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

INDEX

1:INTRO

Les attaques de type "SPOOFING" ont pour simple but de duper un utiliseur ou système informatique sur les réels informations reçues et affichées.

Le spoofing fait régulierement parler de lui dans de multiples scénarios distincts comme l'Adresse URL d'une page Internet , L'indicateur TLS/SSL , l'ip , et la liste est encore longue.

Ce raport va se pencher sur un UNICODE bien particulier pouvant permettre ce genre de scénario sur de multiples Softwares courament utilisés [discussion et échange de données en ligne/Navigateur internet/...) et ainsi augmenter la discrétion d'une possible escroquerie dans l'attente probable d'une intrusion sur les machines ou comptes clients des utilisateurs piégés.

Rappel sur l'unicode RIGHT TO LEFT OVERRIDE

Le RIGHT TO LEFT OVERRIDE est un unicode principalement utilisé pour l'écriture et la lecture de texte Arabes ou Hebreux et qui a donc pour utilité d'inverser l'ordre du sens de lecture des caractère le suivant.

---

2 : RIGHT TO LEFT OVERRIDE et L'extension d'un fichier

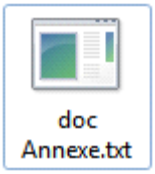
Le spoofing de l'extension d'un fichier sous l'OS MicroSoft Windows que nous évoquons dans cet article est une technique exploitant l'unicode RIGHT TO LEFT OVERRIDE qui aura toujours pour effet d'inverser le sens de lecture des caractères qui le suivent y compris l'extension !

Cet UNICODE dont nous simplifierons l'appellation par RTLO ne se remarque pas du fait que ses caractères et son emplacement sont invisibles.

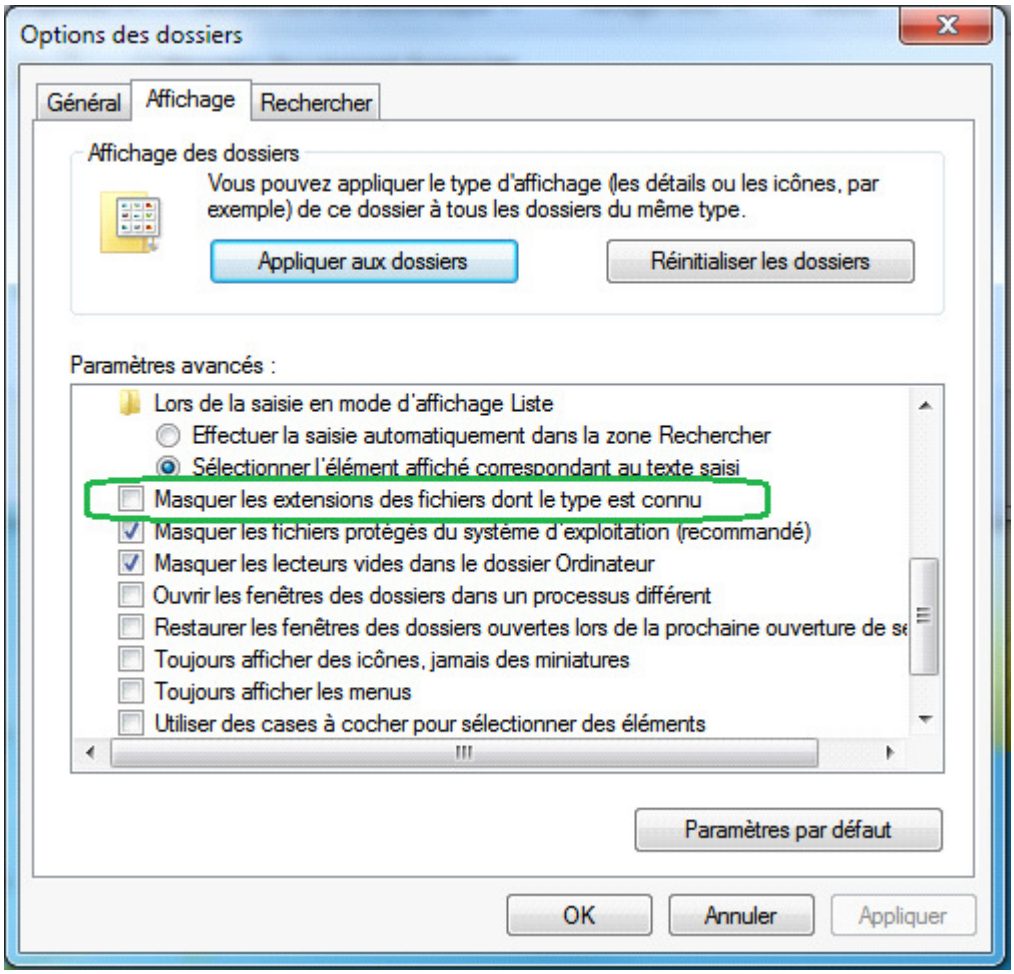
Il va nous servir à inverser le sens de lecture du fichier y compris l'extension de celui-ci tout en gardant les meme types d'exécution.

