Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	691
Risk Level:	4
Date Processed:	2016-04-28 13:06:31 (UTC)
Processing Time:	19.41 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\c17e5c747159dd245b1d0d46babec30d.exe"
Sample ID:	173
Type:	basic
Owner:	admin
Label:	c17e5c747159dd245b1d0d46babec30d
Date Added:	2016-04-28 12:45:08 (UTC)
File Type:	PE32:win32:gui
File Size:	231512 bytes
MD5:	c17e5c747159dd245b1d0d46babec30d
SHA256:	b07f3050fbe0c07f655fc77df4480665c5cde7669589bd68a8f6f9e2b672bbb0
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\c17e5c747159dd245b1d0d46babec30d.exe

["c:\windows\temp\c17e5c747159dd245b1d0d46babec30d.exe"]

Terminates process:	C:\WINDOWS\Temp\c17e5c747159dd245b1d0d46babec30d.exe

Named Object Events

Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens:	C:\WINDOWS\Prefetch\C17E5C747159DD245B1D0D46BABEC-3406E2F4.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\wsock32.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\winhttp.dll
Opens:	C:\WINDOWS\system32\iphlpapi.dll
Opens:	C:\WINDOWS\system32\psapi.dll
Opens:	C:\WINDOWS\system32\uxtheme.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\c17e5c747159dd245b1d0d46babec30d.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server

```
Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key:              HKLM\
Opens key:              HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wsock32.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
Opens key:              HKLM\system\currentcontrolset\control\session manager
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winhttp.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
Opens key:              HKLM\system\currentcontrolset\control\error message instrument\
Opens key:              HKLM\system\currentcontrolset\control\error message instrument
Opens key:              HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:              HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key:              HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key:              HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:              HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
Opens key:              HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters\
Opens key:              HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
Opens key:              HKLM\system\currentcontrolset\services\netbt\parameters
Opens key:              HKCU\
Opens key:              HKCU\software\policies\microsoft\control panel\desktop
Opens key:              HKCU\control panel\desktop
Opens key:              HKCU\software\microsoft\windows\currentversion\thememanager
Opens key:              HKLM\system\setup
```

Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
   Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
   Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
   Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
   Opens key: HKLM\system\currentcontrolset\control\servicecurrent
   Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
   Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[c17e5c747159dd245b1d0d46babec30d]
   Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[c17e5c747159dd245b1d0d46babec30d]
   Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
   Queries value: HKCU\control panel\desktop[multiuilanguageid]
   Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
   Queries value: HKCU\control panel\desktop[lamebuttontext]
   Queries value: HKLM\system\setup[systemsetupinprogress]
   Queries value: HKCU\control panel\desktop[smoothscroll]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
   Queries value: HKLM\system\currentcontrolset\control\servicecurrent[]