

Search Labs

🔍

SUBSCRIBE



```
Dim oldname As String = TextBox1.Text
Dim cutoff As Integer = Len(oldname) - 7
If cutoff >= 0 Then
    Dim newname As String = oldname.Substring(0, cutoff)
    newname = newname + " "
    newname = newname + oldname.Substring(cutoff, 7)
    TextBox3.Text = newname
    If System.IO.File.Exists(oldname) = True Then
        System.IO.File.Copy(oldname, newname)
        MsgBox("File Copied")
    End If
End If
```

CYBERCRIME | NEWS

# The RTLO method

Posted: January 9, 2014 by [Pieter Arntz](#)

After my [post about extensions](#), I received some requests to deal with another method of pretending to be a different type of file. If you have not read that article yet, it will prove helpful to do that first in order to better understand this post.

## What is RTLO (aka RLO)?

The method called RTLO, or RLO, uses the method built into Windows to deal with languages that are written from right to left, the “Right to left override”.

Let’s say you want to use a right-to-left written language, like Hebrew or Arabic, on a site combined with a left-to-right written language like English or French. In this case, you would want bidirectional script support.

Bidirectional script support is the capability of a computer system to correctly display bi-directional text. In HTML we can use Unicode right-to-left marks and left-to-right marks to override the HTML bidirectional algorithm when it produces undesirable results:

left-to-right mark: &#8203; or (U+200E)

right-to-left mark: &#8203; or (U+200F)

## How is RTLO being abused by malware writers?

On systems that support Unicode filenames, RTLO can be used to spoof fake extensions. To do this we need a hidden Unicode character in the file name, that will reverse the order of the characters that follow it.

### ABOUT THE AUTHOR



Pieter Arntz   
Malware Intelligence  
Researcher

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour [Paramètres des cookies](#) améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

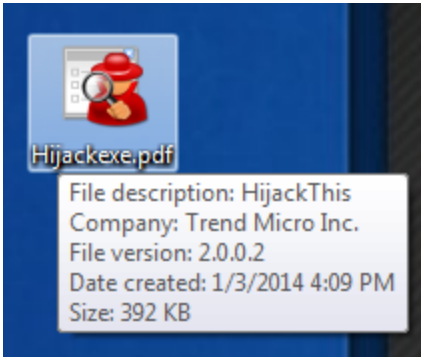
Tout refuser

Autoriser tous les cookies



```
Dim newname As String = oldname.Substring(0, cutoff)
newname = newname + " "
newname = newname + oldname.Substring(cutoff, 7)
TextBox3.Text = newname
If System.IO.File.Exists(oldname) = True Then
    System.IO.File.Copy(oldname, newname)
    MsgBox("File Copied")
End If
End If
```


Look for example at this file, a copy of HijackThis.exe, that I renamed using RTLO:



The last seven characters in the file name are displayed backwards because I inserted the RTLO character before those seven characters.

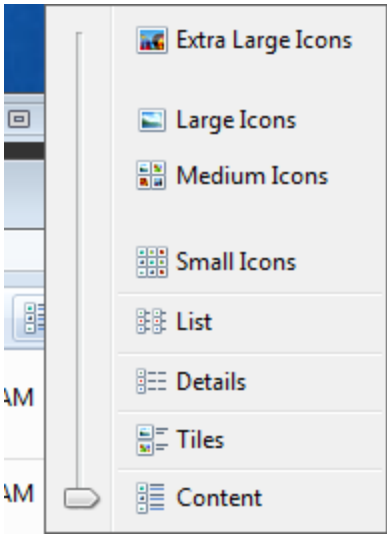
As discussed in the previous article, assigning a matching icon to a file is a triviality for a programmer. So here we have an executable file that seems to have the PDF extension.

Ironically, you will see straight through this deception if you are still running XP, since it does not support these file names:

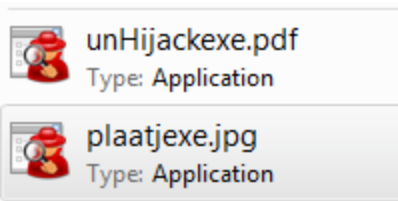
|   |                  |        |             |
|---|------------------|--------|-------------|
|  | plaatj□gpj.exe   | 393 KB | Application |
|  | unHijack□fdp.exe | 393 KB | Application |

The square symbol shows us where the Unicode RTLO character is placed.

