FEBRUARY 28, 2023 / #SECURITY

What is RTLO in Hacking? How to Use Right-to-Left Override and Defend Against it

Daniel Iwugo

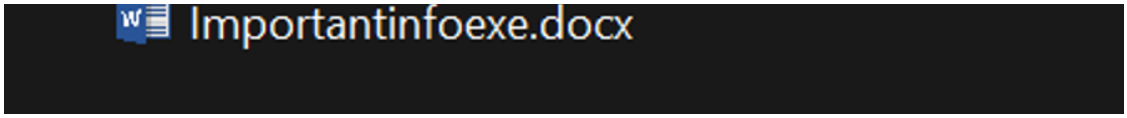
Let's play a lovely game of hide your malware in plain sight. 🐴

Malicious hackers look for all kinds of underhanded tricks to make everyday users victims as a result of common mistakes. They might get someone to click the wrong link, open the wrong website, or execute the wrong program.

Most times, it's easy to identify a suspicious file by the following:

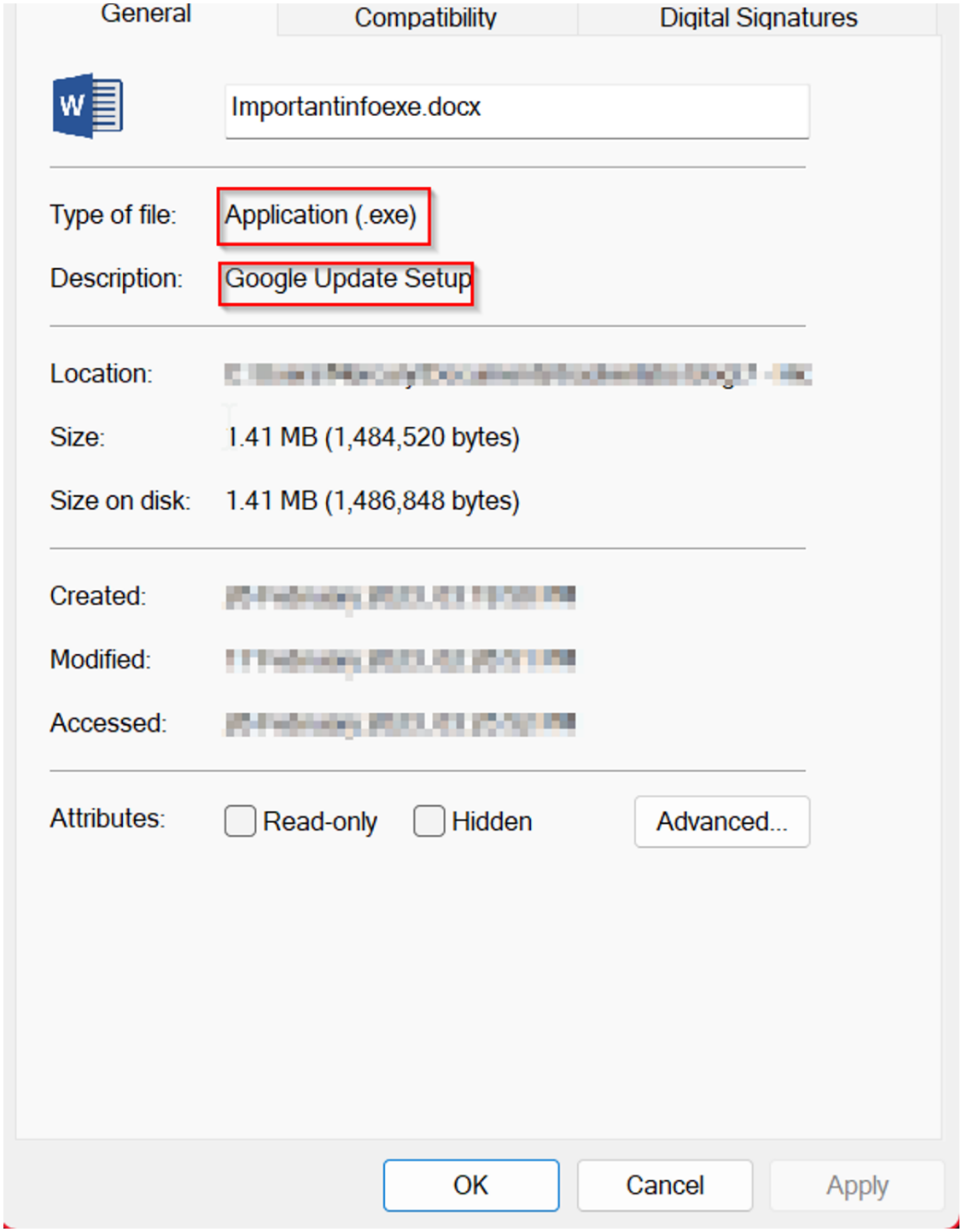
1. The icon does not match the name
2. The extension seems incorrect
3. The file is noticeably bigger or smaller than its proposed file type (Imagine an image of 50mb 🤯)

But would you be suspicious of a file like this?



