

Re: SECTION I - MALWARE ANALYSIS - PART 2 – ISC

October 14, 2005

=====

Hello Pedro!

First of all, these malware quizzes are simply cool - helps to pass the time when the Internet out there is real quiet... =)

Malware-quiz.exe

=====

1) Is this file Packed? If so, which packer was used?

Yes... well the file malware.exe, 30,720 bytes, is "packed" using WinRAR. It is an SFX Rar Archive, or Self-Extracting Rar Archive.

=====

2) Which command did you use to identify it?

I first did an initial physical inspection of the file, malware-quiz.exe, and bingo - some telltale clues abound! =)

<snip>

```
"name="Roshal.WinRAR.WinRAR" type="win32" /> <description>WinRAR archiver.</description> <dependency> <dependentAssembly>"
```

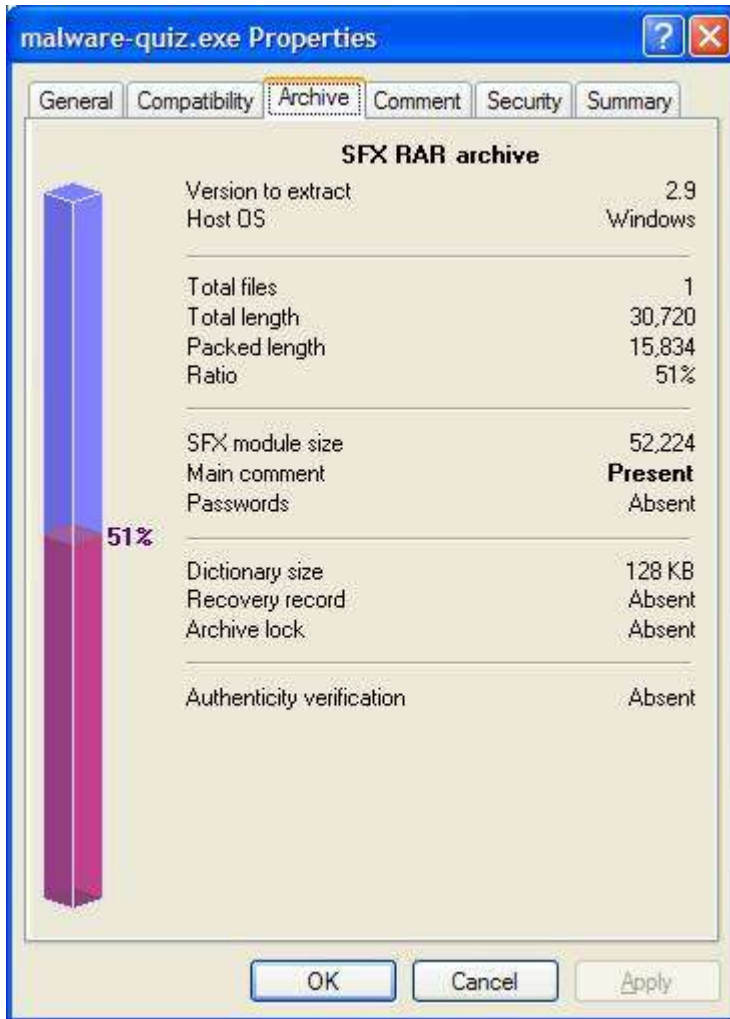
<snip>

*** The UPX0 and UPX1 section names found at the start of the file do 'sometimes' fool some AVs!

=====

3) Do you believe that is there any other way to identify the packer?

