**Lab 8: Malware Behavior (Lab 11-1)**

What you need:

* The Windows 2008 Server virtual machine we have been using.
* The textbook: "Practical Malware Analysis"

**Purpose**

You will practice the techniques in chapter 11.

**Downloading the Lab Files**

In a Web browser, go here:

<http://practicalmalwareanalysis.com/labs/>

Download and unzip the lab files.

Follow the instructions for **Lab 11-1** in the textbook. There are more detailed solutions in the back of the book. The only purpose of this document is to explain what images to turn in.

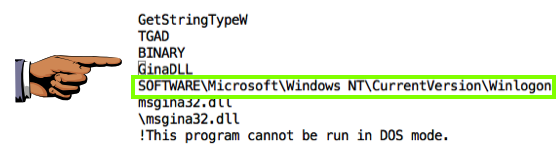
**Static Analysis with Strings**

Examine the strings in Lab11-01.exe.

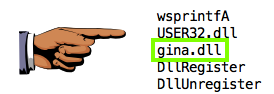
One handy tool to do that is [**BinText**](https://www.mcafee.com/hk/downloads/free-tools/bintext.aspx).

You should find the two items below.

Save an image showing the string **SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** as shown below, with the filename "**Proj 14a from YOUR NAME**".



Save an image showing the string **gina.DLL**, as shown below, with the filename "**Proj 14b from YOUR NAME**".



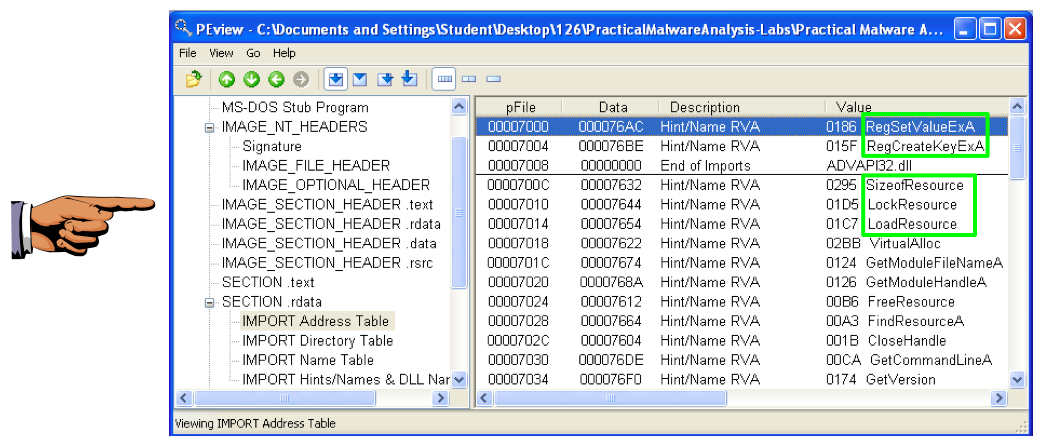
These strings suggest that this is GINA interception malware.

**Static Analysis with PEview**

Examine the Lab11-01.exe file in PEview. Find the items below.

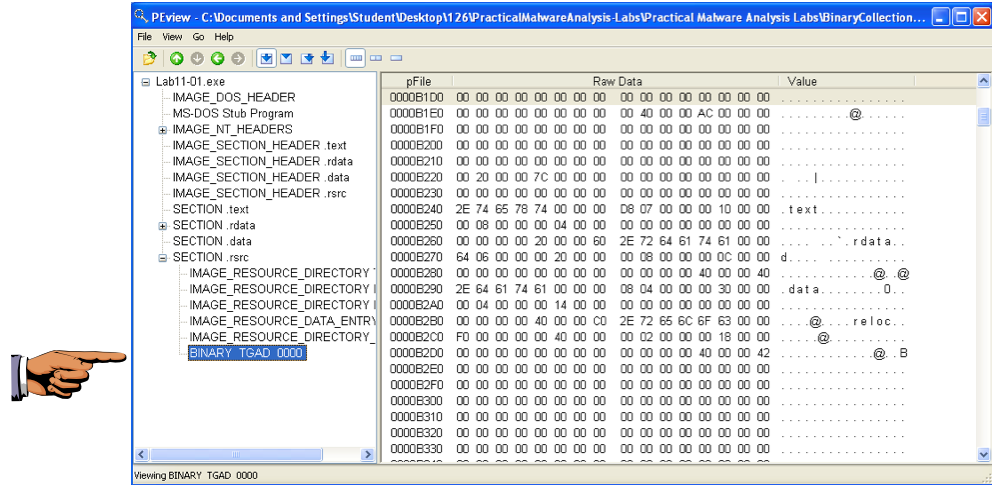
Save an image showing these imports, as highlighted below:, with the filename "**Proj 14c from YOUR NAME**".

* **RegSetValueExA**
* **RegCreateKeyExA**
* **SizeofResource**
* **LockResource**
* **LoadResource**



These API calls suggest that the malware is manipulating the registry and extracting a resource section.

Save an image showing the **BINARY TGAD 0000** section, as shown below, with the filename "**Proj 14d from YOUR NAME**".



This is a PE file, concealed within a resource section.

