# How trojan pretends to be a PDF file using the RLO . method

You cannot guarantee that a file is really an image, video, PDF or text file just by looking at the file extension. On Windows, an attacker can execute a PDF file as if it were an EXE file.

This is quite dangerous, because a file that you download from the Internet and think it is a PDF file, can actually contain an extremely dangerous virus. Have you ever wondered how attackers can accomplish this?

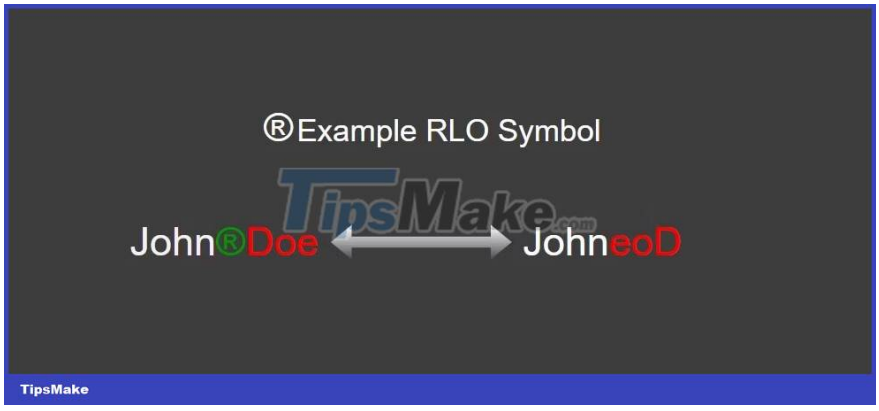
## What is the RLO method?

Many languages ??can be written from right to left, such as Arabic, Urdu and Persian. Many attackers use this language to launch various attacks. A text that makes sense and is safe to read from the left can actually carry different content when read from the right and refer to a completely different file. You can use the RLO method that exists in the Windows operating system to handle languages ??written from right to left.

There is an RLO notation for this in Windows. As soon as you use this character, the computer will start reading the text from right to left. Attackers take advantage of this to hide the executable file name and extension.

For example, you enter an English word from left to right and the word is *Software*. If you add the Windows RLO symbol after the letter T, anything you type after that will be read from right to left. As a result, your new word will be *Softeraw*.

For a better understanding, see the diagram below.




## Can a Trojan be placed in a PDF file?

In some attacks, hackers can put malicious exploits or scripts inside PDF files. Many different tools and programs can do this. This can even be done by changing the existing code of the PDF without using any other program.

However, the RLO method is different. With the RLO method, the attackers present an existing EXE file as if it were a PDF file to deceive the target victim. Only the appearance of the EXE changes, so the target user opens the file believing it to be a harmless PDF file.

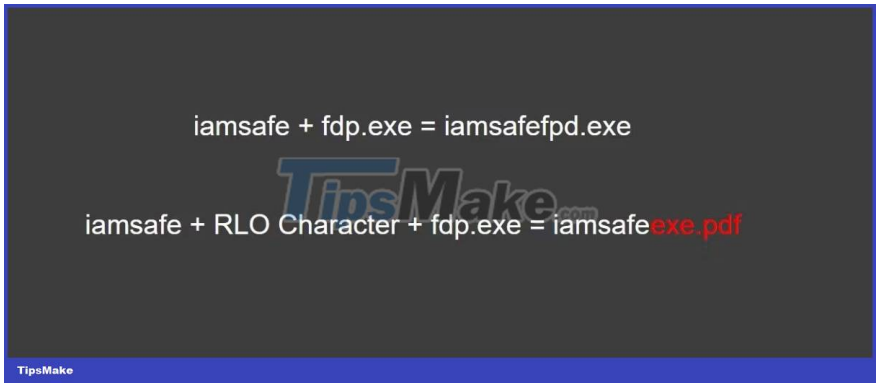
## How to use the RLO . method

Before explaining how to display the EXE as a PDF using the RLO method, review the image below. Which of these files is a PDF?


