RIGHT TO LEFT OVERRIDE UNICODE CAN BE USED FOR MULTIPLE SPOOFING CASES

LANGUAGE : ENGLISH

1: Introduction

2: Right To Left Override and the FileName extension

3: Right to left Override and Hypertext link

4: Some additional notes

5: Links

---

1 : INTRODUCTION

SPOOFING's Vulnerabilities type are simples to deceive users or vulnerables softwares/computerized systems on real received or posted information.

The spoofing regularly makes speak about multiple distinct scenaris like Address URL of WebPage, indicator TLS/SSL, IP adress, and anymore possibility.

This PAPER will to report than particular [RTLO] UNICODE can be used in some Spoofing cases and some scenario on multiple Softwares usually and currently used of Net_surfers [like :WebBrowsers / Instant Messaging/Exchange of data file / …] and thus to increase discretion of possible PHISHING/SCAN Scenaris.

little introduction about Right To Left Override Unicode:

RIGHT TO LEFT OVERRIDE is a unicode mainly used for the writing and the reading Arabics or Hebrews text and who thus has utility to reverse the order reading'sens of the following characters.

2: RIGHT TO LEFT OVERRIDE & FILENAME EXTENSION

The spoofing of an extension file on OS Microsoft Windows which we report in this PAPER is a technique exploiting the RIGHT TO LEFT OVERRIDE unicode and than it will always cause the directional reverse reading order of others characters followed it including the extension-type of malicious file!

This UNICODE of which we will simplify name by [RTLO] doesnt can see owing to the fact that its characters and its place are invisible.

Use RTLO for reverse the direction of reading of the file names including the extension of concerned file while keeping same the types of execution.

Example: To use a syntax like “SexyPictureGirlAl[RTLO]gpj.exe” be read “SexyPictureGirlAlexe.jpg”.

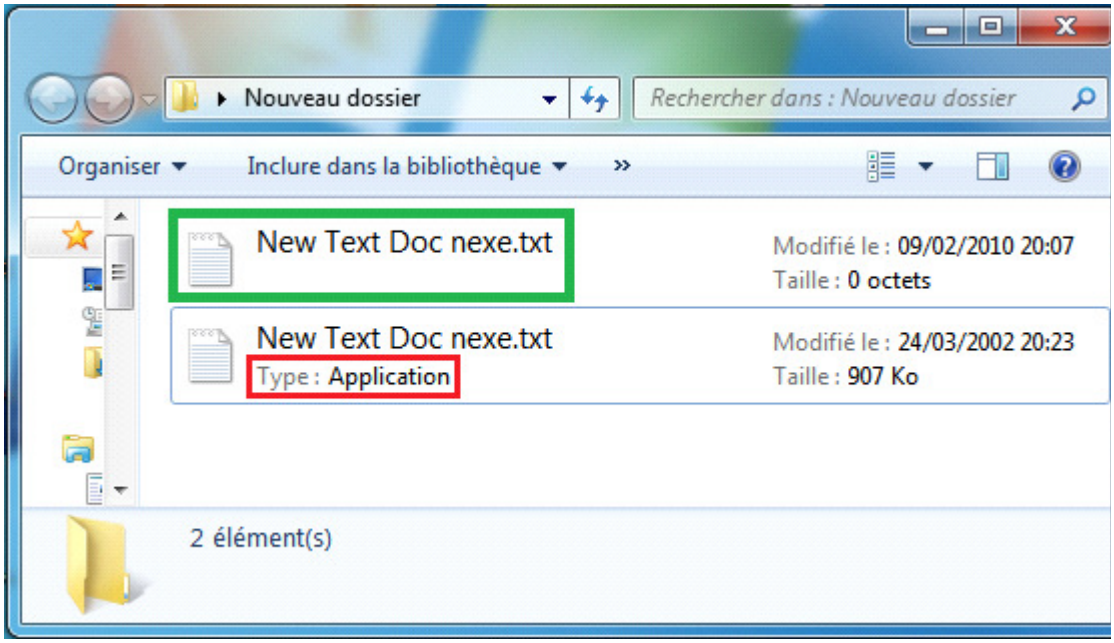
That so make it possible of mislead users and to encourage them to download & execute the malicious file with spoofed filname extension by RTLO unicode while believing to open a kind of non risked file, moreover, some software applications "black-list" this unicode on download file name(like : google chromium/firefox [corrected since the updates to: Firefox 3.5.4 & Firefox 3.0.15] /etc).

