

La chasse aux gangs de spams

Microsoft et les autorités américaines ont annoncé le démantèlement d'un réseau de spams. Mais les «pourriels» ne sont pas près de disparaître.

TEXTE | *Jean-Cosme Delaloye*

L'opération «b 107» a porté ses fruits. Menée par les autorités américaines et le groupe informatique Microsoft, elle a permis en mars dernier le démantèlement du réseau «botnet» (multiples ordinateurs utilisés pour générer du spam) Rustock. Il comprenait un million d'ordinateurs infectés par un virus. Contrôlées à distance par des hackers, ces machines pouvaient envoyer jusqu'à 30 milliards de «pourriels» par jour. «La destruction d'un botnet n'est qu'une goutte d'eau dans l'océan, car d'autres émergent rapidement», prévient Olivier Bourgeois, patron de la société Fastnet à Saint-Sulpice (VD).

A l'heure actuelle, entre 75 et 95% des e-mails envoyés chaque jour à travers le monde sont des pourriels. La compagnie Symantec, spécialiste mondiale de la sécurité internet, estime leur nombre quotidien à plus de 150 milliards. «Un ordinateur sur cinq est infecté et peut être utilisé dans un botnet», explique Christian Buchs, professeur à la Haute école d'ingénieurs et de gestion du canton de Vaud (HEIG-VD). En 2009, le groupe Ferris Research à San Francisco, a chiffré le coût du spam à 130 milliards de dollars (117 milliards de francs), une somme qui a doublé depuis 2005.

Les principaux spammeurs sont connus et recensés par le Spamhaus Project, un groupe anti-spams. Parmi eux, on retrouve plusieurs Russes

dont Leo Kuvayev alias BadCow ainsi que le groupe ukrainien Canadian Pharmacy. «C'est difficile de lutter contre ces gangs, explique Brett Stone-Gross, doctorant à l'Université de Californie et coauteur d'une enquête sur le réseau botnet Cutwail. La plupart d'entre eux opèrent depuis des pays comme la Russie, où l'envoi de spams n'est pas un crime.» Le Spamhaus Project estime qu'une centaine de groupes de spammeurs est à l'origine de l'envoi de 80% des pourriels.

La principale stratégie de lutte contre les pirates informatiques consiste à infiltrer leurs réseaux et à identifier leurs serveurs. Des professeurs et chercheurs de la HES-SO ont lancé le projet Internet Surveillance for Criminal Intelligence Analysis qui a pour but de recueillir le plus de données possible sur les spams, pour les transmettre ensuite aux autorités. «Nous faisons l'extraction de toutes les informations techniques des spams, glisse Christian Buchs. Nous essayons notamment de les cataloguer grâce à la géolocalisation d'adresses IP.»

Une étude de l'Université de Californie datant de 2008 montrait qu'un spam sur 12,5 millions obtenait une réponse. Un taux qui suffit à assurer aux spammeurs un revenu conséquent. Brett Stone-Gross estime que le gang derrière le réseau Cutwail a gagné entre 1,7 et 4,2 millions de dollars depuis juin 2009. ☹



Avec son projet *Polyspam*, la photographe espagnole Cristina De Middel s'est intéressée au phénomène du pourriel et des escroqueries par e-mail. Elle a recréé les décors et les circonstances narrées dans certains de ces messages et en propose sa propre vision. *Polyspam* a été exposé dans le cadre du festival veveysan Images 2010. Née en 1975, Cristina De Middel travaille pour plusieurs quotidiens espagnols, tout en développant parallèlement des projets plus personnels, sur la prostitution ou le tourisme de masse, par exemple.



