Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 22, Task ID: 86

Task ID:	86
Risk Level:	6
Date Processed:	2016-04-28 12:48:50 (UTC)
Processing Time:	61.28 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\19d65dfe30cb0a78383421747366f94e.exe"
Sample ID:	22
Type:	basic
Owner:	admin
Label:	19d65dfe30cb0a78383421747366f94e
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	666112 bytes
MD5:	19d65dfe30cb0a78383421747366f94e
SHA256:	e8e38e33ec7f35a0e61bf284e7c4001846ae47c079e9519c622bb3a6de6e8e70
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\19d65dfe30cb0a78383421747366f94e.exe ["c:\windows\temp\19d65dfe30cb0a78383421747366f94e.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\19D65DFE30CB0A78383421747366F-20B83463.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\19d65dfe30cb0a78383421747366f94e.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]