

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 43, Task ID: 170

Task ID:	170
Risk Level:	6
Date Processed:	2016-04-28 12:51:49 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\fe72666915b3eda0c4b8bf9d63c42ede.exe"
Sample ID:	43
Type:	basic
Owner:	admin
Label:	fe72666915b3eda0c4b8bf9d63c42ede
Date Added:	2016-04-28 12:44:54 (UTC)
File Type:	PE32:win32:gui
File Size:	76800 bytes
MD5:	fe72666915b3eda0c4b8bf9d63c42ede
SHA256:	8fd96bcd4219331b6cfbee0d8d3aaa113e617210e1c787fe5f3bd4f387f0a4ea
Description:	None

Pattern Matching Results

- 6 PE: File has TLS callbacks
- 2 PE: Nonstandard section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: File contain TLS callbacks

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\fe72666915b3eda0c4b8bf9d63c42ede.exe
["c:\windows\temp\fe72666915b3eda0c4b8bf9d63c42ede.exe"]	

File System Events

Opens:	C:\WINDOWS\Prefetch\FE72666915B3EDA0C4B8BF9D63C42-391AEF4E.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\fe72666915b3eda0c4b8bf9d63c42ede.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]