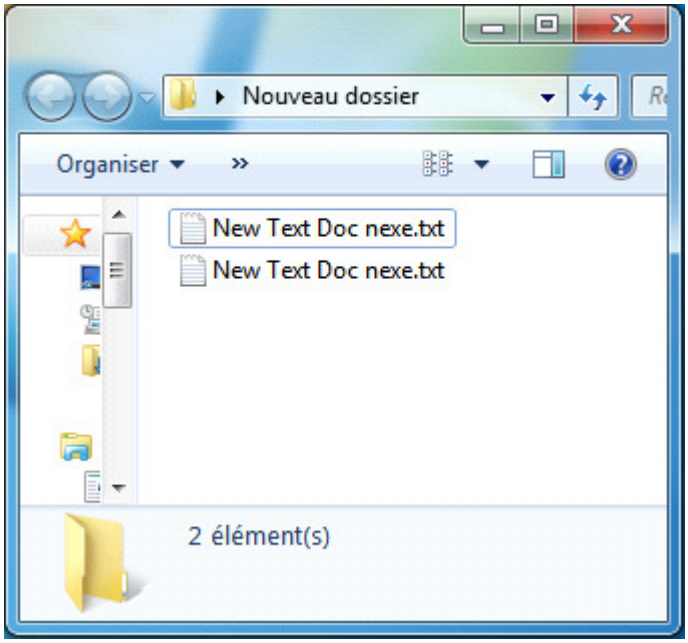
But That does not allow however the remote loading of file (.ZIP/.RAR…), containing files with the spoofed extensions. A technique innovating when it is known that one of the principal points of safety's den is its extension file type.

Recalling that most of the users of Microsoft Windows define in their WINDOWS Options the viewing extension's file witch an known execusion type (necessary that for realizable spoof).

Moreover the file type necessarily does not appear in the repertories and that allows, in certain cases, a total resemblance

(without more user verifications !) between a non-dangerous original extension (like: .jpg/.txt…) , and a malware with spoofed file extension.

