FUTURA

Gmail : 2,5 milliards de comptes piratés ?

Podcast écrit et lu par Adèle Ndjaki

[Générique d'intro, une musique énergique et vitaminée.]

Votre compte Gmail est-il en grand danger ? C'est le décryptage de la semaine dans *Vitamine Tech*.

[Fin du générique.]

2,5 milliards de comptes Gmail... C'est le nombre qui circule après une attaque qui pourrait bien avoir visé Google. Alors forcément, une question se pose : est-ce que votre compte fait partie du lot ? Bonjour à toutes et à tous, je suis Adèle Ndjaki et aujourd'hui dans *Vitamine Tech*, je vous explique comment cette attaque a fonctionné, ce qu'on sait vraiment et surtout, si vous devez vous inquiéter.

[Une musique électronique calme.]

Tout commence discrètement en juin 2025, il y a donc quelques mois. Entre ses murs, Google vit un véritable drame : le géant de la tech est victime d'une intrusion. Salesforce, une plateforme très utilisée pour gérer les données client, et dont Google se sert, est piratée. Attention, l'attaque n'est pas immédiatement rendue publique. Ce n'est que début août, via une mise à jour d'un article de blog initialement publié en juin, que Google confirme les faits. Pas de communiqué de presse, pas de conférence. Juste un petit encart dans lequel on peut lire que des données commerciales de base de type : noms d'entreprises, adresses mails et coordonnées...ont été exposées. Il s'agirait de données exclusivement publiques, accessibles par n'importe qui sur Internet. Si officiellement aucun commentaire n'est fait de la part de Google, du côté du grand public l'inquiétude monte : quelques semaines après l'annonce de l'entreprise américaine, des internautes commencent à recevoir des appels, des mails et des SMS les incitant à donner leurs identifiants. Aie ! La mayonnaise monte et le site d'information The Sun rapporte que 2,5 milliards de comptes Gmail pourraient avoir été exposés à la suite de cette attaque. Selon les analystes en cybersécurité de *Google Threat Intelligence* (GTIG), le groupe à l'origine de l'attaque est UNC6040. Pas commun comme nom de supervilain. En réalité Google utilise ce nom comme une désignation neutre pour suivre ces activités d'extorsion en attendant d'avoir des preuves plus solides pour confirmer s'il s'agit d'un groupe qui se fait appelé les ShinyHunters. Leur spécialité ? L'ingénierie sociale, une technique de manipulation. Ils n'ont pas besoin de forcer une serrure, ils vous appellent et vous les laissez entrer. Leur mode opératoire est tellement simple que bluffant : ils se font passer pour un membre du support

IT ; vous poussent à réinitialiser votre mot de passe Gmail sous prétexte d'une cyberattaque en cours ; puis une fois en place, ils dérobent vos données ni vues ni connues. Mais qui sont ces ShinyHunters ? Derrière ce nom qui peut faire penser à la chasse de Pokémon, se cache un réseau bien réel. Selon des documents du FBI et des rapports d'Intel 471, l'activité des ShinyHunters remonte à 2020. Ils seraient liés à plusieurs grosses fuites chez Microsoft via GitHub - une plateforme basée sur le cloud ; AT&T - un opérateur téléphonique américain, ou encore Nitro PDF- une appli pour éditer des fichiers en format PDF pour ne se citer qu'eux. Et devinez quoi, selon un acte d'accusation américain de 2021, trois Français seraient membres du groupe. L'un d'eux, Sébastien Raoult, âgé de 21 ans, arrêté au Maroc, est en attente d'extradition vers les États-Unis, où il risque jusqu'à 20 ans de prison.

[*Virgule sonore, une cassette que l'on accélère puis rembobine.*]

[*Une musique de hip-hop expérimental calme.*]

Ce que montre cette affaire, c'est que les cybercriminels n'ont plus besoin de casser des systèmes complexes pour atteindre leurs objectifs. Leur nouvelle arme, c'est une vieille méthode : l'appel téléphonique. Et contrairement à un virus, aucun logiciel de sécurité ne peut détecter une voix convaincante. Ce type de manipulation humaine, on l'a déjà abordé dans un épisode précédent de *Vitamine Tech*, à propos des fraudes aux virements de salaires. Aujourd'hui, cette approche fait son retour à grande échelle. Ce qui peut étonner, c'est que même des entreprises comme Google peuvent être touchées. Car rappelons que, dans ce cas précis, il ne s'agit pas d'une faille technique, mais bien d'un accès obtenu via des interactions humaines. Mais revenons deux secondes sur les éléments que je vous ai donnés précédemment. Depuis quelques jours, un chiffre revient souvent : 2,5 milliards de comptes Gmail seraient potentiellement concernés. C'est un nombre qui impressionne, mais il est essentiel de le replacer dans son contexte. Cela ne veut pas dire que 2,5 milliards de comptes ont été piratés. À ce stade, aucun élément concret ne prouve que votre boîte mail a été visée. Les données utilisées dans ces campagnes d'hameçonnage pourraient tout aussi bien provenir de sources publiques, récupérées via des outils de collecte automatisée, ou d'anciennes fuites largement diffusées sur le web. Par ailleurs, les identifiants et mots de passe Gmail ne font pas partie des données impliquées dans la fuite signalée en juin dernier. Il n'y a donc aucune urgence à modifier vos accès si vous n'avez pas été alerté par Google. En résumé : il y a bien une offensive en cours, mais son périmètre réel reste flou. Il est légitime d'être vigilant, mais rien n'indique, pour l'instant, que les utilisateurs soient exposés à un risque direct ou massif. Gardez l'œil ouvert, mais inutile de céder à la panique.

[*Virgule sonore, un grésillement électronique.*]

C'est tout pour cet épisode de *Vitamine Tech*. Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous recommande le dernier épisode de *Bêtes de Science* dans lequel Gaby Fabresse vous emmène à la rencontre du lézard des murailles, un reptile capable de faire tomber et repousser sa queue en un claquement de doigt ! Pour le reste, je vous remercie pour votre fidélité à *Vitamine Tech*, je vous souhaite tout le meilleur, et, comme d'habitude, une excellente journée ou une très bonne soirée et rester branché !

[*Un glitch électronique ferme l'épisode.*]