La version complète de la revue
est en vente sur le site
www.revuehemispheres.com

De: Marisol@bp06.net
Objet: Marisol
Date: vendredi 6 juin 2008, 10:00
A: info@lademiddel.com
Répondre à: marisol@astrologi-gratuita.com

Bonjour, Je m'appelle Marisol, j'ai 37 ans et je pratique la voyance avec passion depuis dix-neuf ans. Au cours des dix dernières années j'ai participé à plus de 50 émissions télévisées. (...) Je n'ai recherché ni gloire ni argent, j'ai connu des passes difficiles, des moments de doute, des difficultés financières, des tourments, la dépression. (...) J'ai fondé l'Ecole de voyance de Madrid. Les meilleurs professionnels d'Espagne travaillent dans mon cabinet (clairvoyants, astrologues et tarologues). Aujourd'hui, je suis une professionnelle réputée qui met toutes ses compétences au service de sa vocation. (...) Je peux me permettre de ne pas vous faire payer pour mes services, si vous souhaitez bénéficier de mes conseils vous pouvez m'appeler au 806.556.336*. Marisol

* Seul le coût de l'appel vous sera facturé: 1,16 € depuis votre téléphone fixe et 1,51 € depuis votre téléphone portable.



La version complète de la revue
est en vente sur le site
www.revuehemispheres.com

De: s.nzi005@yahoo.fr
Objet: Salut mes chers
Date: 16 janvier 2008 19:01:32
GMT+01:00
A: s.nzi005@yahoo.fr
Répondre à: s.nzi2007@yahoo.fr

Salut mon cher, Comment ça va avec votre famille?
Aujourd'hui est un bon jour pour écrire mais ce n'est pas obligatoire et je ne vous oblige en aucune façon de faire quoi que ce soit contre votre gré. Je m'appelle Sandrine Nzi. J'aurai 25 ans demain. Je suis la fille unique du chef (feu) M. Joseph Nzi. De son vivant, mon père était un mineur d'or réputé en Côte d'Ivoire. (...) Avant sa mort, l'orateur a demandé au secrétaire qui l'accompagnait à l'hôpital et lui a dit qu'il avait déposé la somme de US \$10'500'000 dans l'une des principales banques à Abidjân, Côte d'Ivoire. Il lui a également dit que l'argent était déposé en mon nom et qu'il avait donné des consignes écrites à son avocat qui affirme qu'il est en possession de tous les moyens et documents juridiques en rapport avec ce dessous et la banque. J'ai à peine 20 ans et suis étudiante à l'université et ne sais vraiment pas quoi faire. Maintenant je veux un compte à l'extérieur sur lequel on peut transférer l'argent. (...) Répondrez-vous à cette offre? S'il vous plaît, réfléchissez-y et manifestez-vous dans les meilleurs délais. Merci d'être là pour moi. Cordialement, Sandrine Nzi.



La version complète de la revue
est en vente sur le site
www.revuehemispheres.com

De: susan-morrison@excite.com
Objet: Re: Salutations
Date: 10 septembre 2006 03:33:57
GMT+02:00
A: info@lademiddel.com

Bonjour, Vous serez peut-être surpris de recevoir ce courriel, en le lisant n'ayez pas trop pitié de moi car je sais que tout le monde meurt un jour. Je m'appelle Mme Susan Morrison, une femme d'affaires à Londres. J'ai été diagnostiquée avec un cancer de l'œsophage à un stade très avancé car j'ai été laxiste avec ma santé. Mon cancer est désormais résistant à tout type de traitement et d'après les médecins il ne me reste que quelques heures à vivre. (...) Les derniers fonds dont aucune personne n'a connaissance sont déposés en espèces dans l'une des banques ici. Je souhaite savoir si vous pouvez m'aider à transférer ces fonds à des organisations caritatives. 20% du montant total de \$ 1'500'000 (un million cinq cent mille dollars) vous sont réservés pour le temps et la patience que vous consacrerez à l'exécution de cette tâche. En d'autres termes, vous conserverez \$ 300'000 (trois cent mille dollars) et verserez le reste à une organisation caritative. Que Dieu soit avec vous car vous avez pris une décision courageuse en acceptant de guérir le monde avec moi, même si je meurs. Je vais maintenant subir une intervention chirurgicale à laquelle je ne pense pas survivre. Meilleures salutations, Susan Morrison.