A totally non-suspicious file | Credit: Mercury

Nothing out of the ordinary right? Seems like your average word document. Let's take a closer look at things.



Properties of the file | Credit: Mercury

In this tutorial, you'll learn:

1. What Right-To-Left Override is
2. How to use it to hide file extensions

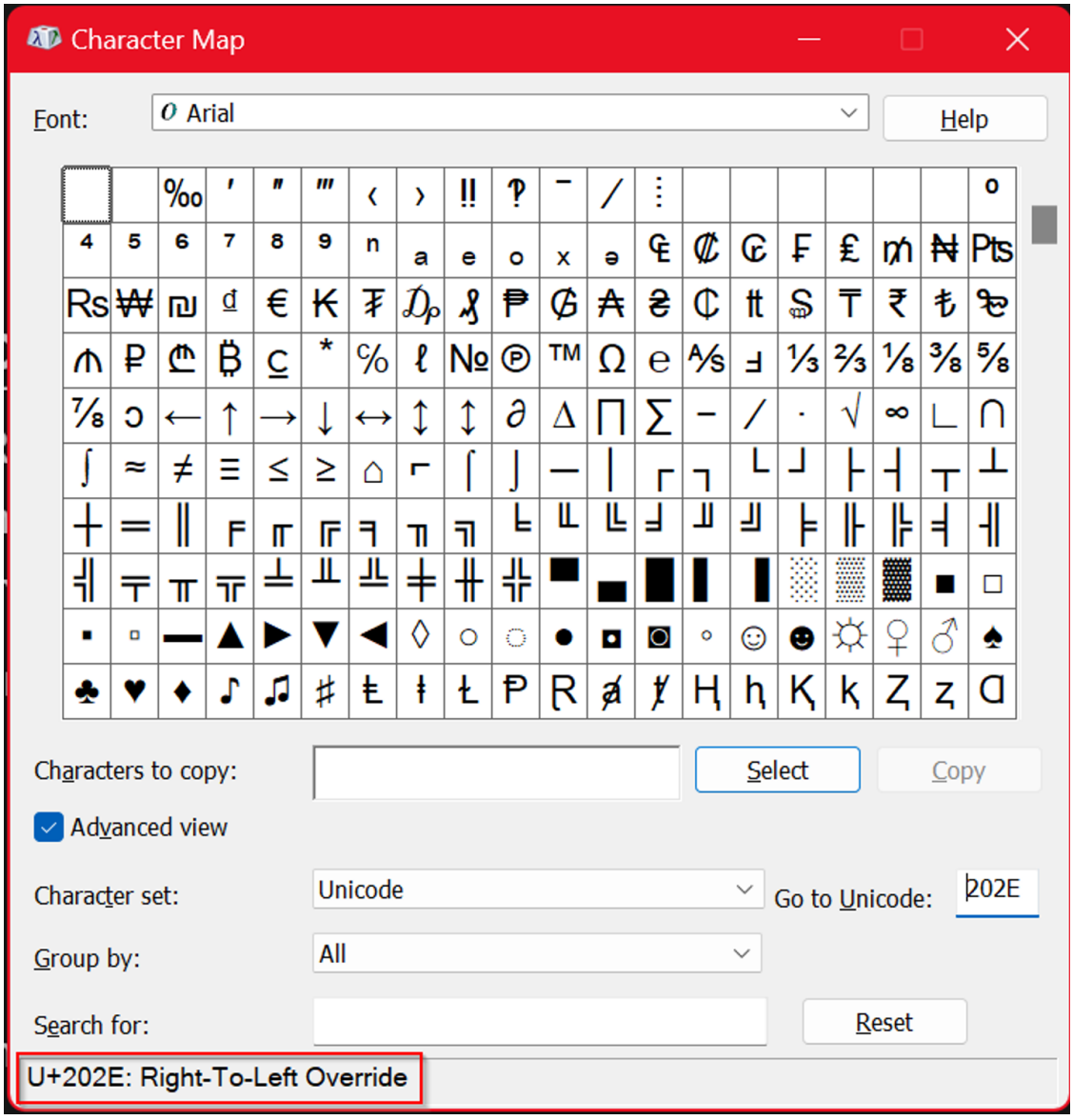
Friendly Disclaimer: This is simply for educational purposes only and is written solely to protect individuals, businesses, and organisations from threat actors. If you still wish to use this in any other way, that's your choice...just get ready for a lovely trip to jail... for a long time. 😊

And with that intro, let's jump in 🙃

What is Right-To-Left Override?

