G Data
Whitepaper 2011

Les dangers du courrier électronique

Sabrina Berkenkopf et Ralf Benzmüller
G Data SecurityLabs

Whitepaper_2011

Go Safe. Go safer. **G Data.**

Table des matières

1 Introduction

1.1 Courrier électronique, un bref aperçu

Le courrier électronique en tant que mode de communication est incontournable aussi bien dans la monde du travail que dans la sphère privée. Economique et rapide, l'envoi électronique a une portée internationale.

Pour travailler avec des courriers électroniques, les utilisateurs utilisent des programmes installés sur leur ordinateur (clients e-mail) ou chargent les courriers électroniques via le navigateur. Une fonction tant appréciée attire naturellement aussi les fraudeurs, qui en exploitent les insuffisances techniques.

Le déroulement de l'envoi et de la réception de courrier est effectué dans ce contexte en arrière-plan et l'utilisateur idéalement ne remarque rien. Le protocole d'envoi se nomme SMTP, Simple Mail Transfer Protocol. Les courriers électroniques sont reçus via le protocole POP3 (Post Office Protocol, version 3) ou IMAP (Internet Message Access Protocol).

La structure du courrier électronique est répartie de la même manière qu'une carte postale. Les informations de l'expéditeur, du destinataire, la date, l'objet etc. sont consignées dans l'en-tête de l'email. La deuxième composante est la partie texte (corps de texte), qui transporte le contenu proprement dit.

Comme aucune identification de texte clair n'a lieu lors de l'envoi d'un message par le protocole SMTP, c'est ici que les fraudeurs passent à l'action : il est par exemple possible de modifier dans l'en-tête l'adresse de l'expéditeur et ainsi de faire miroiter une fausse identité au destinataire. Les contenus peuvent également être manipulés sans trop d'efforts.

Toutes les propriétés positives des courriers électroniques déjà évoquées ont également leurs inconvénients. La boîte de messagerie électronique déborde de courriers indésirables contenant des promesses publicitaires suspectes, des offres d'emplois de rêve, des invitations au flirt et autres. L'objet de l'énervement quotidien des utilisateurs informatiques du monde entier est le ☞spam[1]. Ces courriers électroniques massivement reçus mais non sollicités sont non seulement perturbants en raison de leur grand nombre, mais peuvent également se révéler dangereux.

Les courriers électroniques frauduleux et dangereux existent dans de nombreuses variantes. Sous forme de courrier publicitaire indésirable, d'hameçonnage, de programme malveillant avec leur pièce jointe ou lien vers des sites contrefaits. Avant de décrire les différentes procédures et pièges mis en place par les fraudeurs, il s'agit d'en étudier les raisons.

[1] Les explications des termes spécialisés accompagnés d'un ☞ figurent dans le glossaire

1.2 Qui se dissimule derrière l'envoi de spam ?

Les cybercriminels continuent à utiliser fréquemment les courriers électroniques en tant que supports pour leurs actes frauduleux. L'envoi massif de courriers électroniques indésirables, appelés spam, est l'une des branches commerciales les plus connues de l'économie souterraine. Au cours du quatrième trimestre 2010, en moyenne 83 % du trafic de courrier électronique était du spam, ce qui correspond à une moyenne de 142 milliards de spam par jour.[2]

Cette popularité s'explique entre autres par un simple calcul de rentabilité : l'envoi d'un million de spam coûte entre 399 et 800 $ chez différents prestataires. Des offres spéciales, telles que l'on peut en voir sur une boutique en ligne légale, permettent même l'envoi de 2 millions de messages pour le prix d'un...

General Email Marketing Campaign Prices			
# of Emails Delivered	Price	Cost p/ Thousand	
100,000	$99	$1.00	Order Now!
250,000	$199	$.80	Order Now!
400,000	$249	$.62	Order Now!
1,000,000 (Get a 2 million campaign	$399* for the price of 1 million)	$.19	Order Now!
3,000,000	$549	$.18	Order Now!
10,000,000	$1499	$.15	Order Now!
25,000,000	$1999	$.08	Order Now!
50,000,000	$2499	$.05	Order Now!

Capture d'écran 1 : *la liste de prix d'un service d'envoi d'email en masse (Bulk e-mail) sur Internet. Ces prix s'appliquent pour l'envoi de spam général, sans groupe-cible fixe*

Des listes d'adresses contenant des personnes ciblées sont également proposées sur les marchés parallèles ou directement vendues par les prestataires d'envoi d'e-mail en masse et, si nécessaire, également ajustées en fonction du client. Il est ainsi possible d'acheter des adresses classées par groupes, cibles. Par exemple des listes spéciales contenant des joueurs en ligne ou des personnes provenant de certaines régions ou encore beaucoup d'autres catégories.

Georgraphic Email List Options	Price	
1 Country or 1 State or 1 City or 1 US Zip Code	$298	Order Now!
2 Countries or 2 States or 2 Cities or 3 US Zip Codes	$398	Order Now!
3 Countries or 4 States or 4 Cities or 6 US Zip Codes	$498	Order Now!
6 Countries or 8 States or 8 Cities or 15 US Zip Codes	$798	Order Now!
12 Countries or 14 States or 14 Cities or 25 US Zip Codes	$1198	Order Now!
Larger List Packages	Inquire	Order Now!

Capture d'écran 2 : *Suppléments pour envoi de courriers ciblé – dans ce cas, il s'agit de groupes-cibles locaux*

Les courriers sont envoyés principalement par ☞botnet. Avec un botnet relativement petit composé d'environ 20 000 ☞ordinateurs zombies, un exploitant de botnet met environ 25 secondes pour l'exécution d'un ordre contenant 1 000 000 d'email (2 messages par seconde pour chaque bot ☞

[2] Commtouch, 4ème trimestre 2010 Internet Threats Trend Report. Les chiffres se basent sur le flux de données non filtré, sans trafic interne à l'entreprise

actif). En calcul pur, un exploitant d'un botnet relativement petit peut donc gagner jusqu'à 115 200 $ par heure.

1.3 Base psychologique du spam

Quelle que soit la forme sous laquelle le courrier électronique atterrit dans la boîte de réception, les astuces des fraudeurs se basent fréquemment sur le ☞Social Engineering (piratage psychologique). Des émotions, avis, attitudes et comportements sont exploités pour attirer le destinataire du courrier dans le piège. Ces tentatives d'accès à des données confidentielles via des manipulations psychologiques constituent une sorte de « faille de sécurité humaine ».

