Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	663
Risk Level:	5
Date Processed:	2016-04-28 13:05:17 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0c05a151bc2c66fd6112346d6c7e0e06.exe"
Sample ID:	166
Type:	basic
Owner:	admin
Label:	0c05a151bc2c66fd6112346d6c7e0e06
Date Added:	2016-04-28 12:45:07 (UTC)
File Type:	PE32:win32:gui
File Size:	108544 bytes
MD5:	0c05a151bc2c66fd6112346d6c7e0e06
SHA256:	3a4d8bd4c397c5b06bc8abf72d1cf547630b92336ff59e7001574a201a802531
Description:	None

Pattern Matching Results

`2` PE: Nonstandard section
`4` Checks whether debugger is present
`5` PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\0c05a151bc2c66fd6112346d6c7e0e06.exe

["c:\windows\temp\0c05a151bc2c66fd6112346d6c7e0e06.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\0C05A151BC2C66FD6112346D6C7E0-02E7633D.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\0c05a151bc2c66fd6112346d6c7e0e06.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]