Le phishing

Etat des lieux

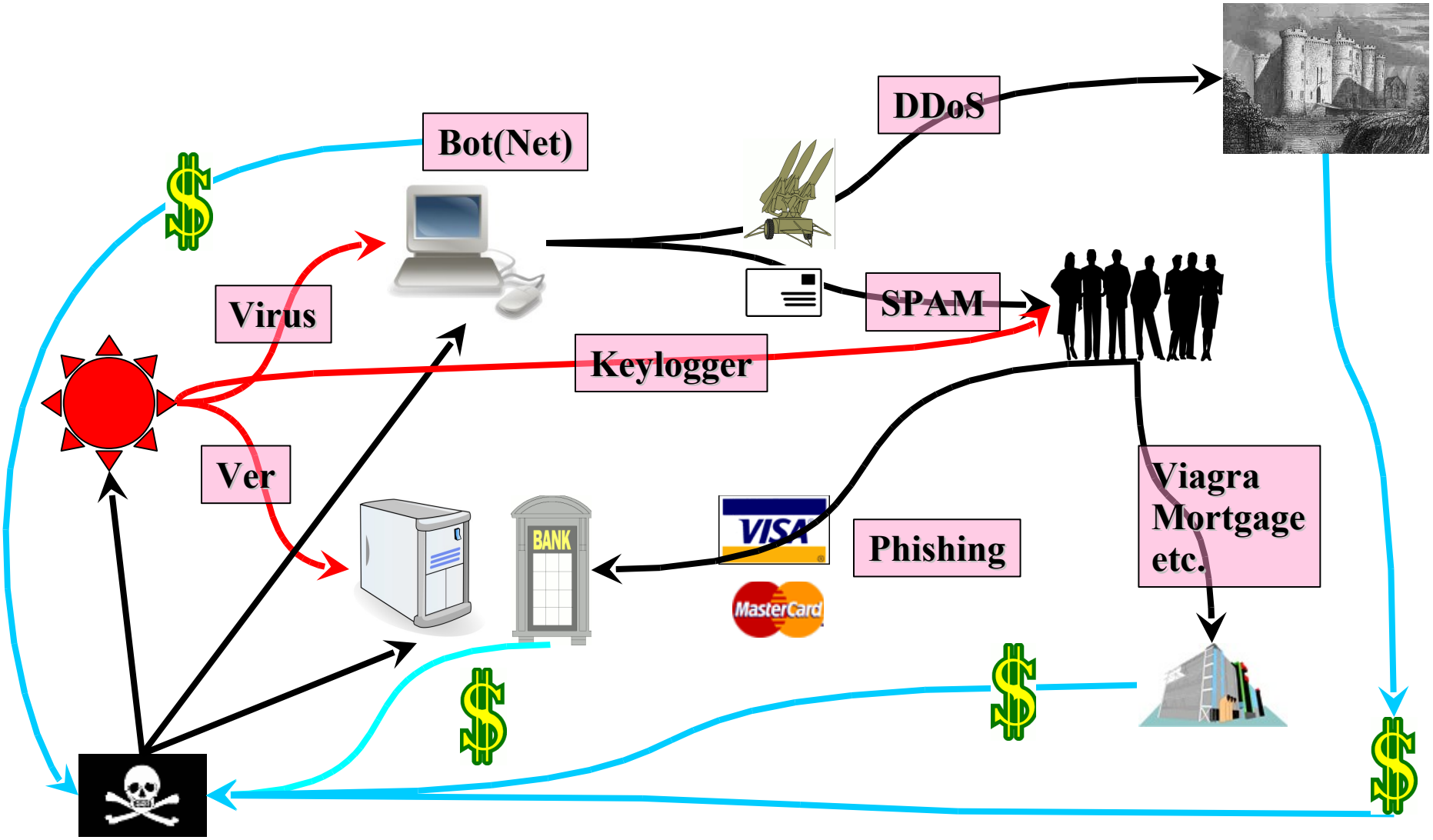
Contexte

- Internet est à l ’image du monde dit réel
  - avec ses gens « bien »
  - avec ses délinquants
- A la différence que pour les déliquants
  - les actions se font à distance
  - sur une très large population
  - avec une très grande rapidité
  - sans implication psychologique
  - par des procédés techniques incompréhensibles

Contexte

- Gagner de l ’argent rapidement
  - Vendre n’importe quoi (SPAMs)
  - Vendre des réseaux de vente (Botnet) : « 10000 infected pc's for 25$ », avec l'aide de « mules »
  - Racketter (DDoS)
  - Escroquerie
    - SCAM
  - Revendre des objets virtuels (MMORPG)

Schéma « financier »



Définition du phishing

- Obtenir des informations directement ou indirectement moneyables
- Mélange de fishing (pêche) et phreaking (piratage téléphonique)
- Aussi appelé « hameçonnage »

Mécanisme

- Envoi d ’un mail « piégeur »
- Présentation d ’un site web d ’apparence connue
- Mécanismes psychologiques
  - Paresse intellectuelle
  - Peur
  - Envie
- Mécanismes techniques (en appui de mécanismes psychologiques)

Cibles

- Clients de banques
  - d ’abord américaines
  - puis européennes
- Clients de sites monneyables
  - Site d'enchères (eBay, Yahoo, etc.)
  - Site de paiement en ligne (Paypal)
- Plus récemment : le trésor public américain

