AL2023_07 Large-scale credential stuffing attack targets PayPal accounts (January 20, 2023)

Description

Thousands of PayPal users have been receiving warnings from PayPal about their accounts being breached through credential stuffing attacks.

Summary

PayPal has confirmed that some amount of personal data from thousands of users' accounts have been leaked as these accounts experienced a large-scale credential stuffing attack. Credential stuffing is a cyberattack method in which attackers use lists of user credentials available from data leaks online to breach into a system. The attack uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services; this is known as password recycling.

PayPal had explained that this credential stuffing attack occurred between December 6 and December 8 of 2022. PayPal managed to detect and mitigate the attack after two days but began investigation to determine how attackers managed to obtain unauthorized access to those accounts. It was revealed that the attackers logged in using valid credentials and it was not due to a breach in PayPal’s electronic payments platform to obtain the credentials.

According to the data breach report from PayPal, 34,942 users had their accounts accessed by attackers, where confidential information of the users were available such as full names, dates of birth, postal addresses, social security numbers, individual tax identification numbers, transaction histories, connected credit or debit card details, and PayPal invoicing data. However, PayPal claims that the attackers did not manage to perform any transactions from the breached PayPal accounts, stating that "We have no information suggesting that any of your personal information was misused as a result of this incident, or that there are any unauthorized transactions on your account". PayPal reset the passwords of all the affected PayPal accounts and has implemented enhanced security controls to combat the situation.

Remediation

PayPal strongly recommends changing your PayPal and other online accounts using a unique and long string password. Typically, it is recommended to implement a password with at least 12-characters long and includes alphanumeric characters and symbols.

Moreover, PayPal advises that users activate two-factor authentication (2FA) protection on your account, which can prevent attackers from gaining access to your account, even if they manage to obtain your username and password.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B (2023, January 19). *PayPal accounts breached in large-scale credential stuffing attack*. Retrieved from the BleepingComputer. https://www.bleepingcomputer.com/news/security/paypal-accounts-breached-in-large-scale-credential-stuffing-attack/
- PayPal. (2023, January 18). *NOTICE OF SECURITY INCIDENT*. Retrieved from https://s3.documentcloud.org/documents/23578067/paypal-notice.pdf