Cybercrime Prevention Flyer

CPF 0027-2022-CID361-9H 15 September 2022

Brute Force Password Attacks

Brute force password attacks describe a category of cyberattacks that uses trial and error to gain access to a resource. In a digital context, the resource is usually a user account and the attack vector is a combination of usernames and passwords (i.e., credentials) that unlock the resource.

Although there are several types of brute force attacks, the common thread and easily addressed vulnerability is weak passwords.

The simplest brute force attack is when someone makes educated guesses at a valid password. That might be a child's name, a street address, a school name, or something familiar to a person because it is easily remembered. For anyone who is even minimally active on social media, that personal information is very likely readily available. To defend against this simple attack, do not use personal information when setting passwords.

Another type of brute force attack is a dictionary attack, which tests a predefined list of words against a single account until one is found that unlocks it. To defend against a dictionary attack, do not use common words found in a dictionary. That could mean swapping some letters for other characters. Instead of *Circadian,* try *Cir_c*dian* or *$ircadian_*. As an alternative, try fabricated words like *$n0rdGl0p*.

A credential stuffing attack occurs when illegally obtained but valid credentials are tested against many different web resources until one of them is unlocked. Credential stuffing works because people use identical credentials on multiple websites. To defend against credential stuffing, do not reuse login information; use unique username and password combinations for each site.

Password spraying is a brute force attack that tests a few common passwords against many different usernames (e.g., *123456*, *qwerty*, and *password* are, according to a 2022 study, among the most commonly used passwords). To defend against a password spraying attack, avoid the temptation to use simple, predictable passwords.

Brute Force Attack Defense

- Where available, use passphrases rather than passwords.
- Use two-factor authentication whenever possible.
- Use longer passwords, strive for 12 character passwords or longer.
- Use a combination of uppercase and lowercase characters, numbers, and symbols.
- Do not use words that can be found in a dictionary.
- Do not use personal identifiers regardless of how closely held they might be.

Report a crime to U.S. Army Criminal Investigation Division

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

Additional Resources:

Password Complexity Checker

25+ Password Statistics

Strong Passwords for Greater Protection

Password Spraying 101

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF