Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	963
Risk Level:	5
Date Processed:	2016-04-28 13:14:13 (UTC)
Processing Time:	2.62 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d02d9ed231437b31fcbb8b3f581987f5.exe"
Sample ID:	241
Type:	basic
Owner:	admin
Label:	d02d9ed231437b31fcbb8b3f581987f5
Date Added:	2016-04-28 12:45:15 (UTC)
File Type:	PE32:win32:gui
File Size:	196608 bytes
MD5:	d02d9ed231437b31fcbb8b3f581987f5
SHA256:	d829e38792f116d0636bb565cb0daaf0f3a0722f4ebb7859694ca76dc89af2da
Description:	None

Pattern Matching Results

`5` Possible injector

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\d02d9ed231437b31fcbb8b3f581987f5.exe

["c:\windows\temp\d02d9ed231437b31fcbb8b3f581987f5.exe"]

Terminates process:	C:\WINDOWS\Temp\d02d9ed231437b31fcbb8b3f581987f5.exe

Named Object Events

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

File System Events

Opens:	C:\WINDOWS\Prefetch\D02D9ED231437B31FCBB8B3F58198-3AE267D7.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\winmm.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\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

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\d02d9ed231437b31fcbb8b3f581987f5.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
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\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\version.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.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\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\languagepack
  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:              HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:              HKLM\software\compsoft\doro
```

```
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[d02d9ed231437b31fcbb8b3f581987f5]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[d02d9ed231437b31fcbb8b3f581987f5]
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:                HKCU\control panel\desktop[smoothscroll]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
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:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
Queries value:                HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
```

```
Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
Value changes:          HKLM\software\microsoft\cryptography\rng[seed]
```