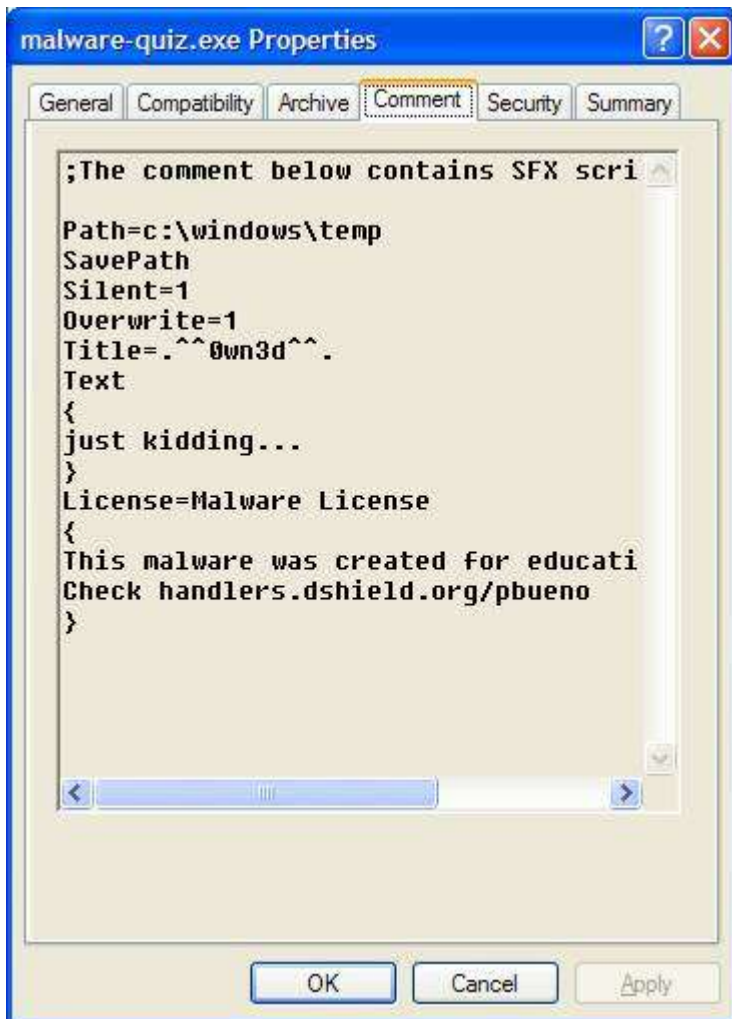
Yes... Another way of identifying it is by right-clicking on the file and click on Properties. And then whoa - there is an Archive tab!



As we can see here in the snapshot:

- a) There is one file inside the archive.
- b) The file inside the archive has a size of 30,720 bytes. (This is the same malware.exe stated above).
- c) There is a comment! Hmmm... More clues perhaps? ;-p
- d) And yes... the RAR archive has no password! =)

Shown below are the contents of the Comment section...



Bingo! And now we have an answer to number 4 below.

Simply right-clicking again on the file, malware-quiz.exe, and then choosing "Extract to malware-quiz\" will save the malware.exe file in the malware-quiz folder. (This is possible when WinRAR is installed, however). =)

*** But then again, double-clicking on the malware-quiz.exe will "silently" "install" or drop the malware.exe file in the c:\windows\temp folder!

=====

4) Please describe the directory which this file will be installed?

The file, malware.exe, will be saved in c:\windows\temp directory:

```
Path=c:\windows\temp
SavePath
```

If the directory doesn't exist, it will be created.

=====

5) In the process to unpack this file, please describe all the options that you saw. And by 'describe' I mean tell me what does it do when unpacking or not...

Options?

Based on the options "embedded" in this SFX Rar archive:

```
Path=c:\windows\temp --> directory where the file, malware.exe, is saved
SavePath --> Save and Restore paths (Path to extract)
Silent=1 --> Silent Mode (Hide All)
Overwrite=1 --> Overwrite Mode (Overwrite All Files)
Title=.^0wn3d^. --> Text Title of SFX Window
Text --> Text to display in SFX Window
{
just kidding...
}
License=Malware License --> Title of License Window
{
This malware was created for educational purpose only.
Check handlers.dshield.org/pbueno
}
--> License text
```

*** And I must say that MSN icon was real tricky – even a folder icon can be used and viola! ;-p

=====

6) What does this malware do?

malware-quiz.exe – drops or extracts the file malware.exe in the c:\windows\temp folder

malware.exe – opens up a command window, prints the line "Oh my...am I a really malware?????" for a couple of times and then closes the command window.

By the way, the "payload" text, "Oh my...am I a really malware?????", is printed 100 times!

=====

7) And finally, as a bonus question: What is the meaning of life?

And the answer is...

(This can be found in the dump of the malware.exe file!)

<snip>

"Oh my...am I a really malware????
Do you know what is the meaning of life? It is 42!"

<snip>

The answer is 42!

*** One interesting thing I found in this exercise is an 'advanced option' one can embed in the SFX – and that option is the "Files to Delete in the destination folder". It actually automatically deletes whatever file you indicate! Hmmm... And add to that a folder icon and using a silent mode – what do you get? Real Nasty stuff! Has this been actually looked into? Hmmm... I wonder... I have to do some more tests on this and update you...

=====

By the way, it's nice seeing you around MWP! Keep up the good work!

Cheers!

With Best Regards,

Ivan M. Macalintal
Global Anti-Virus Research Group
TrendLabs, Trend Micro Inc.
www.trendmicro.com