Hi Everyone,

I would like to share about a password **attack**that happened in May 2019 with **Canva**, Australian graphic design tool website Canva suffered an attack that exposed email addresses, usernames, names, cities of residence, and salted and hashed with bcrypt passwords (for users not using social logins — around 61 million) of 137 million users. Canva says the hackers managed to view, but not steal, files with partial credit card and payment data.

# **What was compromised in the attack?**

* The **profile database of 139 million users** was accessed. This contained usernames, email ids, public profile ids.
* **Encrypted passwords** using bcrypt hashing algorithm. bcrypt is still considered to be one of the most secure algorithms.
* **A claim of access to the OAuth login tokens**of those users who had logged in using Google. (OAuth tokens are what applications use to make requests on behalf of the user for the authorization of the specific application.)
* **Limited viewing of card details and payment data.**Fortunately for Canva, it never stores complete credit card information in one place. Therefore even though the attacker might have viewed these files momentarily, they couldn’t have used it for carrying out payments.

# **Why were the users not thought to be at much risk?**

* Since the **passwords had been first salted and then protected with a hashing function called [bcrypt](https://en.wikipedia.org/wiki/Bcrypt)**, it was considered then that even though the attackers had access to the hashed password they would never be able to decrypt them and recover the original password. bcrypt is one of the**strongest hash algorithms there is since its iteration count can be dynamically increased with time** to make it slower and thus resistant to brute force attacks.
* The **OAuth tokens too were encrypted using an algorithm called AES128**and the keys for the same were **stored in another separate secure location.** There was no evidence that those keys from that location were accessed. And without the keys, the tokens alone would not prove to be of much use to the attacker.

Later, the company confirmed the incident and subsequently notified users, prompted them to change passwords, and reset OAuth tokens. However, a list of approximately 4 million Canva accounts containing stolen user passwords was later decrypted and shared online, leading the company to invalidate unchanged passwords and notify users with unencrypted passwords in the list.

The suspected culprit(s) — known as **Gnosticplayers** — contacted ZDNet to boast about the

incident, saying that Canva had detected their attack and closed their data breach server. The

attacker also claimed to have gained **OAuth login tokens** for users who signed in via

Google.

**Reference Links:**

<https://www.scmagazine.com/home/security-news/data-breach/hacker-has-designs-on-canva-data-steals-info-belonging-to-139m-users/>

<https://www.miamioh.edu/it-services/news/2020/02/canva-breach.html>

<https://codeburst.io/inside-canvas-security-breach-that-affected-139-million-user-accounts-78467e315681>