Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 230, Task ID: 920

Task ID:	920
Risk Level:	1
Date Processed:	2016-04-28 13:12:34 (UTC)
Processing Time:	61.13 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
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Opens:	C:\Windows\Prefetch\0BE85123FCF951B2F52C115972E37-48B0CC40.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\0be85123fcf951b2f52c115972e373cb.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens:	C:\windows\temp\winspool.drv
Opens:	C:\Windows\System32\winspool.drv
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\windows\temp\0be85123fcf951b2f52c115972e373cb.ENU
Opens:	C:\windows\temp\0be85123fcf951b2f52c115972e373cb.ENU.DLL
Opens:	C:\windows\temp\0be85123fcf951b2f52c115972e373cb.EN
Opens:	C:\windows\temp\0be85123fcf951b2f52c115972e373cb.EN.DLL
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\System32\en-US\user32.dll.mui

```
  Opens:                      C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                      C:\Windows\Fonts\sserife.fon
  Opens:                      C:\Windows\system32\uxtheme.dll.Config
  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\WindowsShell.Manifest
  Opens:                      C:\windows\temp\RICHED32.DLL
  Opens:                      C:\Windows\System32\riched32.dll
  Opens:                      C:\windows\temp\RICHED20.dll
  Opens:                      C:\Windows\System32\riched20.dll
  Opens:                      C:\Windows\win.ini
  Opens:                      C:\Windows\System32\rpcss.dll
  Opens:                      C:\windows\temp\CRYPTBASE.dll
  Opens:                      C:\Windows\System32\cryptbase.dll
  Opens:                      C:\Windows\Fonts\arialbd.ttf
  Opens:                      C:\Windows\Fonts\arial.ttf
  Opens:                      C:\Windows\devisen.ini
  Opens:                      C:\Windows\Fonts\tahoma.ttf
  Opens:                      C:\Windows\Fonts\meiryo.ttc
  Opens:                      C:\Windows\Fonts\msgothic.ttc
  Opens:                      C:\Windows\Fonts\msjh.ttf
  Opens:                      C:\Windows\Fonts\msyh.ttf
  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\system\currentcontrolset\control\session manager
  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\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                  HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                  HKCU\
  Opens key:                  HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                  HKLM\software\policies\microsoft\mui\settings
  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\microsoft\windows\currentversion\sidebyside
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                  HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                  HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:                  HKLM\system\currentcontrolset\control\error message instrument
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:                  HKLM\
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                  HKLM\software\microsoft\ole
  Opens key:                  HKLM\software\microsoft\ole\tracing
  Opens key:                  HKLM\software\microsoft\oleaut
  Opens key:                  HKCU\software\borland\locales
  Opens key:                  HKCU\software\borland\delphi\locales
  Opens key:                  HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:               HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:               HKLM\software\microsoft\windows\windows error reporting\wmr
  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\fontlink\systemlink
  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\segoe ui
  Opens key:               HKLM\system\currentcontrolset\control\cmf\config
  Opens key:               HKCU\control panel\international
  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\languagepack\surrogatefallback\ms sans serif
  Opens key:               HKLM\software\devisenrechner
  Opens key:
HKLM\software\microsoft\ctf\compatibility\0be85123fcf951b2f52c115972e373cb.exe
  Opens key:               HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:               HKLM\software\microsoft\ctf\
  Opens key:               HKLM\software\microsoft\ctf\knownclasses
  Queries value:           HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  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:           HKCU\control panel\desktop[preferreduilanguages]
  Queries value:           HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\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\microsoft\windows
nt\currentversion\compatibility32[0be85123fcf951b2f52c115972e373cb]
  Queries value:           HKLM\software\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\control\nls\customlocale[en-us]
  Queries value:           HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:           HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  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:            HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:            HKCU\control panel\international[itlzero]
  Queries value:            HKCU\control panel\international[s1159]
  Queries value:            HKCU\control panel\international[s2359]
  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\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:            HKLM\software\microsoft\ctf[enableanchorcontext]
```