perimeterx | Infographic

E-COMMERCE EDITION

2022 Automated Fraud Benchmark Report

The Automated Fraud Benchmark Report is an annual survey that explores the web app traffic and threat patterns experienced by some of the largest and most respected brands in retail e-commerce. The anonymized data was taken from the online interactions of millions of consumers and hundreds of millions of bots.

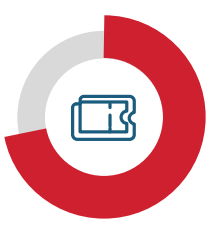
Bot Attacks Increased YoY

106.21%
YoY increase in **bad bot attacks**

111.61%
YoY increase in **carding attacks**

240%
YoY increase in **scraping attacks**

93.84%
Peak **malicious login attempts** in 2021 — an increase from the 2020 peak of 84.71%



71.61%
Scalping bot attacks during hype sales events in 2021 — an increase from the 2020 peak of 46.87%

Get the 2022 Automated Fraud Benchmark Report to see more bot attack trends!

Top Attack Types

PerimeterX tracked the most critical automated fraud attack types for this report including:

Account Takeover
Gaining unauthorized access to consumer accounts

Carding
Testing stolen credit and debit card data to make fraudulent purchases online

Credential Stuffing
Automated fraudulent login attempts to access user accounts

Gift Card Cracking
Carding attacks where bots enumerate gift card numbers to find valid combinations

Denial of Inventory and Scalping
Automated shopping bots repeatedly purchase in-demand items for later resale

Web Scraping
Automated bots harvest price, inventory and product images and descriptions without authorization

Top 3 Takeaways

E-commerce accounts are treasure troves of value, making them a rich target for bot attacks.

The pandemic is continuing to drive bot attacks, including credential stuffing, account takeover (ATO), carding, scalping and web scraping.

E-commerce brands must disrupt the web attack lifecycle to protect against ongoing and future bot attacks.

Read the blog for more detailed takeaways from the 2022 Automated Fraud Benchmark Report

6 Steps To Web Application Security

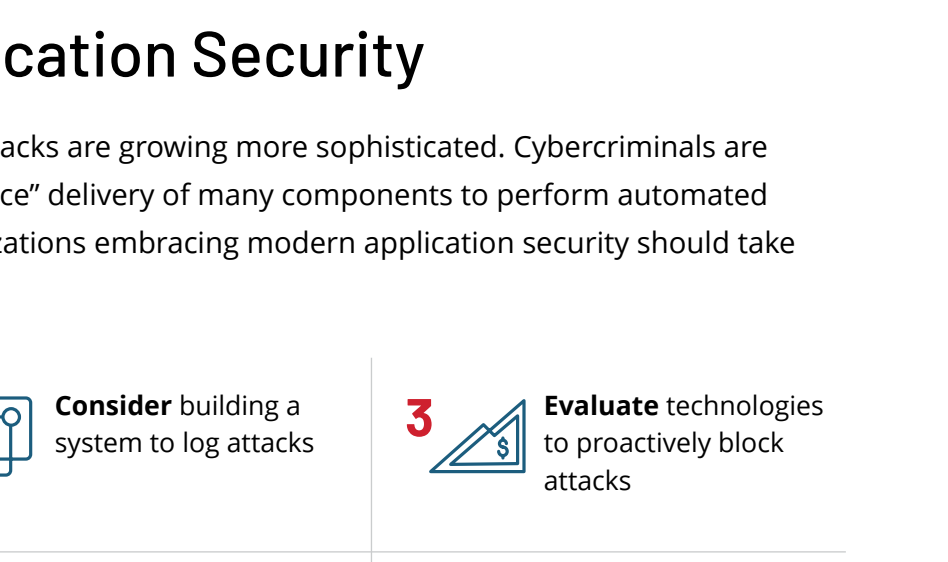
In an ever-changing security landscape, attacks are growing more sophisticated. Cybercriminals are leveraging specialized tools and "as-a-Service" delivery of many components to perform automated attacks. To keep pace, e-commerce organizations embracing modern application security should take the following steps:

1. **Assess** potential risks and audit exposures
2. **Consider** building a system to log attacks
3. **Evaluate** technologies to proactively block attacks
4. **Analyze** impact of challenges on checkouts and abandonment
5. **Identify** product pages that are targeted and protect them from scraping bots
6. **Adopt modern solutions** that leverage machine learning to proactively identify and block automated attacks

"I found PX to be the ultimate vendor with [an] amazing support team, great vision, and an ever-growing hunger for success."

— Reference Customer from the Forrester Wave™: Bot Management, Q2 2022

PerimeterX Bot Defender identifies and blocks malicious bots with unparalleled accuracy. The solution leverages behavioral analysis, intelligent fingerprinting and predictive methods to detect bad bots and stop attacks. Bot Defender uses machine-learning technology that adapts in real time to stay ahead of today's increasingly sophisticated bots.



See Bot Defender in Action

BOOK A DEMO