Romain PONS
Gaetan CORIN

Les fondamentaux en cybersécurité

Attaque informatique sélectionné :

Piratage de porte-monnaie virtuels sur les comptes d'utilisateur Vinted.

Lien article :

https://www.bitdefender.com/blog/hotforsecurity/cybercrooks-target-hundreds-of-vinted-second-hand-fashion-store-shoppers-how-can-you-limit-the-damage/

Articles liés :

https://www.20minutes.fr/high-tech/4029505-20230324-vinted-pirates-vide-porte-monnaie-virtuels-centaines-utilisateurs

Résumé :

Vinted, né en 2008 est un marché d'échange de vêtements basé en Lituanie où les utilisateurs vendent des vêtements/accessoires d'occasions. Avec près de 45 millions d'utilisateurs actifs, la plate-forme attire de nombreuses escroqueries, vente de faux vêtements haut de gamme et de nombreux faux comptes.

Mais aux alentours du 24 mars 2023, une nouvelle escroquerie voit le jour, les utilisateurs en France, en Italie et en Espagne de l'application Vinted ont signalé le piratage de leur compte utilisateur ainsi que la perte de leur cagnotte.

Plusieurs centaines de victimes font appellent à la plate-forme pour obtenir de l'aide afin de récupérer leur argent.

Les escrocs ciblent des comptes avec beaucoup de ventes dernièrement afin de s'assurer le plus possible que la cagnotte contient de l'argent. Leur méthode est d'envoyer un sms/mail ou encore d'appeler les victimes dans le but de leur demander leur identifiant et réussir à leur soutirer l'argent contenu dessus.

Romain PONS
Gaetan CORIN

Conséquences :

Au cours des deux semaines suivants l'attaque, des clients Vinted en France, en Italie et en Espagne sont venues se plaindre sur les forums et les médias sociaux afin de signaler de pertes de plusieurs centaines à plusieurs milliers d'euros.

A la suite de cette attaque, Vinted à bloquer l'accès aux comptes de plusieurs des victimes, en raison de l'accès frauduleux des comptes qui ont été constaté.

Malgré le fait que les informations bancaires des victimes n'ont pas directement fuité du site de Vinted, et que le vol d'informations est réalisé par un système de phishing extérieur au site, la marque a décidé de rembourser l'intégralité des comptes volés.

Failles et vulnérabilités :

La plupart des phishings réalisés durant cette attaque s'est produit sous forme d'emailing, de SMS, ou d'appel téléphonique.

Ces démarches visées à demander aux utilisateurs de fournir des identifiants permettant aux attaquants de s'emparer des comptes Vinted, et de changer le compte bancaire associé afin de transférer les fonds dans un autre compte appartenant au voleur.

La faille de sécurité mis en évidence durant ce vol relève des droits des utilisateurs à effectuer un virement bancaire, alors qu'ils viennent juste de modifier leur compte RIB / IBAN associé à leur compte interne Vinted.

La vulnérabilité présentée durant ce vol est la méconnaissance des utilisateurs vis-à-vis des méthodes de phishing.

Impact réel de confidentialité :

Durant la réalisation du phishing, de nombreux comptes et mot de passes ont été volés par les hackers.

Cela représente un vrai problème de confidentialité, que cela soit aussi bien vis-à-vis des comptes Vinted concernés, mais aussi de tout autres comptes créés sur des plateforme tierces avec le même nom de compte et mot de passe.

Impact réel d'intégrité :

Il n'y a pas véritablement d'impact réel d'intégrité dans cette attaque, car très peu de données ont été modifiés ou supprimés.

La seule perte de données par compte utilisateur représente leur RIB qui ont été modifiés sans leur consentement. Il s'agit donc de perte d'informations de la part de Vinted.

Romain PONS
Gaetan CORIN

Impact réel de disponibilité :

Après avoir vidé le compte des victimes, les pirates mettent en vente du contenus interdit dans le but de bloquer leur compte après avoir supprimé leur RIB.

Les victimes se retrouve alors avec un compte vidé de son argent et surtout inaccessible car bloqué par la plate-forme pour du contenu inapproprié.

Type de menace implémenté :

Ce type de menace s'appelle le « phishing », ce qui consiste à tromper les utilisateurs en se faisant passer pour quelqu'un/un service de la société Vinted (pour notre exemple) afin d'obtenir de leur part leur identifiant et avoir accès a leur compte Vinted.

Choix de contre mesure :

Le choix de contre-mesure pour lutter contre ce type de piratage est de rajouter des précautions supplémentaires sur le cas d'utilisation de retrait bancaire à la suite d'une modification de RIB.

Il serait judicieux de mettre en place des préventions afin d'avertir les utilisateurs sur les risques du phishing.