Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 219, Task ID: 875

Task ID:	875
Risk Level:	4
Date Processed:	2016-04-28 13:11:42 (UTC)
Processing Time:	61.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\73c74c060890db0006f89fc31e55022a.exe"
Sample ID:	219
Type:	basic
Owner:	admin
Label:	73c74c060890db0006f89fc31e55022a
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	288784 bytes
MD5:	73c74c060890db0006f89fc31e55022a
SHA256:	0449b0d5d1fe843662306b8afadf24fd0391997a81e30129ede98f9b7b6b23bb
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\73c74c060890db0006f89fc31e55022a.exe ["c:\windows\temp\73c74c060890db0006f89fc31e55022a.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\73C74C060890DB0006F89FC31E550-34DF09E7.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\winspool.drv

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\73c74c060890db0006f89fc31e55022a.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]