Spams, hacks, vers et virus: l'internet de tous les dangers (21/05/2004)

Imprimer | Envoyer à un ami

EMMANUEL GRANDJEAN

Dessin Tirabosco

- **Alertes aux vers et courriels indésirables se multiplient. Surfer sur le web n'a jamais été aussi périlleux qu'aujourd'hui.**
- **Comment les Etats-Unis, l'Europe et la Suisse cherchent à juguler l'épidémie.**
- **Filtres antispam, fire-wall et antivirus: les gestes qui sauvent.**

Des fenêtres qui s'ouvrent en cascade, le tiroir du CD-ROM qui godille sans raison apparente et des aspirateurs à mots de passe camouflés en fausses pages web (la technique du "phishing"): se lancer sur l'internet, en ce moment, c'est s'embarquer sur une drôle de galère. Remarquez, si la Toile ressemble à un coupe-gorge, la faute en incombe en partie aux utilisateurs. Par manque de vigilance, voire par ignorance, l'internaute non averti participe en plein à l'épanchement de cette épidémie électronique. Et sa vitesse de propagation est fulgurante. Car depuis le début de l'année 2004, ce sont des dizaines d'attaques virales et de vers e-mail qui grignotent le fruit numérique. Sans compter la recrudescence des spams, ces courriels indésirables dont le nombre atteint un niveau affolant dans les messageries du monde entier.

Faut-il pour autant succomber à la parano et noyer son computer au fond d'un plot de béton? On serait tenté de ne répondre ni oui ni non. Tout est ici affaire de comportement. L'internaute ne le sait peut-être pas, mais dans la poudreuse du net, le surf laisse des traces. Et pas que des petits sillons. Les sites enregistrent les goûts et les préférences de leurs visiteurs, demande leurs adresses e-mail. Quoi de mal après tout à donner le nom de sa boîte aux lettres? L'ordinateur, lui, fait minutieusement son boulot. Il retient la liste des endroits où il fait bon musarder et, le cas échéant, garde en mémoire les mots de passe, histoire de gagner du temps.

La théorie des chapeaux

Question temps, le gain profite surtout aux mass maileurs qui achètent à bon prix des listes d'adressages et aux hackers qui connaissent ainsi les habitudes de leurs clients. Reste à connaître les raisons profondes qui animent ces empêcheurs de surfer en rond. Pour les spammeurs, elles sont plutôt faciles à deviner: l'argent. Les polluposteurs peuvent amasser une véritable fortune à force de sollicitations intempestives.

Du côté des hackers, les intentions divergent. Les spécialistes de la protection de données subdivisent ces monte-en-l'air cyber en trois clans: les "White Hat" (les chapeaux blancs), qui testent la sécurité informatique des entreprises à des fins prophylactiques, les "Black Hat" (les chapeaux noirs), qui annoncent clairement la couleur, et les "Grey Hat" (les chapeaux gris). Les plus dangereux pour les spécialistes, car leurs intentions restent imprécises. Ceux-ci farfouillent sur le réseau sans coup férir en pouvant d'un coup verser du côté obscur. Reste que la grande majorité d'entre eux s'adonne à l'intrusion par jeu, tout simplement. Un jeu à l'échelle mondiale et dont le nombre de participants est impossible à comptabiliser.

Le casse-tête wi-fi

Du coup, les créateurs de virus informatiques se livrent à une course effrénée. Objet de la compétition? Une certaine forme de gloire. C'est à celui qui fera le plus de dégâts, le plus rapidement possible et sans se faire pincer. Si le créateur de Sasser vient tout juste de se faire serrer par les autorités allemandes, les programmeurs de Netsky, MyDoom et Bagle, eux, courent toujours. Quitte à se provoquer par message interposé inclus dans le code-source de leurs petits programmes nuisibles. "Bagle, t'est nul" trompetait ainsi la dernière mouture de Netsky. Réponse du berger à la bergère: "Ne ruinez pas notre petit commerce. Vous voulez la guerre?" claironnait le pirate visé entre les lignes de sa réplique virale.

Mais le pire des casse-têtes reste à venir. On veut parler de la technologie wi-fi qui, si elle permet de se connecter à l'internet sans fil à la patte, secoue méchamment les anges gardiens du cyberspace. Comment sécuriser un système qui transporte de l'information par ondes radios? Autant essayer d'attraper des papillons avec une poêle à frire. Pour l'heure, c'est le Wardriving qui préoccupe les esprits. Le principe consiste à quadriller les rues avec un ordinateur portable équipé d'une petite antenne. Chemin faisant, le pirate repère l'une de ces connexions ouvertes à tous les vents. Ni vu ni connu, le voilà qui profite non seulement de la ligne mais peut également tenter une petite visite dans l'ordinateur squatté.

