Mots de passe : nos conseils pour une sécurité maximum

Mots de passe : nos conseils pour une sécurité maximum

password, admin, 123456, abcdef, qwerty, j'en passe et des meilleures… Voilà des mots de passe encore bien utilisés si l'on en croit le palmarès 2013 des 25 mots de passe les plus fréquents (publié par la société SplashData, éditrice de logiciels). Mais de véritables passoires en termes de sécurité ! A l'heure du cloud et des services Web qui numérisent toujours un peu plus nos vies, la vigilance ne saurait souffrir de négligences. De l'importance de sécuriser ses mots de passe, nous vous expliquons le pourquoi et le comment.

Paranoïa, quand tu nous gagnes…

On a beau être d'un naturel plutôt stoïque, la lecture du rapport P@$$1234: the end of strong password-only security publié en janvier 2013 par le cabinet d'expertise Deloitte donne tout de même quelques sueurs froides… Il s'appuie sur un travail intéressant de Mark Burnett (du site Xato.net), lequel a décortiqué une liste de 6 millions de duos login plus mot de passe uniques pour en extraire des statistiques.

- 98,8 % de cette base d'utilisateurs emploient les 10 000 mots de passe les plus fréquents ;
- 91 % se concentrent sur 1 000 mots de passe ;
- 40 % font avec 100 mots de passe ;
- 14 % (soit 840 000 personnes tout de même) piochent dans le top 10 !

Et le problème de ces mots de passe ultra bateau, dont « password » et « 123456 », c'est qu'ils représentent le degré zéro de sécurité, puisqu'ils seront les premiers à être testés par tout hacker qui se respecte. Le souci de sécurité n'est visiblement pas encore rentré dans toutes les têtes…

Pour mieux se protéger de l'ennemi, il faut tenter de le comprendre. Comment les hackeurs fonctionnent dans les grandes lignes ? Quatre scenarii sont à envisager : le piratage en direct, le vol de bases de données, le phishing (ou plus globalement le *social engineering* précise Paul Rascagnères, analyste malware chez l'éditeur d'antivirus G DATA) et les virus.

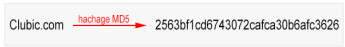
Le premier, qui consiste à tester tous les mots de passe possibles et imaginables dans une interface de connexion sur la base d'un identifiant connu, n'est plus possible aujourd'hui ou très rarement. Cela, parce que la grande majorité des sites sérieux bloquent les comptes au bout de quelques tentatives ratées, trop peu nombreuses même pour un mot de passe évident (quoique avec password et 123456…).

Non, le gros des dangers tient dans le vol, les virus et le *social engineering*. Pour ce dernier, une sorte de vol avec consentement non éclairé, la complexité d'un mot de passe n'a pas d'intérêt : le hackeur se fait passer pour quelqu'un d'autre (email, coup de fil ou faux site officiel), et s'il parvient à duper l'utilisateur, il en profite pour récupérer ses identifiants, en clair. La pratique est courante, les données sont ensuite utilisées ou revendues sur des marchés parallèles. Le seul remède dans ce cas, c'est la vigilance. Idem pour l'aspect virus, un malware avec keylogger peut intercepter vos saisies au clavier ou chiper les identifiants stockés dans le navigateur par exemple : votre ordinateur doit être protégé par un antivirus, à jour, et en programmant des analyses régulières.

? Un hash qui part d'autant plus vite en fumée que le mot de passe est simple ?

C'est en matière de vol qu'il est intéressant de comprendre les mécanismes. Tous les couples identifiants / mots de passe des services Web sont stockés sur les serveurs des entreprises respectives, et forment ainsi autant de bases de données. Ces vols sont assez ponctuels mais malheureusement massifs (par milliers voire millions d'entrées). Très rarement (et normalement pas en France puisque c'est illégal), ces bases de données sont stockées en clair. Si dérobade il y a, la complexité du mot de passe sera vaine.

Mais dans la majorité des cas, les identifiants et mots de passe sont hachés, c'est-à-dire brouillés par un algorithme. Quand quelqu'un veut se connecter à son service, le mot de passe qu'il entre est également haché en temps réel, puis comparé à celui stocké sur les serveurs. Les hackeurs qui se procurent pareilles bases de données vont devoir utiliser des logiciels spécifiques pour déterminer quelle fonction de hachage (hash en anglais) a été utilisée, après quoi ils peuvent automatiser les tests. Tests qui vont consister à choisir un mot, le hacher, le comparer à l'empreinte hachée de la base de données volée : s'il y a correspondance, le mot de passe est trouvé, sinon il faut tester un autre mot, etc. Un hash qui part d'autant plus vite en fumée que le mot de passe est simple.



