Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	288
Risk Level:	6
Date Processed:	2016-04-28 12:55:22 (UTC)
Processing Time:	61.13 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1e5ef6a6d5a102f3d81459d04866cc96.exe"
Sample ID:	72
Type:	basic
Owner:	admin
Label:	1e5ef6a6d5a102f3d81459d04866cc96
Date Added:	2016-04-28 12:44:57 (UTC)
File Type:	PE32:win32:gui
File Size:	233984 bytes
MD5:	1e5ef6a6d5a102f3d81459d04866cc96
SHA256:	279e9eedd1e2ff5273edd2eb4695fa0dcaf1c8678f87fe34f763b6024c0c7166
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\1e5ef6a6d5a102f3d81459d04866cc96.exe

["C:\windows\temp\1e5ef6a6d5a102f3d81459d04866cc96.exe"]

File System Events

Opens:	C:\Windows\Prefetch\1E5EF6A6D5A102F3D81459D04866C-C9EF6ED9.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]