Exemple BNP


BNP PARIBAS
Cher client de **BNP Paribas**,
Le département technique de BNP Paribas procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.
Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.
http://www.secure.bnpparibas.net/banque/portail/confprocedure.asp
Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

Exemple Société générale

Cher client de **SOCIÉTÉ GÉNÉRALE**

Le département technique de Société Générale procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

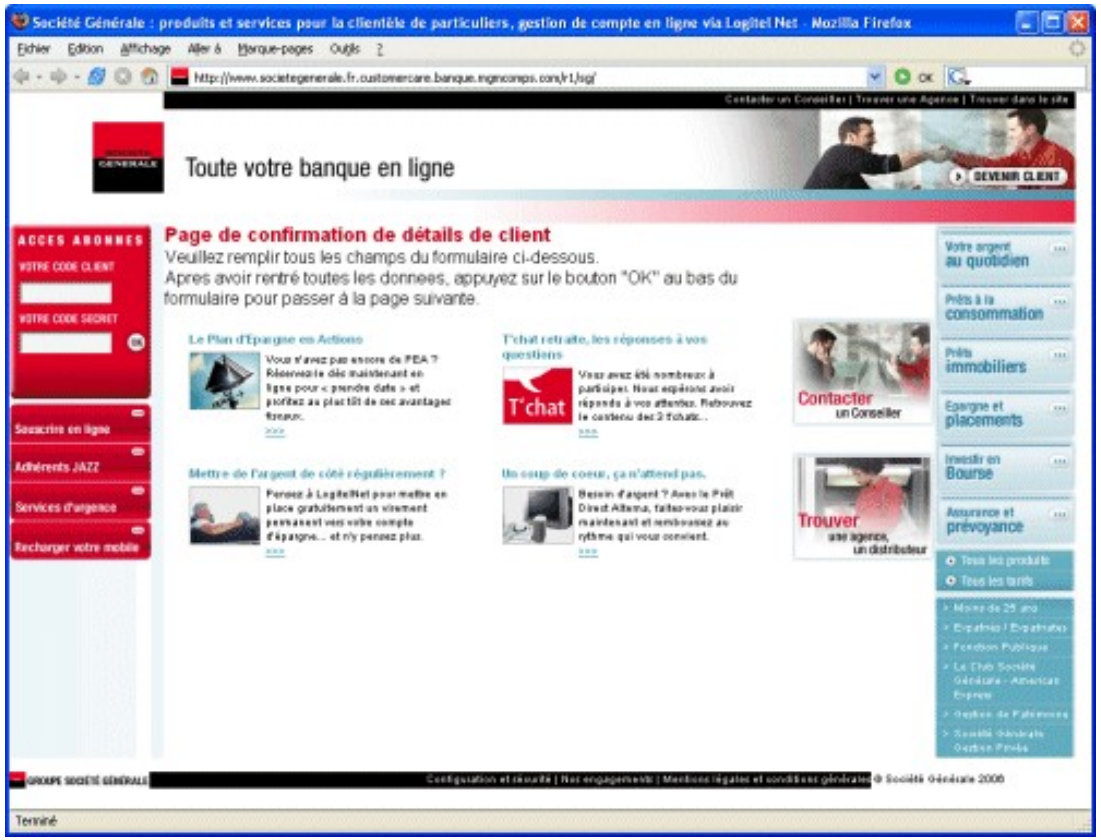
Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.societegenerale.fr/customercare/banque/confprocedure.asp

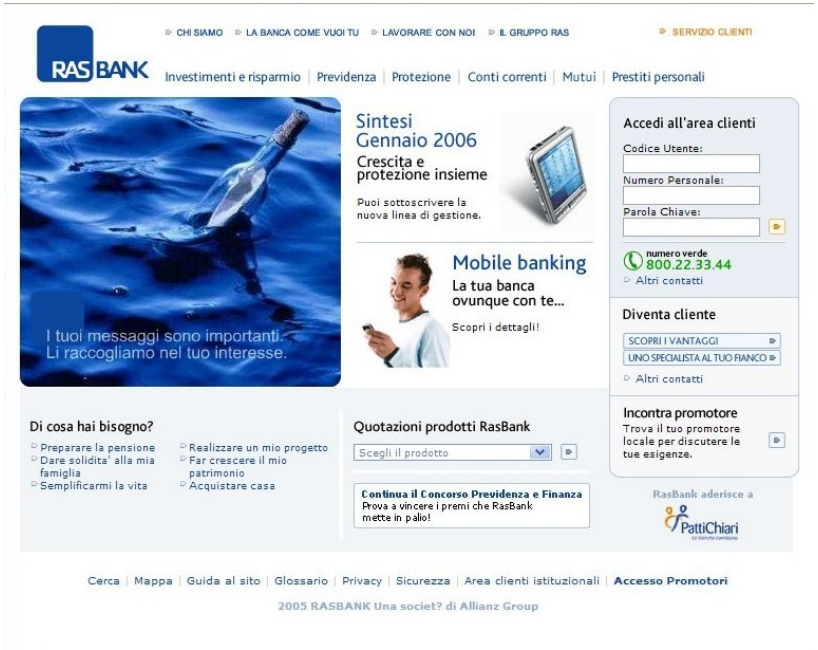
Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

