

REMOTE INTERNAL PHISHING AND LOCATION BAR & SSL INDICATOR FALSIFICATION

À Propos :

Ces défauts de sécurité sont abordés dans cet article par Jordi Chancel (Alias j0) & 599eme Man.

Jordi Chancel : neocoderz1@msn.com

599eme Man : flouf@live.fr

501337 Magazine

I. Introduction

Le « Remote Internal Phishing » et le « Location Bar & SSL Indicator Falsification » sont de nouveaux moyens de piéger un utilisateur lambda par le biais d'un navigateur internet. Ces techniques sont évidemment effectuées à distance et peuvent nécessiter diverses méthodes de persuasion et de mise en confiance de l'utilisateur, comme pour une technique d'hameçonnage ordinaire.

En quoi consistent-elles ? Comment fonctionnent-elles ?

Ces nouveaux types de phishing consistent à berner un utilisateur en modifiant certains aspects d'un popup spécifique à un navigateur. Cela est possible grâce à la fonction « `window.open()` » du langage javascript. Cette fonction permet d'ouvrir une fenêtre avec des tailles modifiables, affichage de la barre de location ou non, plein écran ou non ; ce sont ces trois options dont nous allons être totalement dépendant.

Pour le « Location Bar & SSL Indicator Falsification », le but est donc, vous l'aurez compris, d'enlever la barre de location (grâce au paramètre `location=no` de la fonction « `window.open()` ») pour la remplacer par une barre de location "falsifié" affichant les informations relatives à une visite authentique sur le site cible (une image ou un élément flash peut être utilisé pour la falsification de la barre de location et de l'indicateur SSL, mais encore beaucoup d'autres possibilités sont valables). La taille est modifiable pour vous adapter à l'utilisateur ou tout simplement suivant la modélisation du site, etc.

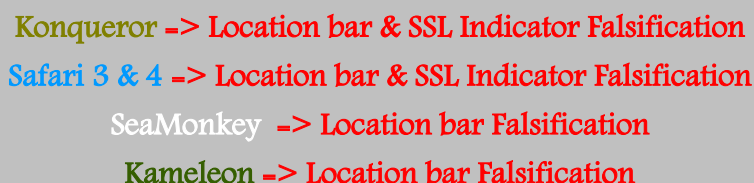
Dans un contexte différent, l'option `fullscreen` va nous permettre de créer une page de « Remote Internal Phishing » dont nous parlerons plus tard.

II. Location Bar & SSL Indicator Falsification

1°) Navigateurs touchés

Tel que l'introduction l'a expliqué, ce type de phishing a une méthode d'exploitation relativement simple à mettre en place. Cependant, certains navigateurs utilisent une politique de sécurité ne permettant pas ce type d'escroquerie (Comme pour les versions supérieures de Mozilla Firefox 3 qui affichent la location du popup même si celui-ci a été lancé avec le paramètre "location=no").

Suite à diverses recherches et tests, nous avons donc établi une liste des navigateurs touchés. En voici un aperçu :



