Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 196, Task ID: 783

Task ID:	783
Risk Level:	4
Date Processed:	2016-04-28 13:08:52 (UTC)
Processing Time:	62.4 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\525a6ed3472d29161413f166baa05543.exe"

Sample ID:	196
Type:	basic
Owner:	admin
Label:	525a6ed3472d29161413f166baa05543
Date Added:	2016-04-28 12:45:10 (UTC)
File Type:	PE32:win32:gui
File Size:	35840 bytes
MD5:	525a6ed3472d29161413f166baa05543
SHA256:	8331e8b4881aca591f454faf4911e68716dde5b3dbec79f717545105627f4e88
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\525a6ed3472d29161413f166baa05543.exe ["c:\windows\temp\525a6ed3472d29161413f166baa05543.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\525A6ED3472D29161413F166BAA05-0583040C.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\525a6ed3472d29161413f166baa05543.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]