Pour exploiter efficacement le piratage psychologique, les fraudeurs se servent du (faux) expéditeur, de la ligne d'objet et du contenu du courrier électronique. Le nom du fichier en pièce jointe, une double extension de fichier, des icônes populaires ou le nom de domaine du lien peuvent également être utilisés pour dissimuler une tentative d'escroquerie. Jordan et Goudey ont identifié dans une étude parue en 2005[3] les 12 facteurs psychologiques suivants comme bases des vers les plus couronnés de succès entre 2001 et 2004 :

- Inexpérience (inexperience)
- Curiosité (curiosity)
- Avidité (greed)
- Manque de confiance en soi/timidité (diffidence)
- Politesse (courtesy)
- Amour de soi (self-love)
- Crédulité (credulity)
- Désir (desire)
- Envie et amour (lust)
- Menace (dread)
- Réciprocité (reciprocity)
- Amitié (friendliness)

Un an plus tard, M. Braverman a ajouté[4] :

- Conversation générale (generic conversation) : Expressions courtes, telles que « Cool », etc.
- Avertissements relatifs à des virus et correctifs logiciels
- Logiciels malveillants détectés sur l'ordinateur PC
- Message de vérification antivirus à la fin du courrier
- Informations ou messages relatifs à des comptes : le cheval de Troie Telekom, par exemple, qui se présente comme une facture téléphonique excessive
- Messages d'erreur relatifs à la distribution du courrier
- Attraction physique (Physical attraction)
- Accusations (Accusatory) : par exemple, le cheval de Troie BKA qui prétend avoir détecté des fichiers illégaux
- Événements actuels
- Articles gratuits (free stuff) : certaines personnes se laissent totalement duper dès que quelque chose de gratuit leur est proposé

[3] voir Jordan, M., Goudey, H. (2005) « The Signs, Signifiers and Semiotics of the Successful Semantic Attack ». Dans : Proceedings of the EICAR 2005 Conference, p. 344 - 364.
[4] voir Braverman (2006) « Behavioural Modelling of Social Engineering-based Malicious Software ». Dans : Proceedings of Virus Bulletin Conference 2006, p. 15-22.

2 Les différents pièges

2.1 La réinscription (vol de données, logiciel malveillant)

Le courrier électronique suggère qu'un système en ligne ou un programme a été mis à jour et qu'une mise à jour immédiate des données de clients doit avoir lieu, afin que les fonctions du service puissent toujours être utilisées correctement. Le lien vers site Web soi-disant mis à jour est indiqué directement dans le courrier électronique et il est généralement possible de distinguer en jetant un œil à l'adresse mise en lien qu'il ne s'agit pas de l'adresse originale. Le site Web mis en lien est souvent une copie identique de l'original et d'un point de vue purement optique, il est presque impossible de détecter qu'il s'agit d'une contrefaçon.

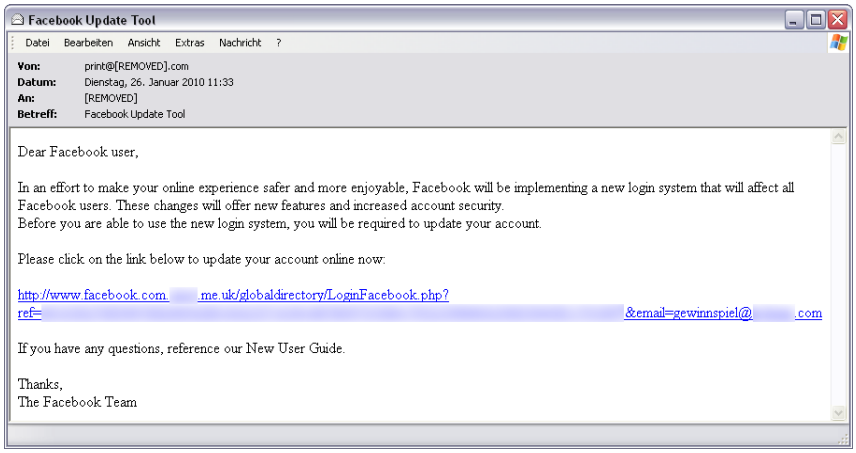
Le groupe-cible : Chaque utilisateur Internet, mais en particulier les clients de banques et services en ligne payants, ainsi que les utilisateurs de logiciels populaires, de réseaux sociaux, de jeux en ligne, de services de courriers électroniques gratuits et d'applications Web.

Approches psychologiques : inexpérience, crédulité, sensibilisation en matière de sécurité

Le danger : Si la victime entre les données demandées sur le site Internet usurpé, les fraudeurs reçoivent automatiquement ces informations. Celles-ci peuvent s'étendre, en fonction du type et de la conception du site, du nom et de l'adresse de la personne aux numéros de carte bancaire. L'utilisation abusive de ces données est programmée à l'avance !

L'autorité joue dans ce piège un rôle important. Les utilisateurs inexpérimentés sont facilement incités à cliquer et à effectuer des actions lorsqu'elles sont commandées par un (faux) expéditeur ou entreprise connue.

Exemples d'objets : Facebook Password Reset Confirmation. Customer message
Yahoo Warning!!! (Verify Your Account Now To Avoid Service Suspension..)
Urgent Notice: Paypal Limited
Your account has open issues !!!
Facebook Update Tool
World of Warcraft Account - Subscription Change Notice



Capture d'écran 3 : *E-mail avec appel à la mise à jour via un lien. Ce lien ne mène pas à la page Facebook.com, mais vers une page avec le domaine de second niveau .me.uk*

2.2 L'irrégularité (hameçonnage)

Ce piège fait peur à la victime potentielle, l'informant qu'un problème avec son compte se serait produit et qu'il doit de ce fait être immédiatement bloqué. Pour éviter ce blocage, l'utilisateur doit immédiatement (!) entrer ses données de compte sur un site Internet communiqué.

