Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 87, Task ID: 347

Task ID:	347
Risk Level:	4
Date Processed:	2016-04-28 12:56:35 (UTC)
Processing Time:	2.42 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9051f3a2023c56661804fd664e27c74c.exe"

Sample ID:	87
Type:	basic
Owner:	admin
Label:	9051f3a2023c56661804fd664e27c74c
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	312320 bytes
MD5:	9051f3a2023c56661804fd664e27c74c
SHA256:	8ac177e931c1a04d468ba07162f5acdf48cbb1e1351afbbbf6ca99dac795e079
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\9051f3a2023c56661804fd664e27c74c.exe ["c:\windows\temp\9051f3a2023c56661804fd664e27c74c.exe"]
Terminates process:	C:\WINDOWS\Temp\9051f3a2023c56661804fd664e27c74c.exe

Named Object Events

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

File System Events

Opens:	C:\WINDOWS\Prefetch\9051F3A2023C56661804FD664E27C-358FB6D1.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\msvcp100.dll
Opens:	C:\WINDOWS\system32\msvcr100.dll
Opens:	C:\WINDOWS\system32\winhttp.dll
Opens:	C:\WINDOWS\system32\imm32.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\9051f3a2023c56661804fd664e27c74c.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\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.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\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winhttp.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:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\appid
  Opens key:                HKCR\appid
  Opens key:                HKCU\software\classes\appid\{068808b5-8e5c-463b-97ec-548be3668d1d}
  Opens key:                HKCR\appid\{068808b5-8e5c-463b-97ec-548be3668d1d}
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
```

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  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[9051f3a2023c56661804fd664e27c74c]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[9051f3a2023c56661804fd664e27c74c]
  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]
```