Arkose Labs

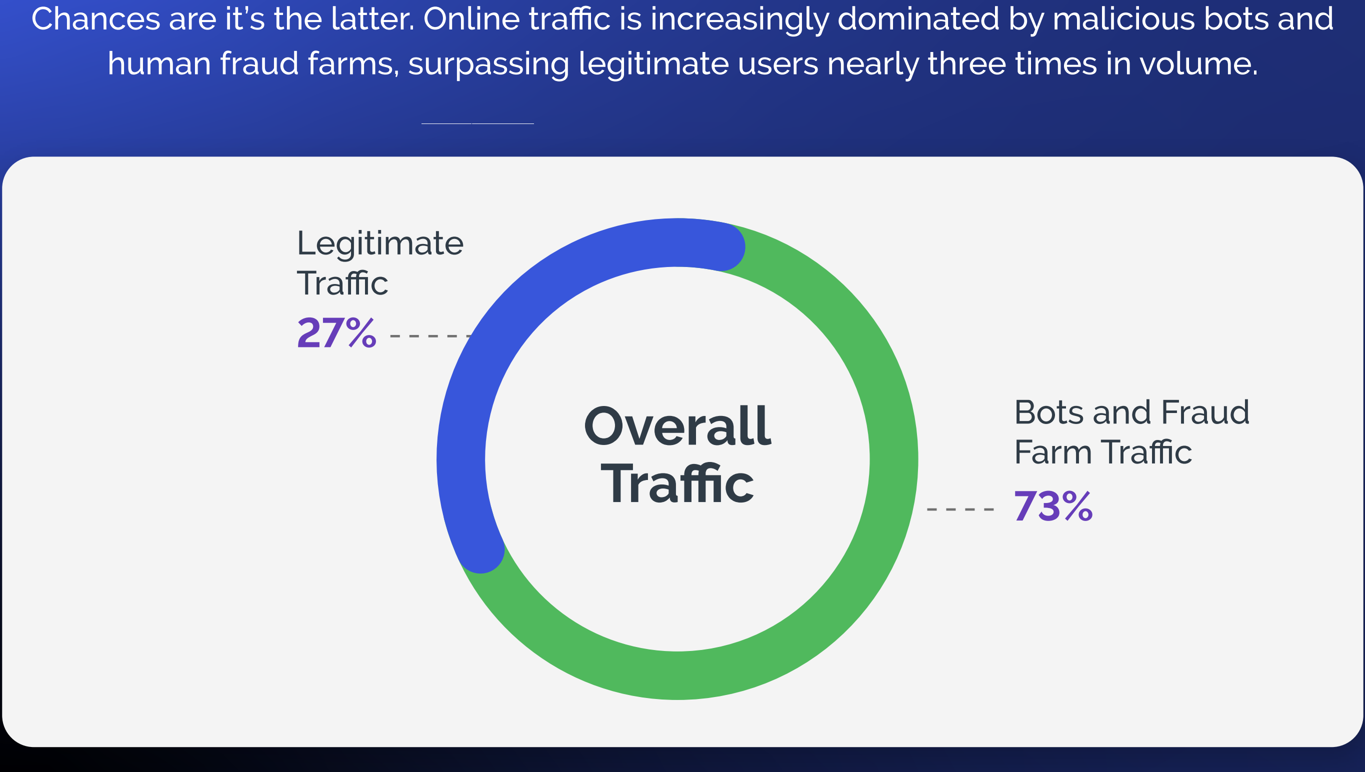
HIDDEN FIGURES: HOW BOTS AND HUMAN FRAUD FARMS ARE ATTACKING YOUR ENTERPRISE

Bot and human fraud farm attacks are way, way up. Across industries, across regions, and across attack vectors, the problem is escalating in unprecedented ways.

The new report Breaking (Bad) Bots: Bot Abuse Analysis and Other Fraud Benchmarks, Q4 2023 unveils the enormity of the threat.[1] Here's a dive into the numbers.

ONLINE TRAFFIC, UNMASKED

Is that a genuine consumer or a fraudster attempting to access your website or app? Chances are it's the latter. Online traffic is increasingly dominated by malicious bots and human fraud farms, surpassing legitimate users nearly three times in volume.



ATTACK ACCELERANTS: GENERATIVE AI (GENAI) AND CYBERCRIME-AS-A-SERVICE (CAAS)

Two key technologies are pouring fuel on the digital attack fire.