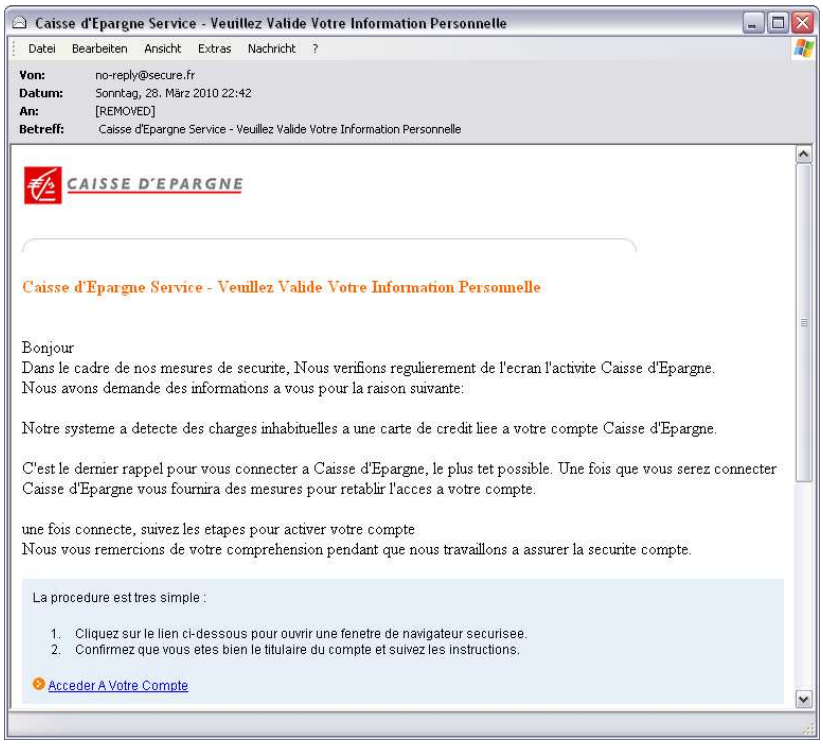
Le groupe-cible : tout internaute, mais en particulier les clients les plus divers de banques et de services de paiements ou de services de webmail.

Les utilisateurs de services dont le seul contrôle d'accès consiste en un identifiant et un mot de passe, sont des cibles particulièrement rentables – en particulier si de l'argent peut être transféré par le biais des services ou s'ils possèdent une valeur dans l'économie souterraine (blanchiment d'argent, envoi de spam, envoi de marchandises volées etc.)

Approches psychologiques : Inexpérience, timidité et menace

Le danger : Comme pour le piège de réinscription, la cible principale est les données personnelles telles que les codes d'accès au service visé ou le vol des données bancaires. Dans ce cas également, l'acceptation de l'autorité est un critère de réussite de ces attaques.

Exemples d'objets : Attention! Your PayPal account has been violated!
Your Pay PalAccount May Be Compromised
Multiple Logon Errors on your Account.
Notification of Limited Account Access RXI034
Santander Merger Important Urgent Message
<<< IMPORTANT MESSAGE FROM SECURITY CENTER >>>
Attn. All Webmail Users



Capture d'écran 4 : *Un courrier électronique d'hameçonnage, qui imite la correspondance officielle d'une banque*

2.3 La carte de vœux (logiciel malveillant)

De fausses cartes de vœux sont diffusées toute l'année, mais elles attirent spécialement l'attention des fraudeurs et des victimes au moment des fêtes et jours fériés. La tentation de lire les vœux d'un « ami » présumé est grande, mais c'est à ce moment précis que le piège se referme.

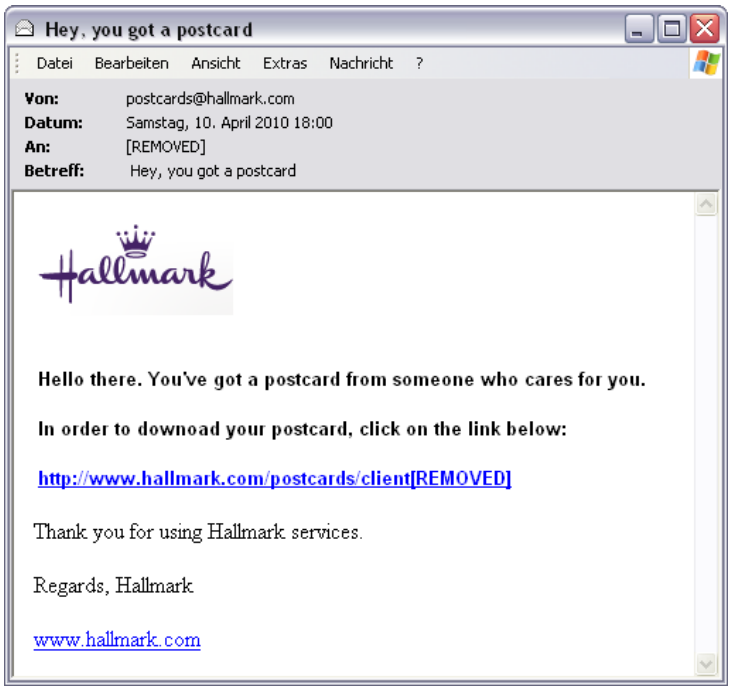
Il existe plusieurs types de messages. Il existe d'une part des courriers contenant des pièces jointes camouflées sous forme de eCard, qui exécutent leur attaque dès qu'elles sont ouvertes. Il existe ensuite les courriers qui invitent l'utilisateur sur un site Internet à installer un présumé codec ou un lecteur multimédia, pour pouvoir afficher la eCard présumée. Et enfin, il existe encore les courriers qui déclenchent une infection « Drive By » invisible lors de la visite du site Web contenant la soi-disant carte de vœux.

Le groupe-cible : tout utilisateur Internet

Approches psychologiques : Curiosité, amabilité

Le danger : Tout comme pour le piège appelé « regarde par ici », l'utilisateur est exposé au code nuisible dès qu'il se rend sur une page, ouvre la pièce jointe ou installe le programme de lecture camouflé. Il en résulte alors les possibilités pour les programmes nuisibles de voler des données personnelles et/ou de causer d'autres dommages.

Exemples d'objets : Kiss You My Love! Happy Valentine's Day!
You have received a Christmas Greeting Card!
Despina sended you a giftcard!
You Have a dGreetings card from a friend .
You have received a greeting from somebody who cares you !!!
Hey, you have a new Greeting !!!



Capture d'écran 5 : *Le courrier électronique semblant légitime contient un lien dangereux – celui-ci présente un fichier EXE exécutable et non pas le site Web du fabricant de la carte de vœux*

2.4 Le piège de l'envoi de colis (logiciel malveillant et hameçonnage)

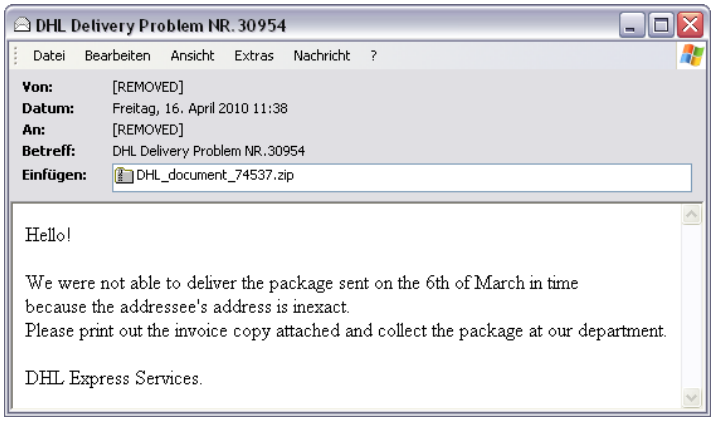
Le destinataire reçoit un courrier électronique contenant un message sur une procédure d'envoi soi-disant échouée. Pour résoudre le problème, ou pour obtenir davantage d'informations, le destinataire doit ouvrir un fichier joint ou suivre un lien indiqué. Les criminels lorgnent ici souvent sur les clients de prestataires d'expédition, dont les paquets et colis peuvent être retirés sans délai à l'aide d'un PIN dans un dépôt. Les prestataires d'expédition de renommée internationale sont souvent les instruments de ces campagnes d'hameçonnage.

