Plain-Text Leaked Passwords

Hackers always first go for the weakest link to quickly gain access to your online accounts. Online users habit of reusing the same password across multiple services gives hackers the opportunity to use the credentials gathered from a data breach to break into their other online accounts.

Researchers from security firm 4iQ have now discovered a new collective database on the dark web (released on Torrent as well) that contains a whopping 1.4 billion usernames and passwords in clear text.

The aggregate database, found on 5 December in an underground community forum, has been said to be the largest ever aggregation of various leaks found in the dark web to date, 4iQ founder and chief technology officer Julio Casal noted in a blog post.

Though links to download the collection were already circulating online over dark-web sites from last few weeks, it took more exposure when someone posted it on Reddit a few days ago, from where we also downloaded a copy and can now verify its authenticity.

Researchers said the 41GB massive archive, as shown below, contains 1.4 billion usernames, email, and password combinations—properly fragmented and sorted into two and three level directories.
The archive had been last updated at the end of November and didn't come from a new breach—but from a collection of 252 previous data breaches and credential lists.

The collective database contains plain text credentials leaked from Bitcoin, Pastebin, LinkedIn, MySpace, Netflix, YouPorn, Last.FM, Zoosk, Badoo, RedBox, games like Minecraft

and Runescape, and credential lists like Anti Public, Exploit.in.
“None of the passwords are encrypted, and what’s scary is that we’ve tested a subset of these passwords and most of them have been verified to be true,” Casal said. “The breach is almost two times larger than the previous largest credential exposure, the Exploit.in combo list that exposed 797 million records.”

“This new breach adds 385 million new credential pairs, 318 million unique users, and 147 million passwords pertaining to those previous dumps.”
The database has been neatly organized and indexed alphabetically, too, so that would-be hackers with basic knowledge can quickly search for passwords.
For example, a simple search for “admin,” “administrator” and “root,” returned 226,631 passwords used by administrators in a few seconds.

Although some of the breach incidents are quite old with stolen credentials circulating online for some time, the success ratio is still high for criminals, due to users lousy habit of re-using their passwords across different platforms and choosing easy-to-use passwords.
The most common yet worst passwords found in the database are “123456”, “123456789”, “qwerty,” “password” and “111111.”

It is still unclear who is responsible for uploading the database on the dark web, but whoever it is has included Bitcoin and Dogecoin wallets for any user who wants to donate.
To protect yourself, you are strongly advised to stop reusing passwords across multiple sites and always keep strong and complex passwords for your various online accounts.