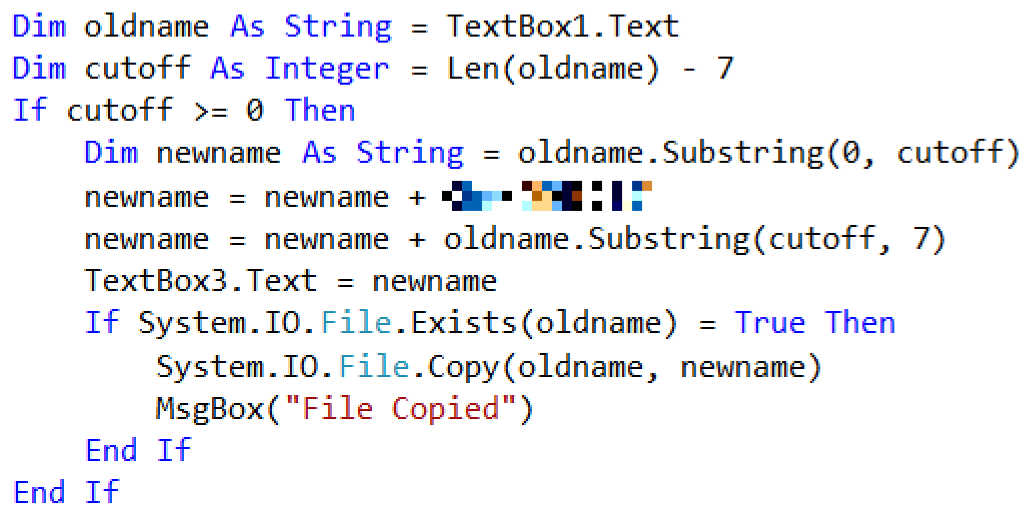


```
Dim oldname As String = TextBox1.Text
Dim cutoff As Integer = Len(oldname) - 7
If cutoff >= 0 Then
    Dim newname As String = oldname.Substring(0, cutoff)
    newname = newname + [redacted]
    newname = newname + oldname.Substring(cutoff, 7)
    TextBox3.Text = newname
    If System.IO.File.Exists(oldname) = 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)?

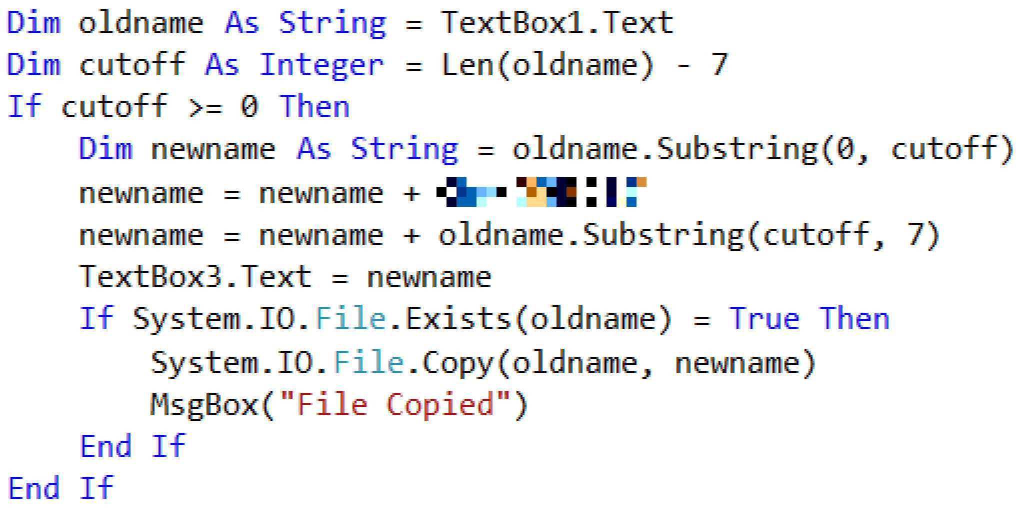
The method called RTLO, or RLO, uses the method built into Windows to deal with languages that are written from right to left, the "Right to left override".

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

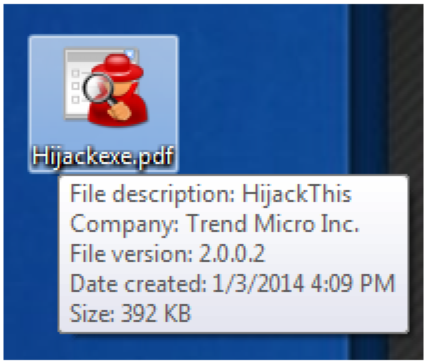
How is RTLO being abused by malware writers?

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.



```
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 + [illegible]
    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:



File description: HijackThis
Company: Trend Micro Inc.
File version: 2.0.0.2
Date created: 1/3/2014 4:09 PM
Size: 392 KB

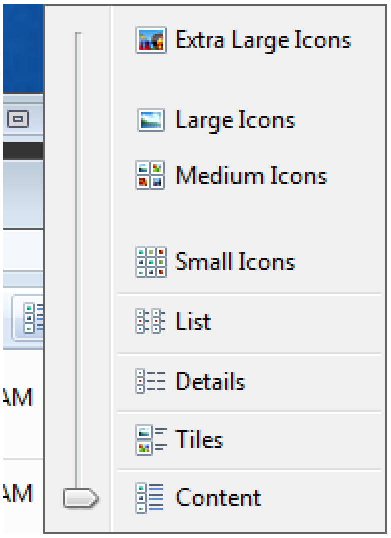
The last seven characters in the file name are displayed backwards because I inserted the RTLO character before those seven characters.

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.

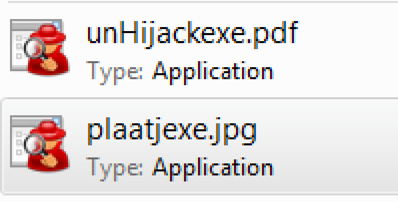
Ironically, you will see straight through this deception if you are still running XP, since it does not support these file names:

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.



unHijackexe.pdf
Type: Application

plaatjexe.jpg
Type: Application

This may be a good idea for your “Download” folder(s), so you can check if you have downloaded what you expected to get.

Is the RTLO method actively being used?

The technique has been know for quite a while and is starting to re-surface. It is not only being used for filenames by the way.

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 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://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

RELATED ARTICLES

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

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

October 29, 2024 - Apple has issued patches for several of its operating systems. The ones for iOS and iPadOS deserve your immediate attention.

CONTINUE READING

0 Comments

goods and the criminals behind them

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

CONTINUE READING

0 Comments

News

A week in security (October 21 – October 27)

October 28, 2024 - A list of topics we covered in the week of October 21 to October 27 of 2024

CONTINUE READING

0 Comments

ABOUT THE AUTHOR

Pieter Arntz

Malware Intelligence Researcher

SEE ALL

COMPANY

About Us

Contact Us

Careers

News and Press

Blog

Scholarship

Forums

Vulnerability Disclosure

FOR PARTNERS

Managed Service Provider (MSP) Program

Resellers

MY ACCOUNT

Sign In

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?

ADDRESS

One Albert Quay
2nd Floor

Malwarebytes LABS

Legal

Privacy

Terms of Service

Accessibility

Imprint