When nothing goes right, go left | Credit: Wallpaperflare.com

Right-To-Left Override (RTO or RTLO) is a Unicode non-printing character used to write languages read in the right-to-left manner. It takes the input and literally just flips the text the other way round. Such languages include Hebrew, Arabic, Aramaic, and Urdu.



Character map | Credit: Mercury

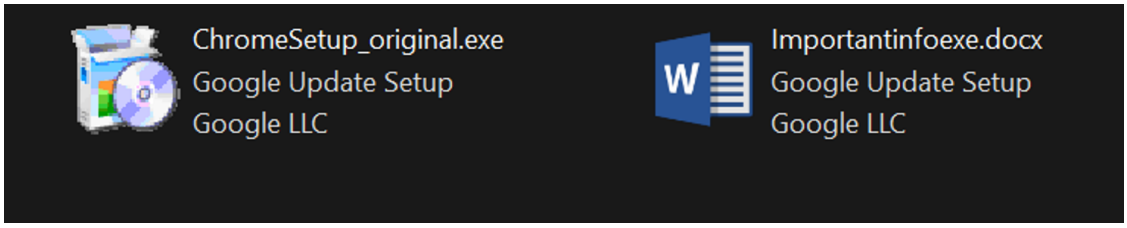
Below is a demonstration of how it is used:

RTLO Demonstration | Credit: Mercury

As you may see, the two statements typed are the exact same thing, except that the one below is written in the inverse because the RTLO character was inserted before typing it.

How RTLO Can Be a Malicious Tool

Perhaps at first glance this character looks innocent enough. What's the harm in flipping some text anyway? The answer: File extensions.



A Chrome installer as an installer and word document | Credit: Mercury

Below are some hacks carried out in the past using this technique:

1. **Telegram**: In 2018, Kaspersky reported in a blogpost on Securelist that Russian cybercriminals exploited RTLO gaps in the wild on Telegram Windows Clients. As demonstrated

2. **Scarlet Mimic**: In 2016, Unit 42 from Palo Alto Networks released a report on the tactics of a threat group known as Scarlet Mimic. The group is commonly known for targeting minority activists. According to the report, one of the groups common tactics included using RTLO characters to mask the actual file extensions of self-extracting archives (SFX/SEA) 🎭.

3. **Famous Messaging apps**: In 2022, Bleeping computer released a news article about phishing techniques on messaging and email platforms using RTLO. Platforms such as iMessage, WhatsApp, Signal, and Facebook Messenger (I wonder who uses the last one 😳) were vulnerable to such tactics. It allowed an attacker to inject an RTLO character in between two links. On the left was a legitimate domain such as (google.com) and on the right was a malicious one. This made it appear as one link and if a user clicked on the left side, they were safe. However, if they clicked on the right side, they were not.

4. **PLEAD**: In 2017, Trend Micro released an article on three campaigns performed by a threat group known as BlackTech. One of these campaigns was named PLEAD, which focused on information theft and was targeted at the Taiwanese government and organisations. According to the article, spear-phishing emails were used to deliver and install a backdoor. The notable part of this attack was that the installers where disguised as documents using RTLO characters and decoy documents were also added to trick users 📄.

5. **Apple's OS X**: Despite being common in Windows, this technique could be used to target Mac users. In 2013, a

shows the real file extension and when run, the file quarantine notification is written backwards (Nice one Apple 😉🍎).

How to Hide a Potentially Malicious File

A Guy Fawkes Mask | Credit: Wallpaperflare.com

RTLO can be used in any attack that leverages tricking the user about written text. As we saw in the above hacks, links, email attachments and executable scripts and files are the most common attack vectors.

But this tutorial will focus on locally hosted files because it gives the basic idea and its variations can be used to carry out other attacks.

2. Change the file icon

The file icon needs to be changed to mimic the fake extension to make it easier to trick a user.

