ENZOIC

Cracking Dictionaries

WHAT YOU NEED TO KNOW

Passwords are the standard authentication factor across sites and systems, but how we deal with passwords has changed over time.

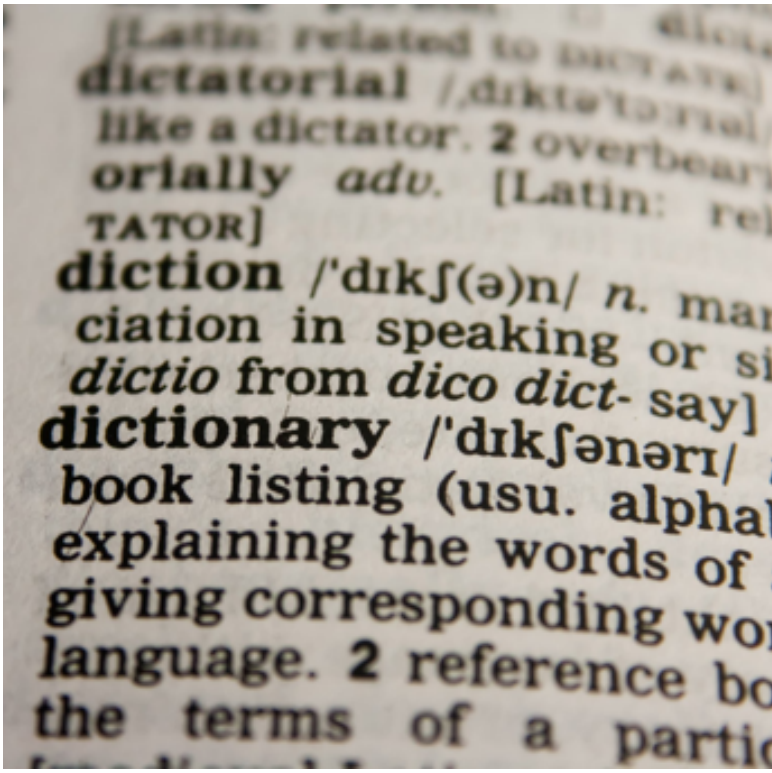
Today, password hashing is a critical security measure organizations should leverage to protect passwords. Because many organizations leverage password hashing to protect passwords, cracking dictionaries have evolved to crack those password hashes.

Here is a quick overview.

What Are Cracking Dictionaries?

Cracking dictionaries are large lists of data, often cleartext strings, that can be used to crack passwords. These lists can include words in the form of dictionary words, common passwords, iterations of common passwords, and exposed passwords. They can also contain passwords that used to be hashed but have been subsequently cracked because they were stored in a weak password hashing algorithm.

As data breaches and password exposure increases year-over-year, more-and-more dictionaries of reverse-engineered hashed passwords are emerging.



Cracking Dictionaries & Passwords Explained

Passwords have been a common feature of the internet landscape since its inception, and until recently, they were the only thing protecting your data.

Cybersecurity experts recommend multi-factor account protection with things like biometrics, authenticators, and two-factor authentication, but many people still do not turn on MFA if it is optional because it takes longer to access their account. MFA is not a standard for many websites and many internal systems. Passwords are still the standard authentication factor because no other method has proven to be easier yet, while also being more secure.

How we deal with passwords has also changed over time. Ten or fifteen years ago, it wouldn't have been unusual to walk past a colleague's computer and see a post-it note with their password scribbled on it stuck to their screen. Such a huge security mishap may seem shocking today, but it was common in a time when data breaches were rare and cybersecurity awareness was lacking.

In the digital age, as major data breaches are happening almost daily, cybercriminals can get access to more passwords and are able to crack password hashes faster as technology advances.

Why Cybercriminals Prefer to Use Password Cracking Dictionaries

This is where cracking dictionaries can offer a benefit. Bad actors can use entire databases of pre-cracked passwords, common passwords, leaked passwords, and standard dictionary words to try and hack into an account, without the time and complexity of a social engineering attack. This type of attack is quick, so the victim often won't know of the unauthorized access until it's already too late.

Over the years, cybercriminals have developed a good understanding of what a typical password looks like, and they conduct their attacks based on this information. With a cracking dictionary, attackers apply the list of cracked passwords against a system and try to gain access.

- This is called a dictionary attack, which is a form of a brute force attack. A dictionary attack is where the attacker, instead of trying all possible combinations, tries password from a dictionary file. The file will have some of the most commonly used passwords and iterations to those passwords since so many people use similar passwords to their old passwords.

But these dictionaries can also be useful for standard brute force attacks and password spraying attacks.