GenAI

Not only is GenAI used in content creation for items like pristine phishing emails, but it has unleashed **web scraping attacks.**

432%
Increase in web scraping attacks from Q1 to Q2

Top 3
Scraping is the third most deployed attack vector

100%
of scraping attacks are perpetrated by bots

CaaS

The growth of cybercrime-as-a-service, a vast network in which cybercriminals can easily purchase ready-made bots – sometimes even with how-to guides and tech support – has lowered the barrier of entry, because fraudsters now longer need coding skills to attack at voluminous scale. Enterprises will likely be facing off against more bot attacks in a time when many security teams are under-resourced.

$1.6B
Damages caused globally by CaaS each year[2]

Top 5
Information security risk in 2023[3]

38%
increase in cybercrime-as-a-service targeting business email[4]

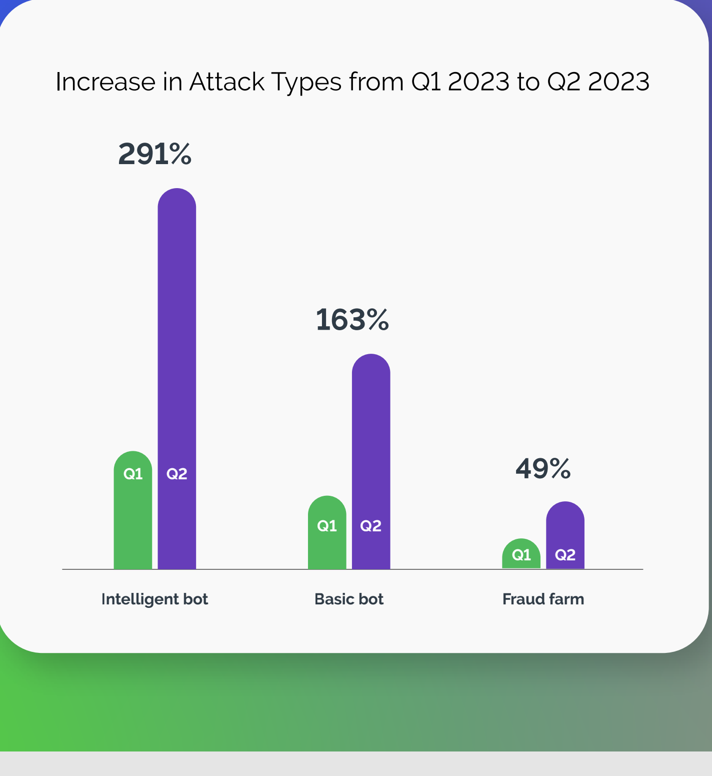
A MALICIOUS TRIO OF ATTACK VECTORS

Leveraging automation, speed, repetition, disguise, and scalability, three critical tools in the cybercriminals' arsenal are basic bots, intelligent bots, and human fraud farms.

Basic Bots
Limited bots that perform simple, repetitive tasks

Intelligent Bots
Bots capable of complex, context-aware interactions

Human Fraud Farms
Organized networks, powered by coerced labor or work-from-home employees in low-wage areas. They leverage solvers that often use automation



Intelligent bots are on the rise. From Q1 to Q2 2023, intelligent bot traffic far outpaced basic bots and heavily contributed to a total increase of approximately 167% for all bot attacks.

When bots can't make it past a company's defenses, attackers often turn to human fraud farms for tasks like solving traditional CAPTCHAs.

49%
Increase in human fraud farm attacks from Q1 to Q2 2023

30%
Of malicious traffic is from human solvers

26%
Increase in human fraud farm attacks from Q2 to Q3 2023

WHAT THEY DO IN THE SHADOWS

Cybercrime has become an economy unto itself, fueled by financially motivated bad actors building "dark" businesses and making lots of money. Here's how they carry out their crimes.

