Arkose Labs

Data Drain: Website Scraping by the Numbers

The evolution of generative AI (GenAI) has unleashed web scraping attacks. Once limited to a handful of industries, website scraping has expanded to new verticals. Social media companies experienced a QoQ double-digit increase in scraping attacks. Adversaries use bots to scrape data that is then used to fine-tune their AI models.

Discover other fresh findings on just how much this attack has grown with new data from Breaking (Bad) Bots: Bot Abuse Analysis and Other Fraud Benchmarks, Q4 2023.[1]

A SKYROCKETING ATTACK TYPE

Scraping is now the third most popular attack type, behind fake account creations and account takeovers in volume.

Top 5 Attack Types

Fake Account Creation
Attacks connected with initial registration for an online account

Account Takeover
Attacks associated with logging into an account, such as ATO and credential stuffing

Scraping
The scraping of data, content, and images for malicious purposes

Account Management
Attacks on customer support call centers, including password resets

In-Product Abuse
Abuse including inventory hoarding, loyalty point abuse, chat abuse, bogus gaming sessions, cheating services, and win-loss trading

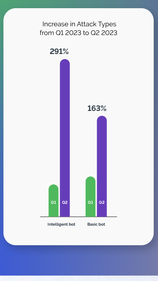
Web scraping shows no signs of slowing down. It was the fastest growing attack in the first half of 2023.

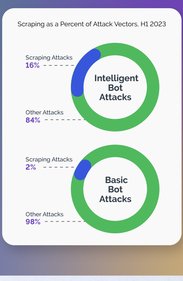
BOT-POWERED ASSAULTS

How do scraping attacks happen? The answer is straightforward: Bots give scraping attacks efficiency and effectiveness at scale. Not only do bots far outpace legitimate human traffic in overall volume, but they're responsible for virtually all scraping attacks.

100% of scraping attacks perpetrated by bots

Bots are also getting smarter. Intelligent bot attacks are increasing at a faster pace than basic bot attacks, and website scraping makes up a much higher proportion of intelligent bot attacks than it does basic bot attacks.





INDUSTRIES IN THE SPOTLIGHT: TRAVEL/HOSPITALITY AND SOCIAL MEDIA

Travel & Hospitality

Scraping has long plagued the travel and hospitality industry, where rivals harvest valuable information like inventory and pricing data to gain a competitive edge. In the third quarter of 2023, nearly 3 of 4 attacks in this sector were scraping attacks.

Social Media

A relatively recent target industry, bad actors have begun scraping social media sites en masse, using this treasure trove of information for malicious purposes like identity theft or social engineering schemes.

11% Rise in social media scraping attacks, Q2

3rd Biggest attack type on social media platforms is scraping

16% Of all attacks on social media are scraping

12% Of all social media traffic is malicious scraping

THREE NOTABLE SCRAPING TRENDS

Arkose Labs threat researchers have observed three important landscape changes.

Evolution
The progression from simple scrapers to ATO class infrastructure

Growth
An increasing number of commercial scraper services

Expansion
Developer groups scraping data for new purposes like training GenAI app

ARKOSE BOT MANAGER STOPS MALICIOUS SCRAPING

The Arkose Bot Manager platform provides the most effective protection against website scraping across all industries. Advanced risk profiling identifies suspicious sessions, while targeted enforcement challenges block automated and fraud farm-driven attacks at scale. In addition to consumable data signals for internal risk models and a global threat intelligence network, Arkose Labs offers unparalleled 24x7 SOC support and is backed by an industry - leading SLA.

Learn more about how Arkose Labs can protect your business from escalating bot attacks. Talk to an expert today.

[1]All data in this infographic is from the new Q4 Breaking (Bad) Bots analysis unless otherwise noted