Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	150
Risk Level:	1
Date Processed:	2016-04-28 12:51:02 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	`"c:\windows\temp\785c8b71605e40c35d546b1d9ab1681f.exe"`
Sample ID:	38
Type:	basic
Owner:	admin
Label:	785c8b71605e40c35d546b1d9ab1681f
Date Added:	2016-04-28 12:44:53 (UTC)
File Type:	PE32:win32:gui
File Size:	201688 bytes
MD5:	785c8b71605e40c35d546b1d9ab1681f
SHA256:	fb10cec0b3ad436990c160e95d0c35b995255c736c8283822c410e59821a2bb4
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	`C:\WINDOWS\Temp\785c8b71605e40c35d546b1d9ab1681f.exe` `["c:\windows\temp\785c8b71605e40c35d546b1d9ab1681f.exe" ]`

File System Events

Opens:	`C:\WINDOWS\Prefetch\785C8B71605E40C35D546B1D9AB16-05EB73FD.pf`
Opens:	`C:\Documents and Settings\Admin`

Windows Registry Events

Opens key:	`HKLM\software\microsoft\windows nt\currentversion\image file execution options\785c8b71605e40c35d546b1d9ab1681f.exe`
Opens key:	`HKLM\system\currentcontrolset\control\terminal server`
Queries value:	`HKLM\system\currentcontrolset\control\terminal server[tsappcompat]`