Le groupe-cible : tout utilisateur Internet, mais en particulier les clients de prestataires d'expédition populaires.

Approches psychologiques : Curiosité, convoitise, vigilance

Le danger : Si l'utilisateur démarre un fichier joint à partir du courrier électronique fréquemment dissimule sous forme de bordereau de livraison, il installe involontairement un code nuisible sur son ordinateur, qui peut être extorqué et transférer des données personnelles sous forme de dérobeurs de mots de passe, d'enregistreurs de frappe, etc. Les utilisateurs tombent dans le piège de l'hameçonnage s'ils entrent par exemple leurs données personnelles et des détails de la station de réception du paquet sur une fausse page, semblant pourtant réelle, du prestataire d'expédition. Ainsi, les cyber-délinquants accèdent aux codes d'accès, peuvent y dérober des paquets livrés aux terminaux et également utiliser le lieu en tant que point de livraison pour des expéditions d'actes frauduleux. Des comptes de ces stations sont utilisés dans le souterrain pour l'envoi de marchandises, qui ont été payées via des données bancaires dérobées ou par cartes de crédit. Ils servent enfin au blanchiment d'argent et sont donc convoités. Les utilisateurs qui communiquent donc leurs données en les entrant sur une fausse page d'inscription peuvent d'attendre à des dommages de grande ampleur.

Exemples d'objets : DHL Services. Please get your parcel NR.0841
DHL Office. Get your parcel NR.1572
DHL Express. Get your parcel NR.3029
UPS Delivery Problem NR 68522.
Thank you for setting the order No.538532



Capture d'écran 6 : *Un courrier électronique avec une pièce jointe infectée qui se dissimule sous forme de document officiel*

2.5 Le piège « Regarde par ici » (logiciel malveillant et publicité)

Dans cette variante, les scélérats se fient avant tout à l'art du piratage psychologique (appelé Social Engineering) et rendent les destinataires de courriers électroniques curieux des soi-disant toutes dernières nouveautés du réseau, des images et vidéos apparemment embarrassantes sur leur propre personne ou d'autres thèmes intéressants.

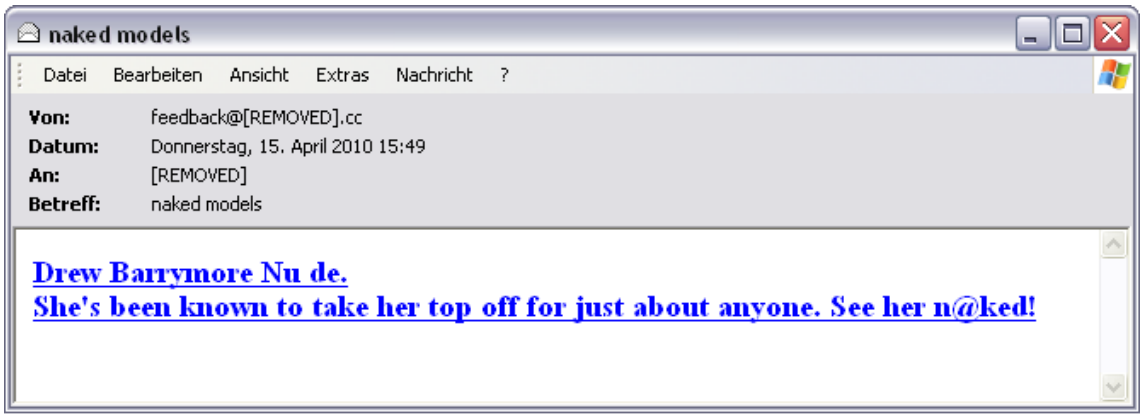
Le code nuisible se cache ici directement dans la pièce jointe infectée du courrier électronique ou sur le site Web auquel mène le lien contenu dans le courrier électronique. Derrière le lien se dissimule la plupart du temps la demande d'installation d'un codec ou d'un nouveau programme de lecture, qui installent ensuite un code nuisible sur l'ordinateur lors de l'exécution.

Le groupe-cible : tout utilisateur Internet, mais en particulier les utilisateurs de réseaux sociaux

Approches psychologiques : Curiosité, envie

Le danger : Dans cette variante, la victime est attaquée par un code nuisible et peut infecter son ordinateur par différents programmes nuisibles. Ces programmes peuvent alors lire les mots de passe, dérober les données de cartes de crédit, relier le PC à un botnet, etc.

Exemples d'objets : Scandale : mort de Britney Spears
Iceland volcano disrupts flights accumulable
200,000 flood Shanghai Expo preview acetabular
NEW SCANDAL VIDEO
are you a teacherin the picture?
Why You?
Fwd: Photo
Windows Live User has shared photos with you



Capture d'écran 7 : *Un courrier électronique qui tente d'attirer les personnes curieuses sur des sites Web infectés. Un exemple très connu de courrier de ce type était l'annonce d'une image d'Anna Kurnikova dénudée en 2001.*

2.6 Le piège de la remise (logiciel malveillant)

Les filtres de spams ont quelque chose à voir avec les publicités indésirables pour des pilules bleues bon marché, des logiciels au prix imbattable, des remises sur des bijoux et des promesses de régime. Dans ce genre de cas, la règle suivante s'applique : Bas les pattes de ces offres qui paraissent trop belles pour être vraies.

Le groupe-cible : tout utilisateur Internet

Approches psychologiques : Convoitise

Le danger : L'utilisateur qui clique sur le lien est conduit vers des boutiques en ligne douteuses. Les cyber-délinquants attendent ici que l'utilisateur entre ses données personnelles précieuses, coordonnées bancaires ou données de cartes de crédit dans un formulaire. Il est fort possible qu'une infection de l'ordinateur en arrière-plan (Drive-by-Download), si les pages mises en lien sont consultées – Des parasites informatiques indésirables en sont la conséquence, causant toute sorte de dommages sur l'ordinateur de la victime.

