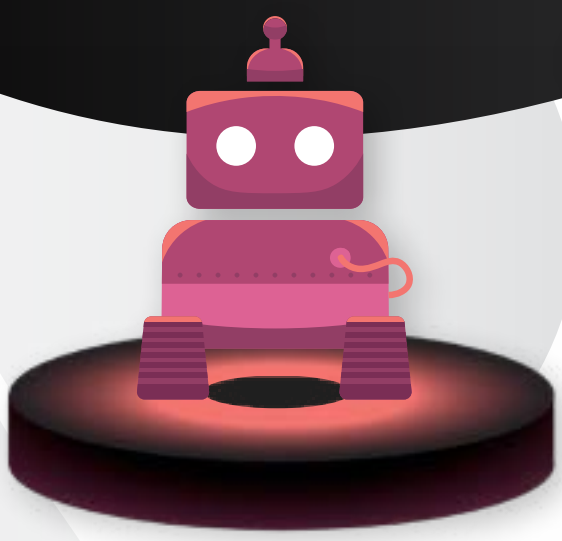
THE EVOLUTION OF **FRAUD BOTS**

neuroID
A part of experian

Fraud bots started as simple scripts designed to execute basic tasks, but have come a long way since. Today's bots leverage generative AI and machine learning to mimic humans—and traditional bot detection systems can no longer stop them.

How did bots get so powerful, so quickly? And where do fraud prevention tools go from here?



FIRST-GENERATION BOTS

The Most Basic Bots

First-gen bots execute simple, basic scripting that make cURL-like requests to websites using a limited number of IP addresses.

Evolved Capabilities

Scraping, carding, and form spam

Detecting First-Generation Bots

IP Blocklisting and user-agent analysis can quickly block first-gen bots. First-gen bots can't store cookies,execute JavaScript, or imitate human behavior, making them easy to detect with behavioral analytics and other tools.

SECOND-GENERATION BOTS

Key Evolutionary Traits

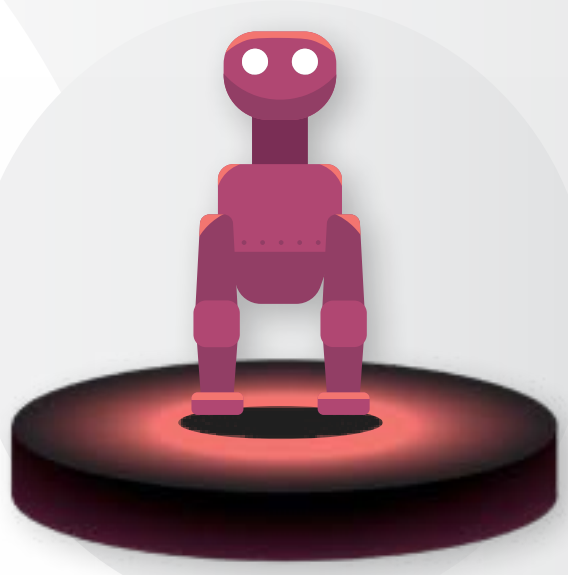
Second-gen bots built on first-gen bots' strengths and eliminated some of their weaknesses. They use headless browsers and can maintain cookies and execute JavaScript, making them more capable than Gen 1.

