**1. Town of Salem: 28 December 2018**

https://blog.dehashed.com/town-of-salem-blankmediagames-hacked/

7.6M unique user email addresses alongside usernames, IP addresses, purchase histories, payment information

and passwords stored as phpass hashes.

Happened because of an entree-level vulnerability known as “LFI” / “RFI”.

**2. Yahoo: 11 July 2012**

nearly half a million usernames and passwords stored in plain text

Compromised via a SQL injection attack

**3. Patreon: 1 October 2015**

https://www.zdnet.com/article/patreon-hacked-anonymous-patrons-exposed/

more than 2.3M unique email addresses, millions of personal messages and passwords stored as salted bcrypt hashes

Patreon was compromised on September 28 via a debug version of the Patreon website which was publicly available.

**4. Live Auctioneers: 19 June 2020 discovered 11 July 2020**

https://portswigger.net/daily-swig/liveauctioneers-data-breach-millions-of-cracked-passwords-for-sale-say-researchers

3.4 million records including names, email and IP addresses, physical addresses,

phone numbers and passwords stored as unsalted MD5 hashes

security breach at a LiveAuctioneers data processing partner that occurred on June 19

**5. Exploit.in: 13 October 2016**

https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/

Credential stuffing list

593 million unique email addresses, many with multiple different passwords hacked from various online systems

**6. 123RF: 22 March 2020**

https://www.bleepingcomputer.com/news/security/popular-stock-photo-service-hit-by-data-breach-83m-records-for-sale/

email, IP and physical addresses, names, phone numbers and passwords stored as MD5 hashes

How the breach happened is unknown

**7. 8fit: 1 July 2018 discovered 8 February 2019**

https://8fit.zendesk.com/hc/en-us/articles/360017746394-Notice

over 15M unique email addresses alongside names, genders, IP addresses and passwords stored as bcrypt hashes

How the breach happened is unknown

**8. 8tracks: 27 June 2017**

https://blog.8tracks.com/2017/06/27/password-security-alert/

18 million emails and passwords stored as salted SHA-1 hashes, for users who didn't sign up with either Google or Facebook authentication

"the vector for the attack was an employee’s GitHub account, which was not secured using two-factor authentication"

8tracks does not store passwords in a plain text format, but rather uses one-way hashes to ensure they remain difficult to access. These password hashes can only be decrypted using brute force attacks, which are expensive and time-consuming, even for one password.

Passwords on 8tracks are hashed and salted, meaning that even we can’t tell you what your password is by looking at the database. Although the decryption of one particular user’s password through brute-force techniques is unlikely,

**9. Adecco: 3 January 2021**

https://cybernews.com/security/5-million-adecco-com-users-data-leaked/

over 4M unique email addresses as well as genders, dates of birth, marital statuses, phone numbers and passwords stored as bcrypt hashes (with a cost of 10).

Unknown how the breach happened, data was found being sold on a forum

**10. Adobe: 4 October 2013**

https://www.troyhunt.com/adobe-credentials-and-serious/

153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password (3DES) and a password hint in plain text

Unknown how the breach happened

**11. Ancestry: 7 November 2015 discovered 24 December 2017**

https://www.ancestry.com/corporate/blog/rootsweb-security-update/

almost 300k email addresses and plain text passwords

RootsWeb server leak

**12. Android Forums: 30 October 2011**

https://www.pcworld.com/article/459834/online\_android\_forum\_hacked\_user\_data\_accessed.html

745k email addresses, user birth dates and passwords stored as a salted MD5 hash

Unknown how the breach happened

**13. Animal Jam: 12 October 2020**

https://www.animaljam.com/en/2020databreach

over 7 million unique email addresses. Impacted data also included usernames, IP addresses and for some records, dates of birth (sometimes in partial form), physical addresses, parent names and passwords stored as PBKDF2 hashes

a hacker was able to penetrate the server of a third-party vendor WildWorks uses for intra-company communication

**14. AnimeGame: 27 February 2020**

https://www.itsecuritynews.info/animegame-1431378-breached-accounts/

1.4M subscribers and exposed email addresses, usernames and passwords stored as salted MD5 hashes

Unknown how the breach happened

**15. Appen: 30 July 2020**

https://www.bleepingcomputer.com/news/security/hacker-leaks-386-million-user-records-from-18-companies-for-free/

almost 5.9 million names, email addresses and passwords stored as bcrypt hashes

unknown how the leak happened

**16. Aptoide: 13 April 2020**

https://blog.aptoide.com/aptoide-credentials-information/

20M emails, names, IP addresses and passwords stored as SHA-1 hashes without a salt

Unknown how the breach happened

**17. Armor Games: 1 January 2019 discovered 29 January 2019**

https://techraptor.net/gaming/news/armor-games-data-breach-confirmed-took-place-in-january-2019

10.6 million email addresses were impacted by the breach which also exposed usernames, IP addresses, birthdays of administrator accounts and passwords stored as salted SHA-1 hashes

Unknown how the breach happened

**18. Army Force Online: 18 May 2016**

https://www.incibe-cert.es/en/early-warning/cybersecurity-highlights/15-million-accounts-stolen-massive-online-game-army-force

1.5M usernames, email, IP addresses and MD5 passwords

Unknown how the breach happened

**19. Artsy: 1 April 2018**

https://www.artnews.com/art-news/news/artsy-data-stolen-security-incident-11904/

1M accounts were impacted and included IP and email addresses, names and passwords stored as salted SHA-512 hashes

Unknown how the breach happpened

**20. Artvalue: 19 June 2019**

https://haveibeenpwned.com/PwnedWebsites#Artvalue

158k names, usernames, email addresses and passwords stored as MD5 hashes

"Artvalue.com left their 158k member subscriber base publicly exposed in a text file on their website"

Artvalue was the last one added to the database that still has notes. Everything in the database after Artvalue doesn’t have notes yet.