Exemples d'objets : Commandez et économisez 40 %, en mars uniquement
Offres de logiciels qui vous réjouiront !
Dear […], 15-22 March 2010 +4833 78% 0FF.
Save thousands of dollars on original D&G accessories.
Bvlgari jewelry would look great on your girlfriend.
Plus économiques que jamais - montres de luxe

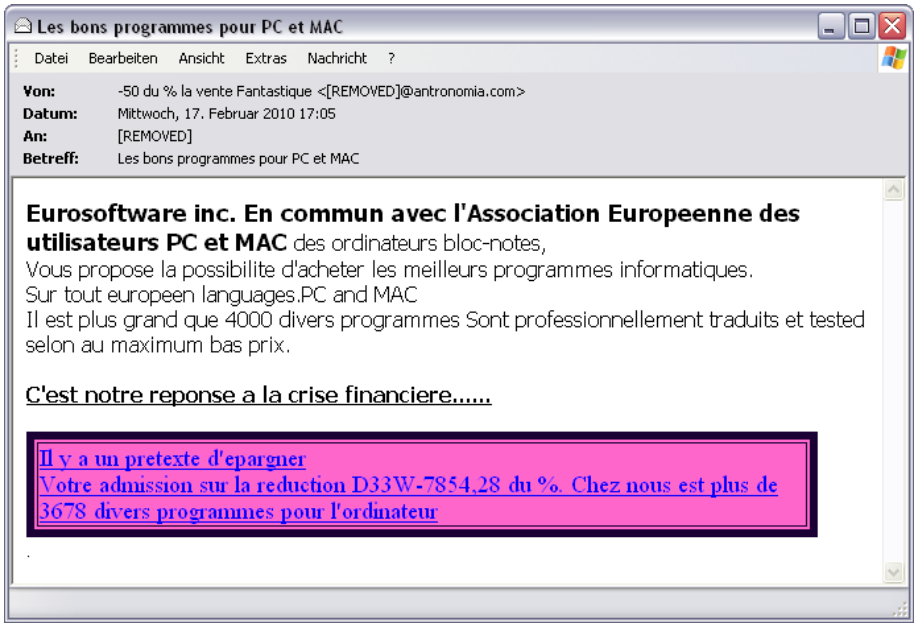
} Remises

Worlds only herball pill that corrects erectile dysfunction, strengthens erections and enhances libido

} Pharma

You can be another on the long list of Quick Slim Success stories.
Comment Madonna a perdu du poids
Le sport est un supplice
Trop gros ? Perdez du poids !

} Régime



Capture d'écran 8 : *Ce courrier électronique séduit par des remises importantes*

2.7 Piège des grades et titres universitaires (hameçonnage et abus)

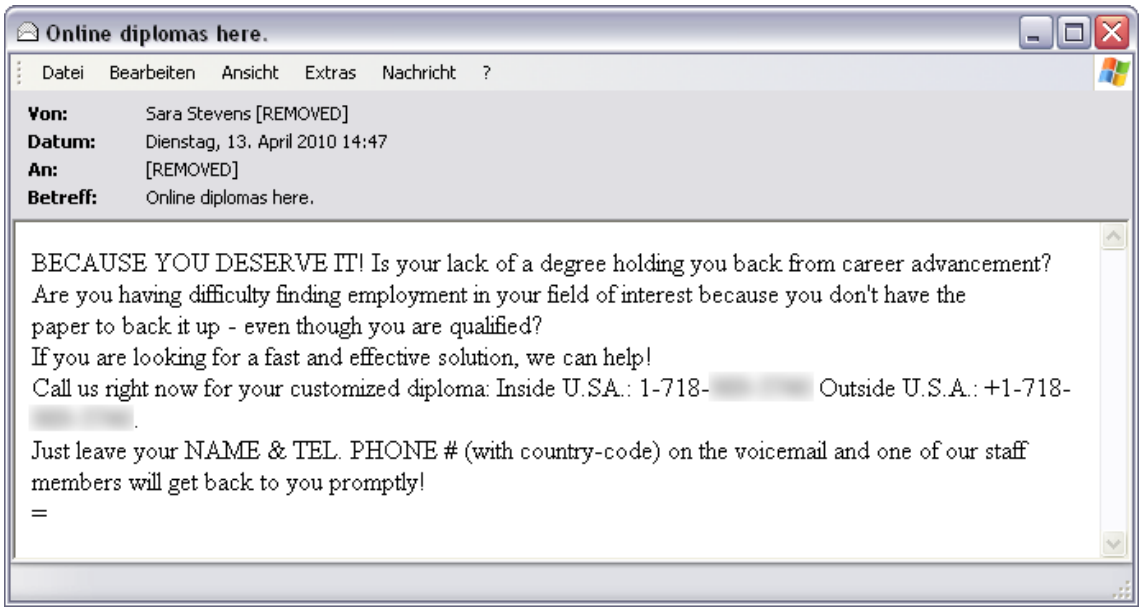
Les textes publicitaires attirent les utilisateurs en leur promettant d'obtenir rapidement et facilement des degrés ou des titres académiques – sans avoir suivi aucune étude ni obtenu aucun diplôme.

Le groupe-cible : tout utilisateur Internet

Approches psychologiques : Désir, crédulité

Le danger : L'utilisateur qui appelle les numéros de téléphone indiqués ou écrit aux adresse e-mail, doit tout d'abord indiquer de nombreuses données personnelles, et communique ainsi des informations précieuses. L'utilisateur qui achète même un titre auprès de ce prestataire perd sans aucun doute également l'argent qu'il a versé. Toute personne se prévalant de documents universitaires douteux et utilisant le titre acheté est passible d'une amende en Allemagne selon le *§* 132a du code pénal.

Exemples d'objets : Doctorate degree can be yours.
Online diplomas here.
Re: MBA- qualification & award
Get a diploma for a better job.



Capture d'écran 9 : *Ces courriers électroniques proposent des diplômes universitaires à l'achat, afin d'améliorer ses opportunités de carrière*

2.8 Piège du casino en ligne (hameçonnage et abus)

Le jeu de hasard en ligne sous toute forme que ce soit est de plus en plus apprécié. Le poker en ligne a particulièrement la cote depuis longtemps. Les courriers spams suggèrent qu'il est possible de gagner beaucoup d'argent en misant peu – Des bonus de départ sont promis pour le premier versement ou bien un crédit existant est présent.

