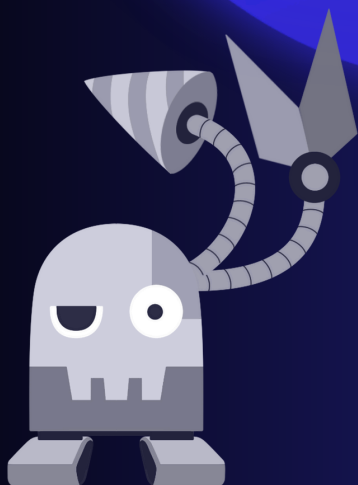


KNOW YOUR BOTS!

STORMBIRD



SCRAPER BOTS

Mimic legitimate users to collect data via slow, low-volume GET requests.

Use rotating IPs/UAs.

- Data theft, competitive espionage, fake clones

SNEAKER/BUYING BOTS

Target high-demand product drops using automated browsers or APIs. Operate from residential IPs and mimic headers.

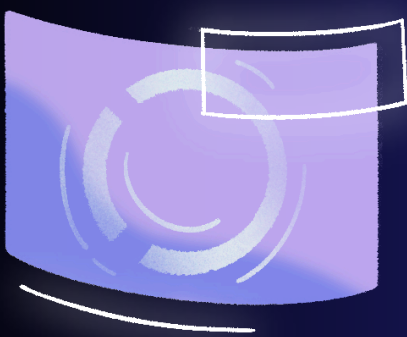
- Inventory hoarding, revenue loss, black-market resale



CREDENTIAL STUFFERS

Automate login attempts with leaked username/password pairs from breaches. No browsing; just API logins.

- Failed login spikes, account lockouts, detection evasion



ACCOUNT TAKEOVER (ATO)

Attempt to gain control of specific accounts via credential stuffing, phishing-replayed sessions, or reset flows.

- Fraud, data breaches, unauthorized purchases

DDOS ATTACKERS

Overload the website with bursts of requests either from single IPs or coordinated botnets across networks.

- Service disruption, performance degradation

