What is a credential stuffing attack?

Credential stuffing typically refers to specifically using known (breached) username / password pairs against other websites.

Credential stuffing is the automated or manual injection of stolen username and password pairs ("credentials") into website login forms, in order to fraudulently gain access to user accounts.

Since many consumers will re-use the same password and username/email across multiple online accounts or services, when those credentials are exposed (by a database breach or phishing attack, for example) submitting those sets of stolen credentials into dozens or hundreds of other sites can allow an attacker to compromise those accounts too.

Credential stuffing is a subset of the brute force attack category. A brute force attack will attempt to try multiple passwords against one or multiple accounts; guessing a password, in other words.

Connect webhooks can be found on Mastercard Developers.

Solution

If an attack is underway:

- Remove accounts associated to the attacker.
- Detect and block accounts created with fake email addresses.
- Detect and block IP addresses of the bad actors creating the accounts.

Send all questions to AskOBSecurity@mastercard.com

1. Always subscribe to Connect webhooks including "added", "discovered" and "invalidCredentials" and the SDK. This will help identify bad actors utilizing your platform for credential stuffing attacks.
2. Reduce the number of financial sub accounts to 8 or less.
3. Block temporary emails during sign up if possible.
4. Implement an email validation routine that will block bad actors using email addresses that majorly involved in attack.
5. Prevent registrations and login from well-known hacking sources such as Russia, Ukraine and North Korea and for best practice geo block all countries your business does not currently serve.
6. Monitor for more than 2x accounts linked to the same FI (i.e., 12 accounts tied to Financial Institution X).