Exemple:

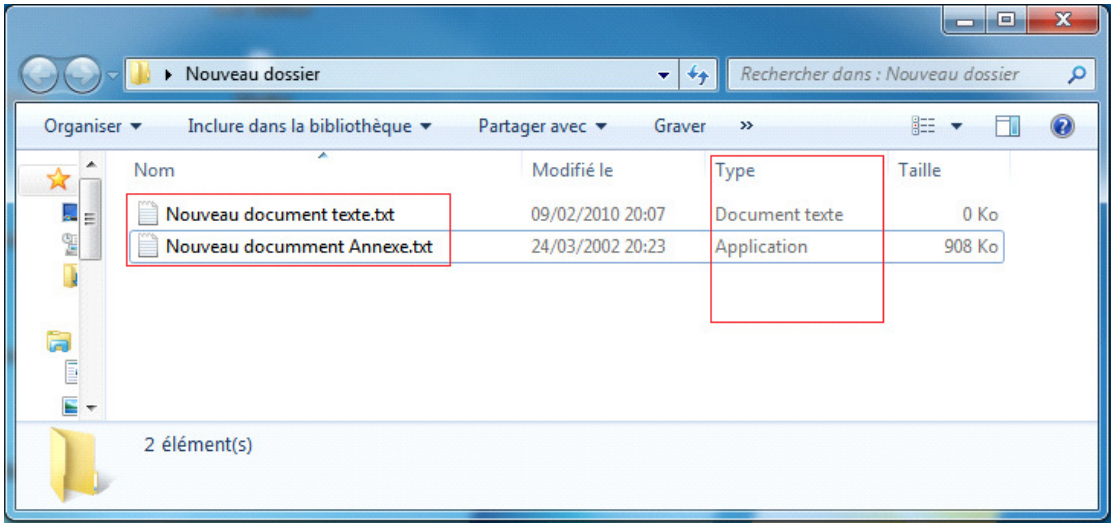
Utiliser une syntaxe de nom comme "Nouveau Document Ann[RTLO]txt.exe" se lirait donc "Nouveau Document Annexe.txt".

