Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 173, Task ID: 690

Task ID:	690
Risk Level:	4
Date Processed:	2016-04-28 13:06:30 (UTC)
Processing Time:	5.82 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
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\c17e5c747159dd245b1d0d46babec30d.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\wsock32.dll
Opens:	C:\Windows\SysWOW64\winhttp.dll
Opens:	C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\winnsi.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\nsi.dll
Opens:	C:\Windows\SysWOW64\ws2_32.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll

```
  Opens:                   C:\Windows\SysWOW64\psapi.dll
  Opens:                   C:\Windows\SysWOW64\gdi32.dll
  Opens:                   C:\Windows\SysWOW64\user32.dll
  Opens:                   C:\Windows\SysWOW64\advapi32.dll
  Opens:                   C:\Windows\SysWOW64\shlwapi.dll
  Opens:                   C:\Windows\SysWOW64\shell32.dll
  Opens:                   C:\Windows\SysWOW64\imm32.dll
  Opens:                   C:\Windows\SysWOW64\msctf.dll
```

Windows Registry Events

```
  Opens key:               HKLM\software\microsoft\wow64
  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
  Opens key:               HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:               HKLM\system\currentcontrolset\control\nls\language
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:               HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:               HKLM\software\policies\microsoft\mui\settings
  Opens key:               HKCU\
  Opens key:               HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:               HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  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\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:               HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:               HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:               HKLM\system\currentcontrolset\control\session manager
  Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  Opens key:               HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:               HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:               HKLM\
  Opens key:               HKLM\software\wow6432node\microsoft\ole
  Opens key:               HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:               HKLM\software\microsoft\ole\tracing
  Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:               HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:               HKLM\software\microsoft\sqmclient\windows
  Opens key:               HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:               HKLM\software\wow6432node\microsoft\rpc
  Opens key:               HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  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:            HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[c17e5c747159dd245b1d0d46babec30d.exe]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[c17e5c747159dd245b1d0d46babec30d]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
  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\rpc[idletimerwindow]
```