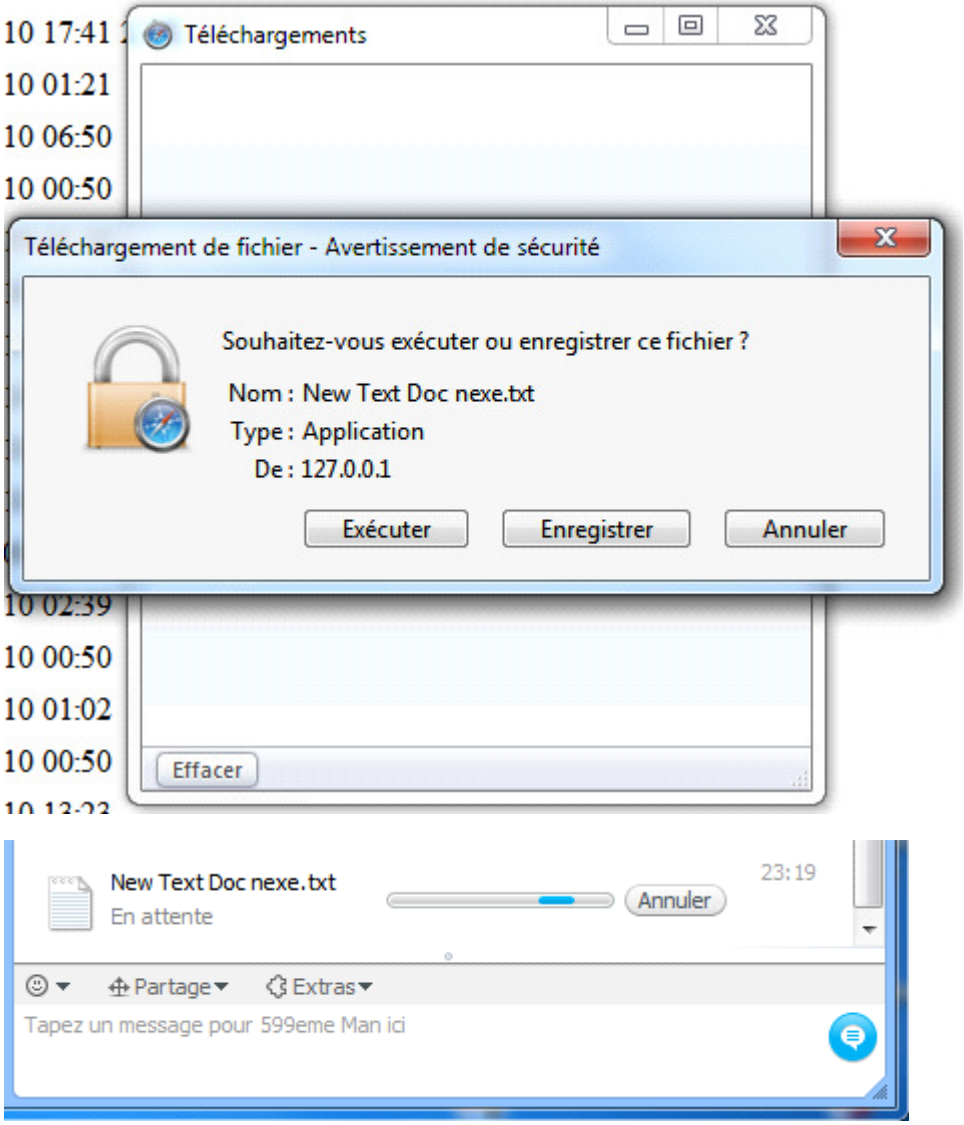


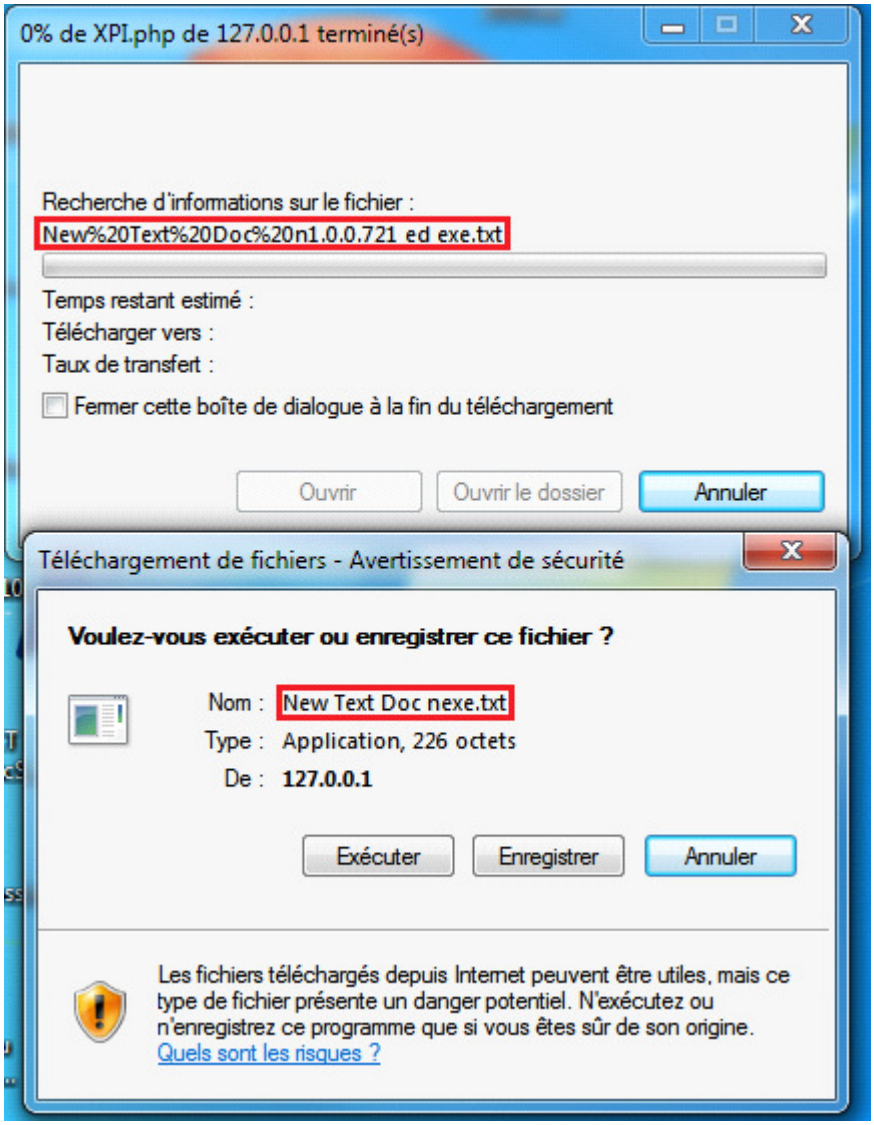


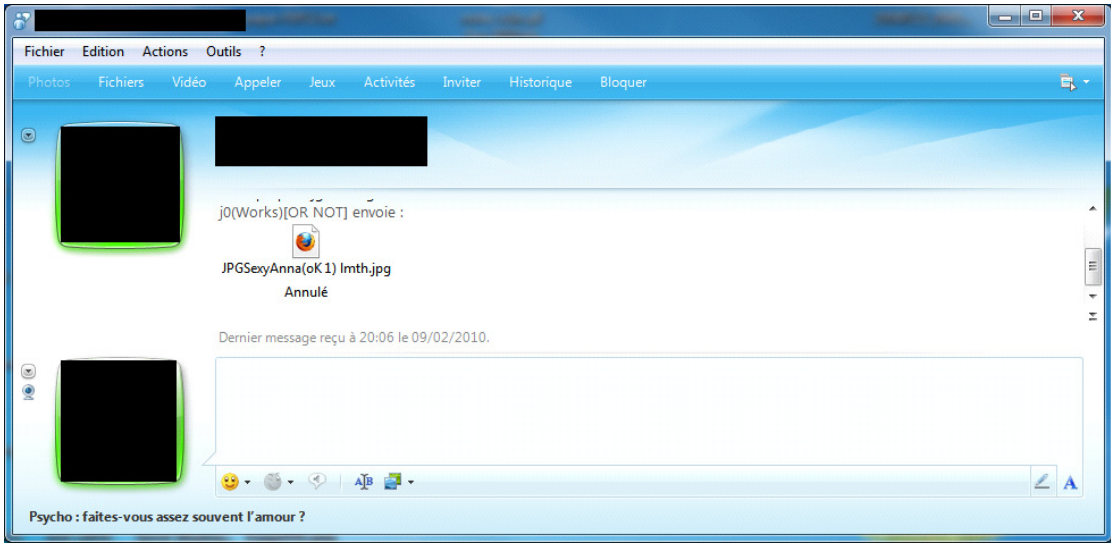
Great softwares used for WEB access as discussions on line and exchanges of data is

unaware of the dangerosity of such a remote downloading or neglect it and refuse to "black-listed" this unicode.

At this time, the swindles in WEB don't stop to multiply and bring back illegally more and more money to the gangster networks.




0% de XPI.php de 127.0.0.1 terminé(s)
Recherche d'informations sur le fichier :
New%20Text%20Doc%20n1.0.0.721 ed exe.txt
Temps restant estimé :
Télécharger vers :
Taux de transfert :
Fermer cette boîte de dialogue à la fin du téléchargement
Ouvrir
Ouvrir le dossier
Annuler
Téléchargement de fichiers - Avertissement de sécurité
Voulez-vous exécuter ou enregistrer ce fichier ?
Nom : New Text Doc nexe.txt
Type : Application, 226 octets
De : 127.0.0.1
Exécuter
Enregistrer
Annuler
Les fichiers téléchargés depuis Internet peuvent être utiles, mais ce type de fichier présente un danger potentiel. N'exécutez ou n'enregistrez ce programme que si vous êtes sûr de son origine.
Quels sont les risques ?



I exchanged some e-mails with the Microsoft Windows agency in charge of the vulnerability Reporting for Microsoft's application software and those answered me that their security policy does not consider for the moment this handling as a negligence of safety owing to the fact that the indicated type of execution remains the same one.

Conclusion:

Swindles by remote downloading/sending of malware with its standard extension spoofed could then given a rate of result very high.

It's regretable not to see Microsoft Considering this action as dangerous.

3: To falsify address URL of a Link with RTLO

The links hypertext on the languages like HTML can obviously take any values and this in spite of the destination on which it will direct you this is why the navigator Web use “Satus Bar*” posting address URL being relative to him, with the passage of your cursor over this one.

Part of the instant message services (public Tchat/Espace comment/Instant messaging) allow to send hypertext links , but automatically reprocessed it by value URL adress writes before submission . Impossible to use of the same assets as language HTML and to form malleable hypertext link.

