More than 60% of passwords are cracked by AI in less than 60 seconds

According to Kaspersky researchers, with the help of AI, about 61% of passwords can be cracked in less than a minute, nearly three times higher than traditional cracking methods.

Passwords are often created by users as plain text, then hashed to create a string of characters that is nearly impossible to read or reverse. To detect passwords, hackers often use the brute-force method (brute-force attack), which means testing character strings until they find the password. According to Kaspersky research, about 23% of passwords can be detected in under 60 seconds this way, 9% can be cracked in 1-60 minutes.

However, in the context of AI developing and being used for malicious purposes, attackers can build their own AI models to improve the ability to guess and even reverse passwords encoded into original characters. First, take advantage of previously exposed passwords. For example, these models will use the data source of 10 billion passwords leaked in July to detect passwords.

Cracking time	Bruteforce, %	Intelligent, %
< 60 s	23	61
60 s to 60 min	9	17
60 min to 24 h	13	8
24h to 30 d	11	5
30 d to 365 d	7	2
> 365 d	37	7

Calculation for RTX 4090 GPU, MD5 with a salt

The AI ??research team at Kaspersky trained an AI model to analyze leaked passwords. As a result, about 32% of passwords can be recovered from hashed form in less than 60 minutes.

When running the AI ??application on RTX 4090 GPU hardware and the MD5 hash function at a speed of 164 billion hashes per second, the results were that about 61% of passwords were cracked in just 60 seconds and 17% were cracked in 1- 60 minutes, three times higher than the old brute-force method.

Statistics of password cracking rates over each period of time between Kaspersky's brute-force method and AI application (right). Screenshot

The user's habit of setting passwords using related characters or common character strings such as "admin", "password", "qwerty12345", "nguyen". is one of the factors that makes it easy for AI to crack. .

Experts recommend that users should set long passwords, containing letters, numbers, special characters, or use a random password generator to reduce the possibility of being cracked.

In the context of AI being increasingly applied in life and work, attackers also have many new methods.

AI is a powerful tool that is increasingly being applied in life and work, but bad guys can also use it for bad purposes such as writing malicious code, automating attacks, and creating social engineering attacks. on the user.