You cannot determine this at a glance. Instead, you need to see the contents of the file. (In case you're curious, the file on the left is the actual PDF file).

This trick is quite easy to do. First, the attackers write malicious code and compile it. The compiled code gives output in exe format. Attackers change the name and icon of this EXE file, changing its appearance to a PDF. So how does the renaming process happen?

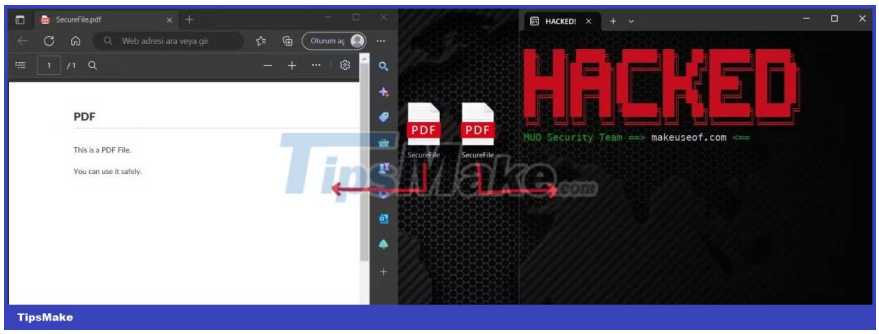
This is where RLO comes into play. For example, suppose you have an EXE file named *iamsafefdp.exe.* At this stage, the attacker will put an RLO symbol between iamsafe and fdp.exe to rename the file. It's pretty easy to do this in Windows. Just right click while renaming.



The principle is simple, after Windows sees the RLO symbol, it will read from right to left. File is still EXE, nothing has changed. It just looks like a PDF in appearance only.

After this stage, the attacker will replace the icon of the EXE file with the icon of the PDF file and send the file to the target.

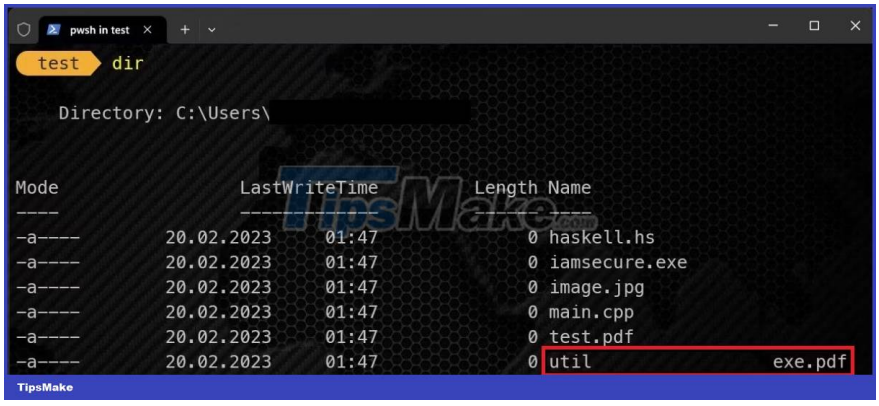
The image below is the answer to the previous question. The EXE you see on the right was created using the RLO method. In appearance, both files are similar, but their contents are completely different.




## How to counter this type of attack?

As with many security incidents, there are some precautions you can take to prevent this type of attack. The first is to use the rename option to check the file you want to open. If you choose the rename option, the Windows operating system will automatically select the editable area, in addition to the file extension. The unselected part will be the actual file extension. If you see EXE format in the unchecked section, you should not open this file.

You can also check if hidden characters are inserted using the command line. To do this, simply use the dir command as follows.




As you can see in the screenshot above, **util** is a weird file, so you should question it.

## Be careful before downloading files!

As you can see, even a simple PDF file can leave your device in the hands of attackers. That's why you shouldn't arbitrarily download every file you see on the Internet. No matter how safe you think they are, be careful!

Before downloading a file, you can take some precautions, like making sure that the website you are downloading from is trustworthy and scanning the file with an online file checker.

You finished reading the article "**How trojan pretends to be a PDF file using the RLO . method**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

---