Remarquez, tout n'est pas perdu pour tout le monde. Le marché de la sécurité internet est florissant et le gâteau plutôt alléchant à se partager. La firme américaine Basex estime à 20 milliards de dollars la somme dépensée par les entreprises pour parer aux dangers du net. Et le chiffre grossit d'année en année.

Lexique

Hacker. Inventé par le philosophe finlandais Pekka Himanen, le mot désignait à l'origine un internaute soucieux de partager son savoir avec la communauté connectée. Aujourd'hui, il qualifie les intrus du net qui écument le réseau à la recherche d'un mauvais coup à perpétrer.

Virus. Pour faire simple, le virus est un programme autorépliquant qui se lie à d'autres applications déjà existantes. La contamination se déroule à partir d'un logiciel pirate où d'une connexion douteuse, histoire de toucher le plus grand nombre d'ordinateurs possible dans un laps de temps très court.

Ver. Type particulier de virus, les vers (ou Worms) représentent l'écrasante majorité des attaquants du net. Comme Sasser, dernier cyberlombric en date. Ces derniers se propagent via l'e-mail en envoyant des missives à l'intégralité du carnet d'adresses infecté.

Spam. Ce sont les courriels intempestifs qui occupent votre boîte électronique. Le "spam" tire son nom d'un fabricant de corned-beef américain dont les Monty Python firent autrefois la renommée. A noter que les gardiens de la langue française préfèrent parler de "pourriels".

Spyware. La guigne du web, le spyware, s'installe comme un grand sans rien demander à personne. Ce programme espion connaît ainsi vos habitudes de surf, les données personnelles enregistrées sur votre disque dur et ouvre des fenêtres à répétition (pop-up) pendant que vous musarder sur le réseau.

PC-Dialer. Celui-là se niche sur des sites généralement réservés aux adultes. L'opération se déroule comme suit: une fenêtre prévient l'internaute que l'accès à l'information demandée nécessite l'installation d'un programme spécifique. Le benoît donne son accord. Et voilà le PC-Dialer (ou Webdialer ou encore Dialer tout court) qui s'en va modifier le numéro de téléphone de la connexion contre un autre supermajoré. La facture de téléphone prend d'un coup l'ascenseur. A noter que l'opération frauduleuse ne touche pas les abonnés à l'internet haut débit.
E. G.

Quelques règles d'or pour un surf en argent

Imaginez une porte à battant à travers laquelle une foule compacte entre et sort en même temps. Internet, c'est un peu la même chose. Sauf que des issues, votre ordinateur en compte 65 000. Appelez-les des ports. Des ports qu'il s'agit de bien

contrôler pour éviter de voir n'importe qui s'y insinuer. C'est par là que le hacker se faufile et par là aussi que votre ordinateur, sans penser à mal, communique des informations sensibles.

La généralisation des connexions haut-débit (ADSL) ouvertes en permanence sur le web favorise du coup les intrusions. S'équiper d'un programme pare-feu (fire-wall) constitue, avec l'acquisition d'un antivirus, l'un des premiers gestes de survie de l'internaute consciencieux. ZoneAlarm tient gracieusement à votre disposition un fire-wall épatant et qui ne coûte pas un rond (www.zonealarm.com). Pour le reste, voici en quelques points les autres règles d'or à respecter.

- **Contre les spams**
  Ne jamais diffuser son adresse e-mail. Ne jamais ouvrir un message d'un destinataire qui vous est totalement inconnu. Utiliser des filtres anti-spam. L'astuce ne fonctionne pas toujours. Mais c'est toujours mieux que rien.

- **Contre les spywares**
  A moins de posséder des doigts de fées et des connaissances pointues en informatique, faites confiance à certains produits du marché pour éradiquer ces espiogiciels. Il en existe deux parfaitement efficaces et parfaitement gratuits. Ad-Aware (www.lavasoftusa.com) et Spybot (spybot.eon.net.au) reniflent le registre de votre navigateur et suppriment ceux qui n'ont rien à y faire.

