Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	692
Risk Level:	4
Date Processed:	2016-04-28 13:06:31 (UTC)
Processing Time:	3.39 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 mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\C17E5C747159DD245B1D0D46BABEC-2BA722CD.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\WSOCK32.dll
Opens:	C:\Windows\System32\wsock32.dll
Opens:	C:\windows\temp\WINHTTP.dll
Opens:	C:\Windows\System32\winhttp.dll
Opens:	C:\windows\temp\webio.dll
Opens:	C:\Windows\System32\webio.dll
Opens:	C:\windows\temp\iphlpapi.dll
Opens:	C:\Windows\System32\IPHLPAPI.DLL
Opens:	C:\windows\temp\WINNSI.DLL
Opens:	C:\Windows\System32\winnsi.dll
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\windows\temp\UxTheme.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\Temp\c17e5c747159dd245b1d0d46babec30d.exe

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
  Opens key:             HKCU\
  Opens key:             HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:             HKLM\software\policies\microsoft\mui\settings
  Opens key:             HKCU\software\policies\microsoft\control panel\desktop
  Opens key:             HKCU\control panel\desktop\languageconfiguration
  Opens key:             HKCU\control panel\desktop
  Opens key:             HKCU\control panel\desktop\muicached
  Opens key:             HKLM\software\microsoft\windows\currentversion\sidebyside
  Opens key:             HKLM\system\currentcontrolset\control\nls\sorting\versions
  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\
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:             HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:             HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:             HKLM\software\microsoft\rpc
  Opens key:             HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:             HKLM\system\setup
  Opens key:             HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:             HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:             HKLM\software\microsoft\sqmclient\windows
  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]
  Queries value:         HKCU\control panel\desktop[preferreduilanguages]
  Queries value:         HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:         HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  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\windows[loadappinit_dlls]
  Queries value:         HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:         HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:         HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:         HKLM\system\setup[oobeinprogress]
  Queries value:         HKLM\system\setup[systemsetupinprogress]
  Queries value:         HKLM\software\microsoft\sqmclient\windows[ceipenable]
```