Le célèbre gestionnaire de mots de passe LastPass hacké

	Le célèbre gestionnaire de mots de passe LastPass hacké

Deux chercheurs ont décortiqué le service en ligne et ont réussi à déchiffrer la base de mots de passe par le biais du processus de récupération de compte.

Diffusé aussi bien auprès du grand public que des entreprises, LastPass est certainement l'un des gestionnaires de mots de passe les plus populaires du moment. Mais est-il réellement sécurisé?
Les hackers Alberto Garcia et Martin Vigo – tous les deux membres de l'équipe sécurité de l'éditeur saleforce.com – ont décortiqué ce service par rétro-ingénierie et viennent de présenter le résultat de leur recherche à l'occasion de la conférence Black Hat Europe 2015. Ils ont trouvé une série de failles qui permettent, dans certains cas précis, d'accéder au Saint Graal : la base de mots de passe.
Dans un premier scénario, ils supposent que l'attaquant a réussi à s'implanter sur l'ordinateur de la personne ciblée, après un première infection. L'une des vulnérabilités présentées par les deux chercheurs – et qui a depuis été patchée – est d'utiliser le processus de récupération de compte. C'est une fonctionnalité fort utile pour les utilisateurs qui ont la mémoire qui flanche, mais qui s'appuie sur un élément fort bizarre: un mot de passe OTP (One Time Password) qui est généré par défaut et stocké en clair sur la machine. En l'intégrant dans une fausse requête de récupération par une requête HTTP, les deux hackers arrivent à ouvrir une session LastPass et à récupérer la version chiffrée de la base de mots de passe.

Un mot de passe boosté aux stéroïdes
Mais ce n'est pas tout: ils reçoivent aussi une version chiffrée de la clé qui permet de déchiffrer la base. Mais le sésame pour déchiffrer cette clé n'est pas très loin: c'est un dérivé de l'OTP par hachage (SHA-256). Bingo, la base est ouverte. Et le mieux dans cette affaire, c'est que cette procédure de récupération court-circuite les protections additionnelles que l'utilisateur peut mettre en place, telles que l'authentification à double facteur ou la restriction d'accès en fonction de l'adresse IP. « D'une certaine manière, l'OTP est un master password boosté aux stéroides », souligne les deux chercheurs, qui ont rapporté leur trouvaille à LastPass.
L'éditeur a, depuis, déployé un correctif qui empêche la création de fausses requêtes de récupération. Par ailleurs, il a introduit il y a quelques semaines un deuxième facteur d'authentification pour valider cette procédure, au travers d'un code envoyé par SMS. Il est vivement recommandé d'activer cette option baptisée « SMS Recovery » dans les paramètres du compte. Les hackers ont également rappelé dans leur présentation qu'il ne fallait jamais cocher la case « Mémoriser le mot de passe » dans le plugin Lastpass. En septembre 2014, ils avaient en effet montré qu'il était possible de le récupérer assez facilement, une fois que l'on a accès à la machine.
Attaque par JavascriptL'autre scénario imaginé par MM. Garcia et Vigo est celui d'un attaquant qui a réussi à accéder aux serveurs de LastPass. Théoriquement, une telle attaque ne devrait pas permettre d'accéder aux mots de passe d'un utilisateur car ils sont stockés de manière chiffrée. Mais les deux chercheurs ont trouvé un moyen détourné. Le service en ligne utilise du code Javascript pour pouvoir renseigner automatiquement les champs d'authentification dans une page web – ce qui est bien pratique.
Exécuté localement sur la machine de l'utilisateur, ce code peut accéder aux identifiants d'un compte en ligne. En insérant son propre code Javascript dans les serveurs de LastPass, un attaquant pourrait alors facilement récupérer ces données secrètes. On peut donc se demander si un tel service est réellement une solution face à des organisations telles que la NSA qui pourraient contraindre l'éditeur à intégrer leur propre code sur leurs serveurs…
Pour autant, pas la peine de jeter le bébé avec l'eau du bain. « LastPass s'est montré très réactif face à ces failles et les a réparé pour la plupart en l'espace de 72 heures », soulignent les chercheurs qui, par ailleurs, continuent à utiliser ce service. Car en dépit des failles potentielles que peut avoir un gestionnaire de mots de passe, ce sera toujours mieux que de noter ses mots de passe dans un tableur !

Source : http://www.01net.com/actualites/black-hat-2015-ils-ont-hacke-lastpass-le-celebre-gestionnaire-de-mots-de-passe-929666.html
Par Gilbert KALLENBORN