5:	9003ab3119bca4c6bf6748d8cc07d9b7
SHA256:	2cb8860918a5d50377365116c6de297fcfed93dbdde0459afc5042f5f0786158
Description:	None

Pattern Matching Results

5	Possible injector
2	PE: Nonstandard section
4	Checks whether debugger is present

Static Events

Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\9003ab3119bca4c6bf6748d8cc07d9b7.exe ["c:\windows\temp\9003ab3119bca4c6bf6748d8cc07d9b7.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\9003AB3119BCA4C6BF6748D8CC07D-05322831.pf
Opens:	C:\Documents and Settings\Admin
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\usp10.dll
Opens:	C:\WINDOWS\system32\winspool.drv

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\9003ab3119bca4c6bf6748d8cc07d9b7.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]