Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 103, Task ID: 412

Task ID:	412
Risk Level:	6
Date Processed:	2016-04-28 12:58:14 (UTC)
Processing Time:	61.13 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\00fb23764cfbd971977575f9ac3df234.exe"
Sample ID:	103
Type:	basic
Owner:	admin
Label:	00fb23764cfbd971977575f9ac3df234
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	150016 bytes
MD5:	00fb23764cfbd971977575f9ac3df234
SHA256:	3ef040cf800ba46d2b275465ac3838a11419d25033ba80f7304f30eb621202ea
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\00fb23764cfbd971977575f9ac3df234.exe ["C:\windows\temp\00fb23764cfbd971977575f9ac3df234.exe"]

File System Events

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]