Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 5, Task ID: 5

Task ID:	5
Risk Level:	6
Date Processed:	2016-08-19 14:57:18 (UTC)
Processing Time:	69.92 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0e17db924eba839ecbb94938c6f6c508b033288c0cd49e893e3f54d91837fcab.exe"

Sample ID:	5
Type:	basic
Owner:	admin
Label:	0e17db924eba839ecbb94938c6f6c508b033288c0cd49e893e3f54d91837fcab
Date Added:	2016-08-19 14:55:41 (UTC)
File Type:	PE32:win32:gui
File Size:	222207 bytes
MD5:	56692e39943d1b4d1300e59bd09d877a
SHA256:	0e17db924eba839ecbb94938c6f6c508b033288c0cd49e893e3f54d91837fcab
Description:	None

Pattern Matching Results

6 PE: Jumps to the last section near the entrypoint

5 PE: Contains compressed section

3 Program causes a crash [Info]

Static Events

Anomaly:	PE: Jumps to the last section near the entrypoint

Process/Thread Events

Creates process:
C:\windows\temp\0e17db924eba839ecbb94938c6f6c508b033288c0cd49e893e3f54d91837fcab.exe
["C:\windows\temp\0e17db924eba839ecbb94938c6f6c508b033288c0cd49e893e3f54d91837fcab.exe"]

Named Object Events

Creates event:	\KernelObjects\SystemErrorPortReady

File System Events

Opens:	C:\Windows\Prefetch\0E17DB924EBA839ECBB94938C6F6C-536D6275.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\SysWOW64\sechost.dll
Opens:	C:\windows\temp\WINMM.dll
Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\windows\temp\0e17db924eba839ecbb94938c6f6c508b033288c0cd49e893e3f54d91837fcab.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest

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\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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                 HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                 HKLM\
  Opens key:                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
  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\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 nt\currentversion\windows
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
  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\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  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\wow6432node\microsoft\windows
nt\currentversion\compatibility32[0e17db924eba839ecbb94938c6f6c508b033288c0cd49e893e3f54d91837fcab]
  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
```

nt\currentversion\windows[loadappinit_dlls]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]