Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 74, Task ID: 295

Task ID:	295
Risk Level:	8
Date Processed:	2016-04-28 12:55:34 (UTC)
Processing Time:	2.13 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\cacecdcda69b31a2d68545070b25b9e7.exe"

Sample ID:	74
Type:	basic
Owner:	admin
Label:	cacecdcda69b31a2d68545070b25b9e7
Date Added:	2016-04-28 12:44:57 (UTC)
File Type:	PE32:win32:gui
File Size:	77576 bytes
MD5:	cacecdcda69b31a2d68545070b25b9e7
SHA256:	13ecc4af80d99d9dda112956559e3bd867b6784b6693cfbe1989bdca578c15c8
Description:	None

Pattern Matching Results

8 Contains suspicious Microsoft certificate

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\cacecdcda69b31a2d68545070b25b9e7.exe ["c:\windows\temp\cacecdcda69b31a2d68545070b25b9e7.exe"]
Terminates process:	C:\WINDOWS\Temp\cacecdcda69b31a2d68545070b25b9e7.exe

File System Events

Opens:	C:\WINDOWS\Prefetch\CACECDCDA69B31A2D68545070B25B-161B2F82.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\iphlpapi.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\imm32.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\cacecdcda69b31a2d68545070b25b9e7.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\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\msvcrt.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\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\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\iphlpapi.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\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\system\currentcontrolset\services\tcpip\linkage
  Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters\
  Opens key:              HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
  Opens key:              HKLM\system\currentcontrolset\services\netbt\parameters
  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\classes\
  Opens key:              HKCU\software\classes\appid
  Opens key:              HKCR\appid
  Opens key:              HKCU\software\classes\appid\{a1b52c72-20e1-495a-8b62-8759bc6b85bb}
  Opens key:              HKCR\appid\{a1b52c72-20e1-495a-8b62-8759bc6b85bb}
  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\terminal server[tsuserenabled]
  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[cacecdcda69b31a2d68545070b25b9e7]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[cacecdcda69b31a2d68545070b25b9e7]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  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]
Value changes:        HKLM\software\microsoft\cryptography\rng[seed]
```