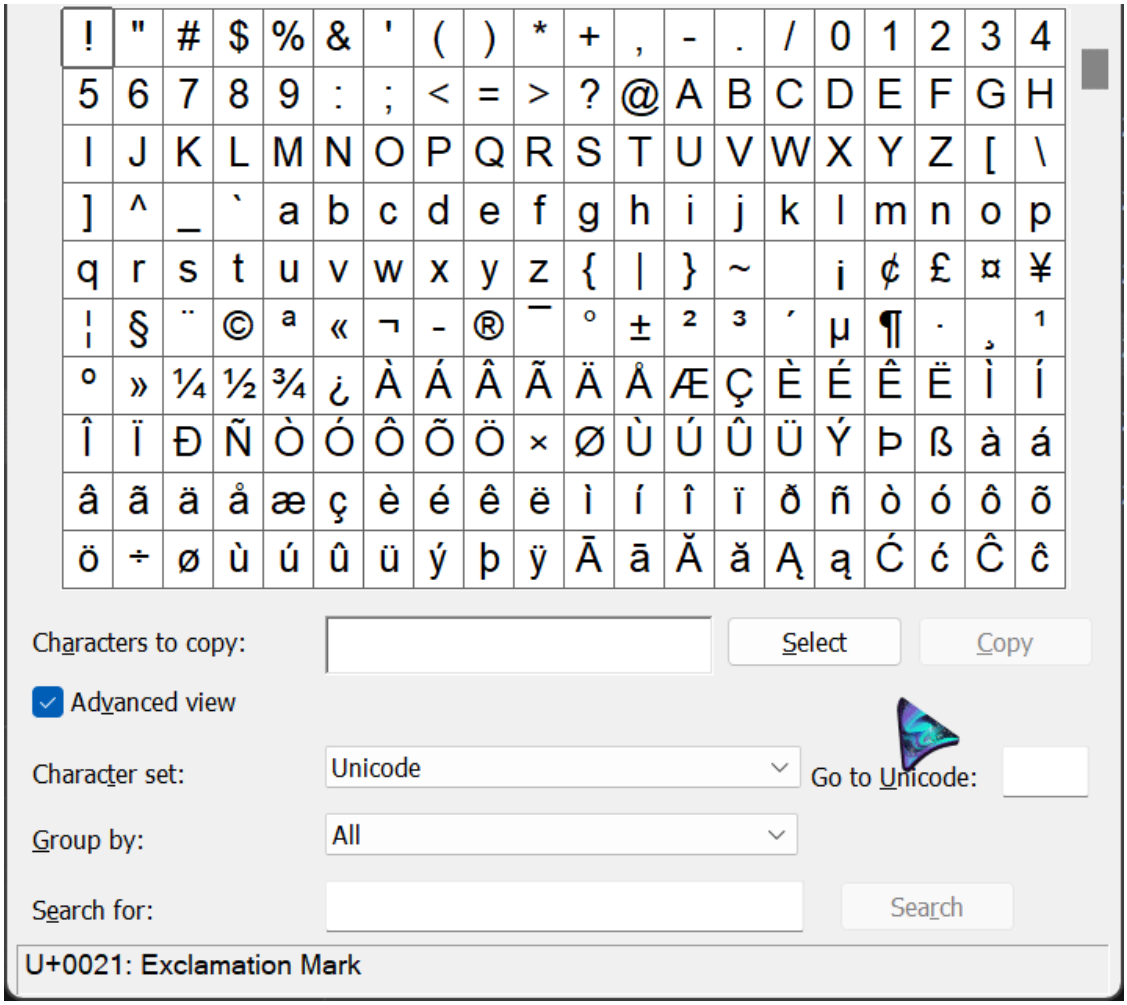
Below are the prerequisites for the procedure:

1. An executable or script – The payload
2. A file icon – Part of the bait
3. Resource hacker – To change the file icon

The file icon could be in .exe, .dll, .res, or .ico format. You can download some from here. And now, let the chaos begin ⚠️.

Step 1 – Insert the RTLO character

Choose a file of your liking and open it in Windows Explorer. Open the Character Map app on Windows and check the 'Advanced View' box. In the 'Go to Unicode' option, type in 202E. Hit the 'Select' and 'Copy' buttons respectively and go to the file you want to modify.



Selecting the Right-To-Left Override Character | Credit: Mercury

Here is the tricky part 🎃. When typing with the RTLO character, it types from right-to-left. This can be confusing when trying to rename the file. If you want to rename a file after injecting the character, spell it backwards.

