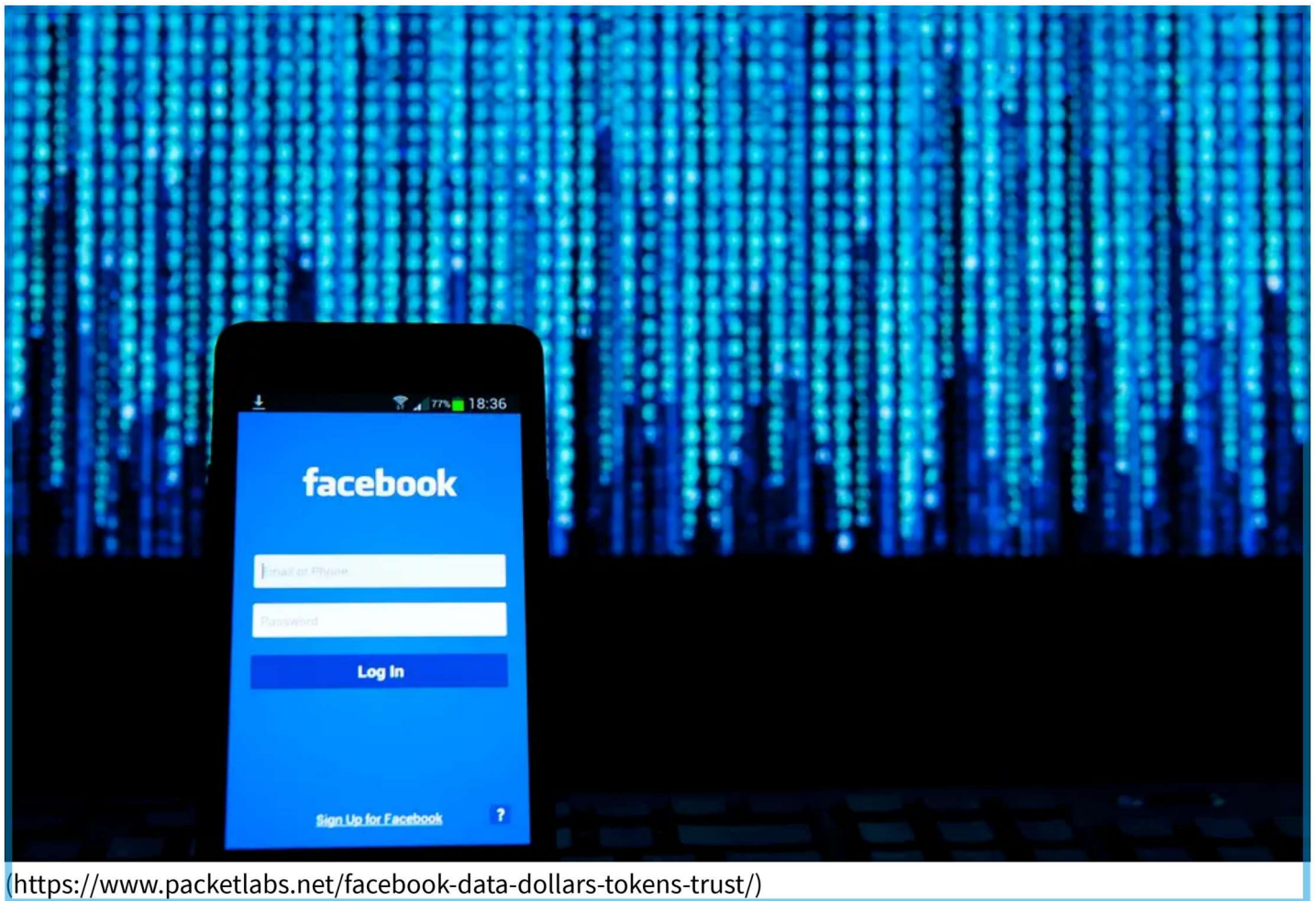


T: 647-797-9320 (tel:647-797-9320) Envoyez-nous un email (<mailto:info@packetlabs.net>)

## Dernières nouvelles



01 OCTOBRE

# Violation de Facebook: données, dollars, jetons et confiance

📁 Catégorie Actualités de l'industrie (<https://www.packetlabs.net/category/news/>)

---

Dans toute relation saine, la plupart des psychologues conviendraient que la confiance est au premier plan. C'est essentiel. Une fois qu'il est perdu, nombreux sont ceux qui supposeraient que, contrairement à l'argent, il ne peut presque jamais être racheté.

Entre les patients et les professionnels de la santé, il existe un accord écrit selon lequel les informations sur les patients resteront privées et ne seront pas divulguées à d'autres. La violation de ces contrats, qu'elle soit sociale ou légale, viole les termes fonctionnels de la relation et conduit presque toujours à nuire à une ou plusieurs personnes.

Et si la relation se situe entre une organisation et 50 millions d'utilisateurs? Les résultats peuvent être cataclysmiques. Pour maintenir la confiance, les organisations investissent souvent dans des contrôles de sécurité afin d'atténuer le potentiel de violation de données; que se passe-t-il quand quelque chose passe entre les mailles du filet? Le 25 septembre 2018, le géant des médias sociaux, Facebook, a informé les utilisateurs d'une violation massive de données affectant plus de 50 millions de personnes.

## Comment est-ce arrivé?

La violation impliquait des lacunes dans la fonction «Afficher en tant que» de Facebook. Cette fonctionnalité couramment utilisée permet aux utilisateurs de voir comment leurs profils apparaissent aux autres utilisateurs. Les attaquants ont réussi à utiliser cette fonctionnalité pour voler des jetons d'accès aux comptes des personnes dont les profils ont été recherchés à l'aide de la fonctionnalité. À partir de là, l'attaque a été chaînée d'un ami Facebook d'un utilisateur au suivant atteignant les jetons d'accès en cours de route.

