Dark Web cyber criminal marketplaces host over 24 billion stolen online credentials

NEWS 20 Jun 2022

The global cyber criminal community has been actively using and trading more than 24 billion usernames and password combinations on the Dark Web and underground marketplaces, threat intelligence firm Digital Shadows has revealed.

A recent report published by threat intelligence firm Digital Shadows has revealed that more than **24 billion usernames and password combinations** are available on the Dark Web and cybercriminal marketplaces. This represents an alarming 65% increase from the number of such combinations recorded in 2020.

According to Digital Shadows, thousands of Internet users worldwide are still using the phrase ‘password’ as passwords for their online accounts. The list of the most commonly-used passwords includes a combination of easily remembered numbers like 123456, which every one in 200 individuals uses. Keyboard combinations, such as ’qwerty’ or ’1q2w3e’, also feature among the top 50 most commonly-used passwords.

“Of the 50 most commonly used passwords, 49 can be ’cracked’ in under one second via easy-to-use tools commonly available on criminal forums which are often free of charge or at minimal cost,” the firm said.

However, adding a 'special character' (such as @ # or _) to a basic 10-character password makes it little difficult for a threat actor to decode and adds approximately 90 minutes to the amount of time an offline attack would take to crack the password. Adding two special characters takes an average of 2 days and 4 hours to crack and is less likely that an individual will fall victim to an attack.

Research conducted by Digital Shadows unearthed several combinations advertised in more than one forum. However, even after removing duplicate combinations, the firm still found 6.7 billion unique credentials which represented an increase of approximately 1.7 billion or 34% in two years.

Chris Morgan, the Senior Cyber Threat Intelligence Analyst at Digital Shadows, said, "We will move to a 'passwordless' future, but for now the issue of breached credentials is out of control. Criminals have an endless list of breached credentials they can try but adding to this problem is weak passwords which means many accounts can be guessed using automated tools in just seconds. In just the last 18 months, we at Digital Shadows have alerted our clients to 6.7 million exposed credentials.

“This includes the username and passwords of their staff, customers, servers and IoT devices. Many of these instances could have been mitigated through using stronger passwords and not sharing credentials across different accounts,” he added.

Digital Shadows recommends using a password manager to keep complex passwords. Users of password managers can access all of their online accounts without having to remember each password. Multi-factor authentication (MFA) can also be used if and when an account provider offers the same and an authenticator app can be used that would generate a new random six-digit code every 30 seconds.

Commenting on the scale at which the global cyber criminal community gains access to Internet users’ online credentials, Rob Griffin, CEO at MIRACL, said, “The digital acceleration has exploded since the pandemic and we need to wake up to the fact that passwords are no longer a secure means of protection. Especially when so many individuals use password combinations that are easy to guess.

“Authentication needs to change, and people need to be aware of the flaws in password-based authentication. Reports such as these highlights the need for other, safer means of authentication that require

multiple factors and can't be phished or brute-forced. Passwords are outdated and this report makes it clear that cyber criminals are capitalising on this vulnerable authentication process," he added.

Cyber Crime