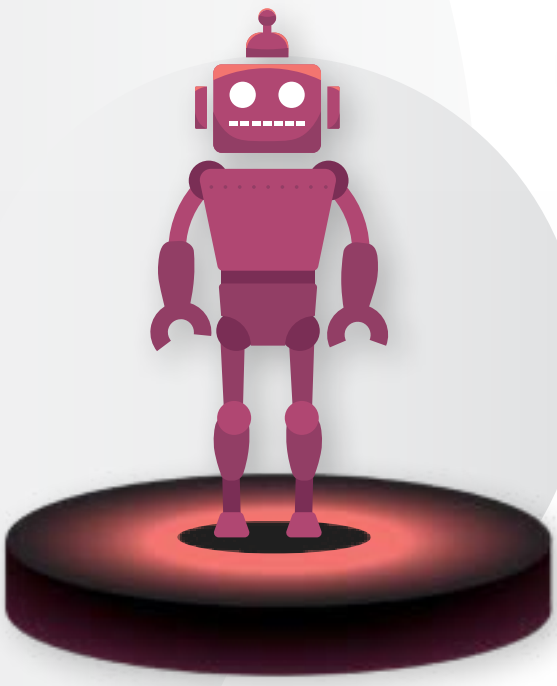
Evolved Capabilities

Application DDoS attacks, scraping, form spam, skewed analytics, and ad fraud

Detecting Second-Generation Bots

Headless browsers and sub-second data entry and field transition speeds are dead giveaways of second-gen bots; they're easy to detect through behavioral patterns and browser and device characteristics analysis.





THIRD-GENERATION BOTS

Key Evolutionary Traits

Third-gen bots operate through full-fledged browsers and simulate basic human interactions, such as mouse movements and keystrokes. Their entry and transition speeds are also slower, better replicating human behavior.

Evolved Capabilities

Account takeover, application DDoS, API abuse, carding, and ad fraud

Detecting Third-Generation Bots

Third-gen bots can bypass many of the device and network signals and clear-cut behavioral patterns that revealed their predecessors, but still lack human-like randomness. They can be detected through behavioral analysis that can identify programmatic sequences in their actions.

FOURTH-GENERATION BOTS

Key Evolutionary Traits

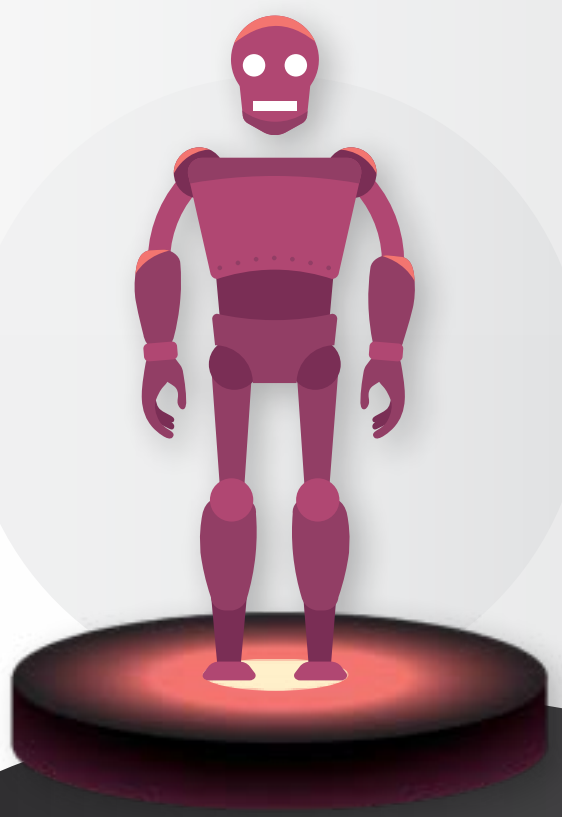
Fourth-Generation Bots exhibit advanced human-like interactions, such as random mouse movements and changing user agents while rotating through thousands of IP addresses. These bots often employ "behavior hijacking," recording and replicating real user interactions to closely mimic human behavior.

Capabilities

Account takeover, application DDoS, API abuse, carding, and ad fraud

Detecting Fourth-Generation Bots

Because of their ability to precisely mimic human behavior, fourth-gen bots require more sophisticated detection systems. Machine learning-based technologies, such as intent-based deep behavioral analysis (IDBA), are crucial to blocking gen-4 bots.



New bots are continuing to evolve, but previous versions aren't going away anytime soon. What does next-gen bot detection look like if the bots are beating every vendor in your stack?

Read *Fighting the Future of Fraud: Understanding and Combating Next-Gen Bots* for a best-practices breakdown and case study snapshots.