Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	443
Risk Level:	4
Date Processed:	2016-04-28 12:59:20 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\4a7749dcc24c8c7d145a39e8e132b17c.exe"

Sample ID:	111
Type:	basic
Owner:	admin
Label:	4a7749dcc24c8c7d145a39e8e132b17c
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	91608 bytes
MD5:	4a7749dcc24c8c7d145a39e8e132b17c
SHA256:	4bd9267536ce850dd8dee4ff1a8c0ff0253170043c1c3295200fc445eb3f2cb2
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\4a7749dcc24c8c7d145a39e8e132b17c.exe ["c:\windows\temp\4a7749dcc24c8c7d145a39e8e132b17c.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\4A7749DCC24C8C7D145A39E8E132B-2500EF7C.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\4a7749dcc24c8c7d145a39e8e132b17c.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]