One way to catch these fakes on more modern versions of Windows is to set the “Change your view” ruler to “Content”.



Set this way, you can see that the files are applications and not a PDF or jpg.



This may be a good idea for your “Download” folder(s), so you can check if you have



A malware known as Sirefef (which Malwarebytes Anti-Malware detects as Trojan.Agent.EC ) uses the RTLO method to trick users into thinking that the entries it puts into the infected machine’s registry are legitimate ones, belonging to Google update.

Does this have any effect on the detection of these files?

No. Detection of malicious file is never done by a filename alone. So your AV and Malwarebytes Anti-Malware will still recognize these files if they were added to their detection, no matter what they are called or how they are written.

**Summary:** RTLO is used to fake extensions by writing part of the filename or other descriptions back to front. Although the detection by your AV or Malwarebytes Anti-Malware is not altered in any way this trick can be deceiving users at first glance.

Sources :  
[http://www.ipa.go.jp/security/english/virus/press/201110/E\\_PR201110.html](http://www.ipa.go.jp/security/english/virus/press/201110/E_PR201110.html)

<http://threatpost.com/sirefef-malware-found-using-unicode-right-to-left-override-technique/102033>

<http://www.w3.org/TR/WCAG20-TECHS/H34.html>

SHARE THIS ARTICLE



Malwarebytes Labs Comment Policy

All comments are moderated. Relevant comments will be published and all URLs will be removed.

Got it

What do you think?

2 Responses



0

Upvote



0

Funny



0

Love



1

Angry



1

Sad

Comments and reactions for this thread are now closed.



0 Comments

1 Login ▼

1 • Share

Best Newest Oldest

This discussion has been closed.

Subscribe Privacy Do Not Sell My Data

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.



## “Phish ‘n Ships” criminals who create fake product listings for in-demand products

November 1, 2024 - Fraudsters running the Phish 'n Ships campaign infected legitimate website and used SEO poisoning to redirect shoppers to their fake web shops

[CONTINUE READING](#)

0 Comments

Android | News

## Android malware FakeCall intercepts your calls to the bank

October 31, 2024 - Android malware FakeCall can intercept calls to the bank on infected devices and redirect the target to the criminals.

[CONTINUE READING](#)

0 Comments

Apple | News

## Patch now! New Chrome update for two critical vulnerabilities

October 30, 2024 - Chrome issued a security update that patches two critical vulnerabilities. One of which was reported by Apple

[CONTINUE READING](#)

0 Comments

Apple | News

## Update your iPhone, Mac, Watch: Apple issues patches for several vulnerabilities

# Europol warns about counterfeit goods and the criminals behind them

October 28, 2024 - There is a whole ecosystem behind the sales and distribution of counterfeit goods. Best to stay away from them.

CONTINUE READING

0 Comments

Contributors

Threat Center

Podcast

Glossary

Scams

Cyberprotection for every one.

## FOR PERSONAL

- Windows Antivirus
- Mac Antivirus
- Android Antivirus
- Free Antivirus
- VPN App (All Devices)
- Malwarebytes for iOS
- SEE ALL

## FOR BUSINESS

- Small Businesses
- Mid-size Businesses
- Larger Enterprise
- Endpoint Protection
- Endpoint Detection & Response (EDR)
- Managed Detection & Response (MDR)

## SOLUTIONS

- Digital Footprint Scan
- Rootkit Scanner
- Trojan Scanner
- Virus Scanner
- Spyware Scanner
- Password Generator
- Anti Ransomware Protection

## LEARN

- Malware
- Hacking
- Phishing
- Ransomware
- Computer Virus
- Antivirus
- What is VPN?



## Cybersecurity info you can't live without

Want to stay informed on the latest news in cybersecurity? Sign up for our newsletter and learn how to protect your computer from threats.

### Email Address

Sign Up

## COMPANY

- About Us
- Contact Us
- Careers
- News and Press

## FOR PARTNERS

- Managed Service Provider (MSP) Program
- Resellers

## ADDRESS

One Albert Quay  
2nd Floor  
Cork T12 X8N6  
Ireland

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.