TRIBUNE DE GENÈVE

Sur le Web, tous les coups sont permis!

CYBERCRIMINALITÉ | De l'injection de liens «pourris» au «clickjacking», les attaques malicieuses deviennent toujours plus subtiles et insaisissables.

LUCA SABBATINI | 21.10.2008 | 00:00

Récemment, une société genevoise très bien référencée sur Google Suisse a été bannie des résultats du moteur de recherche. Ladite société, qui souhaite garder l'anonymat pour d'évidentes raisons d'image, n'avait pourtant rien à se reprocher d'un point de vue moral. Son seul tort?

N'avoir pas vu qu'une faille de sécurité permettait à des personnes malintentionnées de rediriger le trafic de son site vers des vidéos pornos ou des points de vente de Viagra.

La mésaventure de l'entreprise genevoise est loin d'être isolée. Dans les douze derniers mois, plusieurs centaines de sites suisses, dont une église vaudoise et un célèbre publicitaire ayant pignon sur rue à Genève, auraient été ainsi contaminés par des liens «pourris».

Cette attaque fait partie du nouvel arsenal des cybercriminels, dont les techniques deviennent de plus en plus subtiles et difficiles à détecter. Alors que les internautes prennent tout juste conscience des méfaits du phishing, le fameux «hameçonnage» des données personnelles, les nouveaux pièges du Web restent encore mystérieux.

Attaques dévastatrices

Dans quel but des malfaiteurs pénètrent-ils frauduleusement sur un site, non pas pour en extraire des informations sensibles mais pour y injecter du spam? «Leurs motivations peuvent être multiples», souligne Stéphane Koch, spécialiste genevois de la sécurité de l'information, qui a réalisé une vidéo pour expliquer le problème sur son blog Intelligentzia.ch. En exploitant des services tels que Google Alerts, les spammeurs peuvent connaître les mots-clés qui font l'objet de recherches. Ils parviennent alors, en utilisant ces mots-clés, à détourner le trafic des sites légitimes vers leurs propres activités.

L'autre utilisation, comme dans l'exemple genevois ci-dessus, est beaucoup plus perverse: amener un site à être éliminé des résultats des moteurs de recherche qui ont tendance à exclure les adresses Web «douteuses» de leurs réponses. On l'aura compris, c'est l'arme parfaite pour des concurrents sans scrupules.

«Ce type d'attaque peut avoir des conséquences dévastatrices», constate Stéphane Koch. Pour une entreprise dont l'essentiel du chiffre d'affaires se fait sur le Web disparaître des moteurs de recherche peut signifier un manque à gagner considérable – voire la mort.

Le procédé en question utilise des failles de sécurité connues dans plusieurs programmes de publication de forums, de blogs, notamment Wordpress 2.2.3, ou de CMS (Content Management System). «Pour s'en prémunir, il suffit de mettre à jour ces outils», conseille Stéphane Koch.

Webcam piratée

Autre technique malveillante qui vient de sortir: le «clickjacking». Comme son nom l'indique, il s'agit d'un «vol de clic». En exploitant une faille d'un logiciel très répandu, Flash d'Adobe, des cybercriminels seraient capables de créer sur des sites des liens provisoires leur permettant de prendre le contrôle d'une webcam à l'insu de son propriétaire, par exemple. Ou de reconfigurer ses préférences en matière de sécurité, laissant la porte ouverte à tous les abus. De quoi donner bien des sueurs froides aux internautes, même si Adobe s'est dépêché de corriger le défaut.

Moralité: sur le Web comme ailleurs, le mal a toujours une longueur d'avance.