**Dynamic Analysis with Procmon**

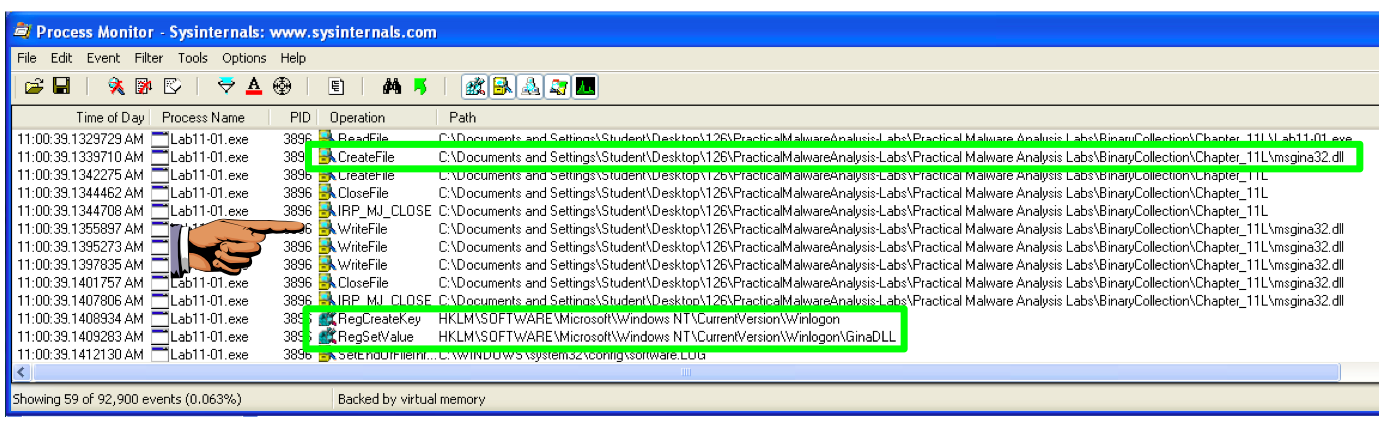
Run the malware in a virtual machine, while running Procmon to see what it does.

In Procmon, click **Filter**, "**Reset Filter**".

Click **Filter**, **Filter**. Filter for a "**Process Name**" of **Lab11-01.exe**.

Save an image showing these events, as shown below, with the filename "**Proj 14e from YOUR NAME**".

* **CreateFile ... msgina32.dll** or **IRP\_MU\_CREATE ... msgina.dll**
* **RegCreateKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon**
* **RegSetValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL**



These actions create a file named **msgina.dll** and insert a path to that file into registry keys that will launch the DLL when the system boots up.

**Resource Hacker**

Next we'll use Resource Hacker to extract the gina.dll file.

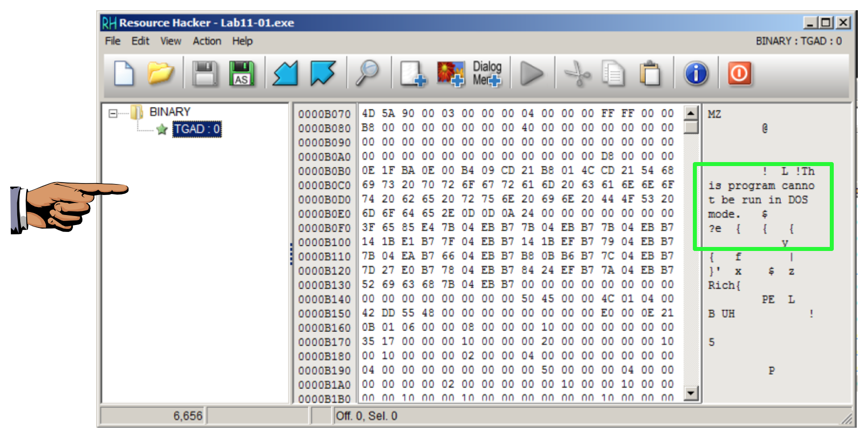
Download Resource Hacker here:

<http://www.angusj.com/resourcehacker/>

Open **Lab11-01.exe** in Resource Hacker.

The "**BINARY TGAD 0**" starts with **MZ** and contains the telltale text "This program cannot be run in DOS mode", as shown below--this is an EXE file.

Save an image showing the "**BINARY TGAD 0**" section, as shown below, with the filename "**Proj 14f from YOUR NAME**".



In Resource Hacker, in the left pane, click **0** to highlight it, as shown above.

Click **Action**, **Save Resource as a binary file...**".

Save the file as **YOURNAME-TGAD0.exe**, replacing the text "YOURNAME" with your own name.

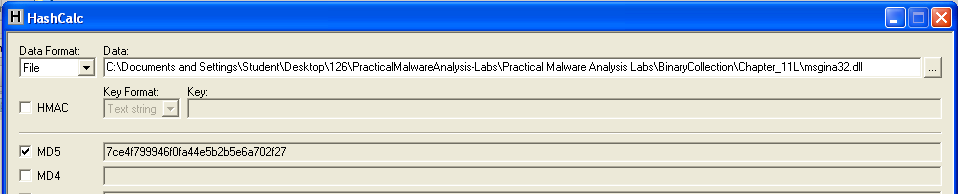
**HashCalc**

If you don't have it, get HashCalc here:

<http://www.slavasoft.com/hashcalc/>

Calculate the MD5 hash of the msgina32.dll file created by running the malware.

The MD5 hash begins with **7ce4**, as shown below.



Calculate the MD5 hash of the **YOURNAME-TGAD0.exe** file, as shown below.

Save an image showing these elements:

* A filename containing **YOURNAME** (you will have to make the window very wide to show it if your malware samples are on your desktop like mine)
* An MD5 hash beginning with **7ce4**

Save the image with the filename "**Proj 14g from YOUR NAME**".

