



G Data – Communiqués de Presse 2010

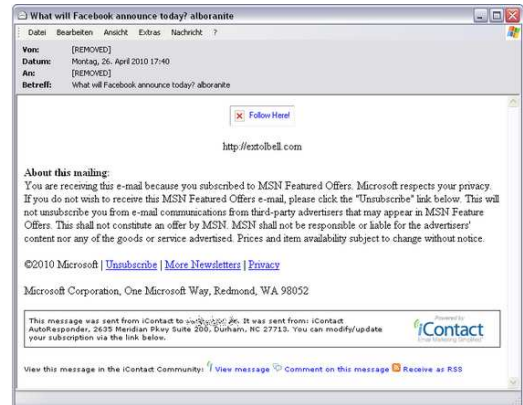
# Le spam « pharmacie » se camoufle mais reste toujours aussi actif.

**G Data Software a analysé une vague de spam « pharmacie » et livre ses conclusions : caché derrière des sujets d'actualités, les courriels indésirables de vente de médicaments continuent d'inonder le Web.**

Les cybercriminels rivalisent d'ingéniosité pour faire cliquer les internautes sur des sites de ventes de produits pharmaceutiques en ligne. Tous les sujets sont bons pour attirer le client. Il y a quelques semaines, les activités du volcan Islandais Eyjafjallajökull étaient à la une des journaux. Elles faisaient aussi le bonheur du spam qui reprenait les titres les plus accrocheurs dans ses objets. Tous les sujets d'actualité sont aujourd'hui utilisés pour contourner les systèmes de filtrage. Pour illustrer ce fonctionnement, G Data Software a analysé une vague de courriels indésirables : 900 spams en apparence différents, mais finalement très proches.

## Un même courriel, mais des objets différents

Le courriel indésirable prend la forme d'une newsletter émise par MSN. Le corps du texte est identique et les adresses mails utilisées sont toutes Russes (extension.ru). Les similitudes s'arrêtent là. Sur les 900 courriels collectés, aucun n'a le même objet. Et tous tournent autour de l'actualité.



## Qui se cache derrière cette campagne ?

Les liens intégrés dans ces courriels pointent tous vers un même site « Canadian Pharmacy». Plusieurs domaines sont utilisés. Tous ont été enregistrés il y a quelques jours par l'intermédiaire de 4 sociétés chinoises.



## Domaines identifiés

- [usuallife.com](http://usuallife.com)
- [extolbell.com](http://extolbell.com)
- [peopleeasy.com](http://peopleeasy.com)
- [flairfew.com](http://flairfew.com)
- [sugarspoke.com](http://sugarspoke.com)
- [themreply.com](http://themreply.com) [hors ligne]
- [seemlychief.com](http://seemlychief.com) [hors ligne]
- [givingvery.com](http://givingvery.com) [hors ligne]
- [allownine.com](http://allownine.com) [hors ligne]
- [quartwin.com](http://quartwin.com) [hors ligne]
- [maxistood.com](http://maxistood.com) [hors ligne]

### **Sociétés propriétaires des domaines**

- CHINA SPRINGBOARD INC (Chine)
- BIZCN.COM, INC. (Chine)
- BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD (Chine)
- 35 TECHNOLOGY CO., LTD (Chine)

Tous les sites Web sont hébergés sur le même serveur situé en Chine. Cependant, les serveurs changent. Depuis le début de la recherche, G Data a déjà identifié deux migrations.

### **Les moyens pour contourner les filtres antispam**

Sur les 900 courriels analysés, il n'est jamais fait mention du terme médicament ou Pharmacie. Ces termes induiraient automatiquement l'activation du filtre antispam sur les solutions avec analyse de contenu. De même, tous les objets sont différents. Ainsi, 825 comportaient un mot unique commençant par « a » (mot en italique dans les extraits ci-dessous). Cette intégration automatique d'un mot à l'extrémité de la ligne d'objet est un autre système utilisé par les spammeurs pour déjouer la vigilance des filtres antispam. Tous les objets étant différents, aucun courriel n'est identifiable comme étant indésirable.

Exemples des objets des courriels indésirables collectés :

- 200,000 flood Shanghai Expo preview *acoustics*
- Air travel updates amid volcanic ash *addibility*
- Alain Robert: Living on the edge *adamances*
- Apple posts record quarter *accordingly*
- AT&T unveils Buzz.com *aerobatics*
- Cairo reporter on the city's best *actifier*
- China pays tribute to quake victims *acarpous*
- China under growing currency pressure *alamos*
- Chrysler in \$143M profit *aitch*
- Conservatives unveil manifesto *acnodes*
- Country profile: Georgia *aglets*
- Cricket: IPL is hit by corruption claims *agnails*
- Enjoy a glass of Georgian wine *acatholic*
- Eruption's disruption to business *actualist*
- Fears volcano chaos will continue *advising*
- Football: Bayern smash seven goals *afters*
- Football: Inter fight back to stun Barca *accommodated*
- Football: Lyon target win over Bayern *adenological*
- Fraud Case upstages Goldman results *agrestic*
- Georgia's 47-year-old prima ballerina *agednesses*
- 'Glee' + Madonna = perfection *acesoeries*
- Goldman Sachs was top Obama donor *abdications*

Pour bloquer les courriels indésirables, G Data Software utilise dans ses solutions un système d'analyse et de blocage basé sur les méthodes d'envoi des courriels, et non sur leur contenu. Une technologie plus efficace contre ces vagues de spam.

Pour toute question ou demande d'interview :

**Jérôme Granger - G Data Software AG**

**Tél. : 01 41 48 51 46 – mob. 06 08 77 32 26 – e-mail : jerome.granger@gdata.fr**

À propos de G Data Software AG : Avec plus de 20 ans d'expérience dans la sécurité informatique, G Data est aujourd'hui un des leaders, présent dans plus de 60 pays. G Data réunit dans ses produits le meilleur de la technologie : par exemple la technologie DoubleScan (deux moteurs d'analyse indépendants), et la protection immédiate OutbreakShield... Depuis 5 ans, aucun autre éditeur de logiciels de sécurité européen n'a obtenu autant de distinctions nationales et internationales que G Data.