- **Contre les vers**
  Ceux-ci pullulant via l'e-mail, gardez un oeil vigilant sur votre messagerie. Car une fois le ver dans le fruit, bonjour la galère. Sachez aussi que ces lombrics nuisibles aiment plus que tout croquer dans la pomme Microsoft. La multinationale met régulièrement à jour les stratégies guerrières de Windows à l'adresse www.microsoft.com

- **Contre les virus**
  Pas la peine de chercher midi à quatorze heures. Pour lutter contre les virus une seule solution: l'antivirus. Il en existe une pleine tripotée. On se bornera à citer les plus célèbres d'entre eux fabriqué par Symantec (www.symantec.com) ou encore McAffee (www.mcaffee.com). Détail important, n'oubliez jamais d'effectuer régulièrement les mises à jour de ces programmes. Contrairement au bon vin, un antivirus se périme avec l'âge.
  E. G.

Un risque de menace pour notre société

Elle milite pour un "Internet pour tous". C'est dire si l'Internet Society, dont l'un de ses sièges se trouve à Genève (www.isocgva.ch), surveille l'évolution de l'affaire. Pour Stéphane Koch, son président, il n'y a pas trente-six solutions pour rendre au web sa fraîcheur d'antan: les internautes doivent se discipliner et les gouvernements prendre leurs responsabilités.

- A quoi est due la recrudescence des attaques virales, des spams et des spywares sur le net?
- Les attaques virales augmentent en même temps que le nombre d'internautes augmente. Il faut aussi prendre en compte un phénomène de résonance des malaises présents au sein de notre société. Les gens ne se sentent plus représentés par les politiques qui favorisent les intérêts des lobbys avant ceux de leurs électeurs. L'"hactivisme" pourrait être une conséquence de cette crise.

Les spywares, au même titre que la majorité des "problèmes" du net (failles de sécurité, cybersquatting, spamming), profitent également d'un vide législatif voulu, ainsi que de la promotion d'une vision économique à court terme.

- Pensez-vous que cette prolifération met l'internet en danger?
- Si l'internet venait à être en danger, c'est la société elle-même qui serait menacée. Les Nouvelles Technologies de l'information (NTIC) font aujourd'hui partie de notre société. Le risque à l'heure actuelle est la course en avant visant à générer du profit et à créer de nouveaux marchés sans prévoir de protection. Et personne ne prend vraiment le temps de réguler ces nouvelles niches commerciales.

La gestion des données personnelles et mercantiles à travers le monde exemplifie le problème. Des entreprises collectent des informations qu'elles peuvent utiliser sans que

des lois régissent ce type de pratiques, si ce n'est localement, et encore selon des critères différents. C'est en partie le manque de législation au niveau des fournisseurs d'adresses e-mail gratuites qui tend à alimenter le trafic des spams.

- Des solutions politiques peuvent-elles résoudre le problème?
- Le problème des gouvernements est leur manque de représentativité ainsi que leur manque de crédibilité. Il y a aussi un manque flagrant de compétences, au sens propre du terme. Les difficultés sont tellement complexes que cela nécessite des expertises que les Etats ne peuvent assumer en raison des coûts induits. Ils pourraient consulter les membres de la société civile qui possèdent les connaissances nécessaires. Mais, craignant des dérives "interventionnistes", ils hésitent à demander leur avis. Rappelons que la société civile a été exclue des réunions "gouvernementales" du Sommet mondial de la société de l'information en décembre dernier.

- N'est-ce pas aux internautes de se discipliner?
- C'est à tout le monde de se discipliner, l'internet est un modèle coopératif. Si la nécessité économique ne poussait pas à "vendre avant de comprendre" et à "acheter sans se soucier", il n'y aurait pas autant de problèmes. Prenons l'exemple de l'ADSL, on en a longtemps fait la publicité sans pour autant parler des protections nécessaires lors de l'installation de ce type de connexion haut débit. C'est aussi invraisemblable que de vendre une voiture de sport à laquelle manqueraient les serrures aux portières. Les entreprises, par souci d'économie, refusent de former leurs
E. G.

La législation européenne se heurte à un axe du mail

Les gros fournisseurs de pourriels empêchent l'Europe d'agir efficacement.

MICHEL EGGS

Depuis le 31 octobre 2003, les Etats membres de l'UE doivent se conformer à une directive (loi européenne) sur la vie privée et les communications électroniques qui s'attaque aux spams. Principe de base: à une exception près les communications s'inscrivant dans le cadre d'une relation client-fournisseur , la prospection commerciale par courrier électronique n'est autorisée qu'avec le consentement préalable des abonnés. Ce principe dit de l'opt-in est également valable pour les SMS et autres messages électroniques envoyés à des terminaux mobiles et fixes.

