Twitter piraté : l'appareil cybercriminel au-delà du scam Bitcoin

L'arnaque aux bitcoins qui s'est déroulée cette semaine sur Twitter ne serait-elle qu'un écran de fumée ? Le réseau social n'a jusqu'alors pas fourni d'éléments de nature à écarter cette hypothèse.

Le premier bilan officiel, communiqué ce jeudi, fait état d'environ 130 comptes ciblés, dont « une petite partie » effectivement compromis. Tous ont fait l'objet d'un verrouillage. Twitter n'y rétablira l'accès que lorsque cela pourra « se faire en tout sécurité ».

> *Based on what we know right now, we believe approximately 130 accounts were targeted by the attackers in some way as part of the incident. For a small subset of these accounts, the attackers were able to gain control of the accounts and then send Tweets from those accounts.*
>
> *— Twitter Support (@TwitterSupport) July 17, 2020*

Le temps de l'enquête, des fonctionnalités peuvent rester inaccessibles à certains utilisateurs. En particulier ceux qui disposent d'un compte vérifié, reconnaissable à son badge bleu. Certains services sont désactivés pour tous sans exception ; par exemple, celui qui permet de télécharger une copie de ses données.

Des messages pas si privés ?

À en croire Twitter, les mots de passe ont été préservés de toute action indésirable. Les membres du réseau social ne devront donc pas – en tout cas jusqu'à nouvel ordre – les réinitialiser. L'entreprise de Jack Dorsey annonce en outre avoir pris des mesures pour limiter l'accès à ses outils d'administration internes, visiblement impliqués dans l'attaque.

Si on admet que les mots de passe sont saufs, qu'en est-il des autres données rattachées aux comptes affectés ? Twitter ne s'exprime pas sur ce point. Alors même que des élus américains l'y invitent. Parmi eux, le sénateur démocrate de l'Oregon Ron Wyden, qui fait remarquer que le chiffrement ne couvre toujours pas les messages privés.

> *In September of 2018, shortly before he testified before the Senate Intelligence Committee, I met privately with Twitter's CEO Jack Dorsey. During that conversation, Mr. Dorsey told me the company was working on end-to-end encrypted direct messages. https://t.co/U4g61oOH20*
>
> *— Ron Wyden (@RonWyden) July 16, 2020*

Twitter n'est pas beaucoup plus expressif sur la question des outils internes. Tout au plus reconnaît-il faire face à une attaque qui a « ciblé avec succès plusieurs de [ses] employés ».

Plusieurs, vraiment ? Sur la base de sources qu'il dit impliquées dans l'offensive, le site spécialisé

Motherboard affirme qu'un employé en particulier aurait ouvert la porte aux cybercriminels, moyennant finance.

Original gangster

TechCrunch confirme le scénario de l'accès à un outil interne, à partir du témoignage d'un hacker. Ce dernier évoque un pair se faisant appeler Kirk et actifs dans le business des OG (« original gangster »). On qualifie ainsi les comptes Twitter qui se monnayent à bon prix, essentiellement de par leur nom.

Le compte @6 entre dans cette catégorie. Le chercheur en sécurité qui le possède actuellement l'a « hérité » d'un pirate qui s'était distingué dans le cadre de l'affaire Chelsea Manning. Mercredi, il a constaté une tentative de changement de mot de passe. Il n'a pas pu s'y opposer, quand bien même il avait activé l'authentification à deux facteurs. Et pour cause : les pirates ont fait en sorte de recevoir le code sur une adresse électronique qu'ils avaient rattachée par avance au compte Twitter… par le biais du ou des fameux outil(s) d'administration.

Sans cet accès privilégié, l'attaque n'aurait probablement pas abouti : l'intéressé avait désactivé le SMS comme facteur d'authentification, au profit d'une application. Une manœuvre qui aurait pu avoir son importance, les auteurs de l'offensive semblant être des adeptes du *SIM swapping* – pratique utilisée avec succès l'an dernier contre Jack Dorsey, le patron de Twitter.

La jeunesse à la manœuvre ?

Pointure de la cybersécurité, Brian Krebs évoque un certain Joseph James Connor, citoyen britannique de 21 ans résidant en Espagne et connu sous le pseudo « PlugWalkJoe ». Et lui prête des liens avec ChucklingSquad, groupe cybercriminel auquel on attribue le piratage du compte de Jack Dorsey.

> *Brian Krebs reporting that the Twitter hacker is a 21-year-old Liverpool, England SIM-swapper who goes by the handle PlugWalkJoe and that the same person was part of the group that was behind the hijacking of Jack Dorsey's account last year. https://t.co/YK860Atkmm*
>
> *— Derek B. Johnson (@DerekDoesTech) July 16, 2020*

Au rang des autres comptes « de type OG » compromis figure @B. Actuellement suspendu, il a relayé quelques captures d'écran de l'outil d'administration qui semble avoir permis d'en prendre le contrôle. Diverses pages archivées donnent davantage de fond à l'affaire, en particulier avec le compte @shinji. Également suspendu, il a lui aussi publié des captures. Son propriétaire revendique d'autres comptes OG, mais sur Instagram (@j0e et @dead).