Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	733
Risk Level:	5
Date Processed:	2016-04-28 13:07:37 (UTC)
Processing Time:	2.62 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\25b0c8aee8cec0c7e2506918fd5835fa.exe"

Sample ID:	183
Type:	basic
Owner:	admin
Label:	25b0c8aee8cec0c7e2506918fd5835fa
Date Added:	2016-04-28 12:45:09 (UTC)
File Type:	PE32:win32:gui
File Size:	996352 bytes
MD5:	25b0c8aee8cec0c7e2506918fd5835fa
SHA256:	07da4de6b46856159b4810b075e010e3fbb30de3f31e8d2e71f512e6dc439c41
Description:	None

Pattern Matching Results

5 Possible injector

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\25b0c8aee8cec0c7e2506918fd5835fa.exe ["C:\windows\temp\25b0c8aee8cec0c7e2506918fd5835fa.exe"]
Terminates process:	C:\Windows\Temp\25b0c8aee8cec0c7e2506918fd5835fa.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\25B0C8AEE8CEC0C7E2506918FD583-694B6292.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\25b0c8aee8cec0c7e2506918fd5835fa.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\temp\DNSAPI.dll
Opens:	C:\Windows\SysWOW64\dnsapi.dll
Opens:	C:\windows\temp\MSVCP100.dll
Opens:	C:\Windows\SysWOW64\msvcp100.dll
Opens:	C:\windows\temp\MSVCR100.dll
Opens:	C:\Windows\SysWOW64\msvcr100.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\SysWOW64\rpcss.dll
Opens:	C:\Windows\SysWOW64\uxtheme.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\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\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\software\wow6432node\microsoft\windows nt\currentversion\windows
  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\oleaut
  Opens key:              HKLM\system\currentcontrolset\services\crypt32
  Opens key:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
  Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  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]
  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[25b0c8aee8cec0c7e2506918fd5835fa]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
```