Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 171, Task ID: 685

Task ID:	685
Risk Level:	4
Date Processed:	2016-04-28 13:05:39 (UTC)
Processing Time:	61.3 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\c1e80ac15b65d55244d768ca6cda77c3.exe"

Sample ID:	171
Type:	basic
Owner:	admin
Label:	c1e80ac15b65d55244d768ca6cda77c3
Date Added:	2016-04-28 12:45:07 (UTC)
File Type:	PE32:win32:gui
File Size:	103200 bytes
MD5:	c1e80ac15b65d55244d768ca6cda77c3
SHA256:	6020c7ba41a20040ad6e5d247aa647c6f58b817b05f3934b8cf26e8605552a90
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\c1e80ac15b65d55244d768ca6cda77c3.exe ["C:\windows\temp\c1e80ac15b65d55244d768ca6cda77c3.exe"]

File System Events

Opens:	C:\Windows\Prefetch\C1E80AC15B65D55244D768CA6CDA7-6924D977.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\c1e80ac15b65d55244d768ca6cda77c3.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.mfc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4bf5400abf9d60b7
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.mfc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4bf5400abf9d60b7\mfc90u.dll
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcr90.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
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\temp\MSIMG32.dll
Opens:	C:\Windows\SysWOW64\msimg32.dll
Opens:	C:\windows\temp\Languages.dll
Opens:	C:\Windows\SysWOW64\Languages.dll
Opens:	C:\Windows\system\Languages.dll
Opens:	C:\Windows\Languages.dll
Opens:	C:\Windows\SysWOW64\Wbem\Languages.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Languages.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\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\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
  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\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]
```