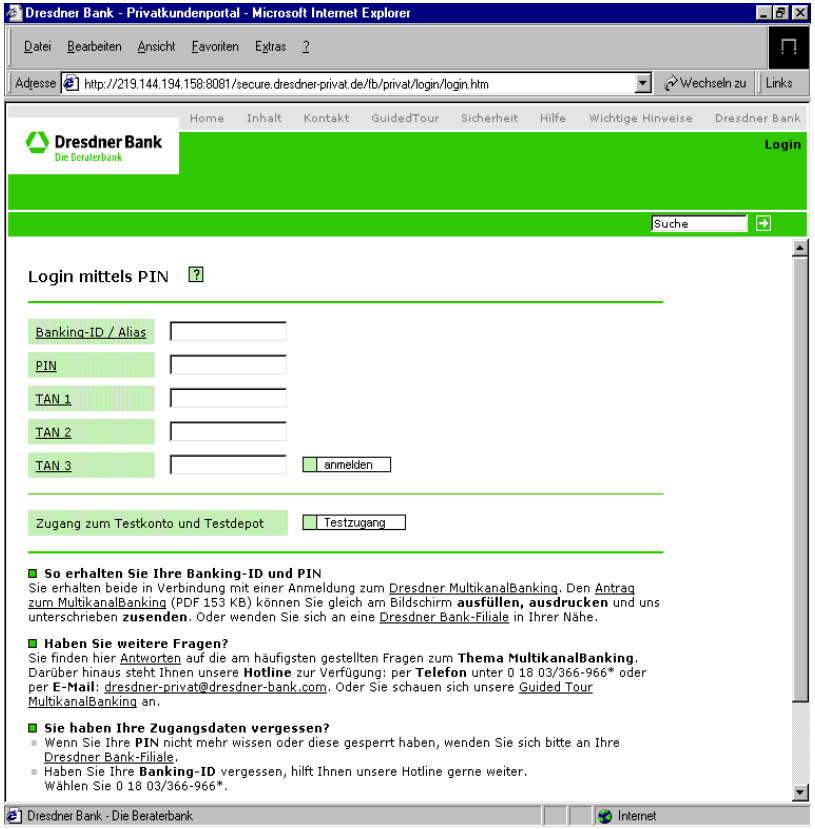
Exemple Société générale

www.societegenerale.fr.customercare.banque.xxx.com/r1/sg/

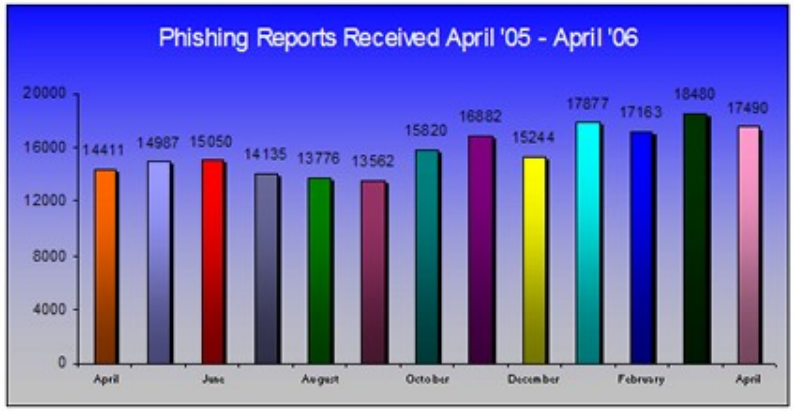


Mais l'Europe entière est touchée





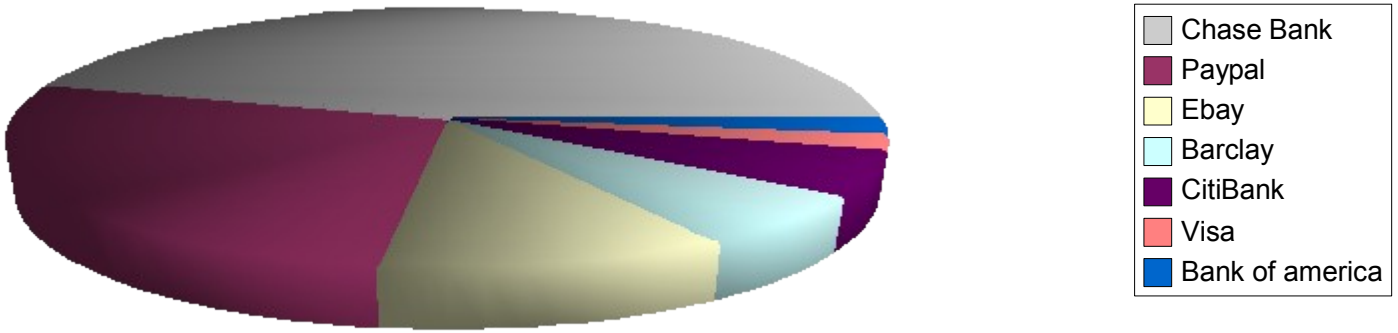
Statistiques



- 10000 sites
- 5 jours de vie
- Vol de x Milliards $
- Défense 800 millions $ en 2008

Quelques statistiques

Proportion de Phishing



Septembre 2006

- Chiffres de septembre 2006
  - 154 marques
  - 23 670 campagnes de phishing
  - 14 191 sites de phishing

