Quelques conseils pour se protéger des pirates informatique

Quelques conseils pour se protéger des pirates informatique

Un élu se fait voler 3000€ via le piratage de sa carte bancaire. Ne soyez plus une victime, cela n'arrive pas qu'aux autres.

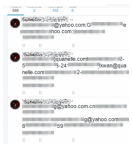
Un élu de Vanne, en Bretagne, vient d'expliquer sa mésaventure bancaire à la presse locale. Ses données bancaires ont été subtilisées. Le pirate a revendu les informations dans le blackmarket. Bilan, des achats de places de cinéma, une location de voiture en région parisienne, un voyage en Thaïlande, des billets d'avion ont été acquis avec la carte bancaire piratée et clonée. Comment l'élu a-t-il pu être ainsi piégé ? Plusieurs cas ont possibles pour le piratage de CB.

D'abord, la fuite de données via un site de vente en ligne.
Même si de plus en plus de sécurité sont mises en place entre le client et la boutique, le fameux HTTPS, que deviennent les données ? Je rencontre encore de très nombreux cas de vols de bases de données avec des informations privées et sensibles (dont les données de la CB) dans des fichiers dérobés sur des sites piratés. Un HTTPS sur le site ? La belle affaire. Le S indique que votre connexion est sécurisée (chiffrée) entre votre ordinateur et la boutique. Parfait pour ne pas se faire intercepter les données via une connexion un peu trop légère (wifi public…). Mais ce HTTPS ne vous sauvera pas si la base de données, ou un malveillant interne à la boutique, met la main sur la base de données. Un exemple que j'ai rencontré dernièrement en est le parfait aperçu. Depuis une dizaine de jours, sur Twitter, un bot pirate recrache les informations des comptes Paypal de centaines de personnes que le pirate trouve sur des sites web.

Vient ensuite le skimming, le piratage de CB par clonage via un système physique collé sur un distributeur de billets automatique, une pompe à essence, un parcmètre…
Le matériel copie la bande magnétique. Une caméra miniature, ou un faux clavier posé sur le vrai, permet de récupérer le mot de passe. Je vous expliquais, il y a peu, comment la police italienne, avec l'aide d'Europol, avait mis fin aux agissements d'un gang de pirates de cartes bancaires qui sévissait dans toute l'Europe.

Chez les commerçants, le remplacement du boitier de paiement par un pirate.
Copie directe, sans que la boutique ne puisse s'en rendre compte en temps réel. Regardez toujours sous ce lecteur de CB si un autocollant protège le matériel.
Le phishing, la copie du site Internet de votre banque, par exemple. Toujours, malheureusement, aussi efficace pour ceux qui ne prennent pas le temps de regarder correctement l'url caché dans le courriel reçu.

Pour finir avec le piratage de CB, la simple copie mentale, par une personne ayant eu accès, même quelques secondes à votre bout de plastique.
Ne perdez JAMAIS de vue votre carte bancaire. C'est le lecteur de CB qui vient à votre moyen de paiement, pas le contraire.
Comme vous avez pu le voir, le piratage de CB peut prendre de multiples formes. Je ne vous relate que les plus courantes. Un dernier point important ! Arrêtez de vous contenter du « Cela n'arrive qu'aux autres » ou, plus grave encore à mon sens « Fort heureusement, j'ai une assurance ! » N'hésitez jamais à déposer plainte. Votre identité numérique est définitivement perdue. Le pirate ne se contentera pas que de votre carte bancaire !



Exemples de piratage de CB et de données

Voici deux exemples, sur 83 vécus cette semaine, visant des données volées à des clients Français.
Le site Internet Demain J'arrête, dédié aux cigarettes électroniques. Le pirate, après avoir fait ses « courses » dans la base de données, a diffusé son forfait sur la toile. Même sanction pour le cas de la boutique en ligne Mayline, un spécialiste de l'ameublement. Noms, adresses postales, mots de passe (hashé/chiffré en MD5), logins, mails… Plusieurs buts dans cette malveillance : effacer ses traces (surtout si des centaines de zozos 2.0 se jettent sur les informations, NDR) ; montrer sa puissance (le 1/4 d'heure Warholien, NDR).
Le problème dans ce genre de vol de données, les identités numériques pillées ne peuvent plus être maîtrisées par les légitimes propriétaires. Mails, adresses postales, téléphones, pseudos, mots de passe. Autant de contenus pouvant être exploités dans des dizaines d'arnaques. Un numéro de téléphone portable ? Diffusion de spams, fraudes aux appels surtaxés, de tentatives d'infiltrations via un MMS piégé… Une adresse physique ? Elles peuvent se vendre quelques dizaine d'euros dans le blackmarket pour être transformées en drop box, des boites aux lettres pirates pour recevoir du matériel volé pendant l'absence des propriétaires. Un mot de passe non chiffré ? Pas besoin de vous faire un dessin sur son utilisation (Espionnage, usurpation…) Bref, les pirates ne cherchent pas que les données bancaires. Les datas qu'amassent les entreprises sur le dos des Internautes sont aussi de véritables mines d'or. !

Mon mot de passe est chiffré ?
Je vais vous expliquer pourquoi avoir un mot de passe fort est une véritable obligation sur la toile, aujourd'hui. L'identifiant de connexion est hashé/chiffré au format MD5 ? Prenons un mot de passe des dizaines de fois rencontré : Football. Dans une base de données sans MD5, le pirate lira le password en clair. Une protection MD5 est installée ? Football se transforme en 37b4e2d82900d5e94b8da524fbeb33c0. Le pirate, au premier abord, ne peut rien en faire. Sauf que je vais vous démontrer qu'un mot de passe fort, avec majuscules, minuscules, chiffres, signes de ponctuations, est loin d'être négligeable. Notre pirate a donc en main 37b4e2d82900d5e94b8da524fbeb33c0. Rendez-vous sur le site http://md5cracker.org est rentré ce mystérieux code MD5. En moins d'une seconde, le « crack » va vous proposer 6 bonnes réponses sur 11 sites proposant de pirater un mot de passe au format MD5. Préférez donc un mot de passe de type J'a1m3_le_F0ot_B4L! qu'un simple football. A noter que si votre mot de passe est « cracké », il se retrouvera obligatoirement dans l'une des nombreuses bases de données regroupant les hash MD5 proposées sur la toile.
Pour finir, un mot de passe, un login et un mail d'identification ne s'utilise que pour un service utilisé. Il faut en changer, au risque d'ouvrir grandes les portes aux intrus… [Lire la suite]

- Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles
- Expertises techniques et judiciaires
- Expertises de systèmes de vote électronique
- Formations en cybercriminalité
- Formation de C.I.L. (Correspondants Informatique et Libertés)
- Accompagnement à la mise en conformité CNIL de votre établissement

Contactez-nous

Réagissez à cet article

Source : *Piratage de CB : Fort heureusement, j'ai une assurance ! – ZATAZ*