

# *Génération Connectés*

pour le meilleur...



et pour le pire





# Contenu du chapitre GC-Sec

## 1<sup>ère</sup> sensibilisation à la sécurité

- Menaces sur vos connexions

Mél

- Scam et escroqueries par courrier

- Hameçonnage simple (envoi vers sites frauduleux)

Web

- Attaques via des sites Web vulnérables (XSS, CSRF...)


# Escroqueries simples... mais lucratives

## *Escroqueries anciennes démultipliées par le mél*

- Scam (arnaque « nigériane »): une veuve africaine vous propose de partager son argent
  - « Lettres de Jérusalem », Vidocq 1836
  - « Prisonnière espagnole » (XVI<sup>e</sup> siècle)
- Message d'un de vos contacts se retrouvant démuné pendant un voyage
  - Utilise des couples Expéditeur-Destinataire de courriels récupérés

*Escroqueries non techniques mais facilement rentables, même avec taux de succès < 1/1000*

# Escroquerie pseudo-technique

- Vous recevez un mail prétendant que votre compte a été piraté !
- Le pirate aurait pris possession de votre ordinateur, dont sa caméra. Il menace de révéler des contenus compromettants et demande le versement d'une rançon
- **Rien n'est vrai dans ce message !** Il est envoyé au hasard.
-  **Gardez votre mot de passe strictement confidentiel** et choisissez-le robuste - en cas de doute, n'hésitez pas à le changer.
  - Sinon vous vous exposez à ce que ce soit possible.

# Hameçonnage (phishing)

- Inciter une victime à consulter un site contrôlé (+/-) par l'attaquant
  - En général par l'envoi d'un message contenant une URL (lien)
  - Par exemple pour lui soutirer des informations

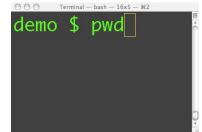
- Exemple typique:

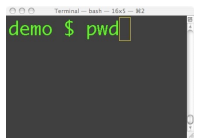
- Message paraissant venir de votre banque (ex. Crédit Lyonnais, LCL) indiquant « Pour garder l'accès à votre compte, veuillez vérifier vos coordonnées sur lcl-banque.fr »
- *Et alors ? Quel problème y a-t-il à s'y connecter ?*



# Hameçonnage vers site frauduleux

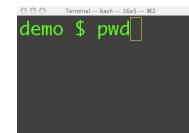
- Même une adresse légitime lcl.fr peut-être dangereuse
  - Vous lisez lcl.fr, mais l'ordinateur se connectera à pirate.ly
    - HTML: `<a href=«pirate.ly»> lcl.fr </a>`
    - Vérifiez bien l'adresse en passant avec la souris
  - Il pourrait aussi se connecter à 1cl.fr au lieu de lcl.fr
  - Ce peut être encore plus vicieux avec des caractères qui ne s'affichent pas ou paraissent exactement les mêmes mais correspondent à un alphabet non latin
    - Ex: [www.paypal.com](#) au lieu de [www.paypal.com](#)  
Caractère « a » du cyrillique
  - L'annuaire DNS pourrait avoir été « empoisonné » pour qu'il donne l'adresse IP d'un site pirate au lieu de la vraie adresse IP de lcl.fr





# Exemple d'hameçonnage bien fait

- Le programme fidélité de la SNCF (carte Voyageur)
  - Lancé au moment où la SNCF en faisait la promotion
  - Avec un mél quasi copié de celui de la SNCF
  - Renvoyant sur le site [sncf-voyages.info](http://sncf-voyages.info)
  - ... en fait site enregistré juste quelques jours avant auprès d'un gestionnaire (registrar) en Australie au nom d'une adresse en Californie...
- Quelques exemples copiant Apple
- Et un hameçonnage débile...



De Voyages-sncf.com <noreply@voyages-sncf.com> ☆

↳ Répondre

« Répondre à tous ▼

→ Transférer

Annuler

04/04/2014 à 13:31

Sujet **Rappel : OFFRE TGV - Carte Voyageur SNCF gratuite + 50 %**

Pour Roland Groz ★



Bonjour ,

La SNCF a enfin dévoilé son nouveau programme de fidélité avec la carte Voyageur. Une carte gratuite qui donne accès à des réductions supplémentaires sur les billets de train, des avantages, des bons plans... Pour voyager moins cher, il faudra la posséder, surtout si vous prenez le train régulièrement. Elle est d'autant plus intéressante qu'elle peut être associée à d'autres cartes de réduction !

Cette nouvelle carte annule la carte qui vous a été envoyée précédemment. avec cette carte vous obtenez une réduction de 50% sur tous les trajets.

**Pour confirmer et continuer l'achat de votre carte veuillez :**

[Inscrivez-vous en ligne gratuite.](#)

cordialement.

