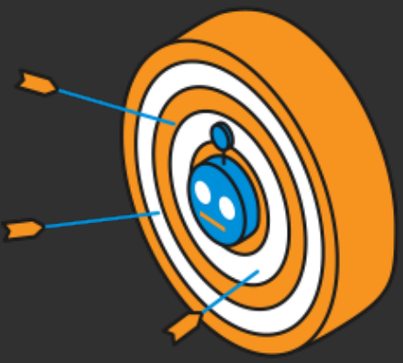
kasada

AUTOMATED THREATS ARE A MOVING TARGET

Bot builders have evolved their methods considerably over recent years to conduct automated attacks and generate significant profits.

As a result, effectively stopping modern advanced persistent bots is a moving target that requires new bot detection and mitigation techniques that don't rely on IP addresses, behavioral analytics, device fingerprinting, CAPTCHAs, poorly protected JavaScript code, or other antiquated methods.



PROXY NETWORKS

Adversaries use residential proxy networks, such as Luminati (now Bright Data), to look like legitimate users when applying their scripts to conduct automated attacks.

TESTING FRAMEWORKS

Open-source web testing tools including Puppeteer, Playwright and Selenium are used to automate scripts to look and act like humans.

STEALTH PLUGINS

Stealth plugins add clever techniques to make attacks less likely to be detected, leveraging new evasion methods discovered by the community including CAPTCHA bypass/ defeat.

DIGITAL HARVESTING

Legitimate digital fingerprints are stolen or purchased containing real cookies and browser sessions and are imported into anti-detect browsers to evade device fingerprinting techniques.

REVERSE ENGINEERING

Bot builders exploit weak obfuscation methods such as those leveraging tools like obfuscator.io, to decipher bot detection sensors that reside within client-side JavaScript.