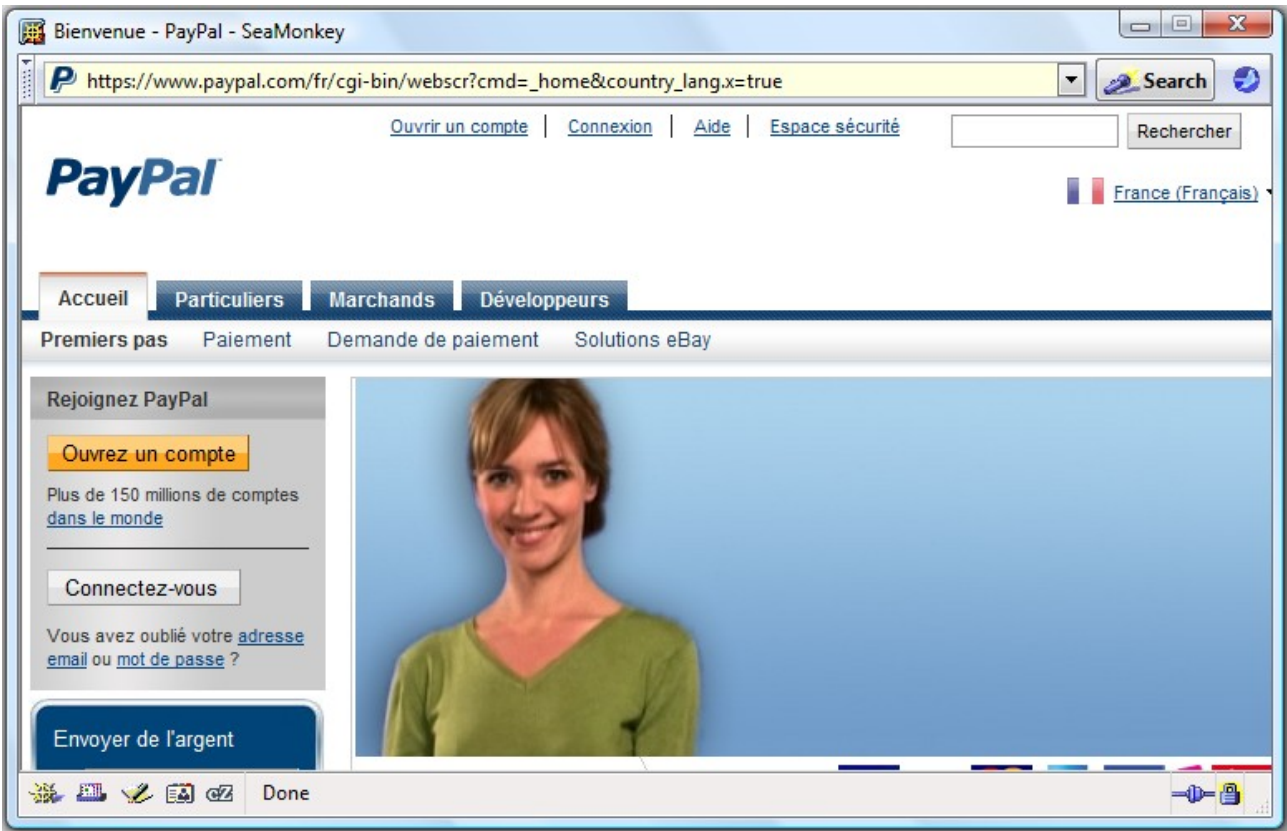
Konqueror -> Location bar & SSL Indicator Falsification
Safari 3 & 4 -> Location bar & SSL Indicator Falsification
SeaMonkey -> Location bar Falsification
Kameleon -> Location bar Falsification

Vous remarquerez que sur certains navigateurs l'indicateur SSL peut être aussi falsifié permettant donc une reproduction plus fidèle des sites cibles possédant un certificat de connections sécurisé, ce qui permet donc aussi de rendre l'escroquerie plus crédible aux yeux d'un utilisateur lambda.

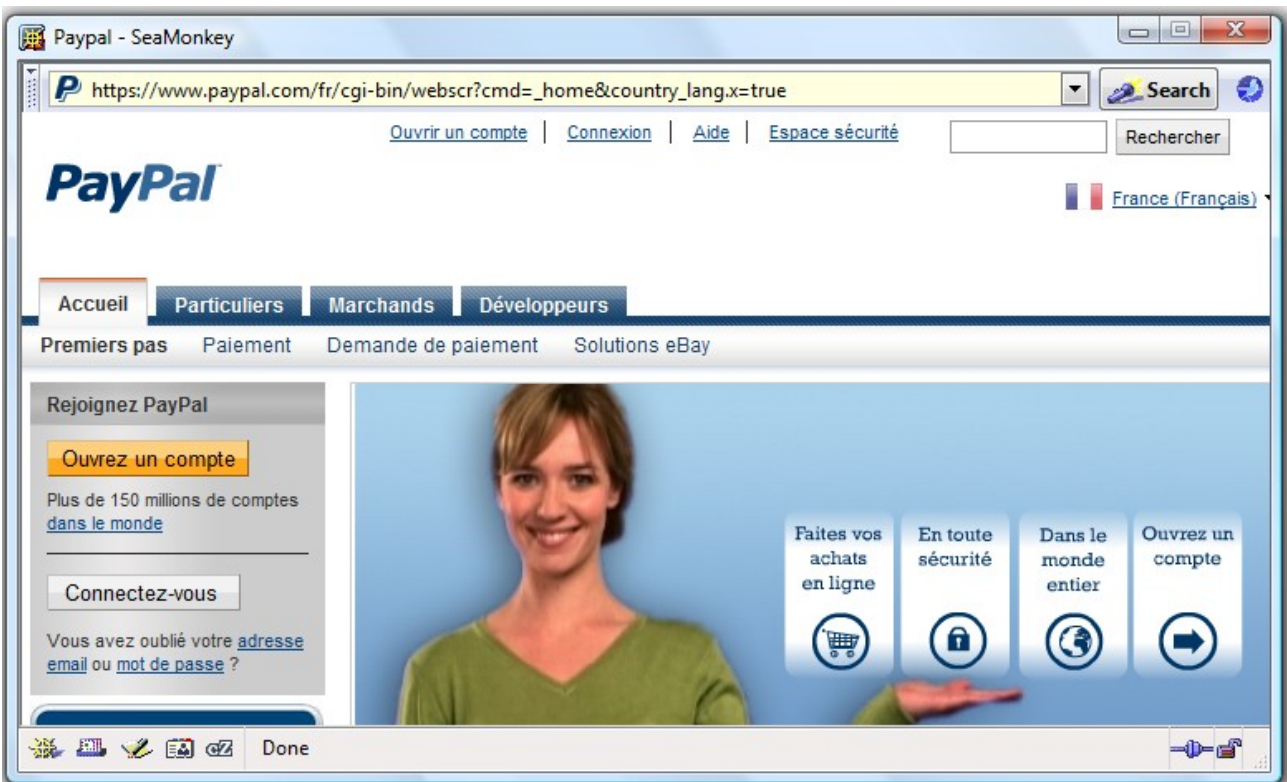
Remarque : Sous le Navigateur Konqueror, la barre d'état peut être également falsifiée ce qui permet de reproduire totalement l'indicateur SSL du fait que celui se trouve aussi bien dans la barre d'état que dans la barre de location. Si le site visé utilise un certificats de connections sécurisé, cette manipulation rend vraiment l'escroquerie plus discrète et plus crédible aux yeux d'un utilisateur lambda.

