Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 61, Task ID: 244

Task ID:	244
Risk Level:	6
Date Processed:	2016-04-28 12:53:54 (UTC)
Processing Time:	61.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\967842de2c778fe74c96b778671a51c7.exe"
Sample ID:	61
Type:	basic
Owner:	admin
Label:	967842de2c778fe74c96b778671a51c7
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	623616 bytes
MD5:	967842de2c778fe74c96b778671a51c7
SHA256:	d395ec62cac671ce4eb25c90632db84e477c0c840f2e26fcad953d1ccd0f6293
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\967842de2c778fe74c96b778671a51c7.exe ["C:\windows\temp\967842de2c778fe74c96b778671a51c7.exe"]

File System Events

Opens:	C:\Windows\Prefetch\967842DE2C778FE74C96B778671A5-793ED337.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]