Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	783
Risk Level:	1
Date Processed:	2016-05-18 10:38:05 (UTC)
Processing Time:	61.46 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe"

Sample ID:	3319
Type:	basic
Owner:	admin
Label:	f0d96afe8a3c58bf99f8b24ff10b1a07
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	93184 bytes
MD5:	f0d96afe8a3c58bf99f8b24ff10b1a07
SHA256:	d04b163e862ba9ead5cf9f379edf96bde8a146b4aea6987312b2a739c0b81701
Description:	None

Pattern Matching Results

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe ["C:\windows\temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?F0D96AFE8A3C58BF99F8B24FF10B1A07.EXE

File System Events

Opens:	C:\Windows\Prefetch\F0D96AFE8A3C58BF99F8B24FF10B1-664BA9E9.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\f0d96afe8a3c58bf99f8b24ff10b1a07.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\msvbvm60.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.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\ole32.dll
  Opens:                    C:\Windows\SysWOW64\oleaut32.dll
  Opens:                    C:\Windows\SysWOW64\imm32.dll
  Opens:                    C:\Windows\SysWOW64\msctf.dll
  Opens:                    C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                    C:\Windows\SysWOW64\uxtheme.dll
  Opens:                    C:\Windows\SysWOW64\sxs.dll
  Opens:                    C:\Windows\SysWOW64\clbcatq.dll
  Reads from:               C:\Windows\Temp\f0d96afe8a3c58bf99f8b24ff10b1a07.exe
```

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 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\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  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\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:                HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:                HKLM\software\wow6432node\microsoft\vba\monitors
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{1857ee93-c29a-4421-bf5e-
4aff9abf109c}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{1857ee93-c29a-4421-bf5e-4aff9abf109c}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{1857ee93-c29a-4421-bf5e-
4aff9abf109c}
  Opens key:                HKCR\wow6432node\clsid\{1857ee93-c29a-4421-bf5e-4aff9abf109c}
  Opens key:                HKCU\software\classes\clsid\{1857ee93-c29a-4421-bf5e-4aff9abf109c}
  Opens key:                HKCR\clsid\{1857ee93-c29a-4421-bf5e-4aff9abf109c}
  Opens key:                HKCU\software\classes\activatableclasses\clsid
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{1857ee93-c29a-4421-bf5e-
4aff9abf109c}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{2433df16-b661-424b-8b68-
94b7c9a8936e}
  Opens key:                HKCR\activatableclasses\clsid\{2433df16-b661-424b-8b68-94b7c9a8936e}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{2433df16-b661-424b-8b68-
94b7c9a8936e}
  Opens key:                HKCR\wow6432node\clsid\{2433df16-b661-424b-8b68-94b7c9a8936e}
  Opens key:                HKCU\software\classes\clsid\{2433df16-b661-424b-8b68-94b7c9a8936e}
  Opens key:                HKCR\clsid\{2433df16-b661-424b-8b68-94b7c9a8936e}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{2433df16-b661-424b-8b68-
94b7c9a8936e}
  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[msvbvm60.dll]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[f0d96afe8a3c58bf99f8b24ff10b1a07.exe]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[f0d96afe8a3c58bf99f8b24ff10b1a07]
  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\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\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[932]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[950]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKLM\software\microsoft\ole[maxsxshashcount]
```