Le groupe-cible : tout utilisateur Internet

Approches psychologiques : Désir, convoitise, curiosité, instinct du jeu

Le danger : Les casinos en ligne, qui ne sont pas domiciliés en Allemagne pour des raisons juridiques, exigent un premier paiement de la part des joueurs potentiels – les utilisateurs fournissent souvent inconsidérément leurs coordonnées bancaires précieuses, voire leurs données de carte de crédit sur des sites de jeux en ligne douteux. Un autre aspect du risque sont les versements d'agent en cas de gain, en effet, les versements sont souvent rejetés pour les raisons les plus diverses et l'argent déposé tout comme l'argent gagné ont tous deux disparu. Aucun recours juridique n'est possible puisque l'offre tout comme la participation à des jeux de hasard en ligne sont interdites en Allemagne depuis janvier 2009.

Exemples d'objets : Conservez les gains après avoir découvert cette offre fantastique
Profitez de nos jeux et de nos super bonus de départ
Bonus de bienvenue généreux
Dernier rappel

Capture d'écran 10 : *Un courrier d'accroche de casino*

2.9 Piège 419 / spam Nigeria (abus)

Ce terme qualifie les courriers de fraude par avance. Le courrier informe le destinataire qu'il doit recevoir pour diverses raisons une grosse somme d'argent
– par ex. comme héritage, en remerciement de la gestion d'occasions ou également en tant que gagnant d'un prétendu jeu-concours. D'autres scénarios misent sur le fait que le destinataire assume une fonction caritative et aide les personnes à la recherche d'un logement ou un animal abandonné – naturellement financièrement également. La seule action nécessaire pour recevoir l'argent/l'assistance est de prendre contact avec la personne mentionnée dans le mail.

La désignation « 419-Scam » pour ce type de spam a vu le jour par la référence au droit pénal nigérian, qui explique dans l'article 419 du chapitre 38[5], les faits et amendes pour les fraudes et escroqueries.

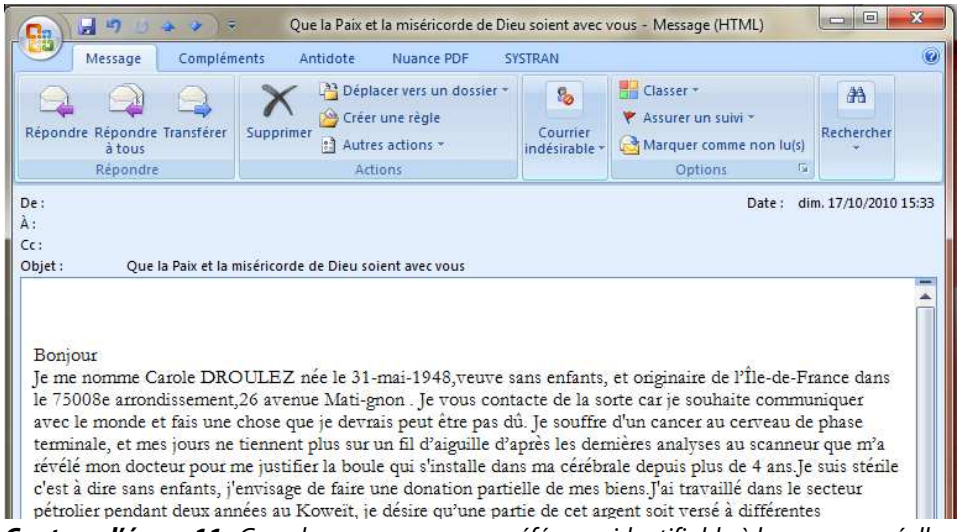
En Allemagne, les dommages s'élèvent à au moins 522 millions de dollars US et aux États-Unis à 2 110 millions de dollars US de pertes causées par le spam 419 et ses conséquences en 2009.[6]

Le groupe-cible : tout utilisateur Internet

Approches psychologiques : Avidité, crédulité

Le danger : Lorsque le premier contact a été établi, le fraudeur essaye de persuader la victime qu'on va lui verser une grosse somme d'argent. Cependant, il est mentionné qu'un montant X est tout d'abord requis pour l'ordre de paiement de l'argent sur le compte de la victime, somme qui doit être versée par la victime par ex. sur un compte Western Union à l'étranger. Des coûts supplémentaires fictifs pour les avocats, procédures auprès des autorités, documents, etc. viennent s'y ajouter. L'argent qui est viré par la victime (au cours de plusieurs étapes) est perdu à jamais et la somme d'argent promise n'est jamais versée.

Exemples d'objets : URGENT !
Reliable Partnership needed
NEED COMFIRMATION OF ACCEPTANCE
Your Notification Letter !!!



Capture d'écran 11 : *Grandes promesses, sans référence identifiable à la personne réelle, mais contenant des négligences grammaticales*

[5] http://www.nigeria-law.org/
[6] Ultrascan Advanced Global Investigations (2010), « 419 Advance Fee Fraud Statistics 2009 » p. 29

2.10 Piège à l'emploi (logiciel malveillant et abus)

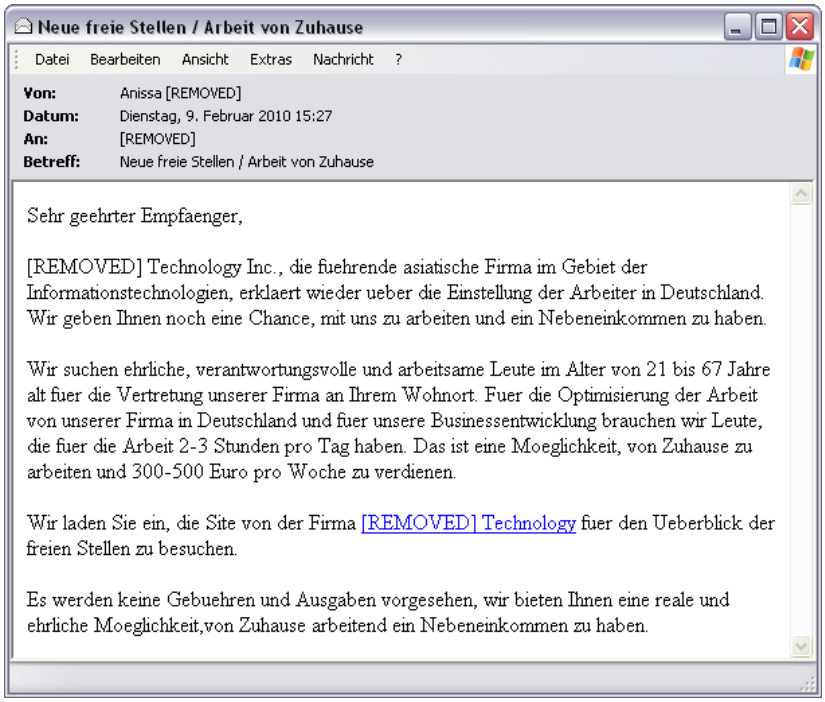
Les promesses de courriers d'emploi promettent des emplois bien rémunérés (dans des entreprises réputées), pour lesquels peu de travail est requis. Les salaires prétendus sont élevés, le temps de travail est faible et le poste de travail est souvent à domicile. Ces perspectives sont un appât efficace au vu de la conjoncture économique actuellement difficile. Ce piège peut être entre autres une partie intégrante d'une attaque scam 419.

