imperva

What are bad bots doing?

Account Takeover

What is it?

Account takeover (ATO) is a form of online fraud in which bad actors gain illegal access to user accounts belonging to someone else. A successful attack can cause extensive damage to customers and businesses alike. Many ATO attacks rely on capturing exposed legitimate login credentials, and then using automation to test them against login pages.

What is the outlook?

The prevalence and sophistication of ATO attacks is constantly rising. If your business has a login page, chances are it will be targeted by Credential Stuffing and Credential Cracking attacks at some point. And if there is money to be made by taking over user accounts on your site, the likelihood of an attack is even higher. With billions of stolen credentials available at a price, ATO is destined to continue to be a thorn in the side of every business.

What industries does it affect?

Any business with a login page.

Scalping

What is it?

Bad actors use bots to purchase sought-after products and services in bulk using scalable methods that are not available to ordinary users. Then, they resell the goods at a significant markup to make a profit. Examples: Ticket Bots, Sneaker Bots, and Grinchbots.

What is the outlook?

Scalpers took advantage of supply chain and chip shortages for gaming and electronics, and "online drops" for limited-edition items. Online ticket and appointment booking services are also targeted, from concerts to healthcare and college enrollment.

What industries does it affect?

Healthcare

Entertainment & Arts

Gaming & Gambling

Retail

Card Fraud

What is it?

Credit card fraud occurs when bad actors use bots to perform Carding and Card Cracking to steal credit card information and make transactions. Gift card fraud involves using automation to test cards and request balances, so that bad actors can steal gift card money anonymously and untraceably.

What is the outlook?

The rise of popularity in online shopping and the increase in the amount of retailers offering gift cards is leading to more card fraud than ever before. Nonprofits are also suffering from credit card fraud, with bots using the donation pages to test stolen credit card numbers.

What industries does it affect?

Airlines & Travel

Event Ticketing

Gaming & Gambling

Non-profits

Financial Services

Web Scraping

What is it?

Bots scrape content, data, and pricing from websites in order to undercut prices and steal copyrighted content.

What is the outlook?

We predict that bad actors will persist in using scraper bots that inspect competing business databases to access pricing information. They will also use bots to scrape content to obtain product information for use in spam and email fraud.

What industries does it affect?

E-Commerce

Job Boards

Gaming & Gambling

Classifieds

Ticketing

Financial Services

Misinformation Campaigns

What is it?

Malicious actors use bad bots to post comment spam on social media, leading to the propagation of unfounded conspiracy theories and fraud related to a wide range of topics.

What is the outlook?

Social media bots are being used to spread fake news messages with links that lead to phishing attacks. The WHO has dubbed the spreading of misinformation the "infodemic." We see no sign that nation-state funders of bad bot activity will stop misinformation campaigning any time soon.

What industries does it affect?

Healthcare

Education

News

Government

Society

What is the solution?

Imperva offers a best-in-class Advanced Bot Protection solution, capable of mitigating the most sophisticated bad bots, including every OWASP automated threat. It leverages superior technology to protect all potential access points including websites, mobile applications and APIs, all without affecting the flow of business-critical traffic.

Advanced Bot Protection

Contact us now to schedule a demo or begin a free trial.

imperva.com