Automated Threats From Login to Checkout

kasada

1 Login

Credential stuffing allows adversaries to take over customer accounts to sell them or commit fraud and fake account creation is used to exploit promotions.

2 Browsing

Motivated attackers or competitors scrape product data for arbitrage, steal assets to commit fraud, check inventory, or find pricing errors.

A **SNIPING** - Freebie bots monitor your site in search of price errors so they can quickly scoop up free or incorrectly discounted items.

B **SPOOFING** - Bots scrape your site to create an identical site with a spoofed domain to deceptively sell counterfeit goods and damage your brand reputation.

C **PRICE SCRAPING** - Competitors scan prices to undercut your business and steal catalog content you've created and paid for.

D **SCANNING** - Scanner bots check to see if your in-demand goods have been restocked before a checkout bot is used to automate the process.

3 Add to cart

Denial of inventory allows adversaries to add massive quantities of stock to their cart for checkout, preventing customers from buying products.

4 Checkout

Adversaries use automation to abuse payment functions like carding and cracking attacks or commit checkout fraud.

A **CARDING** - Cybercriminals test large volumes of stolen cards (like credit cards and gift cards) to see if they're valid.

B **CRACKING** - Bad actors use bots to guess missing values for stolen payment data, like security codes and expiration dates, or to guess active gift cards and loyalty reward IDs.

C **CHECKOUT BOTS** - Used to secure products from hype and limited stock releases quickly at scale

About Kasada

Kasada has developed a radical approach to defeating automated cyberthreats based on its unmatched understanding of the human minds behind them. The Kasada platform overcomes the shortcomings of traditional bot management to provide immediate and enduring protection for web, mobile, and API channels. Its invisible, dynamic defenses provide a seamless user experience and eliminate the need for ineffective, annoying CAPTCHAs. Our team handles the bots so clients have freedom to focus on growing their businesses, not defending it. Kasada is based in New York and Sydney, with offices in Melbourne, Boston, San Francisco, and London.

For more information, please visit www.kasada.io and follow on Twitter, LinkedIn, and Facebook.