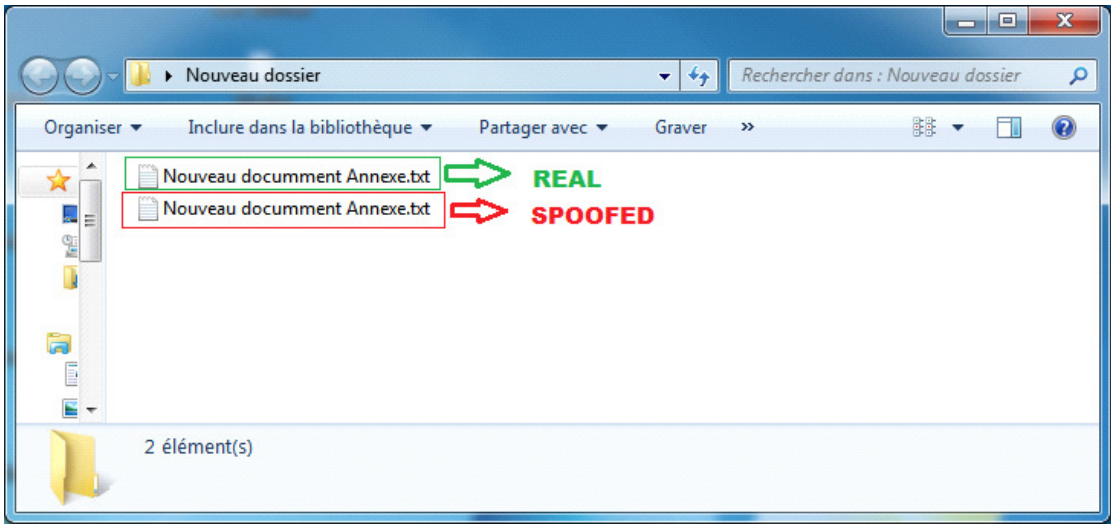


Cela permetrait de dupper les utilisateurs et les inciter à télécharger et exécuter un malware spoofé avec cet unicode tout en croyant ouvrir un type de fichier non risqué, de plus ,malgré que certaines applications le black-list dans le nom du fichier téléchargé (google chrome / firefox[corrigé depuis les MAJ vers: Firefox 3.5.4 & Firefox 3.0.15]/etc) cela n'empeche cependant pas le téléchargement d'archive(.ZIP / .RAR ...), contenant des fichiers aux extensions spoofées . Une technique plutot innovante quand on sait que l'un des principaux points de repaire des utilisateurs est l'extension du fichier qu'ils veulent télécharger ou/et exécuter sans rappeler qu'une grande partie des utilisateurs de Microsoft Windows définissent dans leurs Options l'affichage de l'extension des fichiers dejà connus (nécéssaire pour que le spoof soit réalisable) .



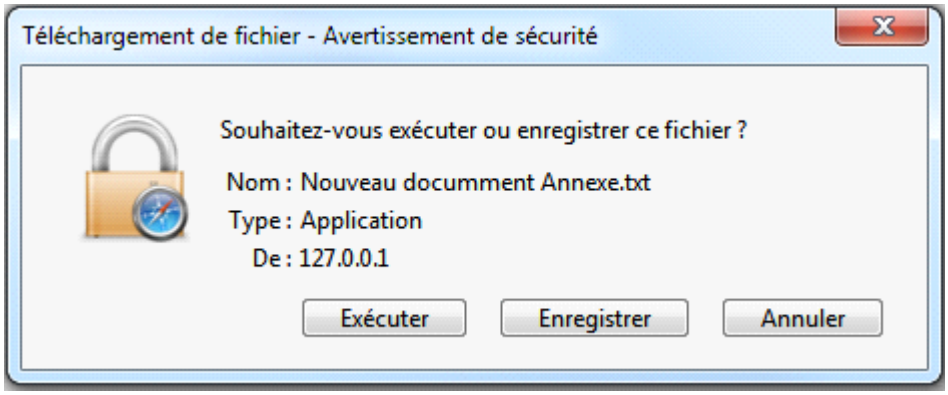
De plus le type de fichier n'apparait pas nécessairement dans les répertoires et cela permet , dans certains cas , une totale ressemblance (sans vérification à effectué) entre une extension original non dangereuse (.jpg / .txt ...) , et le malware spoofé .