**N.B: Vous recevrez cette nouvelle carte de voyageur à votre domicile par courrier postal dans un délai de 5 à 10 jours.**



<http://programme-voyageur.sncf-voyages.info/tgv/>



## Whois Search Results

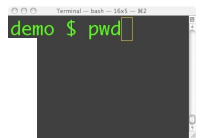
Search again (.aero, .arpa, .asia, .biz, .cat, .com, .coop, .edu, .info, .int, .jobs, .mobi, .museum, .name, .net, .org, .pro, or .travel) :

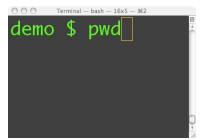
- ☒ Domain (ex. internic.net)  
☐ Registrar (ex. ABC Registrar, Inc.)  
☐ Nameserver (ex. ns.example.com or 192.16.0.192)

Domain Name:SNCF-VOYAGES.INFO  
Domain ID: D52194680-LRMS  
Creation Date: 2014-03-30T16:03:45Z  
Updated Date: 2014-03-30T16:03:47Z  
Registry Expiry Date: 2015-03-30T16:03:45Z  
Sponsoring Registrar:Melbourne IT, Ltd (R141-LRMS)  
Sponsoring Registrar IANA ID: 13  
WHOIS Server:  
Referral URL:  
Domain Status: clientTransferProhibited  
Domain Status: serverTransferProhibited  
Registrant ID:A139572874465680  
Registrant Name:Rodriguez Carlos  
Registrant Organization:Private Registration US  
Registrant Street: PO Box 61359  
Registrant City:Sunnyvale  
Registrant State/Province:CA  
Registrant Postal Code:94088  
Registrant Country:US  
Registrant Phone:+1.5105952002  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email:contact@myprivateregistration.com  
Admin ID:B13961777491174  
Admin Name:Admin PrivateRegContact  
Admin Organization:Private Reg US  
Admin Street: PO Box 61359  
Admin City:Sunnyvale  
Admin State/Province:CA  
Admin Postal Code:94088  
Admin Country:US  
Admin Phone:+1.5105952002  
Admin Phone Ext:  
Admin Fax:  
Admin Fax Ext:  
Admin Email:contact@myprivateregistration.com  
Billing ID:B13961777491175  
Billing Name:Bill PrivateRegContact  
Billing Organization:Private Reg US  
Billing Street: PO Box 61359  
Billing City:Sunnyvale  
Billing State/Province:CA  
Billing Postal Code:94088  
Billing Country:US  
Billing Phone:+1.5105952002  
Billing Phone Ext:  
Billing Fax:  
Billing Fax Ext:  
Billing Email:contact@myprivateregistration.com  
Tech ID:A139572874465681  
Tech Name:Admin PrivateRegContact

← 30/3/2014 soit 5 jours avant l'envoi de l'hameçon

← Site déclaré en Californie, rien à voir avec la SNCF





# Hameçonnage vers site frauduleux

- Même un hameçonnage grossier peut réussir, auprès de victimes naïves ou trop peu soupçonneuses... ou trop promptes à cliquer
  - Comme les arnaques nigérianes: il suffit qu'une victime sur 10000 ou même sur un million se laisse berner
- Pour rire un peu, allez voir:
- <https://www.cigref.fr/archives/entreprise2020/cybersecurite-les-4-films-de-la-hack-academy-cigref/>  
(site officiel garanti sans danger 😊)
  - > *Défiez Willy et les autres candidats de la Hack Academy.*

# Attaques croisées

- Vous vous connectez à un site légitime, via une connexion sécurisée
- Mais un pirate fait exécuter à votre ordinateur des actions nocives via ce site
  - Sans que vous en ayez conscience (non visible de l'utilisateur)
- Parmi le top10 des attaques sur sites Web:
  - XSS (Cross-Site Scripting)
  - CSRF (Cross-Site Request Forgery) Falsification de requêtes Intersites

# XSS

Oscar



Dépose un *commentaire* sur un forum  
ou une *photo* sur un site d'images



Ce *commentaire* anodin  
contient de façon cachée un  
code malicieux  
Javascript



CommentCaMarche.net  
StackOverflow.com

Alice consulte  
cette page

Alice



Elle verra le *commentaire*  
mais son navigateur  
exécutera aussi le code  
malicieux, à son insu



# XSS

- Exemples de façon de cacher du code malicieux

- Ce qu'on voit (image tux.bmp)



- Codage machine dans la page en HTML:

- `<IMG "src=tux.bmp" onmouseover="javascript:`



- `...">`

- Comment a fait Oscar pour tromper le site ?

- Il a donné un nom bizarre à son image: au lieu de tux.bmp comme nom du fichier, il a écrit:

- `tux.bmp "onmouseover="javascript: ... "`

- Code malicieux: va capturer des cookies, se connecter au site d'Oscar, lui envoyer des infos...

# XSS suite

- Normalement les sites filtrent (« sanitization ») les textes saisis par les déposants
- Mais:
  - Il y a beaucoup de possibilités de tromper les sanitizers
  - Les programmeurs de sites ne sont pas toujours attentifs, et les codes des sites contiennent des centaines de formulaires et des milliers de lignes de code
  - La majorité des sites Web ont des vulnérabilités XSS

# XSS et hameçonnage

- Oscar n'a qu'à inciter Alice à se connecter au site légitime
  - Par un hameçonnage
- Alice, même méfiante, pourra vérifier: le site est bien légitime
- Conclusion
  - Alice doit s'en remettre au serveur (Flickr, eBay, Amazon etc) pour combler ses failles XSS
  - Ou supprimer l'interprétation de Javascript dans son navigateur... mais beaucoup de sites ne fonctionneront plus