Avantages

- Rapide
- Peu de risque
- Taux de rentabilité excellent (0,01 %)
  - En 2004 : 20% ont cliqué
  - En 2004 : 1,3% ont donner des informations
- Large audience

La lutte

- Educative
- Administrative
- Technique

La lutte éducative

- On explique aux utilisateurs les risques
- On explique ce à quoi il faut faire attention
  - Les banques font beaucoup d'effort

Faiblesses de la lutte éducative

- Marcus J Ranum : les 6 plus idiotes idées de la sécurité
- Les techniques changent
  - Regardez le cadenas => contourné
  - Regardez l'url (IP) => contourné
  - Regardez le nom de domaine => contourné
  - Les banques n'envoient jamais de mail => faux

Faiblesses de la lutte éducative

- Jouons sur la psychologie
  - https://www.mabanque.cm@site.dupirate.com
  - https://www.lc1.fr (le second L est le chiffre 1)
  - https://www.mabanque.tg.lite.dupirate.com
- Jouons avec la technique
  - les pop-up
  - les frames et Iframes
  - http://cri.univ-tlse1.fr/demonstrations/phishing

La lutte éducative : on arrête ?

- Non !
- Culture du doute : Est-ce normal ?
  - Fautes d ’orthographe
  - Banque qui perde des identifiants
  - Recevoir
- Information sur l ’arnaque en question

La lutte administrative

- Les registrars vérifient les demandes de domaines (AFNIC)
- Les NIC bloquent les domaines « pathogènes »
- Les FAI bloquent les IP « pathogènes »

Faiblesses de la lutte administrative

- Connaître toutes les spécificités d ’un pays
  - Nom de société,
  - Vocables
  - Clavier !
- Délai pour le blocage
  - Détection
  - Vérification
  - Propagation des blocages

La lutte technique

- Réception
- Utilisation
- Serveurs

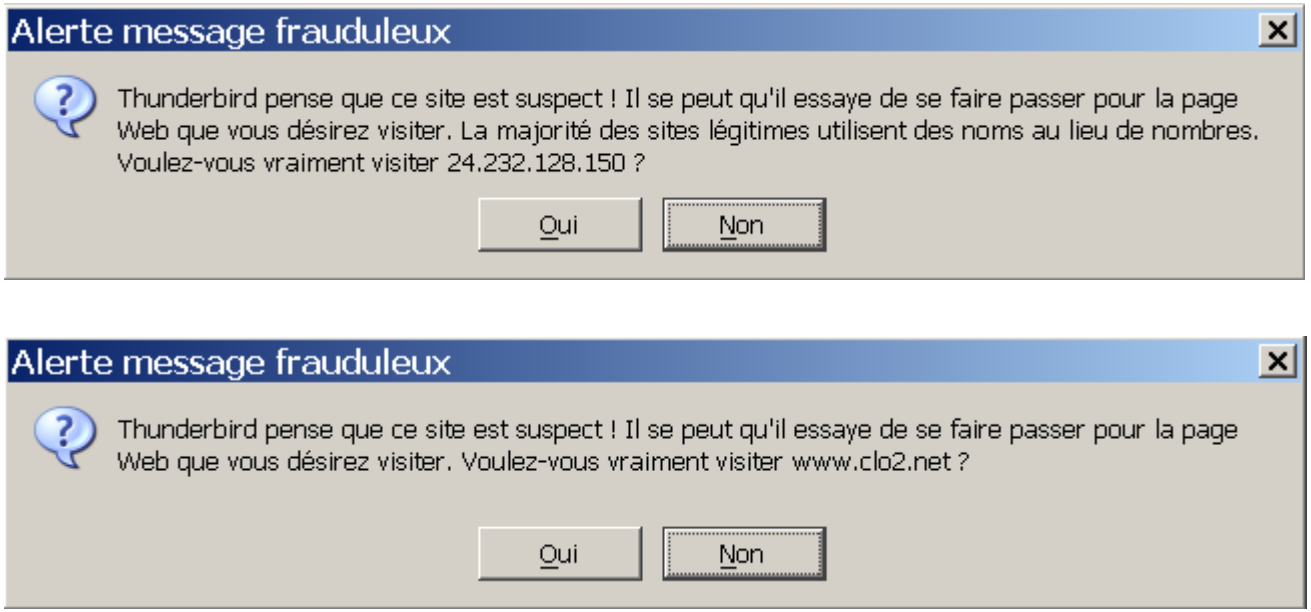
La lutte technique en réception

- Phishing => SPAM
- Même technique que les SPAMs
  - Greylisting
  - RBL (et SURBL)
  - Bayésien / Chaines markoviennes
  - Détection d ’incohérence URL

