Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	88
Risk Level:	6
Date Processed:	2016-04-28 12:48:50 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\19d65dfe30cb0a78383421747366f94e.exe"

Sample ID:	22
Type:	basic
Owner:	admin
Label:	19d65dfe30cb0a78383421747366f94e
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	666112 bytes
MD5:	19d65dfe30cb0a78383421747366f94e
SHA256:	e8e38e33ec7f35a0e61bf284e7c4001846ae47c079e9519c622bb3a6de6e8e70
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\19d65dfe30cb0a78383421747366f94e.exe ["C:\windows\temp\19d65dfe30cb0a78383421747366f94e.exe"]

File System Events

Opens:	C:\Windows\Prefetch\19D65DFE30CB0A78383421747366F-5603794A.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\windows\temp\libkateinterfaces.dll
Opens:	C:\Windows\SysWOW64\libkateinterfaces.dll
Opens:	C:\Windows\system\libkateinterfaces.dll
Opens:	C:\Windows\libkateinterfaces.dll
Opens:	C:\Windows\SysWOW64\Wbem\libkateinterfaces.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\libkateinterfaces.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
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\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
  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]
```