Top 5 Attack Types

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

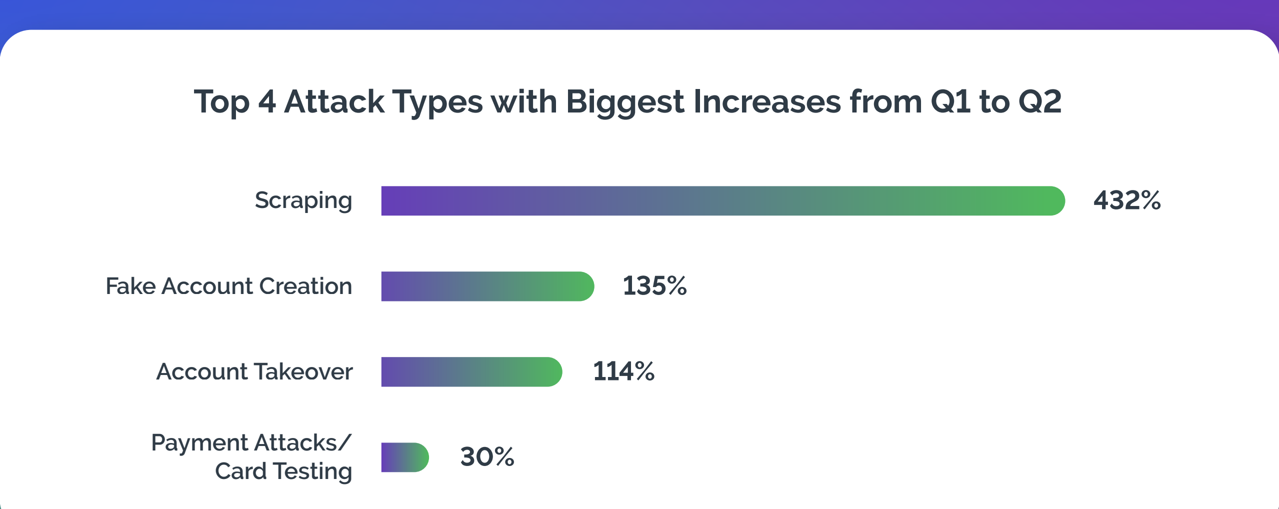
Account Takeover
Attacks associated with logging into an account, such as ATO and credential stuffing

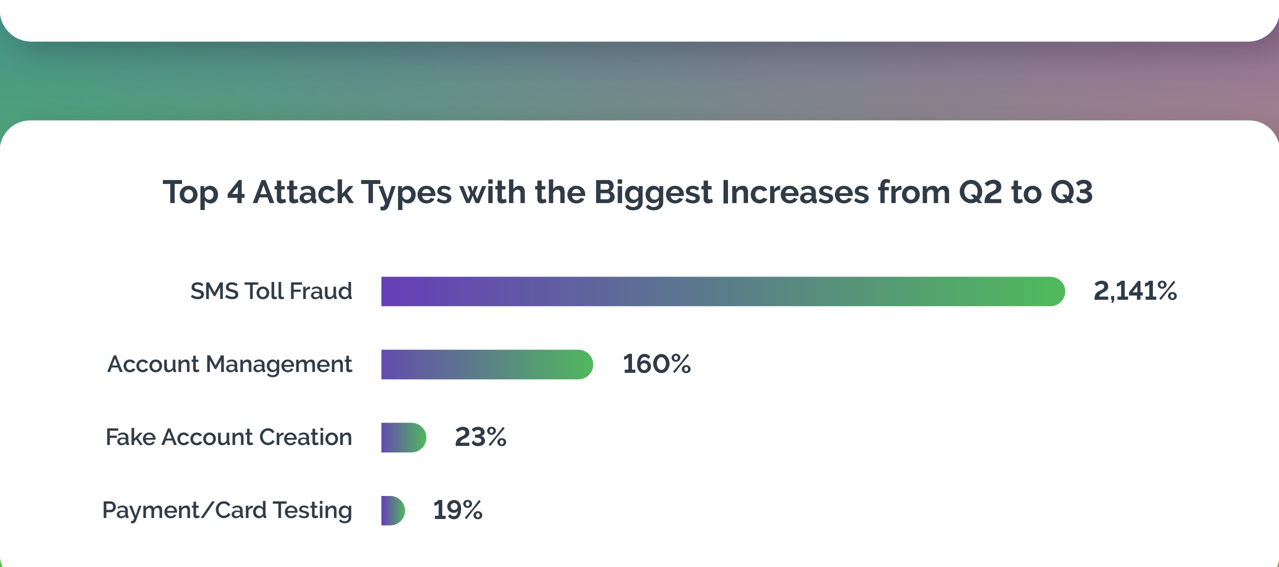
Scraping
The scraping of data, content, and images for malicious purposes

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

Attacks were up significantly almost across the board, rising steadily across the first three quarters of 2023. Most notable attack type increases, by quarter:





INDUSTRY BENCHMARKS

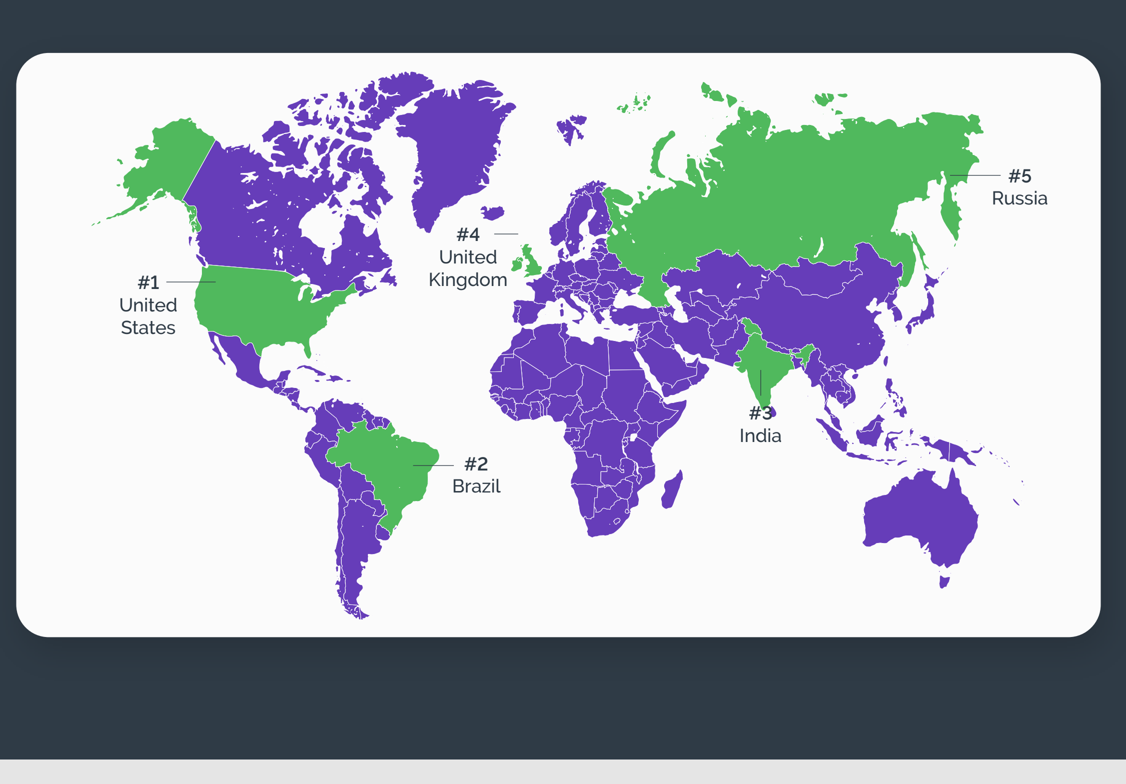
Bots and human fraud farms pose multifaceted threats across industries. In the first half of 2023, nearly every industry experienced an increase in the number of attacks.

Industry	Increase in Overall Attacks from Q1 to Q2	Increase in Bot Attacks from Q1 to Q2	Increase in Human Fraud Farm Attacks from Q1 to Q2
Travel and Hospitality	1270%	1515%	310%
Streaming	316%	334%	57%
Financial Services	159%	156%	355%
Technology	133%	152%	60%
Social Media	109%	216%	16%
Video Gaming	96%	152%	60%
Retail and E-commerce	44%	72%	2%
Gift Card	-36%	-48%	47%

CYBERATTACKS AROUND THE WORLD

Cybercriminals are hiding their points of origin, complicating companies' efforts to implement geographic-based control strategies. But security pros need to know the geographies being used in these campaigns so they can fine-tune their defense strategies.

All Attacks: Top 5 Countries of Apparent Origination



ARKOSE BOT MANAGER HELPS YOU BEAT THE BOTS

The Arkose Bot Manager platform provides the most effective protection against large-scale fake account registrations. 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.

Want to know more about which attacks are escalating the fastest, what industries are the most vulnerable, and how new technologies are reshaping the attack landscape? Download the full report today.

[1] All data in this infographic is from the new Q4 Breaking (Bad) Bots analysis unless otherwise noted
[2] Cybercrime annual revenue is 3 times bigger than Walmart's
[3] Unmasking Cybercrime-as-a-Service: The Dark Side of Digital Convenience
[4] Microsoft Cyber Signals report highlights spike in cybercriminal activity around business email compromise