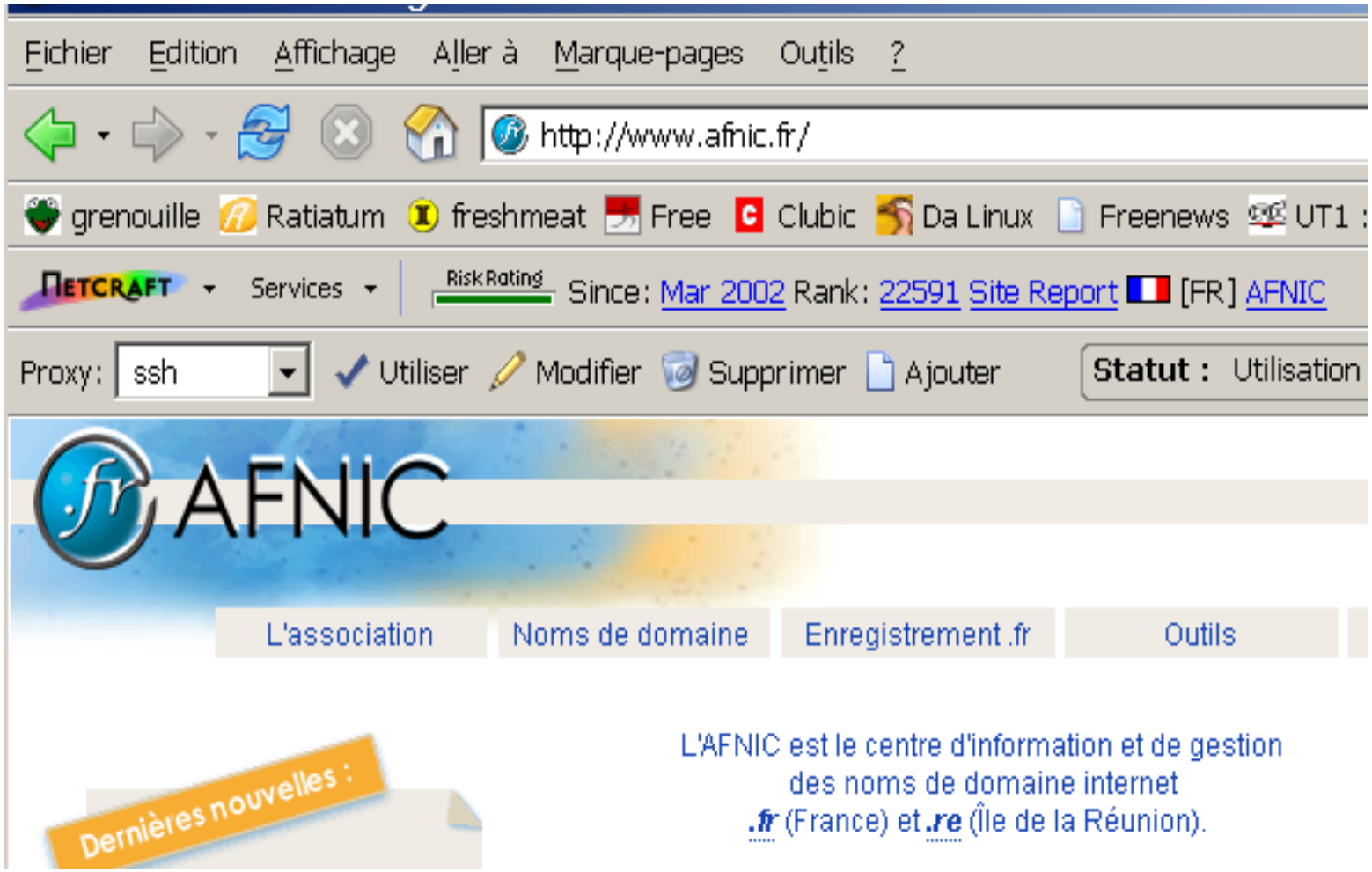
La lutte technique en utilisation

- Empêcher l'utilisation des sites façade
- RBL pour l'utilisation web
  - Proxy filtrant
  - Détecteurs intégrés
- Le blocage des popups

