FICHE 3 - "Piratage" de compte de messagerie : c'est sérieux, comment l'éviter

fiche aloeil.info 04/12/2016
Morgan et Emmanuel

Le piratage des boites de messagerie, une épée de Damoclès suspendue au dessus de nos têtes ? Mais que signifie "être piraté" ? Qu'y peut-on ? Et les conséquences sont-elles si graves que ça ? On pourra lire sur le sujet des dossiers très complets comme par exemple celui d'arobase, "Spam, arnaques et phishing" (http://www.arobase.org/sos/). La présente fiche part de notre expérience et insiste sur d'autres points moins connus comme le piratage des comptes commerciaux et l'importance de récupérer ses mails par POP3. A suivre...

La messagerie de ma voisine a été "piratée"…

Appelé sur les lieux, je constate avec elle que des messages loufoques ont été émis à son insu depuis son adresse (vérification faite) mail et envoyés à ses contacts...

Un pirate (un humain) ou un robot se sont donc forcément introduits dans sa boite aux lettres, le plus simplement du monde, grâce 1) à l'adresse email 2) au mot de passe (qu'il connaissait ou qu'il a découvert)...

Une fois introduit dans la caverne d'Ali Baba, le pirate peut faire quelques dégâts. En général il copie tous les contacts (le carnet d'adresses) pour les revendre à des sites spécialisés. L'envoi de message loufoques (du genre "j'ai besoin de ton aide…") permet de tester que les comptes de messageries sont bien "actifs". Il peut aussi consulter le contenu des messages, les pièces jointes, les éventuels "services complémentaires" (questions secrètes, etc.), et même de changer le mot de passe ce qui pourrait rendre le compte de messagerie définitivement perdu.

Comment le mot de passe a-t-il été découvert ?

La manière la plus simple pour entrer dans la boite aux lettres de quelqu'un est de s'asseoir à son poste si la personne s'est absenté et sa boite est restée ouverte...

...ou de mettre la main sur un smartphone dont (en général) la messagerie reste toujours ouverte…

...ou encore : en utilisant un réseau wifi, un pirate peut accéder à la messagerie ouverte d'un autre utilisateur connecté sur le même réseau (ça marche avec une boîte mail orange sur une box orange)…

Mais le cas de loin le plus répandu est le décryptage du mot de passe (ou "crackage") **par un "robot"** (un programme automatique) qui teste automatiquement des milliers de mots de passe préparés à l'avance et finit par tomber sur le bon, d'autant plus facilement qu'il ressemble à quelque chose de connu (prénoms, dates de naissances...). Si le mot de passe est suffisamment "fort" (s'il ne peut pas être découvert par essais successifs), le robot abandonnera généralement ses tentatives.

Conséquences du piratage

l'ancien mot de passe n'est plus reconnu !

Première conséquence, qui aurait pu être fatale : impossible de se reconnecter, **l'ancien mot de passe n'est plus reconnu** (le pirate l'a remplacé). Le compte de messagerie peut être à ce stade **définitivement perdu** (et son contenu pourra continuer d'être exploité par le pirate...)

Sur Orange, nous avons heureusement pu créer un nouveau mot de passe dans la zone "contrat internet". Est-ce possible sur votre messagerie ?

les contacts sont perdus !

Le pirate a récupéré la liste de contacts et l'a effacée ! C'était une liste d'entreprise… fâcheux… Le pirate pourra donc inonder ces contacts de spams en utilisant n'importe quelle identité de son choix. Ne pas s'étonner si des messages suspects continent d'être envoyés une fois le mot de passe changé.

les traces de vos achats sur l'Internet récupérées !

Quand vous faites des achats sur Internet, on vous demande de créer un compte avec identifiant et mot de passe. Très nombreux sont ceux qui, pour gagner du temps, donnent comme identifiant leur adresse

email principale et comme mot de passe celui de cette messagerie. Or, ces deux informations sont désormais à la disposition du pirate...

