Lesser known tricks of spoofing extensions

September 30, 2016 by Malwarebytes Labs

Last updated: October 26, 2016

It is a well-known fact that malware using social engineering tricks is designed to hide itself from being an obvious executable. Malicious attachments are sent with specially crafted icons that are pretending to be real document files. In addition to this, they often use double extensions, such as ".pdf.exe" or ".doc.exe", taking advantage of the fact that Windows by default hides the extension, so sometimes user wouldn't notice which file is the one it claims to be.

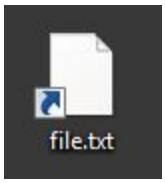
They also use lesser known extensions of executable format, for example ".scr".

But this is not all. In this short article, we will present two other less common tricks used to deceive users.

PIF extension

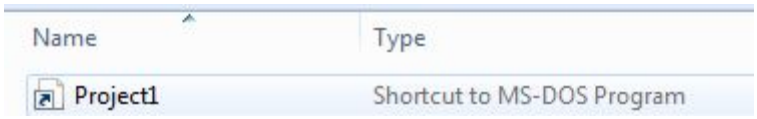
This trick is cunning, because it hides the real extension even if the user has disabled the feature of extension hiding on Windows.

This is how an executable looks like after changing its extension to “pif”— not only is the extension completely hidden, but also the original icon. The full name of the presented file is “**file.txt.pif**“:



The PIF extension still allows the file to be executed. Double-clicking will lead us to deploying it.

If we display details of the file, we can uncover its real file type, which is a “Shortcut to MS-DOS Program”.



This trick has been used in [a recent campaign of Petya/Mischa in Poland](#).

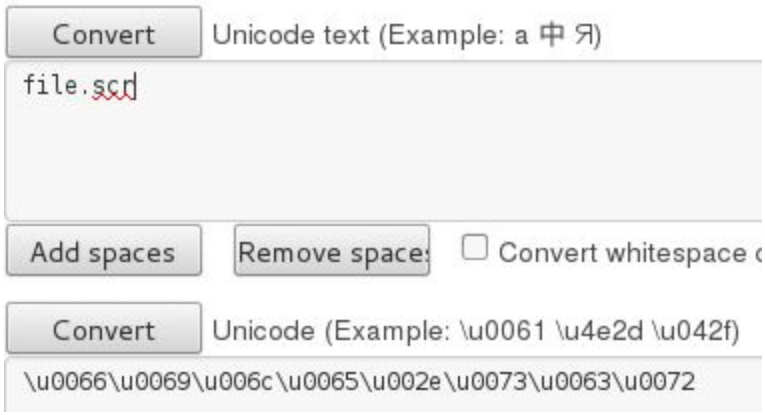
RTLO – Right To Left Override

This trick uses the fact that some languages are being written from right side towards left in contrast to the way used by most countries, including Europe and Americas. In order to support such languages, a Unicode character has been created, which works as a switch between those two modes. It can be used maliciously, in order to displace the displayed extensions. This character has a code: **U+202e**

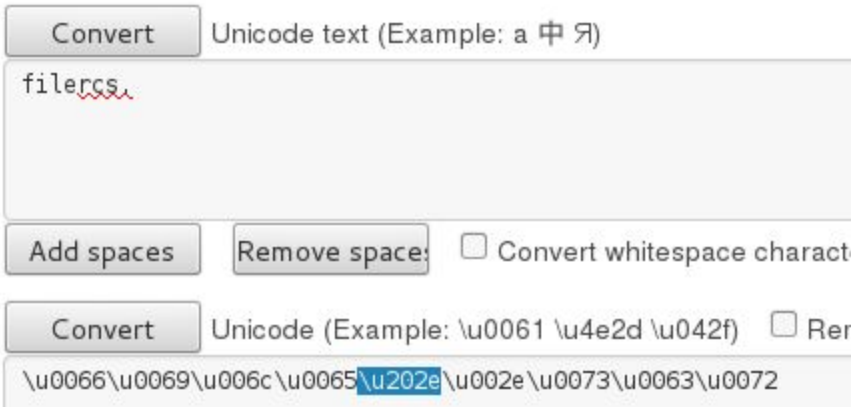
Let’s go over how it works. We can use some online Unicode converter, for example [this one](#).

To demonstrate the trick, first we will make a name for the executable with the extension “scr”. Then, we will try to spoof the extension and make it appear like a “txt”:

Step 1: Create a name for the executable

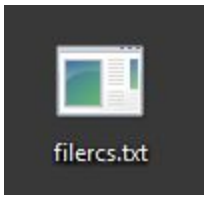


Step 2: Add the character to reverse the order of characters



Step 3: Add a spoofed extension (i.e. “txt”) at the end

Step 4: Copy the prepared name and rename the file



If we change the executable's icon, it would look exactly like a normal text file. Only if we display the details that the real file type is revealed—in this case it is a screen saver:

Also, if we try to rename the file, we can see that the selection pattern is not continuous:

Conclusion

As we can see, extensions can be spoofed in various ways, and disabling the feature of hiding extensions on Windows is not the solution for all the problems. These tricks are very easy to implement and effective. We should be vigilant for every file that we download, no matter if its extension and icon looks harmless.

This was a guest post written by Hasherezade, an independent researcher and programmer with a strong interest in InfoSec. She loves going in details about malware and sharing threat information with the community. Check her out on Twitter @hasherezade and her personal blog: https://hshrzd.wordpress.com.