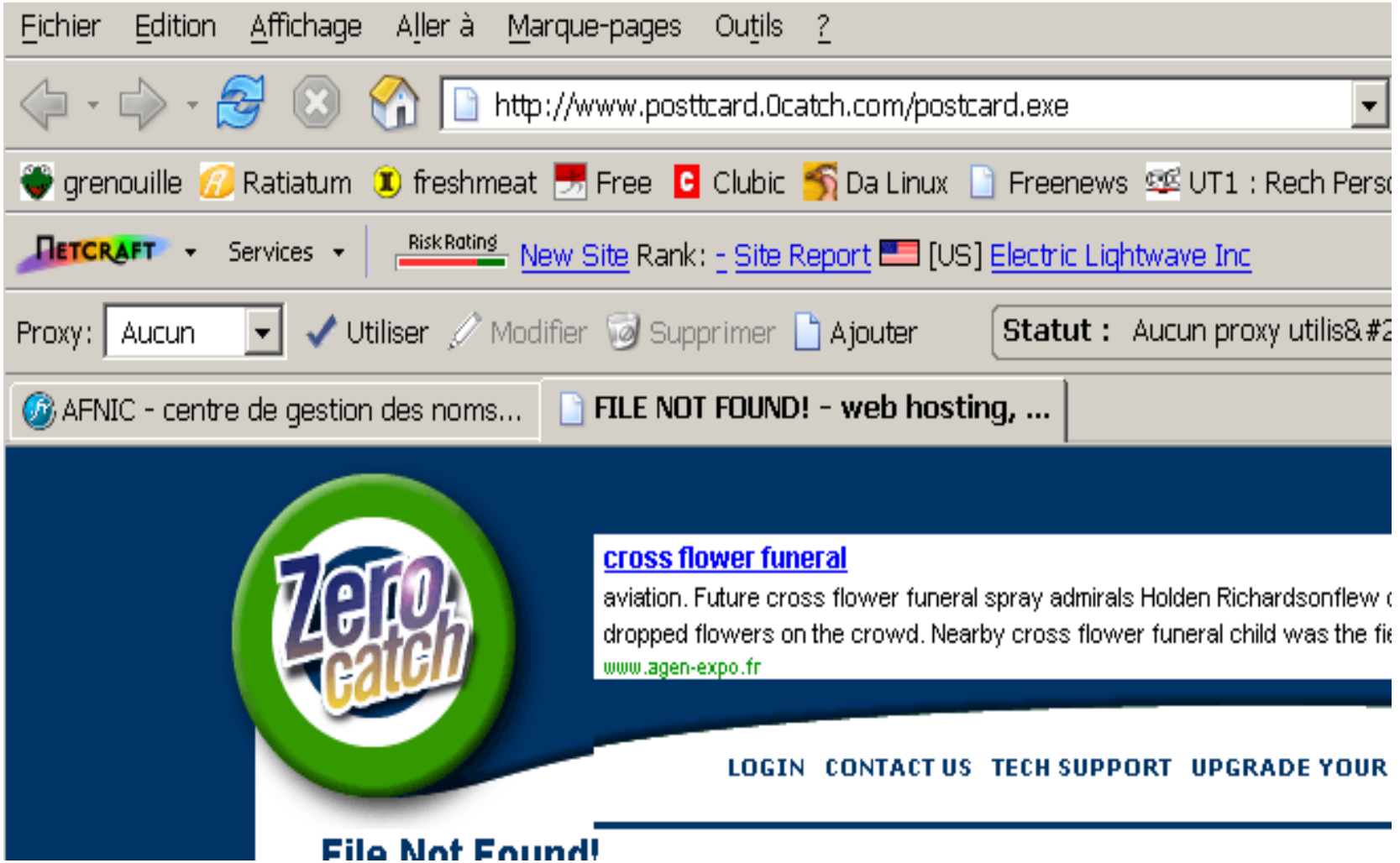
Détection d'incohérence URL



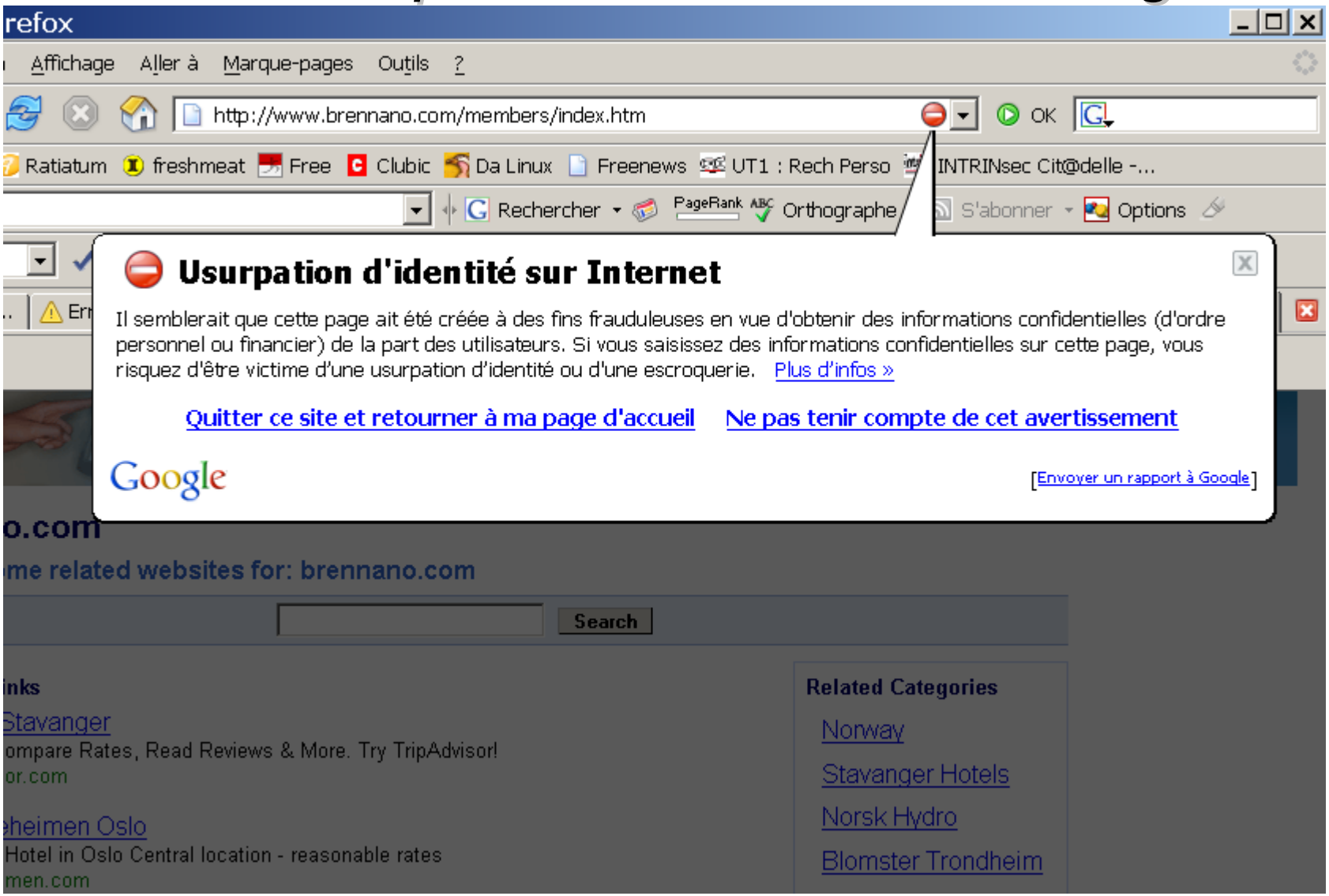
Exemple d'outils : netcraft toolbar



Exemple d'outils : netcraft toolbar



Exemple d'outils : toolbar Google



Exemple d'outils : Filtrage web

