How to turn any .exe file into .jpg, .avi, .doc, or whatever extension you like and disguise your links!

Author: n00bz0r

Introduction

In this e-book we are going to use a spoofing vulnerability, known as RTLO [RIGHT TO LEFT OVERRIDE].

SPOOFING's Vulnerabilities are simple ways to deceive users or vulnerable software-computerized systems on real received or posted information. The spoofing regularly makes speak about multiple distinct scenarios like Address URL of Web Page, indicator TLS/SSL, IP address, and anymore possibility. This e-book will mainly analyze two methods where is exploit can be used: 1) To turn a .exe file into a .txt or .img, or whatever and 2) To spoof a url link to make it real like it is starting from a legit domain (ex. www.paypal.com/random_things_here).

RIGHT TO LEFT OVERRIDE is a Unicode character mainly used for the writing and the reading of the Arabic language or Hebrew text and which thus has the ability to reverse the reading order of the characters after it.

Getting Started

There are many ways to copy this Unicode character but this method will show you an easy one in particular.

Tools you will be needing:

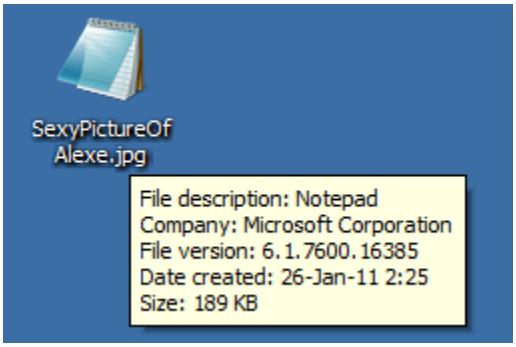
- Quick Unicode Input Tool
  - Download link:
    http://www.mediafire.com/?lz1xlo2l2hvqtdc
- File type icon pack
  - Download link:
    http://www.mediafire.com/?dtrv417qae7xrad
- ResHacker
  - Download link:
    http://delphi.icm.edu.pl/ftp/tools/ResHack.zip
- Tutorial on how to use Reshacker:
  - Link:
    http://www.hackforums.net/showthread.php?tid=243460

Method 1: File Extension Spoofing

In this method you are going to learn how to change the extension of each file to whatever you like and still retain the file's attributes. So if you have an executable file, you can disguise it to an image file and still be able to execute it.

Example:

I will be creating a file, which will be shown as "SexyPictureOfAlexe.jpg" to the user, but it will be an executable file instead (as shown in the picture below):



The actual name of this file is "SexyPictureOfAl[RTLO]gpj.exe"

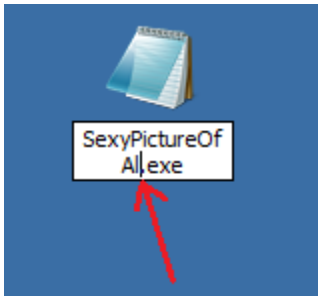
Of course, you can use reshacker to change the icon and make it a jpeg icon, but we'll get to that in a little bit.

So, how to do the above spoofing:

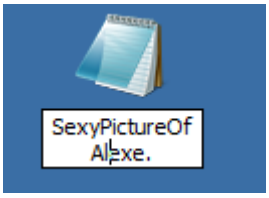
After you download the tools from the links provided above, open the Quick Unicode Input Tool, choose "Arial" and find the character U+202E: Right-To-Left Override, as shown in the picture below.

Don’t be surprised that it is invisible, just choose it, click “Select” and then “Copy”.

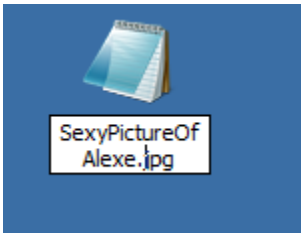
Now go find your file in the folder you have it. Choose to rename your file and then put the cursor right before the dot (.) and hit ctrl-V (paste) to put the character in there. You are going to notice that the dot has moved to the end of the filename. Now type your new extension, but backwards, so for “jpg”, type “gpj”, without moving the cursor out of its original place. You will end up with a file named “****exe.img” (or at least this is what the user sees). See the picture below if you don’t understand what I am talking about.



(put the cursor before the dot)



(paste the Unicode character)

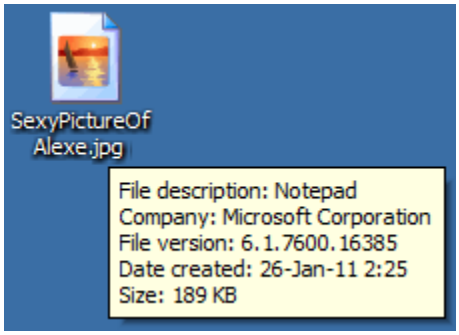


(type “gmi” from the point you were)

The correct place of the cursor is exactly where the arrow points. Then simply type the extension you like backwards without moving the cursor from its place. Don’t worry if you can’t make it work with the first try, just play around with it until you do.

Now we will use ResHacker in order to change our file's icon. You can also use it to change its assembly info. Just choose to replace the icon for now, and choose the jpeg icon.

Here is what you get:



The best thing to do in general is to follow these steps:

1) Bind your server to an image.
2) Change the icon of the exe in jpeg icon.
3) Spoof the extension into .img.
4) Spread.

Now you can upload this somewhere to get a direct link. The link will be like that:

Example: test.fileave.com/SexyPictureOfAlexe.img

So your victim will have no idea that this is an executable file, since it has img extension, a jpeg icon and also an image opens when he clicks it. ☺

You can use the same idea to spread as .avi, .ipa , .pdf, .jpg, .txt, .php, or whatever you can think of, via Warez and Torrents.

This was the end of method 1. Obviously you can use this to change your exe file into any file type you like. Use your imagination ☺

Method 2 : Url Spoofing

Okay, now that you have understood the extension spoofing, the url spoofing will be a piece of cake. I will not go into very much detail because the principle is exactly the same.

The basic steps are:

1) Go to your host and make adjustments so that you have the desired destination in a link alike to the example below (You can have your drive-by in there or whatever).
2) Use the Quick Unicode Input Tool to copy the RTLO character as described in method 1.
3) Share the link along with RTLO character in front of it. This will end up on people seeing the link inversed and thinking that your domain is "paypal.com" in that case.
4) Spread the link.

Example: [RTLO] http://www.maliciouswebsite.com/moc.lapyap.www://ptth
Would show up as: http://www.paypal.com/moc.etisbewsuoicilam.www//:ptth

This is the end of method 2.

Conclusion

This e-book showed you how spoofing works and two of its most important and valuable techniques. There are other fields where spoofing could be used also, but they will not be covered in this e-book.

Feel free to PM me and ask any questions that you may have.

Hope you've enjoyed this e-book
And Best of luck on your Spreading ☺