Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	999
Risk Level:	5
Date Processed:	2016-04-28 13:14:59 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\b94325f7c03f5189ecd0d30601f8568b.exe"

Sample ID:	250
Type:	basic
Owner:	admin
Label:	b94325f7c03f5189ecd0d30601f8568b
Date Added:	2016-04-28 12:45:16 (UTC)
File Type:	PE32:win32:gui
File Size:	169984 bytes
MD5:	b94325f7c03f5189ecd0d30601f8568b
SHA256:	1cf9c6f95c2a3cf2ede85a1a0f34892a6ceb1ae7f27cb81800da2631f6ed98ba
Description:	None

Pattern Matching Results

`5` Possible injector

Process/Thread Events

Creates process: C:\WINDOWS\Temp\b94325f7c03f5189ecd0d30601f8568b.exe
["c:\windows\temp\b94325f7c03f5189ecd0d30601f8568b.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 mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.MK
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.MED
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.MED.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.MED.IC
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens:	C:\WINDOWS\Prefetch\B94325F7C03F5189ECD0D30601F85-26D39D2B.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\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\temp\b94325f7c03f5189ecd0d30601f8568b.ini
Opens:                    C:\Documents and Settings\Admin\Application Data
Opens:                    C:\WINDOWS\system32\MSCTF.dll
Opens:                    C:\WINDOWS\system32\MSCTFIME.IME
Opens:                    C:\WINDOWS\system32\uxtheme.dll
```

Windows Registry Events

```
Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\b94325f7c03f5189ecd0d30601f8568b.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\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\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
Opens key:
HKLM\software\microsoft\ctf\compatibility\b94325f7c03f5189ecd0d30601f8568b.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:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
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:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
Opens key:              HKCU\software\microsoft\windows\currentversion\thememanager
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\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[b94325f7c03f5189ecd0d30601f8568b]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[b94325f7c03f5189ecd0d30601f8568b]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
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\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]
Queries value:          HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value:          HKCU\control panel\desktop[lamebuttontext]
Value changes:          HKLM\software\microsoft\cryptography\rng[seed]
```