Hacker cracked a password of 16 characters in less than 60 minutes

In an experiment of Ars Technica website, 14,800 passwords were successfully hacked, including codes of 16 characters in length.

In an experiment of Ars Technica website, 14,800 passwords were successfully hacked, including codes of 16 characters in length.

The site provided a hacker team of about **16,449 encrypted passwords** , and asked them to decrypt as many passwords as possible within **an hour** . During this time, **Jens Steube,** chief programmer of unlocking software oclHashcat-plus, unlocked **13,486 passwords,** equivalent to **82%** of all passwords assigned. Even, this hacker does not need to use a computer network with terrible power, but only need a computer with 2 graphics cards.

Even the " *poorest* " member of the hacker team (nicknamed radix) also has the ability to unlock up to **62%** of the assigned passwords **within an hour,** and the hacker has even unlocked the password that was just paid. interview. **So, what is the reason why these hackers can work so well?**

With short passwords, hackers only need to use **brute-force measures** . This is a method in which computers try to enter all strings that can be built from characters, such as from aaaaa to ZZZZZ. With a short length, the number of characters that can be created is not much, so the brute-force attack method doesn't take too much time. With longer passwords, hackers need to use more sophisticated methods.

One member of this hacker team, **Jeremi Gosney** , added some parameters to his **brute-force attacks** . He let his computer **guess the 7-8** characters of **the password** , including all lowercase letters (without capital letters). Gosney also uses Markov-style attacks: **The method relies on similarities** in the structure of the password (such as uppercase letters, lowercase letters, strange characters and last digits) To minimize the number of times a computer must guess a password.

Hackers also use **dictionary attacks.** Dictionary attack will detect the required password from a list of available words (called a *"wordlist* "). In fact, *"dictionary" ("wordlist")* in *"dictionary attack"* is many times larger than a regular dictionary. The wordlist you can find for free online contains millions of words from many different languages, and also common passwords like *"password123"*.

Anyone who owns a computer with relative power and an Internet connection can use these tools - even the poorest password detectors can decipher about **60%** of the Password assigned within a few hours. Password searchers can find more passwords at a faster rate. Many passwords can be decrypted because they follow common trends, **so you can rely on the following tips to increase the security of your password:**

- Please use the password as long as possible. The longer the password, the harder it is to be unlocked.

- Use a few uppercase letters, especially in the middle of the password. Passwords use only lowercase letters and numbers are much easier to crack.

- Many passwords start with strange letters or characters and end with numbers. Change this structure to create an unpredictable structured password.

In an age where companies reveal more and more personal information of users, including big names like Twitter or Sony, remember that your responsibility to protect your account is yours first.