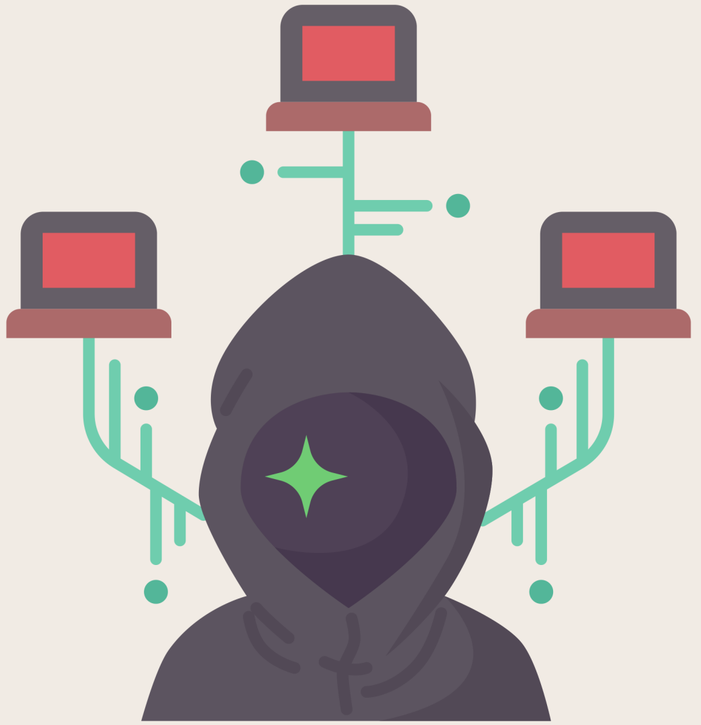
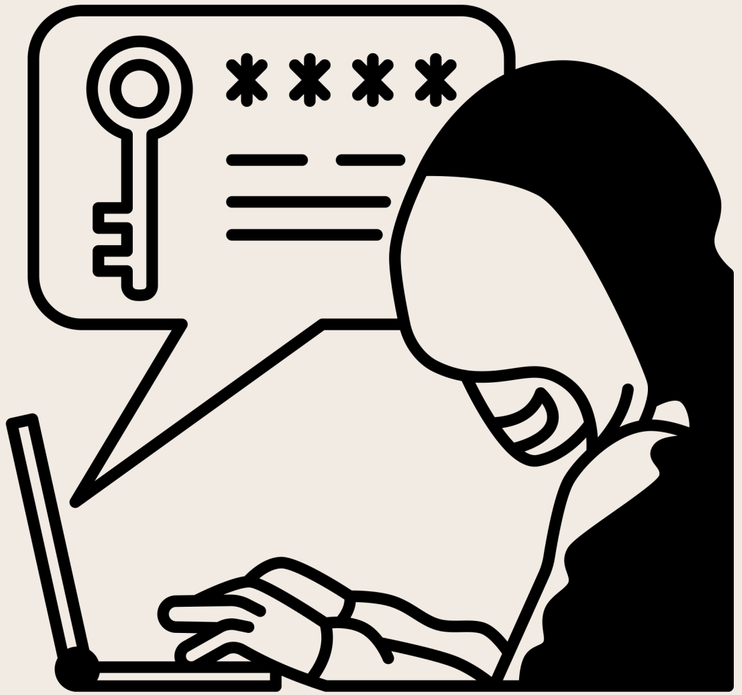
TRELLO DATA BREACH

UNDERSTANDING THE IMPACT AND CONSEQUENCES



Popular project management platform, Trello, has experienced a data breach exposing 15 million users' personal details. The confidential information, including names and emails, has reportedly been collected and is now being sold on the Dark Web.

According to a threat actor using the pseudonym “emo,” the January 16, 2024, Trello data breach exposed the account information.



The perpetrators used email addresses obtained from previous breaches, indicating a sophisticated approach to targeting and exploiting vulnerabilities in the system.

Despite the alarming nature of the breach, Trello maintained that there was no unauthorized access to its systems. That suggests the breach was executed through a method that didn't require breaking into the system's internal networks or databases.

A Atlassian, Trello's parent firm, claims it's taken significant steps to prevent such scraping attacks from recurring, by adjusting the primary API. However, some experts suggest Atlassian might be downplaying its role in the incident.

This security breach saw unauthorised data scraping and extraction from 15 million Trello profiles, sparking severe concerns about user privacy and data protection. The incident, exposing vulnerabilities in Atlassian's API, has underscored the crucial need for more robust security around application programming interfaces to forestall unlawful access.

The breach was officially recognized and added to the "Have I Been Pwned" (HIBP) database on January 22, 2024. HIBP is a widely used resource that allows individuals to check if their data has been compromised in any data breach.

Trello has limited an unauthenticated party’s ability to query users’ public profile information using an email address, effectively slowing down future attacks.

Adding this breach to HIBP serves as a critical alert for the millions of users potentially affected, urging them to take necessary actions such as changing passwords and being vigilant for phishing attempts using their personal information.