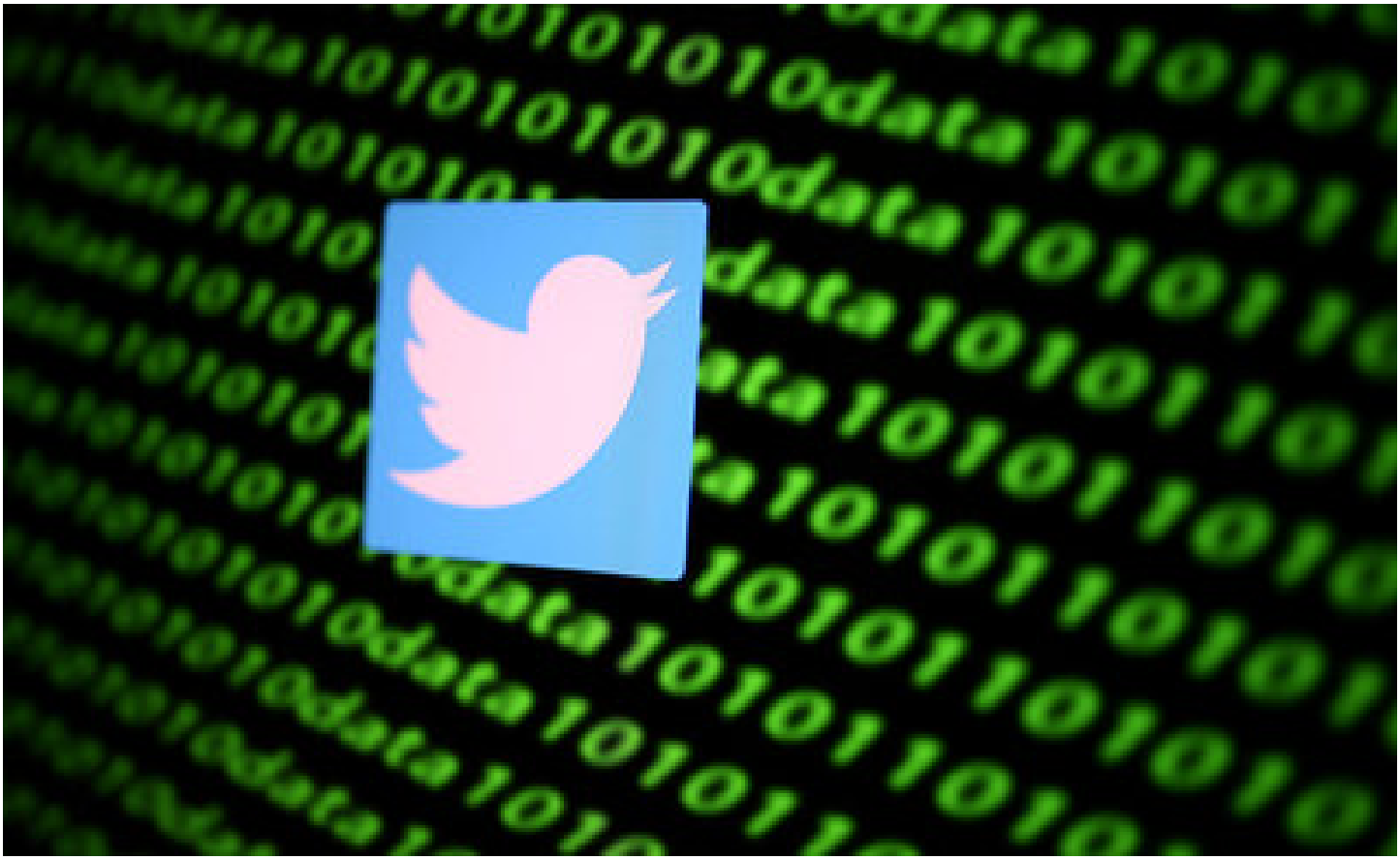
TECHNOLOGIE

Comment Twitter a subi le plus important piratage de son histoire

L'accès aux comptes de Bill Gates, de Kanye West, de Joe Biden ou encore d'Elon Musk a été rendu possible grâce à une attaque visant des employés de Twitter. L'un d'eux aurait même été payé par des pirates informatiques



Anouch Seydtaghia

«Un jour difficile pour nous, chez Twitter. Nous nous sentons très mal à cause de ce qui s'est passé.» Jack Dorsey a publié un message où il fait profil bas. Mais le directeur de Twitter devra rendre des comptes de manière détaillée après le piratage le plus important qui ait affecté le réseau social. Dans la nuit de mercredi à jeudi, les comptes de plusieurs personnalités ont été piratés, sans doute à cause de complicités internes au sein de l'entreprise.

