Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	719
Risk Level:	6
Date Processed:	2016-05-18 10:30:52 (UTC)
Processing Time:	61.33 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\70b2225f430facf31ca65621c234f09e.exe"
Sample ID:	3303
Type:	basic
Owner:	admin
Label:	70b2225f430facf31ca65621c234f09e
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	855552 bytes
MD5:	70b2225f430facf31ca65621c234f09e
SHA256:	375c6e3dfa967d9d6760d4e8ca0868c864fecde2735ce0d1f189b3b2aef512b7
Description:	None

Pattern Matching Results

5	PE: Contains compressed section
6	Tries to detect VM environment

Process/Thread Events

Creates process:	C:\windows\temp\70b2225f430facf31ca65621c234f09e.exe ["C:\windows\temp\70b2225f430facf31ca65621c234f09e.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\70B2225F430FACF31CA65621C234F-988C8555.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\70b2225f430facf31ca65621c234f09e.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\SysWOW64\ufat.dll
Opens:	C:\Windows\SysWOW64\mmcbase.dll
Opens:	C:\Windows\SysWOW64\RpcNs4.dll
Opens:	C:\Windows\SysWOW64\sqlunirl.dll
Opens:	C:\Windows\SysWOW64\ulib.dll
Opens:	C:\Windows\SysWOW64\ifsutil.dll
Opens:	C:\Windows\SysWOW64\mfc42u.dll
Opens:	C:\Windows\SysWOW64\winspool.drv
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\version.dll
Opens:	C:\Windows\SysWOW64\odbc32.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.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\ole32.dll

```
  Opens:                       C:\Windows\SysWOW64\oleaut32.dll
  Opens:                       C:\Windows\SysWOW64\advapi32.dll
  Opens:                       C:\Windows\SysWOW64\shlwapi.dll
  Opens:                       C:\Windows\SysWOW64\shell32.dll
  Opens:                       C:\Windows\SysWOW64\comdlg32.dll
  Opens:                       C:\Windows\SysWOW64\en-US\ulib.dll.mui
  Opens:                       C:\Windows\SysWOW64\imm32.dll
  Opens:                       C:\Windows\SysWOW64\msctf.dll
  Opens:                       C:\Windows\SysWOW64\en-US\MFC42u.dll.mui
  Opens:                       C:\Windows\SysWOW64\en-US\mmcbase.dll.mui
  Opens:                       C:\Windows\SysWOW64\nddeapi.dll
  Opens:                       C:\Windows\SysWOW64\cmdial32.dll
  Opens:                       C:\Windows\SysWOW64\cmpbk32.dll
  Opens:                       C:\Windows\SysWOW64\cmutil.dll
  Opens:                       C:\Windows\SysWOW64\eappcfg.dll
  Opens:                       C:\Windows\SysWOW64\userenv.dll
  Opens:                       C:\Windows\SysWOW64\profapi.dll
  Opens:                       C:\Windows\SysWOW64\cfgmgr32.dll
  Opens:                       C:\Windows\SysWOW64\devobj.dll
  Opens:                       C:\Windows\SysWOW64\setupapi.dll
  Opens:                       C:\Windows\SysWOW64\en-US\setupapi.dll.mui
  Opens:                       C:\Windows\SysWOW64\dnsapi.dll
  Opens:                       C:\Windows\SysWOW64\nsi.dll
  Opens:                       C:\Windows\SysWOW64\ws2_32.dll
  Opens:                       C:\Windows\SysWOW64\IPHLPAPI.DLL
  Opens:                       C:\Windows\SysWOW64\winnsi.dll
  Opens:                       C:\Windows\SysWOW64\mswsock.dll
  Opens:                       C:\Windows\SysWOW64\psapi.dll
  Opens:                       C:\Windows\SysWOW64\iertutil.dll
  Opens:                       C:\Windows\SysWOW64\wininet.dll
```

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\system\currentcontrolset\control\session manager
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  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\dllnxoptions
  Opens key:                   HKLM\system\currentcontrolset\control\nls\extendedlocale
  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\
  Opens key:                HKLM\hardware\description\system
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  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\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\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKLM\software\wow6432node\microsoft\bidinterface\loader
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\microsoft sql server\80\tools\client
  Opens key:                HKCU\software\microsoft\microsoft sql server\80\tools\sqlstr
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion
  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[70b2225f430facf31ca65621c234f09e.exe]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:            HKLM\hardware\description\system[identifier]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[6b1db052-734f-4e23-
af5e-6cd8ae459f98]
  Queries value:            HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[70b2225f430facf31ca65621c234f09e]
  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\software\wow6432node\microsoft\bidinterface\loader[:ldrmsg]
  Queries value:
HKLM\software\wow6432node\microsoft\bidinterface\loader[c:\windows\temp\70b2225f430facf31ca65621c234f09e.exe:2892]
  Queries value:
HKLM\software\wow6432node\microsoft\bidinterface\loader[c:\windows\temp\70b2225f430facf31ca65621c234f09e.exe]
```

```
   Queries value:
HKLM\software\wow6432node\microsoft\bidinterface\loader[c:\windows\temp\*]
   Queries value:              HKLM\software\wow6432node\microsoft\bidinterface\loader[:path]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[f34765f6-a1be-4b9d-
1400-b8a12921f704]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[9c88041d-349d-4647-
8bfd-2c0a167bfe58]
   Queries value:              HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[5f31090b-d990-4e91-
b16d-46121d0255aa]
```