Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	731
Risk Level:	5
Date Processed:	2016-04-28 13:07:37 (UTC)
Processing Time:	2.35 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\25b0c8aee8cec0c7e2506918fd5835fa.exe"
Sample ID:	183
Type:	basic
Owner:	admin
Label:	25b0c8aee8cec0c7e2506918fd5835fa
Date Added:	2016-04-28 12:45:09 (UTC)
File Type:	PE32:win32:gui
File Size:	996352 bytes
MD5:	25b0c8aee8cec0c7e2506918fd5835fa
SHA256:	07da4de6b46856159b4810b075e010e3fbb30de3f31e8d2e71f512e6dc439c41
Description:	None

Pattern Matching Results

5 Possible injector

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\25b0c8aee8cec0c7e2506918fd5835fa.exe

["c:\windows\temp\25b0c8aee8cec0c7e2506918fd5835fa.exe"]

Terminates process:	C:\WINDOWS\Temp\25b0c8aee8cec0c7e2506918fd5835fa.exe

Named Object Events

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 semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens:	C:\WINDOWS\Prefetch\25B0C8AEE8CEC0C7E2506918FD583-266FDCFE.pf
Opens:	C:\Documents and Settings\Admin
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\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\dnsapi.dll
Opens:	C:\WINDOWS\system32\psapi.dll
Opens:	C:\WINDOWS\system32\msvcp100.dll
Opens:	C:\WINDOWS\system32\msvcr100.dll

```
Opens:                    C:\WINDOWS\system32\imm32.dll
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\WindowsShell.Manifest
Opens:                    C:\WINDOWS\WindowsShell.Config
Opens:                    C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens:                    C:\WINDOWS\system32\urlmon.dll.123.Config
Opens:                    C:\WINDOWS\system32\WININET.dll.123.Manifest
Opens:                    C:\WINDOWS\system32\WININET.dll.123.Config
Opens:                    C:\WINDOWS\system32\rpcss.dll
Opens:                    C:\WINDOWS\system32\MSCTF.dll
```

Windows Registry Events

```
Creates key:              HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key:              HKCU\software\microsoft\windows\currentversion\internet settings
Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\25b0c8aee8cec0c7e2506918fd5835fa.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\gdi32.dll
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\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\image file execution
options\msvcrt.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\shell32.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\oleaut32.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\comdlg32.dll
Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.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\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\psapi.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcr100.dll
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp100.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:              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\currentversion\explorer\performance
Opens key:              HKLM\system\setup
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\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:              HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key:              HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters
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\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
   Opens key:
HKLM\software\microsoft\ctf\compatibility\25b0c8aee8cec0c7e2506918fd5835fa.exe
   Opens key:                  HKLM\software\microsoft\ctf\systemshared\
   Opens key:                  HKCU\keyboard layout\toggle
   Opens key:                  HKLM\software\microsoft\ctf\
   Queries value:              HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   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[25b0c8aee8cec0c7e2506918fd5835fa]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[25b0c8aee8cec0c7e2506918fd5835fa]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
   Queries value:              HKLM\system\setup[systemsetupinprogress]
   Queries value:              HKCU\control panel\desktop[multiuilanguageid]
   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\control panel\desktop[smoothscroll]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
```

```
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
    Queries value:               HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
    Queries value:               HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
    Queries value:               HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
    Queries value:               HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
    Queries value:               HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
```

Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
    Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
    Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[25b0c8aee8cec0c7e2506918fd5835fa.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\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]
    Value changes: HKLM\software\microsoft\cryptography\rng[seed]