



# CASES articles

Criminalité sur Internet - Rétrospective de l'année 2007

## Agresseurs et victimes

### Un aperçu de la criminalité sur Internet

Pour plus de sécurité, adoptez les réflexes CASES !

#### Les réflexes de sécurité CASES en réponse à la criminalité sur Internet

Une rétrospective de l'année 2007 permet de constater que l'évolution générale de la cybercriminalité est à la professionnalisation croissante des formes d'attaque. La tendance observée en 2006 s'est donc poursuivie. Les formes d'escroquerie vont de l'arnaque à la vente sur des sites d'enchères, en passant par le vol d'identité, jusqu'aux lettres nigérianes. Les e-mails et les pages web demeurent les moyens favoris des criminels pour prendre contact avec leurs victimes potentielles. Le téléphone, les messageries instantanées ainsi que les lettres traditionnelles sont toutefois toujours utilisés lors de la prise de contact. La connaissance des méthodes d'escroquerie courantes et actuelles permet aux usagers d'Internet d'adopter des mécanismes de protection efficaces face aux attaques.

La perte moyenne des usagers d'Internet ayant été victimes d'une escroquerie de la part de cybercriminels s'élevait à 680 dollars en 2007. Selon les chiffres de l'Internet Crime Complaint Center (IC3) américain, un peu plus de 30 % des victimes déclarent avoir subi un préjudice entre 1000 et 5000 dollars. La perte moyenne par victime a nettement augmenté par rapport aux chiffres de 2006.

Les arnaques à la vente sur des sites d'enchères figurent toujours à la première place de la liste des formes d'escroquerie, bien que leur nombre ait baissé. Suivent ensuite des escroqueries telles que la non-livraison de biens ou de services, l'abus de confiance et la fraude à la carte de crédit. Cette dernière est suivie de près par l'usage frauduleux de chè-

Classement des 10 principaux pays vecteurs d'attaques dans le domaine de la cybercriminalité



1. USA (63,2 %) 2. Royaume-Uni (15,3 %) 3. Nigeria (5,7 %) 4. Canada (5,6 %) 5. Roumanie (1,5 %) 6. Italie (1,3 %) 7. Espagne (0,9 %) 8. Afrique du Sud (0,9 %) 9. Russie (0,8 %) 10. Ghana (0,7 %)

Source : Internet Crime Report 2007, Internet Crime Complaint Center, USA

ques et la délinquance informatique. Vol d'identité, escroqueries à l'investissement, menaces ou encore lettres nigérianes complètent la liste des escroqueries les plus courantes déclarées auprès d'IC3 en 2007. C'est dans le domaine de l'escroquerie à l'investissement que les préjudices subis étaient les plus importants.

En ce qui concerne les pays à partir desquels la plupart des attaques ont été lancées, et toujours selon les chiffres d'IC3, il faut mentionner les États-Unis, suivis à bonne distance par le Royaume-Uni, le Nigeria, le Canada, la Roumanie, l'Italie, l'Espagne, l'Afrique du Sud, la Russie et le Ghana. Ce sont également les États-Unis qui arrivent en tête des pays comptant le plus grand nombre de victimes, suivis par le Canada, le Royaume-Uni, l'Australie, l'Inde, le Mexique, l'Afrique du Sud, l'Allemagne, la France et les Philippines.

Les délinquants recherchent leurs victimes sur toute la planète, l'anonymat garanti par l'Internet leur servant d'écran. Les diverses prises de contact entre les criminels et leurs

victimes sont ainsi le plus souvent effectuées par le biais d'e-mails ou de pages web. Le téléphone et les messageries instantanées sont également des moyens de mise en relation privilégiés.

#### Pièges et arnaques

Certaines formes d'escroquerie sont grandement facilitées par l'Internet. Selon les données d'IC3, ce sont les animaux, les chèques, les spams et les pages de contact sur Internet qui, en 2007, étaient plus particulièrement au centre des escroqueries.

