Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	866
Risk Level:	4
Date Processed:	2016-04-28 13:11:33 (UTC)
Processing Time:	61.61 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\af7d9dfcdc5262aea00f7c8ed6e0adff.exe"
Sample ID:	217
Type:	basic
Owner:	admin
Label:	af7d9dfcdc5262aea00f7c8ed6e0adff
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	961320 bytes
MD5:	af7d9dfcdc5262aea00f7c8ed6e0adff
SHA256:	611a9496aef3dd7edfcf734651f2cc8c77d01b6f0f584f63d60d7b5191df0ecc
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\af7d9dfcdc5262aea00f7c8ed6e0adff.exe
["C:\windows\temp\af7d9dfcdc5262aea00f7c8ed6e0adff.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\AF7D9DFCDC5262AEA00F7C8ED6E0A-BF95386E.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\af7d9dfcdc5262aea00f7c8ed6e0adff.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\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_ba245425e0986353
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_ba245425e0986353\GdiPlus.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\pdh.dll
Opens:	C:\Windows\SysWOW64\wtsapi32.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\SHCore.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\user32.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\iertutil.dll
Opens:	C:\Windows\SysWOW64\wininet.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll

```
Opens:                  C:\Windows\SysWOW64\shell32.dll
Opens:                  C:\Windows\SysWOW64\comdlg32.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\Fonts\StaticCache.dat
Opens:                  C:\Windows\SysWOW64\uxtheme.dll
Opens:                  C:\Windows\SysWOW64\dwmapi.dll
Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
Reads from:             C:\Windows\Fonts\StaticCache.dat
```

Windows Registry Events

```
Opens key:              HKLM\software\microsoft\wow64
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\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\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\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:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\pdh
Opens key:              HKLM\system\currentcontrolset\control\computername
Opens key:              HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key:              HKLM\system\setup
Opens key:              HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
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\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\software\policies\microsoft\sqmclient\windows
    Opens key:                HKLM\software\microsoft\sqmclient\windows
    Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
    Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\af7d9dfcdc5262aea00f7c8ed6e0adff.exe
    Opens key:                HKLM\software\wow6432node\microsoft\ctf\
    Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
    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[af7d9dfcdc5262aea00f7c8ed6e0adff.exe]
    Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
    Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
    Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
    Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[af7d9dfcdc5262aea00f7c8ed6e0adff]
    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\software\microsoft\ole[aggressivemtatesting]
    Queries value:            HKLM\system\currentcontrolset\control\wmi\security[62841f33-387a-4674-
94a4-485c418c57ee]
    Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
    Queries value:            HKLM\system\setup[oobeinprogress]
    Queries value:            HKLM\system\setup[systemsetupinprogress]
    Queries value:            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
    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\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\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:            HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
   Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
```