Le groupe-cible : tout utilisateur Internet

Approches psychologiques : Désir, narcissisme

Le danger : Ces courriers sont parfois envoyés avec des pièces jointes, qui infectent l'ordinateur par des vers à leur ouverture et qui garantissent ainsi une diffusion ultérieure des spams d'emploi. Outre le danger technique, un autre danger se dissimule ici également : les emplois proposés servent souvent de blanchiment d'argent ou au transfert de marchandises acquises illégalement : Souvent, l'utilisation d'un compte privé est l'un des critères principaux dans la description de l'emploi et une personne crédule à la recherche d'un emploi se rend fréquemment coupable de blanchiment d'argent ou de recel en utilisant son compte privé pour les pratiques des fraudeurs. Le vol d'identité n'est également pas exclu en transmettant aux fraudeurs toutes les données personnelles possibles à des fins de prétendues conclusions de contrat.

Exemples d'objets : Offre d'emploi. Contrat. Mi-temps / Plein temps. 8 ans dans la branche
Service consommateur/Offre d'emploi/UPS/MBE
Job d'appoint
Travaillez pour nous
Vous pouvez être embauché
Organisation recherche collègues
Management recherche collègue de travail



Capture d'écran 12 : *Un scam d'emploi qui essaye d'attirer dans le piège des utilisateurs innocents*

2.11 Piège de la femme russe (abus)

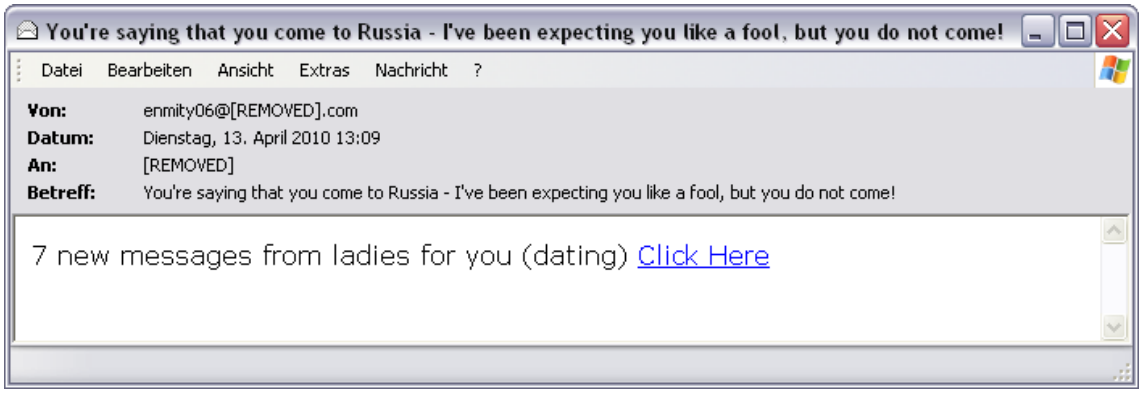
Ces courriers électroniques promettent le grand amour ou bien simplement une aventure amoureuse rapide, avec des femmes blondes, stéréotypées, généralement jeunes et belles, venant de Russie. Les dames attendent soi-disant depuis longtemps une réponse et sont apparemment prêtes à enfin rencontrer et/ou à épouser leur bien-aimé. De tels rendez-vous sont également utilisés pour le blanchiment d'argent. L'amoureux est amené à transférer des marchandises et à virer de l'argent étranger sur son compte pour sa bien-aimée, pour qu'elle puisse lui rendre visite. Les scammeurs 419 utilisent fréquemment ce piège.

Le groupe-cible : tout utilisateur Internet, mais principalement les hommes célibataires d'Europe de l'Ouest

Approches psychologiques : Envie et amour, réciprocité

Le danger : En répondant à ce courrier électronique et en établissant un premier contact avec ces femmes apparemment seules, le thème de l'argent, du mariage et du visa est rapidement abordé. La bien-aimée nécessite de l'argent pour voyager, de l'argent de poche, de l'argent pour se maquiller etc. – transféré sur un compte anonyme en espèces. Si l'homme crédule vire l'argent, il ne le reverra pas, et ne verra très certainement pas non plus un jour sa bien-aimée en chair et en os.

Exemples d'objets : You have new mail from Olga 26 y.o. Russia, dating
Meet Russian women here.
Still single?look at my profile, Olga from Russia
Want to know what the real Russian girls love and warmth?
Russian beauties are waiting.



Capture d'écran 13 : *Un des très nombreux courriers d'appât à caractère de rendez-vous*