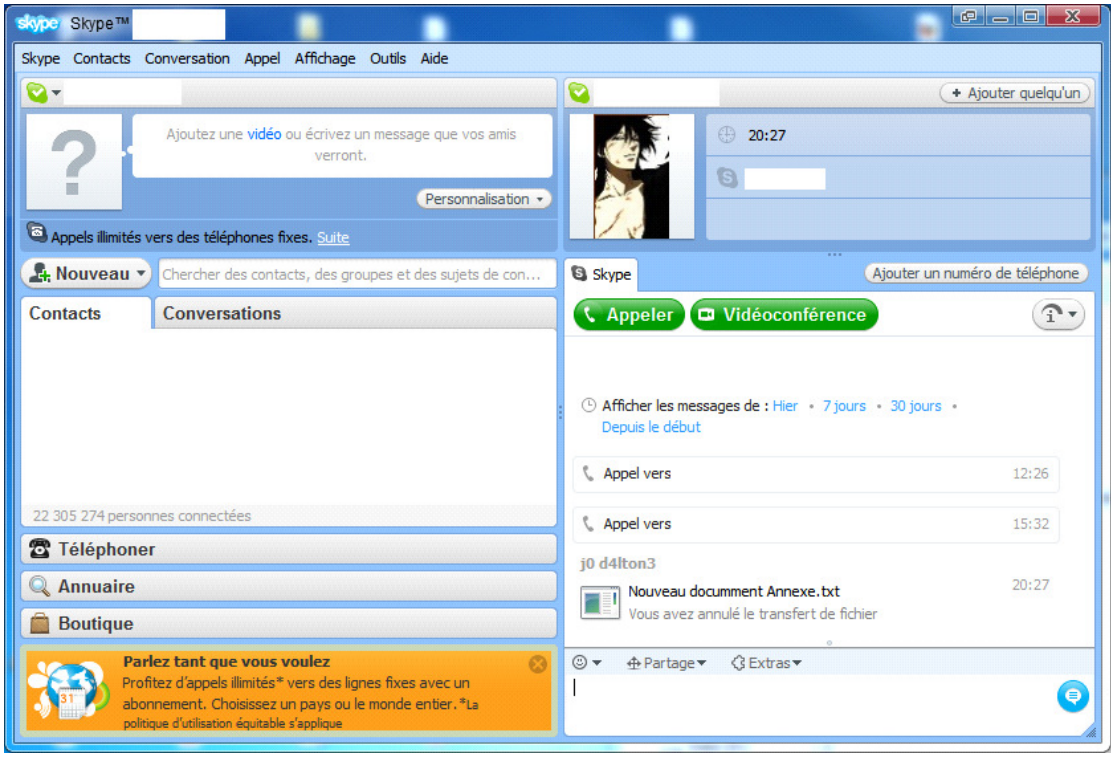


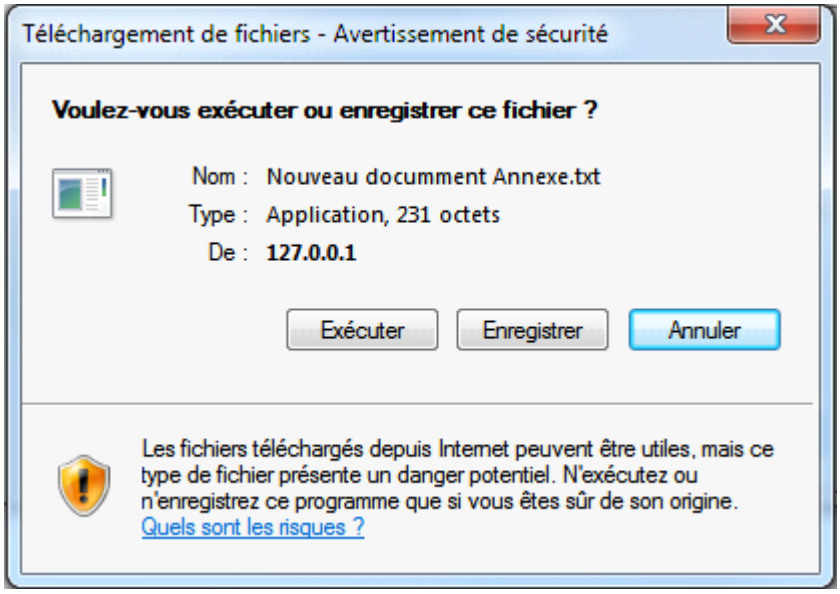


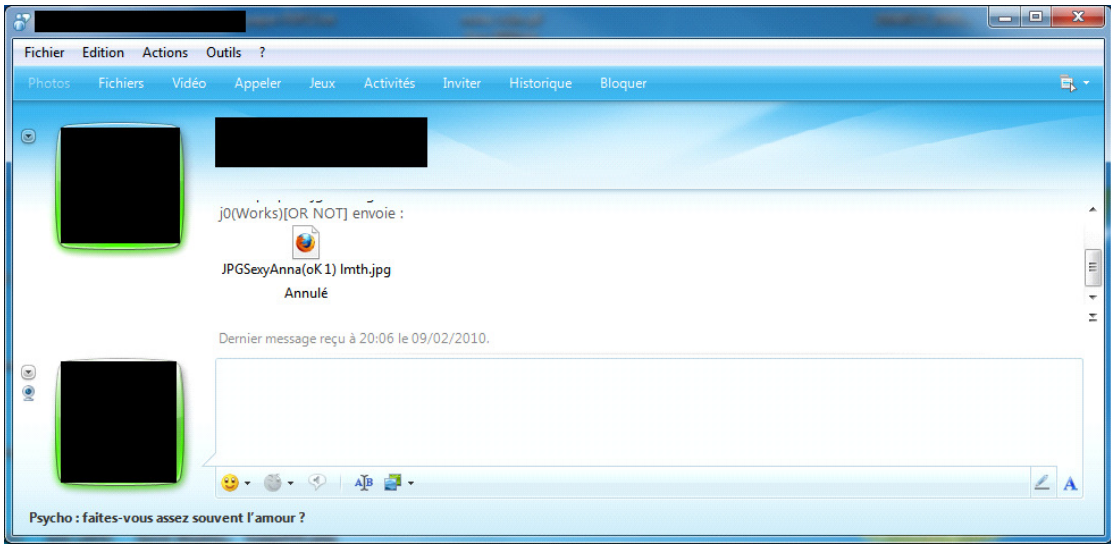
Beaucoup de grands softwares d'acces WEB,discussions en ligne et échanges de données ignorent la dangerosité d'un tel téléchargement ou la négligent et refusent de black-lister cet unicode maglré qu'à l'heure actuelle , les escroqueries en ligne ne sessent de se multiplier et rapporter illégalement de plus en plus d'argent aux réseaux mafieux.

Liste (non-exaustive) : SAFARI / INTERNET EXPLORER / SKYPE / LIVE MESSENGER


Téléchargement de fichier - Avertissement de sécurité
Souhaitez-vous exécuter ou enregistrer ce fichier ?
Nom : Nouveau documment Annexe.txt
Type : Application
De : 127.0.0.1
Exécuter
Enregistrer
Annuler


Skype™
Skype Contacts Conversation Appel Affichage Outils Aide
Ajouter quelqu'un
Ajoutez une vidéo ou écrivez un message que vos amis verront.
Personnalisation
20:27
Appels illimités vers des téléphones fixes. Suite
Nouveau
Chercher des contacts, des groupes et des sujets de con...
Skype
Ajouter un numéro de téléphone
Contacts
Conversations
Appeler
Vidéoconférence
Afficher les messages de : Hier • 7 jours • 30 jours • Depuis le début
Appel vers 12:26
Appel vers 15:32
j0 d4lton3
Nouveau documment Annexe.txt 20:27
Vous avez annulé le transfert de fichier
22 305 274 personnes connectées
Téléphoner
Annuaire
Boutique
Partage
Extras
Parlez tant que vous voulez