Voici donc une comparaison entre deux popup, dont la location de l'un est réellement le site cible et où l'autre utilise une barre de location falsifié (Navigateur SeaMonkey) :

SeaMonkey avec une barre de location réel :



SeaMonkey avec une barre de location falsifié :



Cette négligence de sécurité ouvre aussi la voie sur la possibilité d'utiliser un "FrameWorks orienté Phishing" dont je vais vous expliquer les principes de bases :

Rappelons pour commencer que si la barre de location peut être falsifiée par diverses méthodes, il n'est alors pas exclus de reproduire les fonctions originales d'une barre de location authentique sur les éléments servant à la falsifier, c'est-à-dire que les fonctions utilisées par une véritable barre de location peuvent être aussi utilisées de façon détournée par les éléments utilisés pour la falsification voulu (Affichage du site demandé, etc).

Certains se demanderons évidemment en quoi cette possibilité peut nous être utile ?

La réponse est simple, puisqu'il est alors possible d'écrire l'adresse d'un site dans la fausse barre de location et de pouvoir ainsi le visiter, sans remarquer de différences notoires avec une fenêtre authentique du navigateur comportant une véritable barre de location, il est alors possible de se servir de l'adresse URL demandé avec un code chargé d'aller chercher la source de ce même site (utilisation de PHP/ASP...), de le mélanger avec divers script permettant l'interception des informations voulues (Keylogger Javascript par exemple), avant son affichage dans l'iframe prévue à la visite du site demandé (L'iframe est placé sous la fausse barre de location et ne se remarque pas en comparaison d'un popup classique affichant le contenu d'un site).

Il serait alors possible de voler les données personnelles relatives au site demandé dans la barre de location falsifié quand l'utilisateur les soumet par écriture, ou autre, tout en lui laissant le choix d'écrire l'adresse du site qu'il voudrait visiter.

Une solution innovante quand on sait que les techniques d'hameçonnage traditionnels se basent sur la falsification d'un site bien précis alors que dans ce cas l'utilisateur est libre de sa navigation tout en nous permettant l'interception des données voulues et entrées par celui-ci sur les sites qu'il visite.

2°) Attaque basique : exploitation

Nous allons maintenant passer de la théorie à la pratique avec une forme d'exploitation basique c'est-à-dire : un popup d'une taille conforme avec l'image simulant la barre de location du navigateur affichant l'adresse du site ciblé et l'iframe chargé de contenir la contrefaçon de ce même site.

