520.743.7554
info@computerdimensions.net
www.computerdimensions.net

RockYou2021 is Largest Password Leak of All Time at 8.4 Billion Entries

A compilation file of stolen and leaked passwords, dubbed RockYou2021, recently appeared on a hacker forum. CyberNews reports that an anonymous forum poster uploaded a 100GB TXT file containing 8.4 billion entries of passwords. Although the poster claimed the file contained 82 billion passwords, independent analysis confirmed the number (while still staggering) is actually ten times less. However, it remains the largest password and credentials leak of its kind in history.

By combining 8.4 billion unique password variations with other breach compilations that include usernames and email addresses, threat actors can use the RockYou2021 collection to mount password dictionary and password spraying attacks against untold numbers of online accounts. Since most people reuse their passwords across multiple apps and websites, the number of accounts affected by credential stuffing and password spraying attacks in the wake of this leak can potentially reach millions, if not billions.

Given that only 4.7 billion people are online across the world, the perpetrators may have multiple passwords for millions if not billions of users. The RockYou2021 compilation file may be the steppingstone hackers are looking for to begin more targeted credentials attacks. Since so many people were potentially affected, businesses should begin alerting employees to the danger and mandating password changes across all accounts. Additionally, enterprises should begin (if they have not already) implementing multifactor authentication (MFA) and other critical identity management protections.

Also, your employees and administrators should take the necessary steps to ensure that they make the strongest and most secure passwords possible. Despite passwords being largely ineffectual as a lone authentication factor, the combination of longtime recognition and ubiquitousness ensures their place in access management for years to come.

Therefore, your enterprise should make users aware of the tools at their disposal. Free websites like haveibeenpwned.com allow users to compare their emails to thousands of breaches, seeing where they may have been compromised and prompting new credentials. Meanwhile, password checkers can help employees determine whether their passwords actually measure up to the realities of password crackers and simple guesswork.

Cybersecurity experts strongly advised that today is the day to change all your passwords. You may have been putting this off thinking you are not affected. You are. We all are. Now you have an excellent reason – to protect your privacy and your assets. Anything and everything will come out so waste no time. Change all your passwords immediately. And please make sure they are unique and complex. Also, ensure that usernames/passwords on their own are not enough to gain access to backend systems. Adding a requirement for appropriate and independently verified factors to gain access to your servers will ensure that your business is not affected by credential stuffing attacks based on breaches such as RockYou2021.