Personal data of 15 million Trello users leaked on hacking forum

An unknown hacker recently publicly released more than 15 million email addresses associated with Trello accounts on a hacking forum.

Initial disclosures showed the trove of data was collected using an unsecured API earlier this year.

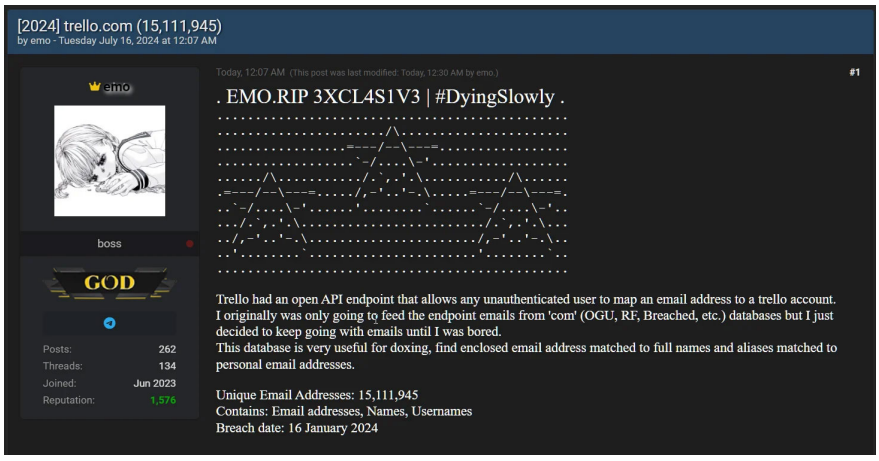
Trello is an online project management tool owned by Atlassian. Businesses often use tools to organize data and tasks into tables, cards, and lists. The advantage of Trello is that it makes it easy to show workflow, project ownership, and completion status.

Previously in January, BleepingComputer reported that a threat actor with the nickname 'emo' was selling the profiles of 15,115,516 Trello members on a popular hacking forum. While most of the data in these profiles is public information, each profile also contains a private email address associated with the account.

Although Atlassian, the owner of Trello, did not confirm at the time how the data was stolen, the hacker himself revealed that the data was collected using an unsecured REST API, allowing developers query public profile information based on Trello ID, username, or email address.

emo created a list of 500 million email addresses and fed them into an API to determine if they were linked to a Trello account. This list is then combined with returned account information to create member profiles for more than 15 million users. emo has now shared the entire list of 15,115,516 profiles on the Breached hacking forum for 8 site credits (worth $2.32).

" *Trello has an open API endpoint that allows any unauthenticated user to map an email address to a trello account* ," emo explains in the forum post. " *Initially I was only going to serve endpoint emails from the 'com' database (OGU, RF, Breached, etc) but I decided to keep using email until I got bored* ."



The leaked data included email addresses and public Trello account information, including users' full names.

This information can be used in targeted phishing attacks to steal more sensitive data, such as passwords. emo also said the data could be used to carry out doxxing, allowing threat actors to link email addresses to people and their aliases. Atlassian has now also confirmed information about the incident.

Unsecured APIs have become a popular target for hackers, who know how to abuse them to combine non-public information, such as email addresses and phone numbers, with public records.

In 2021, a group of hackers abused the API to link phone numbers to Facebook accounts, creating profiles for 533 million users.

In 2022, Twitter also suffered a similar breach when threat actors abused an unsecured API to link phone numbers and email addresses to millions of users of the social media platform. pose significant privacy risks.

Many organizations try to secure APIs using rate limiting instead of through authentication via an API key.

However, an attacker can simply buy hundreds of proxy servers and spin up connections to continuously query the API, making rate limiting useless.