2.12 Piège de la loterie (abus)

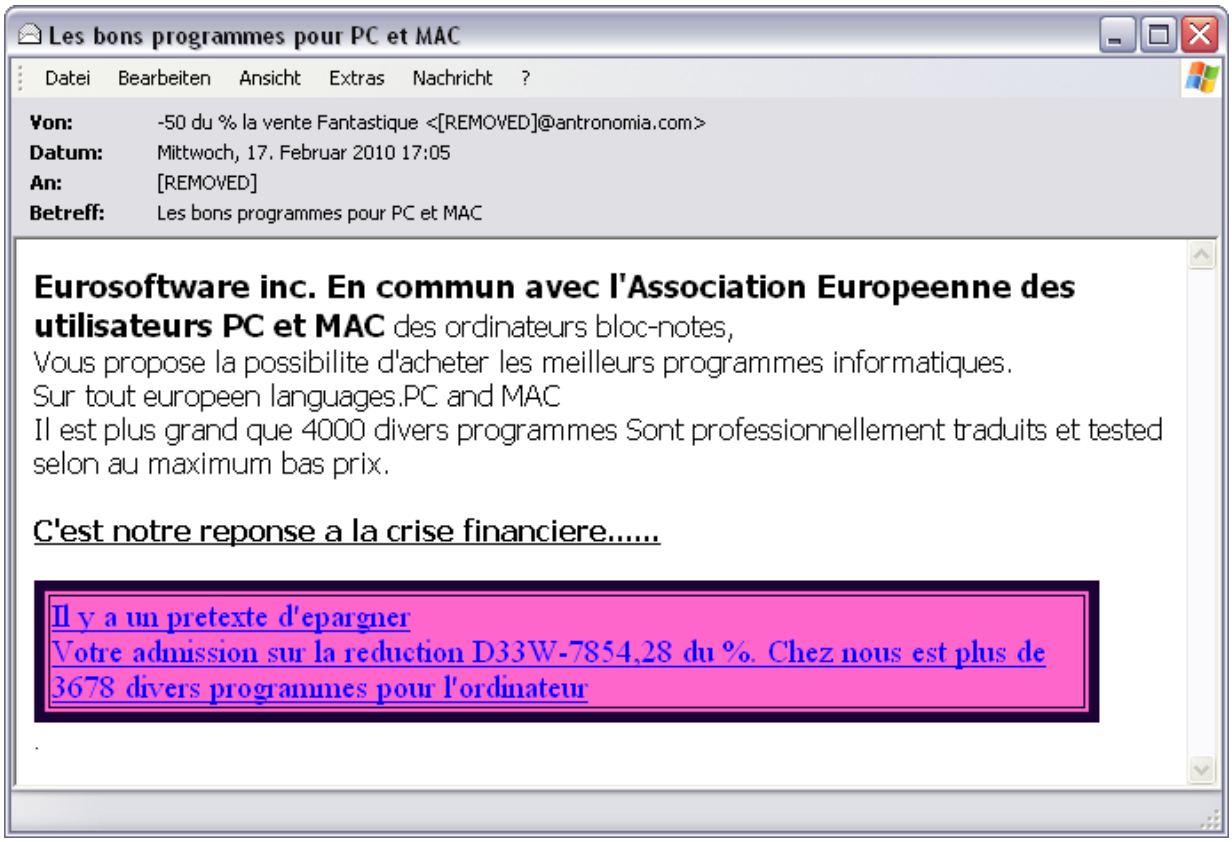
Il est suggéré au destinataire de ce courrier électronique qu'il a soi-disant gagné une forte somme d'argent en euros, en dollars ou dans une autre devise. Il suffit de se signaler auprès de la personne XY en lui fournissant certaines données personnelles. Les loteries sont effectuées soi-disant par des entreprises renommées et les banques impliquées bénéficient apparemment d'une réputation internationale. Ce piège peut également faire partie d'une attaque selon le principe du spam nigérian.

Le groupe-cible : tout utilisateur Internet

Approches psychologiques : Convoitise, désir

Le danger : Pour que ce montant puisse être viré, le gagnant présumé doit tout d'abord envoyer des frais aux fraudeurs – généralement sur des comptes bancaires étrangers et/ou anonymes. La victime passe d'une taxe à l'autre, paye et paye encore et ne (re)verra jamais le gain ni les taxes payées.

Exemples d'objets : REF NR. GOOGLE-0293856-2009
Your E-mail Address Won
NOTICE OF GRANT AWARD (Congratulations you are a winner)



Capture d'écran 14 : *Un avis de gain présumé*

3 Conseils et astuces

Pour ne pas devenir la victime de l'un de ces pièges décrits, les points suivants doivent être observés:

3.1 3.1 Règles de comportement utiles

- Les courriers électroniques d'expéditeurs inconnus doivent être traités avec une méfiance particulière. En cas de réception d'un courrier hors du commun : l'ignorer, le supprimer, mais n'ouvrir en aucun cas ses pièces jointes ni cliquer sur ses URL.
- Ne jamais répondre aux spams. Une réponse montre simplement aux fraudeurs que l'adresse à laquelle ils ont écrit est bien valide.
- Aucune information personnelle et/ou données bancaires ne doivent être communiquées – ni par courrier électronique, ni sur des sites Web douteux.
- Ne jamais verser de l'argent à des inconnus.
- Ne jamais publier son adresse de courrier électronique primaire en ligne, par ex. sur des forums ou des livres de visiteurs, car elles peuvent être récupérées par des fraudeurs. Il est utile de créer à cette fin une adresse annexe.

3.2 3.2 Mesures techniques

- Une solution de sécurité pour l'ordinateur avec fonction anti-spam intégrée protège l'ordinateur contre la réception des courriers électroniques grâce à des filtres.
- L'ouverture de pièces jointes, provenant notamment de destinataires inconnus, comporte des risques. Les pièces jointes doivent tout d'abord être scannées par un programme antivirus et le cas échéant rejoindre la poubelle sans être ouvertes.
- Des liens dans des courriers électroniques ne doivent en aucun cas être suivis de manière irréfléchie. L'URL doit être contrôlé. De nombreux programmes de courriers électroniques permettent de voir la destination du lien, lorsque la souris est déplacée sur le lien visible, sans cliquer réellement sur celui-ci – c'est ce que l'on appelle la fonction Mouseover.

4 Glossaire

Bot : les bots sont des petits programmes dont la plupart fonctionnent en arrière-plan de l'ordinateur de la victime à son insu et exercent diverses fonctions selon leur volume de programmation, des attaques DDoS aux spams et à la lecture de la saisie sur clavier et bien plus encore. La programmation des fonctions dépend premièrement du montant que l'on est prêt à investir dans un bot. Les bots avec de très nombreuses fonctionnalités sont naturellement bien plus chers que les bots plutôt simples ne pouvant effectuer que peu de choses. Ils sont entre autres vendus dans les forums clandestins.

Botnet : un botnet est un ensemble de PC dits zombies. Pour l'administration du botnet sont utilisés des serveurs Command-and-Control (C&C Server). Les botnet sont entre autres utilisés pour lancer des attaques de surcharge ciblées sur des serveurs Web (attaques DoS et DDoS) et pour envoyer du courrier indésirable.

Social Engineering : Tactiques de persuasion utilisées par un pirate informatique pour obtenir des informations d'une personne, qu'il pourra utiliser ensuite pour nuire à la personne ou à son organisation. Il s'agit souvent d'endosser une autorité pour exiger des données d'accès ou des mots de passe.

Spam : au milieu des années 90, ce mot désignait la diffusion massive du même message dans les forums Usenet. Le concept lui-même se réfère à un sketch des Monty Python. Depuis lors, le mot a pris plusieurs significations. De manière générale, il désigne les courriers électroniques en masse non sollicités. Dans un sens plus restreint, le terme spam se limite aux messages publicitaires, c.-à.-d : les vers, canulars, messages d'hameçonnage et auto-réponses n'en font pas partie.

Zombie : on appelle zombie un ordinateur qui laisse un étranger le commander par le biais d'une porte dérobée. Comme dans les films de genre, la machine zombie obéit uniquement à son maître caché dont elle exécute les commandes le plus souvent nuisibles. De nombreux zombies sont rattachés aux dits réseaux de bots.