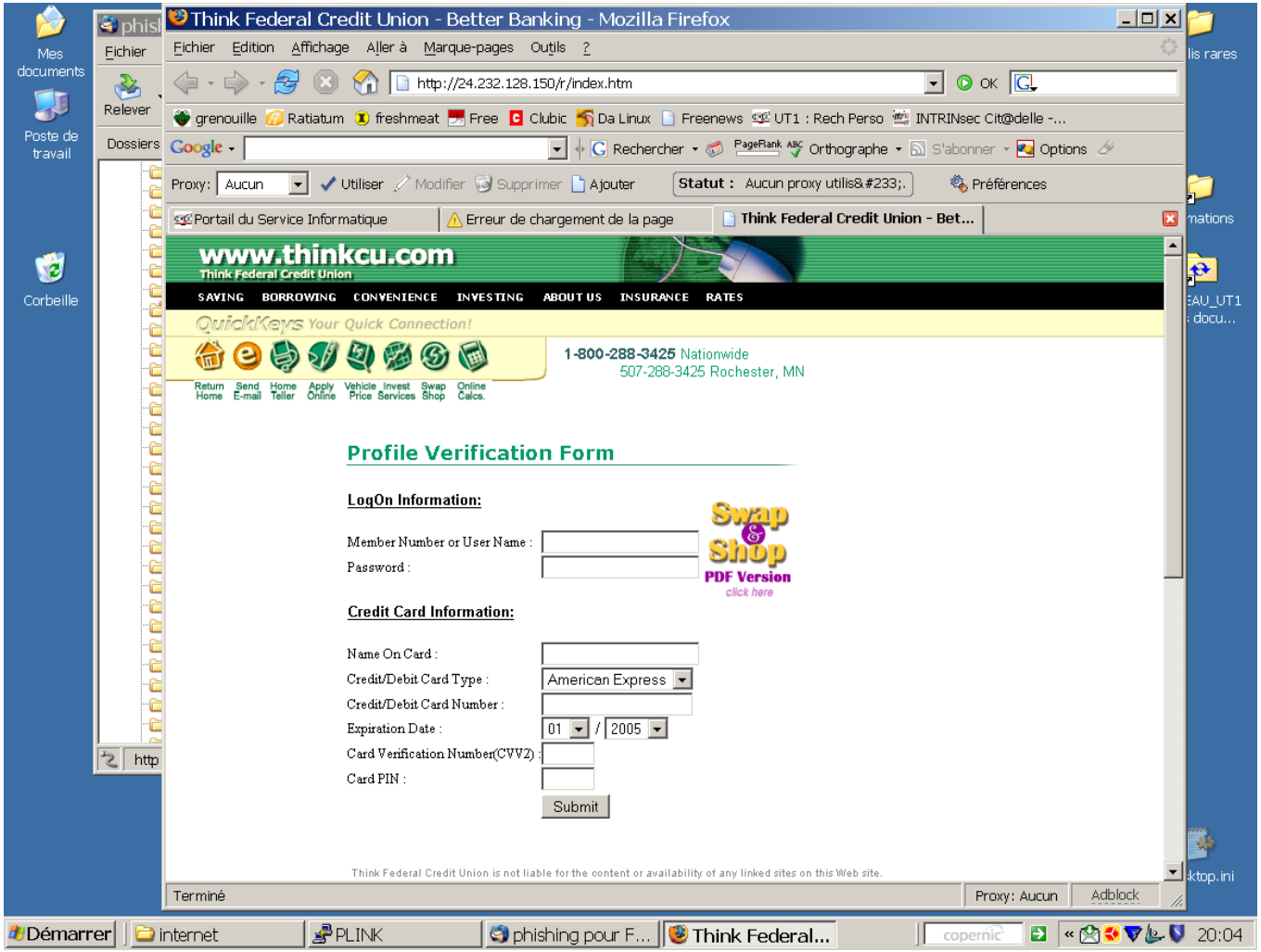
La lutte technique sur les serveurs

- Serveurs peuvent être utilisés
  - Intrusion
  - Failles XSS, IFRAME
- Serveurs DNS peuvent être empoisonnés
  - Pharming
- Programmation correcte des applications web
- Paramétrage correct des serveurs DNS

