Stop Malicious Bots!
Detect & Prevent Automated Attacks

Web App Attack Trends in 2019

- 60% of 2018 breaches occurred via web apps
- 20% of traffic to web apps originate from malicious bots

Most common approaches to cyber attacks:
- stolen credentials
- brute force attacks
- web app attacks
- automated

Malicious Automation Key Facts

Top Targets
- Healthcare institutions that store PII
- Retail, hospitality, and financial services organizations with credit card/bank information
- Social media and review sites where public opinion can be swayed

Characteristics
- Operate at the App Layer
- Abuse App Functionality Intended for Valid Users
- Coordinate Large Numbers of Attacking Nodes from Different IPs
- Often Invisible to Traditional WAFs

Top 4 Malicious Automations

1. Distributed Password Attack
   - What: Bots attempt to break into an account by running a series of username and password combinations. Detection is often avoided through use of various hosts and points of presence.
   - Why: To access high-value information, such as personal information (PII).

2. Credential Stuffing
   - What: Password combinations, typically acquired from a previous data breach, are plugged into registration or sign-in forms until a valid credential is found.
   - Why: To break into a targeted website, identify valid credentials to sell, steal or use to make a purchase.

3. Fake Account Creation
   - What: Automated generation of numerous fake accounts that appear to be legitimate.
   - Why: Tying up retail inventory in online shopping carts or voting fraud, for example.

4. Carding
   - What: Hackers use credit card numbers or gift card IDs acquired on the dark web to attempt automated and fraudulent purchases across numerous sites. Purchases are small and often go unnoticed.
   - Why: To validate the credit card and gift card IDs and resell the information back on the dark web.

Best Practices for Blocking Malicious Bots

- Add MFA to admin and customer interfaces.
- Automatically detect abnormal login failures.
- Monitor aggregate login behavior for all apps.
- Add behavioral profiling to important workflows.
- Add anonymizers as a risk factor when analyzing connections.

Annual spend on bot management personnel: $177K
Average # of minutes to detect a bot: 2,880