Dans le cas des formes d'escroquerie concernant des animaux par exemple, ces derniers sont proposés à la vente par le biais d'Internet mais les acheteurs s'acquittant du prix de vente et des frais de port, ne reçoivent jamais l'animal en question. Les animaleries figurent également parmi les victimes de ce genre de piège : un criminel se faisant passer pour un acheteur envoie, par exemple, un chèque portant sur un montant supérieur à l'achat prévu, mais non couvert, au vendeur. Le commerçant qui, avant d'avoir

procédé à une vérification du chèque par le biais de sa banque, informe l'acheteur malhonnête du montant trop important, est ensuite arnaqué grâce à un mensonge. Le pirate prétend que le montant dépassant le prix prévu est en fait destiné à une tierce personne, censée s'occuper de l'animal pour une certaine période. Il indique qu'il s'agit d'une erreur et prie le vendeur de bien vouloir transférer le montant excédentaire à cette tierce personne. Si le plan du pirate réussit, le vendeur vire le montant en question avant que sa banque ne constate que le chèque n'est pas couvert. Le vendeur devient ainsi victime d'une escroquerie.

Les arnaques concernant les tests de produits fonctionnent de façon similaire : en raison de son expérience en tant que consommateur, la victime est recrutée afin de procéder à des tests confidentiels de produits. Dans ce cas, les criminels utilisent frauduleusement les noms et logos de marques connues pour feindre une véritable embauche. Tout comme pour les animaux, les pirates prétendent virer une somme d'argent supérieure au montant prévu, mais non couverte, et demandent la transmission à une tierce personne. Si les victimes virent la somme en question avant d'avoir constaté que le paiement n'était pas couvert, elles subissent un préjudice. Les escrocs utilisent la même méthode dans les domaines du marché des locations, des ventes de voitures ou encore de la recherche d'emploi. Au Luxembourg, ce genre d'escroquerie touche par exemple de plus en plus de personnes souhaitant vendre leur voiture.

Une autre forme d'escroquerie exploite la générosité des victimes. Les pirates imitent alors l'identité d'organisations caritatives réputées. S'ils disposent des coordonnées des donateurs potentiels, ils procèdent à l'envoi ciblé d'e-mails à ces derniers, les invitant à faire un don. S'ils ne disposent pas de ces coordonnées, les pirates ont recours aux spams. Les contenus typiques de ce genre d'e-mail sont des appels à l'adoption d'enfants orphelins ou encore à la générosité envers les victimes de catastrophes naturelles.

Le phishing fait également partie des formes d'escroquerie les plus répandues. Dans ce cas, les pirates tentent d'obtenir des données, telles que numéros de sécurité sociale, numéros de compte ou mots de passe en usurpant l'identité par exemple d'un établissement financier. Les données ainsi collectées permettent ensuite un accès direct au compte de la victime, ou peuvent être revendues à des tiers en vue de l'utilisation frauduleuse de l'identité. L'identité ainsi usurpée est notamment utilisée afin de contracter des crédits bancaires au nom de la victime ou de demander l'établissement de cartes de crédit.

Les pages de contact sur Internet et les sites des réseaux sociaux sont également des cibles privilégiées pour les cybercriminels : c'est par ce biais qu'ils entrent rapidement en contact avec leurs victimes. Le pirate exploite alors la sympathie exprimée par sa victime. Dans un premier temps, il tente de gagner la confiance de cette dernière en feignant la sympathie, voire l'affection. Le criminel prétend habiter à une grande distance et ressentir un désir impératif de rencontrer la victime, mais que les frais de voyage élevés lui rendent toute visite impossible. Si la victime se laisse tromper, elle procède à des virements au profit du pirate afin de couvrir les frais de voyage. Peu avant, après ou à la date du voyage, le pirate invente des raisons et des prétextes expliquant pourquoi il n'a pas pu partir comme prévu. Ce procédé peut ensuite être répété à plusieurs reprises, chaque fois avec de nouveaux frais. Ce n'est que lorsque la victime perd confiance et qu'elle cesse d'envoyer de l'argent que l'escroquerie se termine.