Heureusement, une fois découvert, Facebook a agi rapidement pour corriger la vulnérabilité. Malheureusement, à ce stade, il était trop tard. Dans une organisation aussi grande que Facebook, le mal était fait. Trop peu, trop tard.

*Cyber-sécurité Définition: les jetons d'accès contiennent des informations d'identification de sécurité pour les sessions de connexion qui identifient l'utilisateur, les groupes de l'utilisateur, les privilèges de l'utilisateur et, dans certains cas, une application particulière.*

Facebook ne sait toujours pas quel type d'informations client a été compromis; cependant, ils sont certains que le piratage a affecté ceux qui utilisent Facebook pour se connecter à d'autres comptes, tels que Instagram, Tinder et d'autres applications tierces qui utilisent cette fonction de connexion. Sur la base des statistiques ci-dessus, la probabilité d'exposition aux informations des utilisateurs est importante.

Facebook Inc. risque une amende (<http://fortune.com/2018/09/30/facebook-data-breach-fine-european-privacy-gdpr-eu/>) potentielle de 1,63 milliard de dollars alors (<http://fortune.com/2018/09/30/facebook-data-breach-fine-european-privacy-gdpr-eu/>) que l'organisme de surveillance de la protection de la vie privée de l'UE enquête pour savoir si le réseau social a violé les lois de l'Union européenne sur la protection de la vie privée, GPDR (<https://www.packetlabs.net/privacy-policy-mayhem-new-regulations-aim-to-protect-the-consumer/>) .

Au-delà de la menace d'amendes, il y a la question inestimable de la confiance et de la confiance des utilisateurs. Peut-être plus précieux que toute amende, les dommages causés sont devenus si vastes que certaines personnes, y compris celles qui ne sont absolument pas affectées par la violation, envisagent de fermer complètement leurs comptes sur Facebook. Avec une base d'utilisateurs bien supérieure à 2 milliards, ce n'est certainement pas un saut de jugement de supposer que même une fraction d'un pourcentage de cette valeur pourrait nuire à l'organisation et à ses parties prenantes.

La question que toutes les organisations devraient se poser, après avoir appris l'existence d'un tel événement, est «Si un nom familier comme Facebook, avec des ressources pratiquement illimitées, est vulnérable, à quel point le nôtre est-il sécurisé?

Pour plus d'informations sur la manière de protéger les plus grands actifs de votre organisation, veuillez contacter l'équipe (<https://www.packetlabs.net/contact-us/>) de Packetlabs pour discuter de nos offres de services de test d'intrusion.

Cyber sécurité (<https://www.packetlabs.net/tag/cyber-security/>) , violation de données (<https://www.packetlabs.net/tag/data-breach/>) , Facebook (<https://www.packetlabs.net/tag/facebook/>)

Partagez ceci



## RECHERCHE BLOG

---

Mot-clé

## CATÉGORIES

---

Étude de cas (<https://www.packetlabs.net/category/case-study/>)

La cyber-sécurité (<https://www.packetlabs.net/category/cyber-security/>)

Éducatif (<https://www.packetlabs.net/category/educational/>)

Nouvelles de l'industrie (<https://www.packetlabs.net/category/news/>)

Informatif (<https://www.packetlabs.net/category/informative/>)

**Autres** (<https://www.packetlabs.net/category/uncategorized/>)

**Conseils** (<https://www.packetlabs.net/category/tips/>)

## DERNIÈRES NOUVELLES

---

**Évaluation des compromis et chasse aux menaces: sont-elles différentes?**  
(<https://www.packetlabs.net/compromise-assessment-vs-threat-hunting/>)

**Tarification des tests de pénétration: 4 facteurs clés à prendre en compte**  
(<https://www.packetlabs.net/penetration-testing-pricing/>)

**À quoi s'attendre d'un rapport de test de pénétration** (<https://www.packetlabs.net/what-to-expect-from-a-penetration-testing-report/>)

**5 raisons d'envisager un professionnel des tests de pénétration OSCP** (<https://www.packetlabs.net/oscp-penetration-testing-professional/>)

**Qu'est-ce qu'une page Web dynamique?** (<https://www.packetlabs.net/dynamic-pages/>)

## PRESTATIONS DE SERVICE (/SERVICES/)

---

Test de sécurité des applications (<https://www.packetlabs.net/services/application-security-testing/>)

Tests de pénétration (<https://www.packetlabs.net/services/penetration-testing/>)

Test de pénétration basé sur les objectifs (<https://www.packetlabs.net/services/objective-based-penetration-testing/>)

Contrôle qualité de la sécurité gérée (<https://www.packetlabs.net/services/managed-security-qa/>)

## MESSAGES RÉCENTS

---

**Évaluation des compromis et chasse aux menaces: sont-elles différentes?**  
(<https://www.packetlabs.net/compromise-assessment-vs-threat-hunting/>)

**Tarification des tests de pénétration: 4 facteurs clés à prendre en compte**  
(<https://www.packetlabs.net/penetration-testing-pricing/>)

**À quoi s'attendre d'un rapport de test de pénétration** (<https://www.packetlabs.net/what-to-expect-from-a-penetration-testing-report/>)

## LIENS RAPIDES

---

Ressources (<https://www.packetlabs.net/resources/>)

Nous contacter (<https://www.packetlabs.net/contact-us/>)

Politique de confidentialité (<https://www.packetlabs.net/privacy-policy/>)

Plan du site (<https://www.packetlabs.net/site-map/>)

Copyright © 2020 Packetlabs. Tous les droits sont réservés.

in



(<https://www.linkedin.com/company/packetlabs->

<https://twitter.com/pktlabs>)

HAUT