Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	918
Risk Level:	1
Date Processed:	2016-04-28 13:12:34 (UTC)
Processing Time:	61.06 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0be85123fcf951b2f52c115972e373cb.exe"

Sample ID:	230
Type:	basic
Owner:	admin
Label:	0be85123fcf951b2f52c115972e373cb
Date Added:	2016-04-28 12:45:14 (UTC)
File Type:	PE32:win32:gui
File Size:	519168 bytes
MD5:	0be85123fcf951b2f52c115972e373cb
SHA256:	8068ea17e55927ec32f7d58e0e5f225b3ac00457763f71dff5ebdfa44704f466
Description:	None

Pattern Matching Results

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\windows\temp\0be85123fcf951b2f52c115972e373cb.exe ["C:\windows\temp\0be85123fcf951b2f52c115972e373cb.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\0BE85123FCF951B2F52C115972E37-48B0CC40.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\0be85123fcf951b2f52c115972e373cb.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\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens:	C:\Windows\SysWOW64\winspool.drv
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\msvcrt.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\advapi32.dll
  Opens:                   C:\Windows\SysWOW64\combase.dll
  Opens:                   C:\Windows\SysWOW64\oleaut32.dll
  Opens:                   C:\Windows\SysWOW64\ole32.dll
  Opens:                   C:\Windows\SysWOW64\shlwapi.dll
  Opens:                   C:\Windows\SysWOW64\shell32.dll
  Opens:                   C:\Windows\SysWOW64\comdlg32.dll
  Opens:                   C:\Windows\SysWOW64\imm32.dll
  Opens:                   C:\Windows\SysWOW64\msctf.dll
  Opens:                   C:\Windows\SysWOW64\uxtheme.dll
  Opens:                   C:\Windows\SysWOW64\dwmapi.dll
  Opens:                   C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                   C:\Windows\Fonts\StaticCache.dat
  Opens:                   C:\Windows\Fonts\sserife.fon
  Opens:                   C:\Windows\SysWOW64\uxtheme.dll.Config
  Opens:                   C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
  Opens:                   C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
  Opens:                   C:\Windows\WindowsShell.Manifest
  Opens:                   C:\Windows\SysWOW64\riched32.dll
  Opens:                   C:\Windows\SysWOW64\riched20.dll
  Opens:                   C:\Windows\SysWOW64\usp10.dll
  Opens:                   C:\Windows\SysWOW64\msls31.dll
  Opens:                   C:\Windows\win.ini
  Opens:                   C:\Windows\Fonts\arialbd.ttf
  Opens:                   C:\Windows\Fonts\arial.ttf
  Opens:                   C:\Windows\devisen.ini
  Opens:                   C:\Windows\Fonts\micross.ttf
  Opens:                   C:\Windows\Fonts\tahoma.ttf
  Opens:                   C:\Windows\Fonts\meiryo.ttc
  Opens:                   C:\Windows\Fonts\msgothic.ttc
  Opens:                   C:\Windows\Fonts\msjh.ttc
  Opens:                   C:\Windows\Fonts\msyh.ttc
  Opens:                   C:\Windows\Fonts\malgun.ttf
  Opens:                   C:\Windows\Fonts\mingliu.ttc
  Opens:                   C:\Windows\Fonts\simsun.ttc
  Opens:                   C:\Windows\Fonts\gulim.ttc
  Reads from:              C:\Windows\Fonts\StaticCache.dat
  Reads from:              C:\Windows\win.ini
```

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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  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
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  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\
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  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\software\wow6432node\microsoft\ole
  Opens key:                HKLM\software\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:                HKCU\software\borland\locales
  Opens key:                HKCU\software\borland\delphi\locales
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                HKCU\control panel\international
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:                HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\system
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\ms sans serif
  Opens key:                HKLM\software\wow6432node\devisenrechner
  Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\0be85123fcf951b2f52c115972e373cb.exe
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\
  Opens key:                HKLM\software\wow6432node\microsoft\ctf\knownclasses
  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[0be85123fcf951b2f52c115972e373cb.exe]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[0be85123fcf951b2f52c115972e373cb]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  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\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:              HKCU\control panel\international[itlzero]
  Queries value:              HKCU\control panel\international[s1159]
  Queries value:              HKCU\control panel\international[s2359]
  Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:              HKLM\software\microsoft\windows
```

```
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
  Queries value:            HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
```