Au Luxembourg, une recrudescence des pièges à l'abonnement, visant en particulier les écoliers, est à noter. Un clic sur une offre alléchante ou sur une version d'évaluation a priori gratuite et le piège se referme : les escrocs ont sciemment dissimulé des clauses ou faussé certains faits et les factures, souvent accompagnées de lettres de relance, ne tardent pas à suivre.

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information suisse (MELANI) a re-

### Exemple concret :

Vol de données de cartes de crédit dans la chaîne de magasins TJX.

Début 2007 il a été rendu public que la chaîne de magasins anglo-américaine TJX avait été victime du vol des numéros de plus de 45 millions de cartes de crédit à partir de juillet 2005. Ces numéros étaient stockés dans les systèmes de traitement des paiements et de sauvegarde de la société. Le vol n'a été découvert qu'en décembre 2006. L'enquête a permis de constater que les attaquants avaient eu accès aux systèmes de l'entreprise de façon répétée. Ce n'est qu'en janvier 2007 que les accès non autorisés ont pu être stoppés définitivement. On estime que près de 30 % de la population de la Nouvelle-Angleterre a été touchée par cette attaque.

censé en 2007 des scénarios d'escroquerie supplémentaires : pour obtenir une brève hausse des cours des actions, et ainsi vendre celles qu'ils détiennent à des prix plus élevés, des pirates procèdent par exemple à l'envoi de spams comportant des recommandations d'achat sur les actions en question. Ils utilisent alors frauduleusement l'identité de prestataires financiers afin de rendre ces recommandations d'achat plus crédibles.

Les criminels n'ont aucun scrupule, l'exemple suivant le démontre de façon évidente : en Suisse, en mai 2007, un e-mail exigeant le virement d'une somme d'argent sous menace de mort à l'encontre des destinataires a été envoyé.

Les attaques pour des motifs politiques ou la défiguration de pages web par des contenus politiques ou pornographiques font également partie des formes d'attaque courantes.

Parmi les menaces et formes d'escroquerie les plus récentes, figurent les attaques iframe via le « World Wide Web », qui sont effectuées en combinaison avec des infections drive-by download. Des sites Internet

sérieux sont alors altérés par l'ajout d'une ligne de code. Cette dernière procède, pendant le chargement de la page en question, au téléchargement et à l'installation de logiciels criminels – des malwares provenant d'un autre serveur – sur l'ordinateur de la victime. Sans avoir cliqué sur un lien, sans avoir ouvert un fichier joint ou reçu un e-mail, il devient ainsi possible d'infecter son ordinateur avec des malwares, simplement en surfant sur Internet.

La révélation non souhaitée de données suite à de l'espionnage industriel et la perte de supports de données restent également d'actualité. Les attaques visant les entreprises sont de plus en plus sophistiquées. Les criminels sélectionnent par exemple, de façon ciblée, certaines personnes appartenant à une entreprise. Ces victimes reçoivent ensuite des e-mails conçus astucieusement et comportant un lien vers une page infectée par un malware ou véhiculant directement le malware en pièce jointe. Les attaques visant les serveurs web ainsi que les infrastructures wireless LAN sont également très à la mode.

Les procédés et méthodes énumérés ci-dessus ne représentent qu'un extrait de la gamme des escroqueries mises en œuvre par les cybercriminels.

## Le milieu des cybercriminels

Le milieu des pirates Internet est désormais très bien organisé et structuré en fonction des tâches, des niveaux de connaissance et de l'énergie criminelle développée. Les « experts » parmi les cybercriminels développent les logiciels malveillants, que d'autres délinquants utilisent ensuite afin de perpétrer des actions criminelles. Ces malwares peuvent être utilisés pour télécommander les ordinateurs d'utilisateurs d'Internet qui, à leur insu, sont devenus les victimes des pirates. Les utilisateurs ne sont en effet pas conscients du fait que leur ordinateur est contrôlé à distance par des tiers et exploité à des fins criminelles.

