Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	427
Risk Level:	4
Date Processed:	2016-04-28 12:58:46 (UTC)
Processing Time:	61.27 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\89412b3b78ebee72a87c2bbd56f0b0c4.exe"

Sample ID:	107
Type:	basic
Owner:	admin
Label:	89412b3b78ebee72a87c2bbd56f0b0c4
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	17304 bytes
MD5:	89412b3b78ebee72a87c2bbd56f0b0c4
SHA256:	4c60ae40c0e3dceb2b98e4b7cf7caab42282eaf74211c7cb53972ad99d8fbf3d
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\89412b3b78ebee72a87c2bbd56f0b0c4.exe ["c:\windows\temp\89412b3b78ebee72a87c2bbd56f0b0c4.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\89412B3B78EBEE72A87C2BBD56F0B-1D408A5A.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\89412b3b78ebee72a87c2bbd56f0b0c4.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]