DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

SURFEZ TRANQUILLE? LES CHERCHEURS AUSSI SONT CONCERNÉS

Publié le 28 décembre 2015

par Christian Du Brulle

Spams, virus, chevaux de Troie, vols de mots de passe ou de données bancaires: sur Internet les scientifiques aussi sont victimes d'arnaques. "Les cybercriminels jouent le plus souvent sur trois registres pour obtenir de leurs victimes des informations qu'elles ne sont pas prêtes à leur donner", explique Olivier Bogaert, Commissaire à la Police judiciaire fédérale, spécialisé en nouvelles technologies. "Il s'agit de nos émotions, d'un pseudo-intérêt professionnel, ou encore de la peur. Les chercheurs ne sont pas à l'abri de ces personnes malveillantes. Souvent, c'est en les flattant subtilement que les arnaques se forgent".

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

Quand il parle de flatterie subtile, le policier, qui vient de signer l'ouvrage "Surfons Tranquille 3.0!", pense par exemple à une invitation à une conférence scientifique. "Cela peut prendre la forme d'une invitation à présenter ses travaux "à la pointe dans leur domaine", par exemple. Le mail renvoie la future victime vers un site d'inscription qui ressemble fortement à celui d'un congrès international. On demande au chercheur de remplir un formulaire en ligne, de communiquer son CV, éventuellement de réserver une chambre d'hôtel."

Des données personnelles trop facilement disséminées

Pourquoi se donner tant de mal? Parce qu'une fois en possession d'informations précises, et cela va jusqu'aux données bancaires ou aux mots de passe, les cybercriminels peuvent réutiliser ces données à leur profit. Se faire passer pour une personne qu'ils ne sont pas, utiliser son carnet d'adresses, mettre ainsi d'autres victimes potentielles en confiance.

Mais qui lâcherait ainsi son mot de passe de messagerie personnelle sur Internet? "On ne le fait pas directement", précise l'enquêteur. "Mais en communiquant beaucoup d'informations personnelles, également via les réseaux sociaux, en légendant une photo, un événement, on donne aux cybercriminels des moyens de pouvoir pirater son compte mail via les services de récupération de mot de passe oublié. En livrant trop d'informations, cela peut permettre d'identifier la réponse à notre "question secrète", susceptible de donner accès à notre boîte de messagerie.

Pièces jointes et cheval de Troie: méfiance

Les pièces jointes aux mails non sollicités doivent également éveiller la méfiance. Ces fichiers peuvent contenir des logiciels malveillants. Et pas uniquement des virus destinés à bloquer nos machines.

"Ces fichiers peuvent servir à l'introduction d'un cheval de Troie dans l'ordinateur du chercheur. Ce logiciel permet d'en prendre le contrôle à son insu et éventuellement de s'en servir comme passerelle vers les serveurs de son institution". précise Olivier Bogaert. "Même les étudiants sont concernés", explique-t-il. "J'ai récemment analysé le contenu d'un PC appartenant à un étudiant. Il contenait deux chevaux de Troie. Pour des personnes mal intentionnées, cela peut permettre de pénétrer les espaces digitaux ouverts dans les universités, via le wifi dans les auditoires par exemple, même avec mot de passe, et ainsi avoir accès aux serveurs de l'institution".

.doc, mp3, JPEG

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

“Et tout cela à cause d’une pièce jointe qu’on ouvre sans trop se poser de question”, précise Olivier Bogaert. “Qu’il s’agisse d’un document .doc, d’une photo JPEG, d’un faux fichier mp3, ces pièces jointes peuvent contenir et activer un petit logiciel espion qui s’installe sur l’ordinateur de la victime, détaille-t-il. Celui-ci peut par exemple inviter l’utilisateur de la machine à mettre son système à jour et le diriger vers un faux site web ressemblant parfaitement à un site officiel. Lors de la pseudo mise à jour, un autre logiciel malveillant plus perfectionné est installé à l’insu de l’internaute. Les cybercriminels ont de l’imagination!”

Comment s’en prémunir? “En réfléchissant avant d’ouvrir des mails non sollicités, en se méfiant des pièces jointes, mais aussi en utilisant des antivirus”, préconise le spécialiste. Quant aux invitations aux congrès, il ne s’agit bien entendu pas de les refuser systématiquement. Mais les victimes sont d’autant moins suspicieuses que l’invitation semble pertinente, voire prestigieuse”, met en garde Olivier Bogaert, dont le livre, divisé en deux grands chapitres (La sécurité et les arnaques), propose une série de conseils pour configurer nos outils numériques et nous aider à profiter sans risque des réseaux sociaux. Tout en nous donnant quelques clés pour déjouer les pièges tendus par les acteurs malveillants qui sévissent sur le Net.