Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	976
Risk Level:	6
Date Processed:	2016-04-28 13:14:19 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d0cf7e0774812903c07c433428f9418d.exe"
Sample ID:	244
Type:	basic
Owner:	admin
Label:	d0cf7e0774812903c07c433428f9418d
Date Added:	2016-04-28 12:45:15 (UTC)
File Type:	PE32:win32:gui
File Size:	264704 bytes
MD5:	d0cf7e0774812903c07c433428f9418d
SHA256:	cc3c1000a1b1226a49576a1eff5edd601de762001be5a0b4c2796340b5213469
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\d0cf7e0774812903c07c433428f9418d.exe

["C:\windows\temp\d0cf7e0774812903c07c433428f9418d.exe"]

File System Events

Opens:	C:\Windows\Prefetch\D0CF7E0774812903C07C433428F94-FBB65E1F.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]