Profitez d'appels illimités* vers des lignes fixes avec un abonnement. Choisissez un pays ou le monde entier. *La politique d'utilisation équitable s'applique





*J'ai échangé quelques mails avec l'agence chargée des reports de vulnérabilité sur les applications de MicroSoft et ceux-ci m'ont répondu que leur politique de sécurité ne considère pour l'instant pas cette manipulation comme une négligence de sécurité du fait que le type d'exécution indiqué reste le même.

Conclusion : L'arnaque par téléchargement/envoi de malware avec son extension type spoofé pourrait alors donnée un taux de résultat beaucoup plus élévé : Il est regrétable de ne pas voir Microsoft considérer cette action comme dangereuse.

3 : Falsifier l'adresse URL d'un lien avec RTLO

Les liens hypertexts sur les langages comme HTML peuvent bien évidemment prendre n'importe quelle valeurs et ce malgré la destination sur la quelle il vous dirigeront c'est pourquoi les navigateur web utilisent une "Satus Bar*" affichant l'adresse URL lui étant relatif , au passage de votre curseur par dessus celui-ci.

Une partie des services de messageries instantanées (Tchat public/Espace commentaire/Messagerie instantanée) permettent l'envoi de liens hypertext , mais ceux-ci ne sont transphormés qu'uniquement par l'écriture de l'adresse URL donné.

Impossible d'user des mêmes atouts que le langage HTML et de former des liens maléables.

