Attack Path: Account Takeover

About

Name:

Demographics:

- Age:
- Gender:
- Location:
- Occupation:
- Language:

Goals

Needs and Wants:

- Access to valuable accounts, attention

Motivation:

- Financial gain, internet clout

Frustrations:

- Quick response by the platform, security measures

Technology Used:

- Devices: High-quality computer
- Apps and Platforms: Telegram- to advertise verified accounts, dark web forums- purchase batches from information stealers

Skills and Tools:

- Level of Sophistication: Intermediate
- Tools: Account checking software, brute forcing tools

Attack Traits:

- Methodologies/Signals:
    - Account API to check accounts

        - Increased platform traffic
        - API calls
        - Likely bot activity
- Indicators
        - Multiple login attempts
        - Multiple devices/unknown devices
        - Multiple IP addresses/countries of log in
        - Customer reports
        - Irregular user behavior

Attack Path

Step 1: Reconnaissance

- Dark web forums
- Public-facing endpoints

Step 2: Initial Access

- Account API to check accounts/credential stuffing
- Password spraying

Step 3: Execution

- Publish “verified” accounts quickly

Step 4: Persistence

- Password change
- Working at scale to race user/platform mitigation

Step 5: Evasion

- tbd

Step 6: Impact

- Potential revenue loss
- Data security Legal/compliance implications
- Infrastructure/resource costs
- Reputational damage