Have I Been Pwned warns of DatPiff data breach impacting millions

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

January 4, 2022 11:22 AM **0**

The cracked passwords for almost 7.5 million DatPiff members are being sold online, and users can check if they are part of the data breach through the Have I Been Pwned notification service.

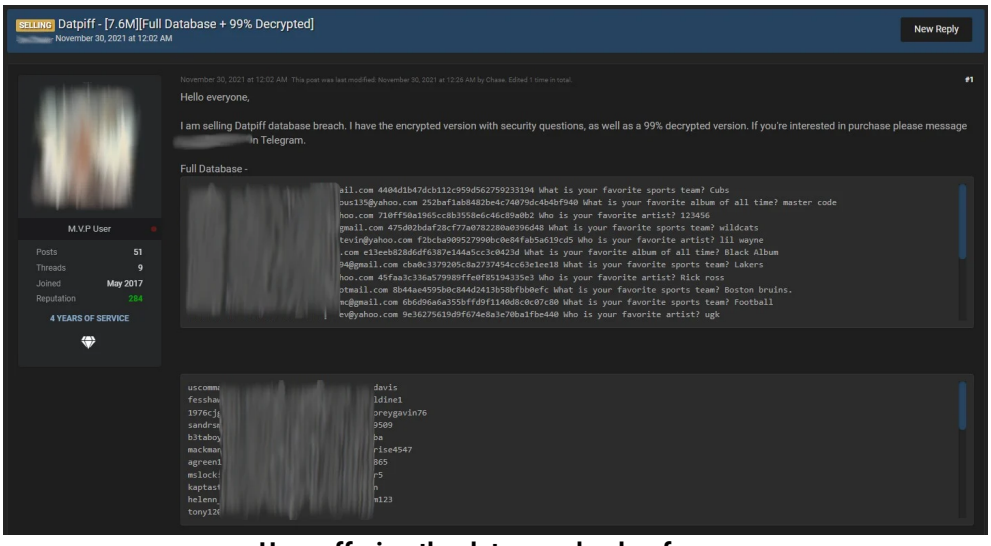
DatPiff is a popular mixtape hosting service used by over 15 million users, allowing unregistered users to download or upload samples for free.

The DatPiff data breach

It is unclear when the data breach occurred, but the DatPiff database was first sold privately and then publicly on hacking forums in July 2020.

The stolen DatPiff database contains 7,476,940 member records, including a user's email address, password, username, and security question.

On November 30th, another data breach collector began selling the database again on the same hacking forum. However, this time, the passwords were dehashed to include the plain-text passwords along with the email address.



User offering the data on a hacker forum

Soon after, another threat actor released the database entirely for free, allowing any other threat actor to use the information.

The passwords in the database could be cracked because DatPiff hashed them with the MD5 algorithm, an old (1992) cryptographic hash function that is considered obsolete and insecure, especially for securing passwords.

To dehash MD5 passwords, crackers can compare hashes to known MD5 wordlists or use cracking tools to brute force the passwords.

BleepingComputer was told in December that a threat actor breached DatPiff using a website vulnerability scanner that allowed them access to the server.

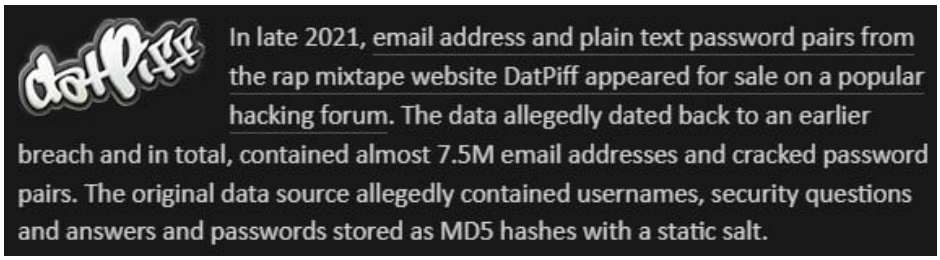
However, it is believed that the threat actor did not breach the actual DatPiff website but rather a server with old database backup

What should DatPiff users do?

While this database is very old, if you have an account on DatPiff, it is strongly advised that you reset your password and use one unique and strong.

Those using the same password on other websites should change it there to avoid falling victim to credential stuffing attacks.

DatPiff members can search for their email addresses on the Have I Been Pwned (https://haveibeenpwned.com/) data breach notification services to see if they are one of the over 7 million users impacted by this breach.



HIBP notice

At the time of writing this, DatPiff hasn't published a statement on this data breach incident, hasn't sent any notices to users, and hasn't forced a password reset.

Bleeping Computer has reached out to the platform, and we will update this piece as soon as we receive a comment from them.