Spoof Using Right to Left Override (RTLO) Technique - InfoSec Resources

Published: 2015-04-16 · Archived: 2026-04-29 02:03:42 UTC

In this article we will learn about the one of the most overlooked spoofing mechanisms, known as right to left override (RTLO).

What is RTLO?

RIGHT TO LEFT OVERRIDE is a Unicode mainly used for the writing and the reading of Arabic or Hebrew text. Unicode has a special character, U+202e, that tells computers to display the text that follows it in right-to-left order. This vulnerability is used to disguise the names of files and can be attached to the carrier like email. For example, the file name with ThisIsRTLOfileexe.doc is actually ThisIsRTLOfiledoc.exe, which is an executable file with a U+202e placed just before “doc.”

Ethical Hacking Training – Resources (InfoSec)

Though some email applications and services that block executable files from being included in messages also block .exe programs that are obfuscated with this technique, unfortunately many mail applications don’t or can’t reliably scan archived and zipped documents, and the malicious files manipulated in this way are indeed being spammed out within zip archives.

For example, let’s create a file with Name TestingRTLO[U+202E]xcod.txt. “U+202E” can be copied and pasted from the above character map present in Windows. To make sure something is present in the character, do the following steps:

- Create a new text document and see its properties and note down its name:

- Now rename the file with the copied U+202E characters and see the change in file name:

- Now rename the File TestingRTLO[U+202E]xcod.txt with characters inserted and see the below results.

File extension types that can be dangerous

The below section lists the common file types that can be used to execute unwanted code in the system:

- .bat
- .exe
- .cmd
- .com
- .lnk
- .pif
- .scr
- .vb
- .vbe
- .vbs
- .wsh

Remediation against RTLO

Though most endpoint security solutions like antivirus detect this type of spoofing, and some IRC clients even change the crafted malicious links back to original form, many mail applications don't or can't reliably scan archived and zipped documents, and the malicious files manipulated in this way are indeed being spammed out within zip archives. The biggest example of this is in the usage of the backdoor "Etumbot". Some features of Windows also help to carry this type of attack, such as Windows hides the file extensions by default. Malicious individuals can set any icon they want for let's say a .exe file. A file named pic.jpg.exe using the standard image icon will look like a harmless image with Windows' default settings.

Uncheck this selection and Windows will stop hiding extension for known file types.

Another good approach is to make sure that the folder where all the downloads take place should have its view set to 'content'.

This will make sure that the files will appear in their original form despite all the changes.

Though this technique is a bit old, it is still being used in backdoors like Etumbot, malware known as Sirefef, etc.

Lohit Mehta is a passionate Information Security professional.