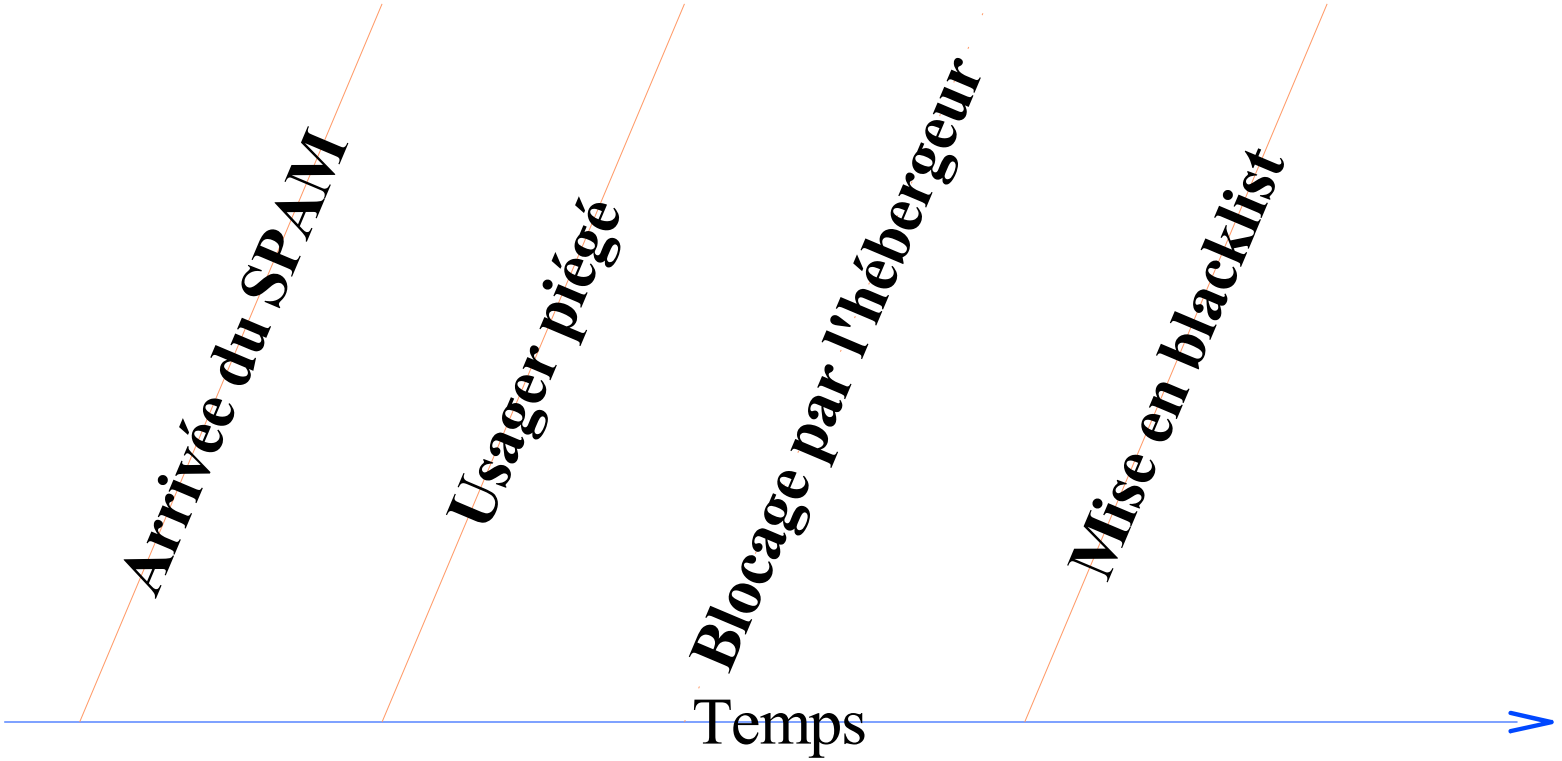
Faiblesses de la lutte technique

- Délai de mise à jour des RBLs
  - Et mise à jour des RBLs
- Les SPAMs s ’améliorent
  - mots cachés, décompilation de message
  - réexpédition de messages (greylisting)

Problème de délai



Chronologie actuelle



L'avenir

- Phishing avec VOIP
  - Numéro de téléphone « local »
  - Répondeur téléphonique
- Zombie, serveurs et DNS « déplaçables »

Conclusions

- Aucune méthode garantie
- Mais la multiplicité des moyens
  1) Lutter efficacement contre le SPAM
  2) Informer de l ’existence des problèmes
  3) Collaboration internationale
  4) Suivre l ’actualité « illégale »
  5) Bloquer l ’utilisation des sites « anormaux »
  6) Programmation correcte des serveurs
- Est la meilleure voie

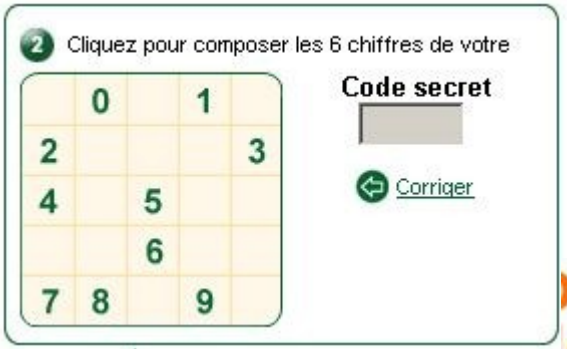
Merci

- Des questions ?

Références

- http://www.antiphishing.org/
- http://www.commentcamarche.net/attaques/phishing.php3
- http://www.fraudwatchinternational.com/
- http://people.deas.harvard.edu/~rachna/ Why phishing works ?

Contre les keyloggers



+ parfois des cartes de codes

Contre les keyloggers

- Vérification postale avant virement
  - Création de code pour chaque destination