- A dictionary can make a typical brute force attack easier. In a brute force attack, an attacker tries to attempt all possible combinations of a password to gain access to an account. It makes brute force attacks easier because it reduces the number of possible combinations. It also can increase the success ratio by using commonly used password combinations.

- A dictionary can also make a password spraying attack easier. Password spraying is an attack that attempts to access a large number of accounts with usernames and pairs them against a few commonly used passwords. With a dictionary, it is possible for attackers to identity the most common passwords and attempt to use those passwords in a password spraying attack.

How Ethical Hackers Use Password Cracking Dictionaries

However, it's not just hackers who use cracking dictionaries, legitimate security professionals do as well. Ethical hackers can also use this data to break hashing algorithms and conduct controlled data breaches to demonstrate how insecure a system is. This often happens in a professional setting, but there are also hash cracking websites available online where you can put in a hashed version of a password, and it will crack it, telling you the password.

> *Example password: Chocolate1*
> *Hash in SHA1:*
> *2285F929D38932996BD99687EB BD732EA3B18AED*

Putting this hash into the website CrackStation, it returned the password almost instantly.

These websites use huge dictionaries of hashed data, some of this data is hashed common passwords, some is dictionary words, some is entire Wikipedia articles, and so on. For the SHA1 and MD5 hashes alone, CrackStation has a lookup table with 15 billion entries.

How Data Breaches Make the Problem Worse

According to Forbes, just the first half of 2019 saw 3,800 publicly disclosed data breaches, amounting to 4.1 billion exposed records. What makes these figures even more alarming is that the number of breaches in 2019 increased by 54% compared to the previous year. The problem is, with each additional breach, more valuable data goes into the hands of these bad actors.

When a large company has their login credentials stolen, cybercriminals now have a huge set of data that provides them insights, such as which passwords are the most popular, for example, which sports team names become common passwords in that area, and so on. These passwords get added to dictionaries. This data is still extremely valuable even when the password has been hashed.

Password hashing has long been considered a secure way of storing passwords. Hashing involves taking the native password, for example, "Yellow3", and converting it into a string of numbers and letters of a fixed length. Hashing algorithms are designed to be difficult to crack and difficult to reverse engineer. All hashing algorithms are deterministic, which means if you input the same value, you'll always get the same hashed output. However, they are also designed so that changing a single character the resulting hash will look completely different. This element of their design makes them considerably more difficult to reverse engineer, but the only thing standing in an attacker's way is a large set of data and a powerful computer.

This is largely why data breaches are becoming so prevalent and increasing each year. Powerful computers and computer components are becoming increasingly affordable and as more hashed passwords are exposed, hackers get better at reverse-engineering these passwords. When quantum computing becomes more mainstream, it will become even easier to reverse engineer hashes.

How Can Organizations Secure Passwords and Make Passwords Harder to Crack?

One way to protect your password is to make it more difficult to crack.

- Passwords should always be stored in strong password hashing algorithms and they should be salted.
- Longer passwords help significantly because the longer the password, the more computational time and energy it takes to crack a password.
- Weak passwords are easily discovered by hackers so should be completely avoided. A password will be considered weak if it is a word picked out of a dictionary or a common pattern on a keyboard, such as "Qwerty123". These passwords are risky because you can almost guarantee that a hacker will already know of that password and have it listed in a table. This is true even if a password is hashed.
- If your users use common words and common leetspeak substitutions, then organizations should assume that the hashed form of those passwords have been cracked. It's the desire for an easy to remember password and the illusion of it being unique that drives so many people to choose weak passwords.

A strong password policy can help organizations create harder-to-crack passwords. There are many different policies and recommendations around what makes a strong and safe password, but here are some common features of a strong organizational password policy:

- Do not allow users to reuse compromised or exposed passwords.
- Require 16+ characters in a password. The longer the password the difficult and time-consuming it is to crack.
- Most security professionals recommend using a 4-word passphrase because it is easy to remember and long (such as: OceanTogetherHappyFace)
- Recommend to your users that they should not use ties to their personal information in their password.
- Do not allow users to use context-specific passwords, such as the company or product name.
- Prevent users from selecting common passwords.
- Enforce password similarity blocking. Block passwords that are too similar to old passwords- these are very easy for attackers to guess.
- Adding a 'salt' to your password hash. A salt is a random string of numbers added to a password to make it more unique and give it a different hash.
- When possible, implement MFA but make sure that if the MFA includes a password factor, that the password is secure with the above items.

Lastly, password monitoring can help organizations determine whether you have a strong password or not. Password screening software will scan your password and compare it to known common passwords, or passwords that have been exposed previously. If password monitoring tools indicate that a password has been exposed in a previous data breach, is a known password, or appears on password blacklists; then you should assume that hackers will try that password and have potentially already cracked the hash for it.