La chute, hors bourse, de 4% du titre de Twitter n'est ainsi peut-être qu'un avant-goût de ce qui attend le réseau social. Par le passé, certains comptes avaient certes été piratés, mais toujours de manière isolée. L'attaque survenue la nuit dernière a touché simultanément plusieurs comptes dits «certifiés» (ce qui signifie que Twitter assure qu'ils appartiennent bien aux personnalités, ou aux entreprises, qu'ils prétendent représenter). Les comptes de Barack Obama, de Kanye West, de Joe Biden, d'Elon Musk ou encore d'Apple ont ainsi été piratés durant plusieurs minutes.

Butin de 120 000 francs

Les attaquants ont réussi à prendre le contrôle de ces comptes en publiant un message incitant les millions de followers à envoyer des bitcoins à un compte, avec la promesse d'en recevoir en retour le double. Au total, les pirates auraient ainsi réussi à récolter l'équivalent d'environ 120 000 francs avant que Twitter ne mette fin à cette attaque. Retrouver les auteurs de ces méfaits s'annonce quasi impossible.

Comment un tel piratage a-t-il pu avoir lieu? Jack Dorsey a promis de «partager tout ce qu'il pourra» lorsqu'il aura une meilleure compréhension de ce qui s'est passé. L'attaque n'a pu être possible qu'en prenant le contrôle d'une console centrale d'administration, pour cibler en même temps plusieurs comptes. «Nous avons détecté ce que nous pensons être une attaque coordonnée d'ingénierie sociale par des personnes qui ont réussi à cibler certains de nos employés ayant accès à des systèmes et outils internes», a commencé à détailler Twitter. «Nous savons qu'ils ont utilisé cet accès pour prendre le contrôle de nombreux comptes très visibles (y compris vérifiés) et tweeter en leur nom.»

Lire aussi: Plusieurs comptes Twitter piratés avec un message en turc

Employé corrompu?

Selon le site spécialisé The Verge, il semblerait que plusieurs pirates aient été à la manœuvre et que les comptes de plusieurs employés ont été utilisés. Mais ce n'est pas tout. Selon le site Motherboard, spécialisé notamment dans la sécurité informatique, plusieurs pirates ont fait circuler, sur internet, des captures d'écran d'un outil d'administration interne à Twitter, outil qui aurait été utilisé pour prendre le contrôle des comptes. Cela s'est produit en créant un nouveau mot de passe pour des comptes e-mail. Motherboard affirme avoir pu échanger avec des pirates, qui disent avoir payé un employé de Twitter pour changer les adresses e-mail de plusieurs comptes populaires, en utilisant l'outil d'administration. Il a ainsi pu prendre le contrôle de ces comptes.

Pour Steven Meyer, directeur de la société de cybersécurité genevoise ZENData, «c'est une illustration des problèmes avec les accès administratifs: en 2017, le compte de Donald Trump avait été fermé par un employé de Twitter mécontent. Il est très difficile de limiter ou de contrôler les accès qu'ont les employés aux outils internes.»

Conséquence: le réseau social devra redoubler d'efforts pour contrôler ses employés et sans doute mettre en place de nouvelles procédures de surveillance. «Heureusement pour nous, ces tweets n'ont été qu'une simple arnaque évidente et n'ont pas été utilisés pour générer un scandale ou une campagne de désinformation géopolitique», conclut Steven Meyer. Mais il est possible, comme le suggère The Verge, que des informations sensibles aient été dérobées des comptes piratés, comme des échanges de messages.