Bonjour à tous et à toutes,

En octobre 2015, une précédente lettre d'information avait donné des recommandations pour éviter le « piratage » de sa messagerie électronique. Depuis, d'autres cas sont encore apparus et il s'avère nécessaire de rééditer cette lettre.

A ce jour, quatre (à notre connaissance) camarades se sont fait « pirater » leur messagerie électronique. Un lien entre ces cas n'est pas exclu et on peut craindre d'autres tentatives de piratages, en cascade…

Le piratage consiste à entrer dans la messagerie (sur le site du fournisseur d'accès ou de messagerie, dit serveur web mail) d'une « cible » dont l'adresse électronique est connue. Bien entendu, ce travail est effectué à l'aide de robots programmés pour « craquer » les mots de passe d'accès aux boîtes à lettres. En cas de succès, le pirate change immédiatement ce mot de passe pour se substituer à l'utilisateur, lui interdisant de facto l'accès à sa boîte.

Il dispose alors de toutes les adresses « d'amis » présentes dans le compte de messagerie (carnet de contacts ou adresses dans les entêtes de messages reçus et émis). Il peut envoyer à ceux-ci des messages comme s'il était le vrai détenteur de l'adresse et recevoir les messages en retour qu'il est seul à pouvoir consulter.

Il tente bien sûr d'escroquer les « amis » en leur demandant, par exemple, un prêt de dépannage d'urgence (achat d'une carte à code de valeur pouvant aller jusqu'à 1 500,00 € et transmission du code) pour l'aider car il est en déplacement et ne peux être contacté que par messagerie, s'est fait voler papiers et argent, etc.

Le même piratage peut être tenté à partir des adresses ainsi récupérées, d'où un effet cumulatif et des chances que cela fonctionne quelquefois.

Comme au moins quatre camarades ont été attaqués avec succès et que le(s) pirate(s) dispose(nt) ainsi de la totalité de leur carnet d'adresses, il est donc hautement vraisemblable que des tentatives concerneront d'autres membres de la promotion et peut-être certaines ont déjà réussi.

Quelques recommandations pour éviter d'être concerné par ce type de piratage ou de propager la menace.

Changer immédiatement le(s) mot(s) de passe de votre (vos) messagerie(s). Il faudrait s'astreindre à renouveler cette opération tous les mois.

Choisir un mot de passe « solide ». C'est à dire déjà non évident comme : « 12345 », « abcd », « azerty », un prénom, un mot du dictionnaire, etc. Prendre au moins 8 caractères mêlant des lettres en minuscule, en majuscule, des chiffres, des caractères spéciaux (certains sont interdits).

Si à l'avenir vous ne pouviez plus accéder à votre messagerie, contacter immédiatement votre fournisseur de messagerie afin qu'il réinitialise un nouveau mot de passe et vous le transmette, par courrier postal. Il conviendra bien sûr de le changer dès réception par un mot de passe respectant les consignes ci-dessus.

Je profite de l'occasion pour ajouter d'autres conseils plus généraux :

Protéger sa machine en installant un antivirus ou une « suite » de protection est indispensable. Des outils gratuits existent, mais il est évident que les payants sont généralement plus efficaces.

Pour adresser un message à plusieurs destinataires, mettre les adresses dans le champ Cci (copie carbone invisible) afin qu'elles soient masquées dans les entêtes des messages reçus.

En cas de transfert d'un message, effacer toutes les adresses qui apparaissent dans le message transféré (en cas de transfert successifs, elles peuvent être en plusieurs endroits) afin de ne pas les diffuser.

Ne pas cliquer sur un lien, une image ou une pièce jointe (surtout si c'est un .exe) sans être sûr de celui qui les a présentés.

Et ne pas hésiter à diffuser tous ces conseils !

Je suis toujours disponible pour des informations complémentaires ou une aide au dépannage.

Colonel Gérard DELLE LUCHE
Webmestre : promotion.koenig@orange.fr