Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 206, Task ID: 823

Task ID:	823
Risk Level:	1
Date Processed:	2016-04-28 13:09:58 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7f5a985a8a280d8fff703341af3baa0a.exe"

Sample ID:	206
Type:	basic
Owner:	admin
Label:	7f5a985a8a280d8fff703341af3baa0a
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	299008 bytes
MD5:	7f5a985a8a280d8fff703341af3baa0a
SHA256:	7054d2ace3b9b6930fc01046cb09f843145dcc12b3ec8630652e49be6e2faffb
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\7f5a985a8a280d8fff703341af3baa0a.exe ["c:\windows\temp\7f5a985a8a280d8fff703341af3baa0a.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\7F5A985A8A280D8FFF703341AF3BA-10D72505.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\winmm.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\7f5a985a8a280d8fff703341af3baa0a.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]