imperva

Bad Bot Classification

Simple

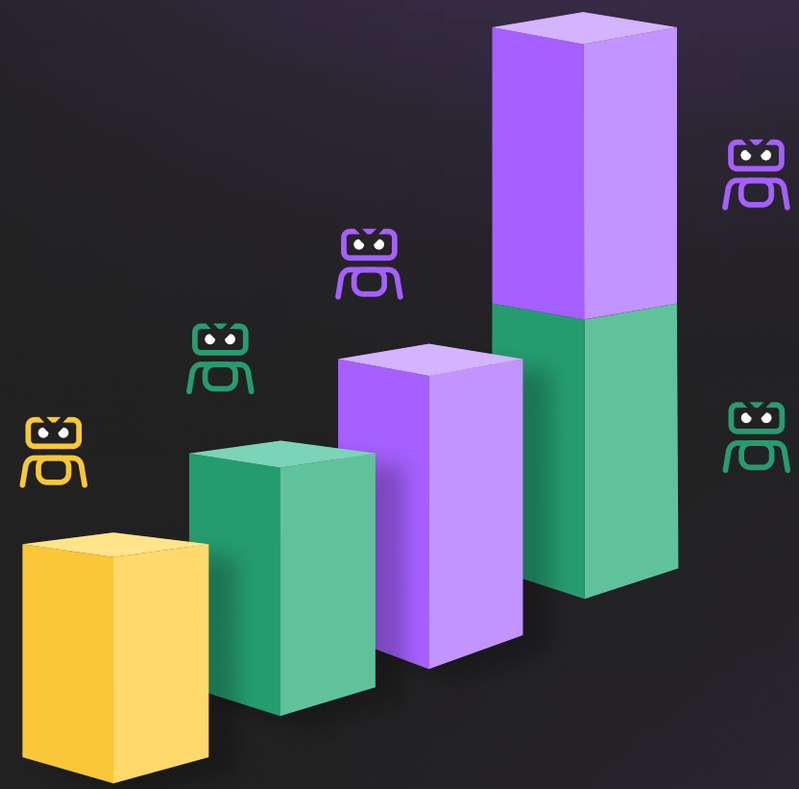
Connecting from a single, ISP-assigned IP address, this bot connects to sites using automated scripts. This bot doesn't self-report as a browser.

Moderate

This more complex bot uses "headless browser" software that simulates browser technology, including the ability to execute JavaScript.

Sophisticated

Emulating human user behavior like mouse movements and clicks to spoof bot detection. They use browser automation software, or malware installed within real browsers, to connect to sites.



Evasive Bad Bots

Technological advancements in bad bot evasion techniques in recent years have further thinned the line between moderate and advanced bad bots. For this reason, we are offering another perspective on bad bot traffic analysis by grouping both Moderate and Advanced bots together. As their name suggests, Evasive bots use the latest evasion techniques, including cycling through random IPs, entering through anonymous proxies, changing their identities, mimicking human behavior, delaying requests, defeating CAPTCHA challenges, and more. They use a mix of sophisticated technologies and tactics to evade detection while maintaining persistence on target sites. They often choose a "low and slow" approach, which enables them to carry out significant attacks using fewer requests and even delay requests, allowing them to not stand out from the normal traffic patterns and avoid triggering rate-based security detection thresholds. This method reduces the "noise," or big traffic spikes generated by many bad bot campaigns.