Dans cet exemple nous nous servirons donc d'une page de paypal contrefaite avec une barre de location falsifié :

```
<!-- Index.htm, page où la victime va devoir ouvrir le popup.  
Ce popup va ouvrir une page de taille 400x753 sans barre de location -->  
  
<a href="Paypal.htm"  
onclick="javascript:window.open(this.href,'Popup','height=400,width=753,scrollbars=no,location=no,fullscreen=no');return false;">Popup</a>
```

```
<!-- Paypal.htm, cette page affichera votre image de la barre de location convenant au site  
ainsi que la page de phishing. -->  
  
<div  
style="position:absolute;width:500px;height:25px;background:#C0C0C0;border:10  
px;left:0px; top:0px; z-index:1;"></img></div>  
  
<br ><br >  
  
+ IFRAME POINTANT VERS LA PAGE CONTREFAITE DU SITE (ici  
paypal.com).
```

D'après les deux screens d'exemple ci-dessus, vous pourrez déjà constater que cette méthode nécessitera :

- Une barre de location falsifiée du navigateur avec laquelle la victime va être piégée.
- Utiliser un popup avec des dimensions adaptées (Divers critères entrent en jeu pour utiliser une taille X plutôt qu'une taille Y, libre à vous de définir qu'elle sera la meilleure solution pour le site concerné).
- Une page contrefaite du site cible avec divers dispositifs permettant l'interception des données envoyées (Keylogger en Javascript par exemple).

Les pages sont prêtes, il ne vous reste plus qu'à utiliser une méthode de persuasion visant à convaincre l'utilisateur de se connecter sur le site cible par l'intermédiaire de votre page piégé.

II. L'option « FullScreen »

1°) Quoi de plus ?

L'option « Fullscreen » est une option de la fonction window.open. Nous allons nous y intéresser, mais uniquement sous Konqueror qui est le seul navigateur à réellement « fullscreené » la page dans les conditions adéquates qui vont alors permettre une technique d'hameçonnage visant les applications internes de la machine d'un utilisateur ciblé. Cette technique a été baptisée : « Remote Internal Phishing ».

2°) Remote Internal Phishing

Le Remote Internal Phishing est une technique d'hameçonnage visant les applications internes de la machine d'un utilisateur ciblé (applications de services mail, de messageries, de connexion à un jeu, etc). Cette nouvelle méthode via Konqueror est une des plus étonnante technique de phishing du fait qu'elle ne vise pas exclusivement les applications web ou autres applications utilisant le navigateur comme moyen de connexion. Cette technique nécessite cependant une interface plus ou moins avancée permettant donc une cohérence entre les applications internes visées et celle qui seront utilisées par l'utilisateur. Il y a donc de multiples scénarios d'escroquerie possible.

La ressemblance est vraiment poussée, il suffit donc d'inciter un utilisateur à entrer ses informations personnelles relatives à l'application interne visée et le tour est joué.

Exemple :

```
<!-- Index.htm, page où la victime va devoir ouvrir le popup.  
Ce popup va ouvrir une page fullscreené -->  
<a href="page.html"  
onclick="javascript:window.open(this.href,'Popup','height=400,width  
h=753,scrollbars=no,location=no,fullscreen=yes');return  
false;">Popup</a>
```

```
<!-- Page.html qui sera ouverte en  
fullscreen, elle comportera l'élément de  
falsification de l'application interne à  
piéger avec un dispositif permettant  
d'intercepter les informations... -->
```

...

Si ces explications vous paraissent encore vagues, une démonstration vidéo est à votre disposition :

[Video](#)

III. Conclusion

Le « Remote Internal Phishing » et le « Location Bar & SSL Indicator Falsification », par Jordi Chancel et 599eme Man, sont donc des nouvelles méthodes de phishing offrant de multiples avantages sur la discrétion ou/et les possibilités de ce type d'escroquerie. Pour le Remote Internal Phishing les applications visées ne se limitent alors plus uniquement aux applications web, mais aussi aux applications internes qu'utilise la machine de l'utilisateur ciblé.

Rappel des deux méthodes traitées dans cet article :

- Le « Location Bar & SSL Indicator Falsification » permettant donc de tromper la victime grâce à une falsification de la barre de location et de l'indicateur SSL d'un navigateur, dans le but de garantir un plus grand taux de réussite d'utilisateurs piégés et d'augmenter la discrétion de ce type d'escroquerie.
- Le « Remote Internal Phishing » permettant l'hameçonnage d'application interne via un navigateur, c'est-à-dire : des applications utilisées sur la machine de l'utilisateur ciblé.