Il peut donc se rendre sur le compte d'achat (par ex. chez Amazon.fr), changer l'adresse de livraison, commander ce qu'il veut. Arrivé au paiement, **il pourra même parfois payer**... si le moyen de paiement est resté actif depuis la dernière transaction (ce qu'il ne faut jamais faire bien sûr, et que beaucoup de sites incitent pourtant à faire pour faciliter le paiement rapide "en 1 click").

conséquence gravissime mais rarissime

The last but not the least : La plus grave de toutes ces conséquences est **l'usurpation d'identité**, gravissime, mais heureusement rarissime, il n'empêche qu'on ne doit pas laisser des copies de son état-civil en pièces attachées.

Que faire pour ne pas être piraté(e) ?

1) La solution impérative anti-piratage : "blinder" son mot de passe

Règle d'or : un robot échouera à cracker si le mot de passe est **suffisamment fort** (suffisamment "incassable") ou, du moins, il se découragera après de longs essais.

D'après un site spécialisé américain, un mot de passe comme 123456 est cracké instantanément, pour johnny1981 c'est 1 jour pour un robot moyen et pour **cajpam3***brDDD!** mot de passe créé ci-dessous, 1 milliard d'années, de quoi faire fondre la banquise.

Créer un mot de passe "infaillible" (et "facile" à retenir)...

Une bonne méthode est de choisir une phrase si possible inventée par soi-même et de prendre le 1ere lettre de chaque mot, puis d'agrémenter le résultat de petits signes, de majuscules et minuscules.

Exemple : "*cette année je prends au moins 3 bonnes résolutions dormir dormir dormir*"
Résultat : cajpam3brddd. Agrémenté : cajpam3***brDDD!
je teste ensuite la force du mot de passe sur le site suivant gouv.fr
(test à partir du nombre de caractères et des signes utilisés)
http://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/
16 caractères ; palette de symboles : 70 symboles. Verdict : "Force correcte" sans plus ! 98 bits.
On peut rétorquer que ce mot de passe est horriblement difficile à retenir. A chacun-e de voir...

2) Assécher sa messagerie sur Internet

Même si l'accès de votre messagerie est désormais très bien protégé par un excellent mot de passe, vous pouvez préférer ne pas laisser traîner sur votre compte en ligne des informations sensibles (pièces attachées, identifiants de comptes commerciaux ou de cartes bancaires). Vous allez donc décider de transférer ces messages sur votre disque dur.

Seulement, rapatrier des messages un par un quand la messagerie a enflé démesurément est une corvée et sera vite illusoire ! Un principe beaucoup plus simple de ne RIEN laisser sur l'Internet, de TOUT rapatrier sur un disque dur local. (Si bien sûr on possède un ordinateur de bureau ou portable.)

Pour cela, on utilise un logiciel – libre – installé sur l'ordi appelé "**client de messagerie**" (par exemple Thunderbird) : son rôle est de **télécharger automatiquement les messages** au fur et à mesure de leur arrivée **et ensuite de les effacer du serveur de messagerie** (protocole appelé POP). On pourra assouplir ce procédé en n'effaçant les messages pas immédiatement mais après un délai (1 semaine, 1 mois…) pour permettre de consulter les messages depuis d'autres ordinateurs ou smartphones pendant ce délai).

Le nettoyage en ligne est enfin très fastidieux et personne ne le fait comme il faudrait le faire en pratique. Les messageries commerciales, qui incitent à consommer le plus d'espace disponible ("illimité" étant le summum), ne sont pas organisées pour faciliter le nettoyage ! Si vous avez la fibre écolo, vous préférerez éviter de laisser des centaines et centaines de mégas dormir inutilement sur les serveurs de l'Internet, ce qui consomme une énergie considérable. **Moins stocker sur Internet a un avantage écologique : moins je stocke, moins je fais tourner les serveurs qui hébergent inutilement mes données et moins je gaspille d'énergie.**

3) A suivre…

Le site arobase.org vous donne de nombreux autres informations et conseils http://www.arobase.org/sos/. Nous reprendrons plus tard d'autres points importants de sécurité concernant les messageries.