For example, if you want to write the extension '.pdf', you have to type it as 'fdp.' It takes some time getting used to but it's easy after a few tries.

Short renaming demonstration | Credit: Mercury

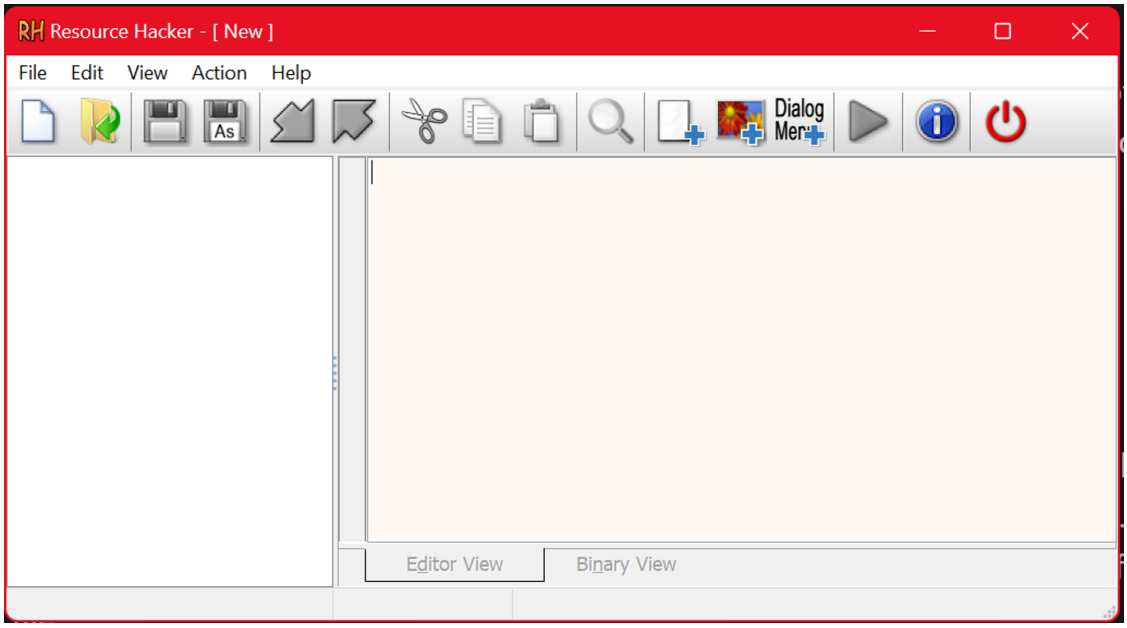
In File Explorer, check the option to show file extensions. Go to the file, right-click and hit rename. Change the name to whatever you want but make sure not to ever edit the extension itself so the file works as intended ❗ .

Set the cursor just before the extension name. Paste the RTLO character. You will observe it seems like nothing happened but that's how it is supposed to look. Next type in 'xcod' to get 'docx' and hit enter.

Renaming the target file | Credit: Mercury

Step 2 – Change the Icon

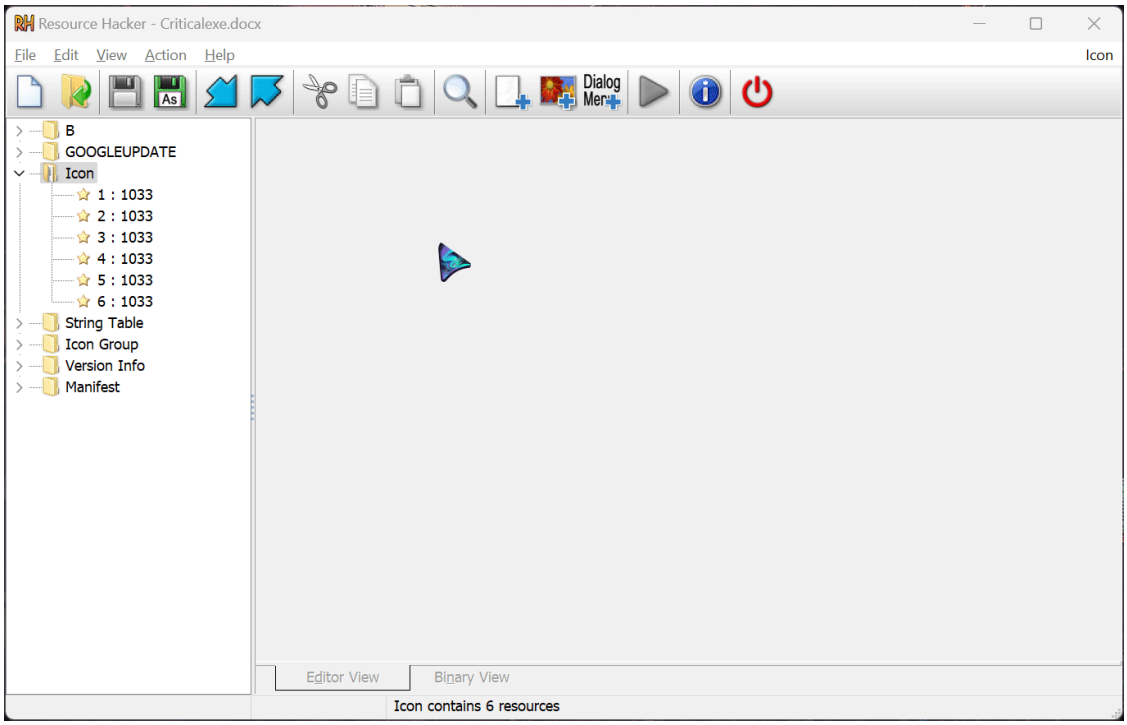
Now for the final part of our amazing trick – changing the icon 🪄. Download and install a software called resource hacker. Open it and hit Ctrl + O. Next, select your target program. There's a lot of information here that we can edit, but we just want to focus on the icon.