En hachant un mot via un algorithme, on obtient une empreinte de ce type. Il existe plusieurs algorithmes, proposant des niveaux de sécurité plus ou moins élevés : MD5, SHA-1, SHA-2, etc…

Le hasard fait parfois bien les choses, mais les statistiques les font encore mieux. Pour éviter de tâtonner au doigt mouillé, les hackeurs recourent à des dictionnaires, ou mieux encore, à des listings de mots de passe qui ont été établis au fil des différents vols de données, comme la base du réseau communautaire RockYou.com et ses 32 millions d'entrées évaporées dans la nature en 2009. De vrais mots de passe, couramment employés, et qui ne changent pas beaucoup, comme en témoigne la constance des palmarès des mots de passe les plus fréquents, d'une année sur l'autre. Les cas de vols de données ne manquent pas : Ebay,Orange, Domino's Pizza ou encore Adobe pour les exemples les plus récents.

Vends forfait 4G pas cher, avec livraison à domicile. Seul moyen de paiement accepté : l'abonnement annuel.

Les listings contiennent des mots simples, les logiciels pirates proposent donc des règles complexes. Mais faciles à mettre en oeuvre d'après le journaliste Nat Anderson. Son expérience est instructive. En tentant de se mettre dans la peau d'un hacker, il a potassé le fonctionnement des logiciels pirates, et notamment de Hashcat, qui sont, sans surprise, très bien conçus.

En quelques clics, on peut étoffer la recherche, de sorte à ce que sur un mot de passe comme « clubic » (à tout hasard), le logiciel teste également des ajouts de chiffres ou de lettres (« clubic10 » ou « clubicz »), mais aussi l'ordre inversé (« cibulc »), les ajouts de préfixes et suffixes courants (man, 123, mad, me…), la version *leet*, c'est-à-dire avec des caractères alphanumériques ASCII (« (|_ |_| |3 | (») voire des inversions de lettres. De quoi multiplier les chances du malfaiteur d'arriver à ses fins.


Le logiciel Hashcat

? Un mot de passe à 8 caractères hacké en 5 h 30 ?

Plus efficace encore mais exigeante en ressources, la bonne vieille attaque de force brute. Sur une quantité donnée de caractères, mettons six, la technique un brin bourrine consiste à hacher et tester « aaaaaa », puis « aaaaab », etc. Sachant qu'un clavier français peut produire 142 caractères (avec tous les accents, la casse, les symboles, les chiffres, et encore 103 si on exclut les accents) et que la statistique est exponentielle, ça nous fait 8 198 418 170 944 de combinaisons possibles (8 200 milliards pour ceux qu'autant de chiffres perturberait). Dans l'exemple donné par l'étude du cabinet Deloitte, un mot de passe à 8 caractères (6,1 millions de milliards de possibilités sur un clavier américain à 94 caractères) pourrait être hacké en 5 h 30 par une configuration dédiée haut de gamme (estimée à 30 000 $ en 2012), mais en près d'un an avec un PC correct de 2011.

Représentation visuelle de ces chiffres astronomiques

Le petit point noir, c'est le nombre de combinaisons à 8 caractères, le gros point bleu c'est avec 10 caractères. Les joies de l'exponentiel !

Voilà donc la clef : plus un mot de passe est complexe (avec des caractères spéciaux, un séquençage aléatoire, etc.) et long, plus le hacker aura du fil à retordre. Rien qu'en passant à 10 caractères, courbe exponentielle oblige, on fait grimper les combinaisons sur un clavier français à 3 333 369 396 234 118 349 824 (3 333 milliards de milliards !!!). La même machine de compétition mettrait alors 343 ans pour tester toutes les combinaisons… A cette parade, les hacker répondent par le crowd-hacking : ils confient des fragments de calculs à faire à des milliers de PC normaux infectés (les fameux PC zombies). C'est supposé aller beaucoup plus vite ainsi, mais bon, les hackers préfèrent tout de même les mots de passe courts et basiques.

? nous peinerions à retenir plus de sept chiffres dans notre mémoire à court terme ?

Le remède est simple, sa mise en oeuvre plus délicate. D'après une étude de l'Université de Toronto que cite le rapport Deloitte, les êtres humains limités que nous sommes peinerions à retenir plus de sept chiffres dans notre mémoire à court terme, et même plus que cinq en prenant de l'âge. L'ajout de symboles, de lettres majuscules et minuscules produirait un mix encore moins aisé à retenir. Le rapport se fait plus accablant en ajoutant que la nature humaine a tendance à suivre des schémas de pensée limités par rapport aux possibilités offertes. La majuscule ? En première position dans les mots. Les chiffres ? À la fin. Des 32 symboles présents sur un clavier américain ? Une demi-douzaine seulement est utilisée. De quoi rendre l'aléa théorique plus prédictif pour les hackers. Rien de nouveau cependant. A moins que… le rapport ne pointe du doigt un nouveau frein, imputable aux usages mobiles. L'absence ou la moindre accessibilité des caractères spéciaux sur les claviers des smartphones amène le nomade à simplifier son mot de passe. Tout comme le temps de saisie supérieur qui inciterait un quart des personnes sondées à utiliser un mot de passe plus court pour gagner du temps. De 4 à 5 secondes pour taper un mot de passe de 10 caractères sur un clavier standard d'ordinateur, il faudrait entre 7 et 30 secondes pour faire la même chose depuis un smartphone tactile.

Réagissez à cet article

Source : *Mots de passe : nos conseils pour une sécurité maximum*