Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 8, Task ID: 30

Task ID:	30
Risk Level:	1
Date Processed:	2016-04-28 12:46:47 (UTC)
Processing Time:	4.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\839732664a17eb4effe85e010e105500.exe"

Sample ID:	8
Type:	basic
Owner:	admin
Label:	839732664a17eb4effe85e010e105500
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	46424 bytes
MD5:	839732664a17eb4effe85e010e105500
SHA256:	5171fb029a69b2e42a3720b1587aa210cbd72628c0894a6e1dd3662acaa060f2
Description:	None

Pattern Matching Results

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\839732664a17eb4effe85e010e105500.exe ["c:\windows\temp\839732664a17eb4effe85e010e105500.exe"]
Terminates process:	C:\WINDOWS\Temp\839732664a17eb4effe85e010e105500.exe

File System Events

Opens:	C:\WINDOWS\Prefetch\839732664A17EB4EFFE85E010E105-3AC02DC5.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\imm32.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\839732664a17eb4effe85e010e105500.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
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\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\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\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:              HKCU\software\borland\locales
  Opens key:              HKLM\software\borland\locales
  Opens key:              HKCU\software\borland\delphi\locales
  Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[839732664a17eb4effe85e010e105500]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[839732664a17eb4effe85e010e105500]
  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\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]
  Value changes:          HKLM\software\microsoft\cryptography\rng[seed]
```