Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 252, Task ID: 1007

Task ID:	1007
Risk Level:	6
Date Processed:	2016-04-28 13:15:12 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d81f098d8b2b776256fd9ace0ddba957.exe"
Sample ID:	252
Type:	basic
Owner:	admin
Label:	d81f098d8b2b776256fd9ace0ddba957
Date Added:	2016-04-28 12:45:16 (UTC)
File Type:	PE32:win32:gui
File Size:	396800 bytes
MD5:	d81f098d8b2b776256fd9ace0ddba957
SHA256:	6b5c3780c9375e133e9bebec7e366507aef8435c7f46bd48ade22f67fdda70a3
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\d81f098d8b2b776256fd9ace0ddba957.exe ["c:\windows\temp\d81f098d8b2b776256fd9ace0ddba957.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\D81F098D8B2B776256FD9ACE0DDBA-1D71AB26.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\d81f098d8b2b776256fd9ace0ddba957.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]