Cette directive complète une législation datant de 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

Pays sur la sellette

Mais plusieurs Etats membres, censés avoir transposé dans leur droit national la nouvelle directive, traînent les pieds. Au point que l'Exécutif européen a dû ouvrir une procédure d'infraction contre la Belgique, l'Allemagne, la Grèce, la France, le Luxembourg et les Pays-Bas; ces pays ont jusqu'au 1er juin pour se conformer, sans quoi ils seront poursuivis devant la Cour de justice des Communautés européennes.

La fermeté de Bruxelles ne masque pourtant pas l'inefficacité de cette directive. Elle a certes conduit la plupart des entreprises européennes à cesser le spamming. Mais elle est totalement inopérante pour les messages abusifs provenant de pays tiers. "Il y a un axe du mal du spam, soit les Etats-Unis, la Chine et la Corée du Sud. Et la législation européenne est impuissante à leur égard", commente Lodewijk Asscher, coordinateur d'une étude menée par l'Institute for Information Law (IVIR) de l'Université d'Amsterdam sur la réglementation européenne. Bruxelles en est conscient, qui évalue actuellement des actions complémentaires au sein de l'UE tout en favorisant un accord international dans le cadre de l'OCDE.

Les Etats-Unis, paradis du spam

Depuis le 1er janvier, les USA sont censés interdire l'envoi de courriels indésirables.

Le chiffre alarme. Avec 56,8% de spam provenant des Etats-Unis, la première

puissance mondiale est également celle qui encombre le plus les boîtes e-mail de la planète. Ce qui pendant longtemps n'a pas franchement inquiété le gouvernement américain. Lequel s'est même un peu fait prier pour réagir malgré le fort mécontentement de la population.

Après avoir longtemps minoré les méfaits du spam, le Sénat promulguait le 1er janvier 2004 une loi censée barrer la route des polluposteurs. Le programme s'intitule "Can-Spam Act (pour Controlling the Assault of Non Sollicited Pornography and Marketing Act). Il réclame, en gros, que les mass maileurs demandent l'autorisation préalable des internautes avant de faire rendre gorge à leurs boîtes électroniques. Et gare aux fesses de celui qui passerait outre à la directive! Le gouvernement brandit des peines de prison et de fortes amendes pour infléchir les ardeurs des éventuels contrevenants. Il prévoit également la mise sur pied d'un programme Do-Not-Spam, l'équivalent pour l'internet de la liste rouge du téléphone. Emus par la complexité du texte et par l'écheveau de ramifications juridiques, certains spécialistes doutèrent rapidement de l'efficacité du système.

Un sondage effectué à fin février 2004 par l'Institut Ipsos pour le compte de l'Associated Press confirmait le peu de changements apporté par cette ruade législative. L'enquête révélait que deux mois après son application, huit Américains sur dix continuaient à être assaillis de pourriels. Et qu'un internaute sur dix prétendait même en recevoir davantage qu'auparavant.
E. G.

La lente marche helvétique contre les pourriels

La parade politique contre le spam reste très hypothétique. En Suisse, comme ailleurs, cette lutte passe par un texte de loi. Celui qui régit les télécommunications (LTC), en l'occurrence, et dont le contenu doit prochainement être soumis à modification. Outre d'étudier le dégroupage du dernier kilomètre qui reste pour l'heure l'apanage de Swisscom, la nouvelle loi prévoit également d'interdire l'envoi en masse de messages publicitaires considéré à l'égal d'une concurrence déloyale.

Le débat qui vient d'être accepté par le Conseil des Etats doit encore passer devant le Conseil national pour une application prévue aux alentours de 2006. Dans l'intervalle, l'internaute helvétique a toujours la possibilité d'exiger d'un propriétaire de liste d'envoi d'accéder aux informations personnelles en sa possession.

L'Office fédéral de la communication, elle, a déjà statué sur un autre de ces empêcheurs de se promener. Celui des PC-Dialers qui, une fois installé, se connecte à l'internet via un numéro majoré. Le système compte déjà passablement de victimes qui ont vu leurs notes de téléphone effectuer un bond de comète. Depuis le 2février 2004, l'Ofcom interdit aux titulaires de numéro 0900, 0901 et 0906 de proposer l'installation de PC-Dialer sur les ordinateurs de leurs clients.
E. G.

Tribune de Genève: tél: +41 22 322 40 00 fax: +41 22 781 01 07
11, rue des Rois - CP 5115 - 1211 Genève 11,
Accueil | contacter le Webmaster | contacter la Rédaction