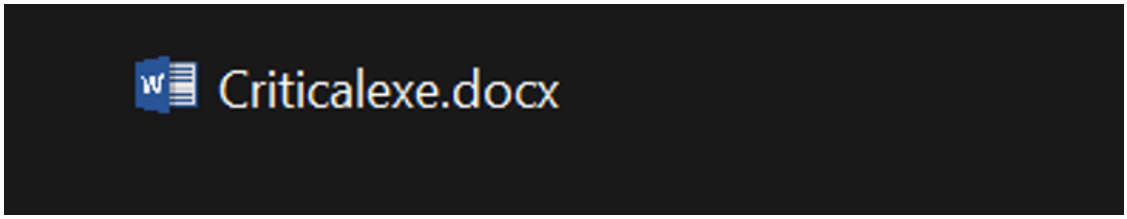
Resource Hacker | Credit: Mercury

In the Explorer, select the file icon you wish to replace on the program and hit the 'Replace' button.

Lastly, hit Ctrl+S to save the file. If you have an Antivirus, you might want to temporarily switch it off before saving the file.



Using Resource Hacker to change the icon | Credit: Mercury



A totally non-suspicious file | Credit: Mercury

Neat, isn't it? Let's look at how to avoid falling for this trick.

Online Security | Credit: Wallpaperflare.com

Since it abuses system features, almost any regular user or tech geek would fall for this hack. So how can you avoid it? Here are some tips:

Never open a file or link of unknown origin

Never underestimate the power of basic cyber hygiene. Don't click random links, or open files that you have no clue where they came from or who sent them.

Set file extensions to be shown

A file name that hides its extension is much more easily noticed to be fishy when file extensions are on.

Be cautious if you notice that just before the extension, the file ends with common file extensions written backwards. For example, 'infoexe.pdf' will be obvious. However, some are less obvious like

Install and keep Antivirus software up to date

In case you have fallen for such, this could be your last line of defense. An appropriate antivirus will take note if a script or executable file with malicious actions has been executed and will quarantine or delete it.

I mean, a $20 yearly subscription sounds better than over $200 down the drain for nothing 💀.

Apply best practices

For the more sophisticated IT people in organisations, implementation of best practices such as Network traffic analysis, firewalls, use of intrusion detection and prevention systems and network segmentation are your best bet.

Conclusion

Let's summarise what you've learned:

1. How to use RTLO characters to manipulate text
2. How to change application icons using Resource Hacker
3. How to identify text manipulated with RTLO characters

Initially it's hard to identify files modified like this. I encourage you to play around with different file names and extensions and see what you get. This will also train you to identify files that are not what they seem.

Hacking?

Resources

1. Other ways to change an app icon
2. More ways to use RTLO

Acknowledgements

Thanks to Anuoluwapo Victor, Chinaza Nwukwa, Holumidey Mercy, Favour Ojo, Georgina Awani, and my family for the inspiration, support and knowledge used to put this post together. You all inspire me daily.

Cover image credit: The Kelpies | Jamie McInall

Daniel Iwugo

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet