Double authentification et numéros premium, attention au hold-up !

	Double authentification et numéros premium, attention au hold-up !

Un chercheur a subtilisé de l'argent à Instagram, Google et Microsoft en appelant des numéros surtaxés via les systèmes de double authentification.

La plupart des services web proposent pour la double authentification l'envoi de code via un SMS. Mais l'utilisateur peut aussi choisir de recevoir un appel et un robot dicte à haute voix le code. Un chercheur en sécurité, Arne Swinnen a montré que les différents services testés ne vérifient pas les numéros appelés. Il a donc réussi à rattacher ses différents comptes, Instagram, Office 365 ou Google à des numéros surtaxés.
Pour Instagram, le chercheur constate qu'une fois le SMS envoyé avec le code à 6 chiffres, le service attend 30 secondes avant d'émettre un appel téléphonique depuis la Californie pour transmettre ce code. Arne Swinnen a acheté un numéro surtaxé localisé au Royaume-Uni à 0,06 livre la minute. Il a automatisé les appels vers son numéro et a obtenu 1 livre sterling au bout d'un peu plus de 17 minutes. Un pirate pourrait alors subtiliser 48 livres par jour, 1440 livres par mois et 17 280 livres par an. Avec un peu de travail, il pourrait même multiplier ses gains par 100 en gérant 100 comptes Instagram sur un numéro surtaxé. Soit une fraude évaluée à 1,728 million de livres sterling.

Google plus difficile mais pas impossible

Pour Google, l'exercice a été plus compliqué, car la firme américaine ne bascule pas automatiquement sur un appel lors du processus d'authentification sur mobile. Il s'agit d'une option qui a ses limites. En entrant un numéro premium, il était bloqué après plusieurs tentatives sans entrer le code fourni. D'où l'idée par Arne Swinnen de passer par un serveur SIP et un client SIP (comme un centre d'appel). Le numéro de téléphone fourni a été accepté par Google en lui ouvrant la voie à 10 appels par heure sans avoir besoin de rentrer le code (ce qui l'a un peu étonné). Pour automatiser le processus, il a écrit des scripts qui lui ont permis de récolter son premier euro au bout de deux heures et de 17 appels. Soit 12 euros par jour, 360 euros par mois et 4320 euros par an. Une opération qui peut être centuplée en liant 100 comptes Google à ce numéro.

Microsoft piégé par le zéro

Dernier exemple, la validation de compte Office 365. Microsoft autorise des numéros premium, mais les bloque au bout de 7 essais invalides. Mais le chercheur a trouvé des moyens de contourner cette limitation. Elles sont au nombre de deux. La première réside dans l'apposition du 0 devant le numéro de téléphone qui revalide ce numéro et permet donc un rappel. Arne Swinnen a poussé le vice à placer 18 fois le 0 devant le numéro et cela fonctionnait encore. L'autre moyen pour contourner les blocages est de rajouter de manière aléatoire jusqu'à 4 chiffres. Un savant calcul donne par numéro premium un retour sur investissement de 668 882 euros.

Récompenses et reconnaissance

Chaque démonstration a été envoyée aux différentes sociétés pour prendre les mesures nécessaires et réparer les erreurs. Microsoft a intégré ces découvertes au sein de son programme de Bug Bounty en allouant au chercheur une prime de 500 dollars. Une prime de 2000 dollars a été également donnée par Facebook dans le cadre de son programme de recherches de bugs. Cette récompense a été doublée, car le chercheur en a fait don à une œuvre caritative. Quand à Google, il remercie Arne Swinnen non pas en espèces sonnantes et trébuchantes, mais par une reconnaissance en le plaçant dans son Hall of Fame (à la 85ème position).
Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Double authentification et numéros premium, attention au hold-up !