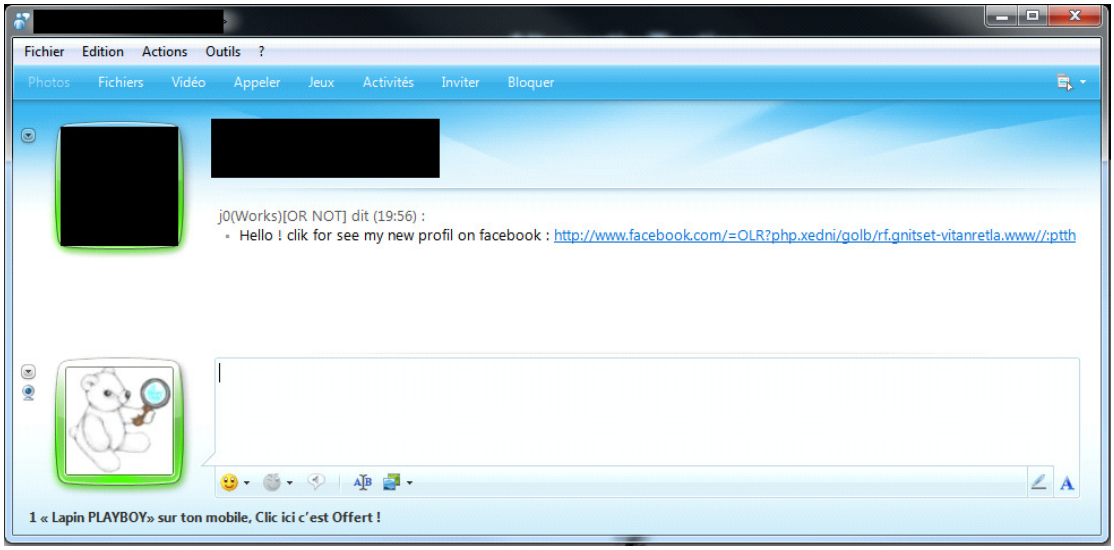
Le RTLO permet là aussi une action sur le sens de lecture d'un lien envoyé ce qui pourait faciliter une possible escroquerie de type SCAM/Phishing.

C'est le cas pour Windows Live Messenger , de plus , ses utilisateurs n'ayant pas pour habitude de recevoir des lien hypertext manipulés , celle-ci pourrait permettre d'augmenter condidérablement le taux de personnes piégées en comparaison d'un lien non officiel de phishing (exemple : www.Faceuboukeu.c0m / www.B4NQ.c0m / ...).

PoC :

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

donnerait comme lien visible :
http://www.facebook.com/moc.etisbewsuoicilam.www//:ptth



Conclusion : la falsification d'un lien peut etre réalisée sur d'autres services que les navigateurs web via les langages web (HTML/JS...) avec la simple utilisation de l'unicode RTLO ce qui équivaut en quelque sorte aux même niveau de dangerosité que la falsification de la "Status-bar" d'un navigateur web.

---

4 : Quelques notes suplémentaires

Notons que certains sites web proposent l'écriture de commentaires et retransforment ou créent automatiquement les liens par leurs adresses de destinations données , là aussi le RLTO inverserait bien sur le sens de lecture du lien affiché ce qui pourait peut être faiblement augmenter le taux de réussite d'une probable escroquerie type phishing/SCAM ,utilisant la même technique précédemment expliquée .

Sans oublier que le sens du contenu de la page le suivant peut être totalement inversé après son injection , ce qui peut constituer une gêne pour les utilisateurs/visiteurs du site concerné...

5 : CONCLUSION FINAL

L'unicode Right to left OverRide permet donc une manipulation risquée pouvant permettre de multiples scénari d'escroquerie visant à la fois les comptes clients des internautes piégés ainsi que l'accès a leurs machines pour ce qui concerne l'execution d'un malware avec son extension "spoofée".

Encores beaucoup d'autres manipulations dangereuses peuvent être effectuées avec celui-ci et nous trouvont très domage que Microsoft Windows ne black-liste pas cet unicode dans le nom de ses fichiers ainsi que sur de mutliples autres actions risquées ou celui-ci peut etre utilisé actuellement.

---

5 : Quelques liens sur le RLO

Info sur le RTLO :

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

Bug réparé par mozilla en Octoble 2009 :

http://www.mozilla.org/security/announce/2009/mfsa2009-62.html

Blog Alternativ-testing.fr:

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

Auteur : Jordi Chancel

Aide sur l'article : 599ème Man