But AGAIN ONE, RTLO there too allows an action on the direction of reading of hypertext link sent what

to facilitate a possible swindle of the SCAM/Phishing type.

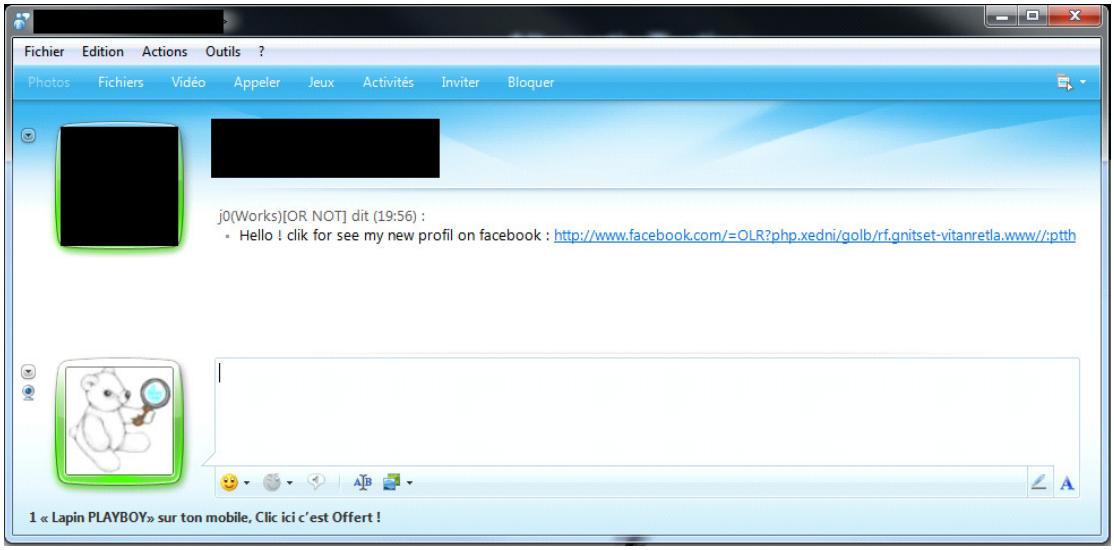
The RTLO there too allows an action on the direction of reading of a bond sent what to facilitate a possible swindle of the SCAM/Phishing type.

It is the case for Windows Live Messenger, moreover, its users not having for practice to receive link hypertext handled, this one could make it possible to increase the rate of people trapped in comparison with a nonofficial phishing links

PoC:

example: [RTLO] http://www.maliciouswebsite.com/moc.koobecaf.www://ptth

would give like visible Link: http://www.facebook.com/moc.etisbewsuoicilam.www//:ptth



Conclusion:

The falsification of a link can be aslo possible out on other services that the navigators Web via the languages Web (HTML/JS…) with the simple use of unicode RTLO what is equivalent to some extent to the same level of dangerousness as the falsification of the “Status-bar” of a navigator Web.

4: Some additional notes

This let us note that certain web sites propose the writing of comments and retransforment or automatically creation of the Url adresse sent by their TO addresses given, the RLTO

would of course reverse the direction of reading of the posted bond what pourait can be slightly to increase the rate of success of a probable standard swindle phishing/SCAM, using the same technique previously explained.

Without forgetting that the direction of the contents of the page the following can be completely reversed after its injection, which can constitute an embarrassment for the users/visitors of the site concerned…

CONCLUSION FINAL

The unicode Right to OverRide left thus allows a risky handling being able to multiples allow scenarios of swindle aiming at the same time the client's accounts of the trapped Net surfers as well as the access has their computers concerning the execution of a malware with its “spoofed” extension.

Again much of other dangerous handling can be carried out with this one and us trouvont

very domage that Microsoft Windows don't black-list this unicode in the name of its files like other actions risky or this one can be currently used.

5: Some links About RTLO & Security

Informations on the RTLO :

http://www.fileformat.info/info/unicode/char/202e/index.htm

Bug repaired by mozilla in Octoble 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-62.html

Blog Alternativ-testing.fr :

http://www.alternativ-testing.fr/blog/index.php

Author: **Jordi Chancel**

Helps on VulnTests, writing & publication : **599ème Man**

ALTERNATIV TESTING