Les données recueillies par les pirates peuvent être vendues sur des marchés clandestins, spécialisés dans ce genre de transactions. Le prix clan-

destin pour l'envoi de 10 millions de spams par jour se situait aux environs de 600 dollars en 2007. Un numéro de carte de crédit sans PIN, mais avec les données requises pour réaliser des opérations d'e-commerce se négociait 25 dollars, un numéro de carte de crédit avec le PIN correspondant revenait à 500 dollars. Selon leur type, les chevaux de Troie peuvent être acquis à des prix allant de quelques centaines à plusieurs milliers de dollars.

## Les réflexes de sécurité comme réponse à la criminalité

La cybercriminalité n'est rentable que si les usagers d'Internet fournissent aux pirates des points d'attaque, c'est-à-dire des failles à exploiter. Une bonne dose de vigilance et de méfiance réduit déjà de façon significative le risque de devenir une victime de ce type d'escrocs. Si l'utilisateur doute de l'authenticité d'une information ou d'un e-mail, un simple appel téléphonique auprès de l'entreprise ou de l'organisation caritative concernée suffit généralement pour clarifier la situation. Il est alors conseillé d'utiliser le numéro de téléphone usuel, tel que communiqué par les renseignements téléphoniques. De plus, Les usagers d'Internet devraient se tenir régulièrement informés des méthodes d'escroquerie « à la mode ». Si des pirates tentent d'avoir recours à de telles méthodes, l'utilisateur ne doit pas hésiter à en aviser immédiatement les autorités compétentes ainsi que le prestataire concerné par une éventuelle usurpation d'identité.

En raison de la haute technicité des méthodes d'attaque utilisées, l'ordinateur du domicile devrait être équipé de moyens de protection techniques adéquats. Il convient ainsi de veiller à ce que tous les programmes et le système d'exploitation soient régulièrement mis à jour, les droits d'accès des utilisateurs soient limités, un logiciel antivirus régulièrement mis à jour ainsi qu'un pare-feu correctement paramétré soient installés et que l'ordinateur soit régulièrement analysé à l'aide d'un logiciel anti-spyware.

### Conseil de sécurité :

Les pages Internet suivantes permettent de se tenir informé des formes d'escroqueries et d'attaques les plus courantes et nouvelles :

[www.lookstoogoodtobetrue.com](http://www.lookstoogoodtobetrue.com)

[www.melani.admin.ch](http://www.melani.admin.ch)

[www.ic3.gov](http://www.ic3.gov)

[www.cases.lu](http://www.cases.lu)

### Définitions :

- Lettres nigérianes

Forme d'escroquerie au cours de laquelle des criminels se font passer pour des représentants officiels et sollicitent de l'aide lors de virements de sommes importantes vers des comptes outre-mer.

- Spams

Les spams sont des messages indésirables, généralement transmis par voie électronique. Ces messages sont des envois en masse ou des envois publicitaires transmis aux destinataires sans que ces derniers les aient sollicités.

- Serveur

Le terme serveur désigne un programme communiquant avec un autre programme afin de mettre à disposition de ce dernier un accès à des services spécifiques. Il désigne également un ordinateur lorsqu'un ou plusieurs serveurs sont en service sur celui-ci.

- Wireless LAN

Un WLAN est un réseau local sans fil fonctionnant par ondes radio.

Pour les entreprises, il est en particulier recommandé de sensibiliser les collaborateurs à la sécurité des informations. Les données devraient, en outre, être cryptées et les applications Internet devraient être vérifiées quant à d'éventuelles failles de sécurité. Il est conseillé d'intégrer une politique de sécurité informatique active au niveau des processus de l'entreprise.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)