Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	391
Risk Level:	4
Date Processed:	2016-04-28 12:57:44 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\a8e55ca7e9168cd0df56a0907a3f0832.exe"

Sample ID:	98
Type:	basic
Owner:	admin
Label:	a8e55ca7e9168cd0df56a0907a3f0832
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	351232 bytes
MD5:	a8e55ca7e9168cd0df56a0907a3f0832
SHA256:	64673dbcdc33f12f759be72ac47fc39a16ffe29d75c078054f37e4e85b23f82b
Description:	None

Pattern Matching Results

3 Long sleep detected
4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\a8e55ca7e9168cd0df56a0907a3f0832.exe ["c:\windows\temp\a8e55ca7e9168cd0df56a0907a3f0832.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

File System Events

Opens:	C:\WINDOWS\Prefetch\A8E55CA7E9168CD0DF56A0907A3F0-398F995D.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_353599c2
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.ATL_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_353599c2\atl90.dll
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e\msvcp90.dll
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e\msvcr90.dll

```
  Opens:                     C:\WINDOWS\system32\imm32.dll
  Opens:                     C:\
  Opens:                     C:\WINDOWS
  Opens:                     C:\WINDOWS\system32\rpcss.dll
  Opens:                     C:\WINDOWS\system32\MSCTF.dll
  Opens:                     C:\WINDOWS\system32\clbcatq.dll
  Opens:                     C:\WINDOWS\system32\comres.dll
  Opens:                     C:\WINDOWS\Registration\R000000000007.clb
  Opens:                     C:\WINDOWS\system32\winlogon.exe
  Opens:                     C:\WINDOWS\system32\xpsp2res.dll
  Reads from:                C:\WINDOWS\Registration\R000000000007.clb
```

Windows Registry Events

```
  Creates key:               HKCU\software\samsung\kies2.0
  Creates key:               HKCU\software
  Creates key:               HKCU\software\samsung
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\a8e55ca7e9168cd0df56a0907a3f0832.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\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\atl90.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcr90.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp90.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\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\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\a8e55ca7e9168cd0df56a0907a3f0832.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\com3
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.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\clbcatq.dll
  Opens key:                HKLM\software\microsoft\com3\debug
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\classes
  Opens key:                HKU\
  Opens key:                HKCR\clsid
  Opens key:                HKCU\software\classes\clsid\{e0241b79-ab3a-49d8-9691-2cf3d6d863b0}
  Opens key:                HKCR\clsid\{e0241b79-ab3a-49d8-9691-2cf3d6d863b0}
  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\a8e55ca7e9168cd0df56a0907a3f0832.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKCU\software\classes\appid\a8e55ca7e9168cd0df56a0907a3f0832.exe
  Opens key:                HKCR\appid\a8e55ca7e9168cd0df56a0907a3f0832.exe
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  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[a8e55ca7e9168cd0df56a0907a3f0832]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[a8e55ca7e9168cd0df56a0907a3f0832]
  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\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[multiuilanguageid]
  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:            HKCU\software\samsung\kies2.0[loglevel]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
  Queries value:            HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
  Queries value:            HKLM\software\microsoft\com3[regdbversion]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:            HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:            HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
```