Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	867
Risk Level:	4
Date Processed:	2016-04-28 13:11:38 (UTC)
Processing Time:	61.08 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:	\BaseNamedObjects__PDH_PLA_MUTEX__
Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.AEH
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.EPF
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.EPF.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.EPF.IC
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens:	C:\WINDOWS\Prefetch\AF7D9DFCDC5262AEA00F7C8ED6E0A-395B422F.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\GdiPlus.dll
Opens:	C:\WINDOWS\system32\pdh.dll
Opens:	C:\WINDOWS\system32\crypt32.dll

```
  Opens:                  C:\WINDOWS\system32\msasn1.dll
  Opens:                  C:\WINDOWS\system32\odbc32.dll
  Opens:                  C:\WINDOWS\system32\odbcbcp.dll
  Opens:                  C:\WINDOWS\system32\wtsapi32.dll
  Opens:                  C:\WINDOWS\system32\winsta.dll
  Opens:                  C:\WINDOWS\system32\netapi32.dll
  Opens:                  C:\WINDOWS\system32\imm32.dll
  Opens:                  C:\WINDOWS\system32\comctl32.dll
  Opens:                  C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\COMCTL32.dll.124.Config
  Opens:                  C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:                  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
  Opens:                  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
  Opens:                  C:\WINDOWS\WindowsShell.Manifest
  Opens:                  C:\WINDOWS\WindowsShell.Config
  Opens:                  C:\WINDOWS\system32\WININET.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\WININET.dll.123.Config
  Opens:                  C:\WINDOWS\system32\shell32.dll
  Opens:                  C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:                  C:\WINDOWS\system32\odbcint.dll
  Opens:                  C:\WINDOWS\system32\MSCTF.dll
  Opens:                  C:\WINDOWS\system32\MSCTFIME.IME
```

Windows Registry Events

```
  Creates key:            HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\af7d9dfcdc5262aea00f7c8ed6e0adff.exe
  Opens key:              HKLM\system\currentcontrolset\control\terminal server
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:              HKLM\
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
```

```
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdiplus.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\odbc32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\odbcbcp.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\pdh.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winsta.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
  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\software\microsoft\windows nt\currentversion\windows
  Opens key:                 HKCU\
  Opens key:                 HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                 HKCU\control panel\desktop
  Opens key:                 HKLM\software\microsoft\ole
  Opens key:                 HKCR\interface
  Opens key:                 HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                 HKLM\software\microsoft\oleaut
  Opens key:                 HKLM\software\microsoft\oleaut\userera
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:                 HKCU\software\classes\
  Opens key:                 HKCU\software\classes\protocols\name-space handler\
  Opens key:                 HKCR\protocols\name-space handler
  Opens key:                 HKCU\software\classes\protocols\name-space handler
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                 HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\system\currentcontrolset\control\wmi\security
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\system\currentcontrolset\services\crypt32\performance
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:                HKLM\software\microsoft\bidinterface\loader
  Opens key:                HKLM\software\microsoft\mdac
  Opens key:                HKLM\software
  Opens key:                HKCU\software\odbc\odbc.ini\odbc
  Opens key:                HKLM\software\odbc\odbc.ini\odbc
  Opens key:                HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\af7d9dfcdc5262aea00f7c8ed6e0adff.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\pdh
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\odbcint.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\af7d9dfcdc5262aea00f7c8ed6e0adff.exe
  Opens key:                HKLM\software\microsoft\ctf\systemshared\
  Opens key:                HKCU\keyboard layout\toggle
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\imm
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
  Opens key:                HKCU\software\microsoft\ctf
  Opens key:                HKLM\software\microsoft\ctf\systemshared
  Opens key:                HKCU\software\microsoft\ctf\langbaraddin\
  Opens key:                HKLM\software\microsoft\ctf\langbaraddin\
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  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[af7d9dfcdc5262aea00f7c8ed6e0adff]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[af7d9dfcdc5262aea00f7c8ed6e0adff]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:            HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:            HKCR\interface[interfacehelperdisableall]
  Queries value:            HKCR\interface[interfacehelperdisableallforole32]
  Queries value:            HKCR\interface[interfacehelperdisabletypelib]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[af7d9dfcdc5262aea00f7c8ed6e0adff.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:            HKCU\keyboard layout\toggle[language hotkey]
  Queries value:            HKCU\keyboard layout\toggle[hotkey]
  Queries value:            HKCU\keyboard layout\toggle[layout hotkey]
  Queries value:            HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:            HKCU\software\microsoft\ctf[disable thread input manager]
  Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
```