Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 233, Task ID: 931

Task ID:	931
Risk Level:	1
Date Processed:	2016-04-28 13:13:08 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0bee7bfb824a58af287f5cfe77bfcde5.exe"

Sample ID:	233
Type:	basic
Owner:	admin
Label:	0bee7bfb824a58af287f5cfe77bfcde5
Date Added:	2016-04-28 12:45:14 (UTC)
File Type:	PE32:win32:gui
File Size:	61440 bytes
MD5:	0bee7bfb824a58af287f5cfe77bfcde5
SHA256:	7b3f0b4f79bb80114b7d15999cd43a0ea966035e7b66f0bb33c71d2e8ffad55b
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\0bee7bfb824a58af287f5cfe77bfcde5.exe ["c:\windows\temp\0bee7bfb824a58af287f5cfe77bfcde5.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\0BEE7BFB824A58AF287F5CFE77BFC-36B7AC6A.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\0bee7bfb824a58af287f5cfe77bfcde5.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]