Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 190, Task ID: 759

Task ID:	759
Risk Level:	4
Date Processed:	2016-04-28 13:08:15 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\592ec975d7f4ee422e9c4a1f5d08497c.exe"

Sample ID:	190
Type:	basic
Owner:	admin
Label:	592ec975d7f4ee422e9c4a1f5d08497c
Date Added:	2016-04-28 12:45:09 (UTC)
File Type:	PE32:win32:gui
File Size:	293848 bytes
MD5:	592ec975d7f4ee422e9c4a1f5d08497c
SHA256:	6414f33b7eb649d1e7b1d18ac5b3f8aacb8dc8028c068bb7b031b66cd3d62b80
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\592ec975d7f4ee422e9c4a1f5d08497c.exe ["c:\windows\temp\592ec975d7f4ee422e9c4a1f5d08497c.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\592EC975D7F4EE422E9C4A1F5D084-01B20D53.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\592ec975d7f4ee422e9c4a1f5d08497c.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]