Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 27, Task ID: 107

Task ID:	107
Risk Level:	6
Date Processed:	2016-04-28 12:49:38 (UTC)
Processing Time:	61.36 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\bd6a26dc159cee72674d4f46853c8329.exe"
Sample ID:	27
Type:	basic
Owner:	admin
Label:	bd6a26dc159cee72674d4f46853c8329
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	645120 bytes
MD5:	bd6a26dc159cee72674d4f46853c8329
SHA256:	e0f2d015b97dccb22fd73c7d4a593fd6d7be3fc3e5632f77a26ce8c76e0203a3
Description:	None

Pattern Matching Results

6 PE: File has TLS callbacks
2 PE: Nonstandard section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: File contain TLS callbacks

Process/Thread Events

Creates process: C:\windows\temp\bd6a26dc159cee72674d4f46853c8329.exe ["C:\windows\temp\bd6a26dc159cee72674d4f46853c8329.exe"]

File System Events

Opens:	C:\Windows\Prefetch\BD6A26DC159CEE72674D4F46853C8-DC4AECF3.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\libkdecore.dll
Opens:	C:\Windows\system32\libkdecore.dll
Opens:	C:\Windows\system\libkdecore.dll
Opens:	C:\Windows\libkdecore.dll
Opens:	C:\Windows\System32\Wbem\libkdecore.dll
Opens:	C:\Windows\System32\WindowsPowerShell\v1.0\libkdecore.dll

Windows Registry Events

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Queries value:	HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]