Arkose Labs | SOLUTION BRIEF

Breaking (Bad) Bots: Bot Abuse Analysis in Australia

Q3 2023 Insights, benchmarks, and strategies

Kevin Gosschalk, Founder and CEO, Arkose Labs

State of the Attack: Today's Global Threat Landscape

- Cybercrime economy will reach $10.5 trillion by 2025 making it as big as the world's 3rd largest economy*
- A fast crime is getting faster
- Seen as a "Grinch bots" problem – but the reality is much more serious

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 ork-from-home employees in low-wage areas. They leverage solvers that often use automation

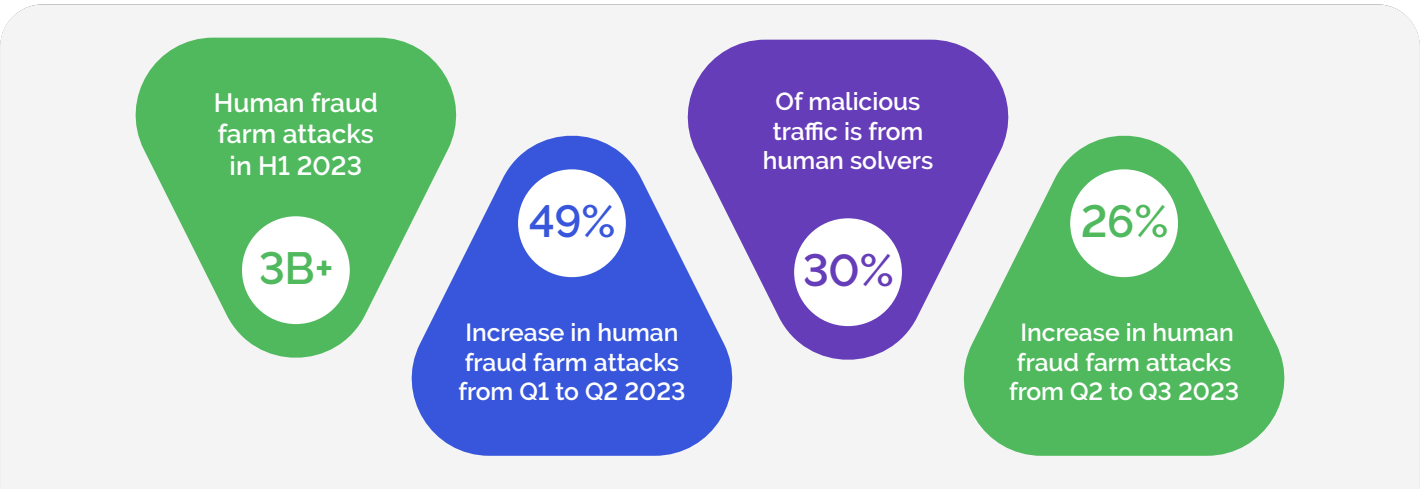
Australian financial services companies are under attack by scammers using bots

94% of attacks on Australian financial services companies were credential stuffing attacks.

- Followed by:
- Account Management attacks (5%) (i.e. password resets, etc)
- Fake account creations (1%) (i.e. phony account set-ups)

*Assessment period: Q3 2023

Australian financial services companies face-off against bots and human fraud farms in Q3 2023



The majority of which tend to be Basic bots, which are easily purchased from the "dark web."

Scammers buy consumers' usernames and passwords to online accounts off the dark web; break-in to drain consumers' accounts of all of their money.

Trend 2: CaaS puts Consumers at Greater Risk

Cybercrime-as-a-Service (CaaS) provides scammers ready-made bots they can just buy right off the dark web market. In addition to selling bots, the developers sell scammers training sessions on how to use the bots to attack and which companies to target. They also provide scammers customer support in case they have questions about the bots they just bought. CaaS makes it easier for scammers with limited technical skills to use fully automated bots at scale that cause widespread damage to enterprises and consumers.

Trend 1: GenAI: A Universal Ingredient

- Used for content generation on a massive scale
- Used scraped data to tune Generative AI models
- Lowered the barrier to entry for adversaries

The mission of Arkose Labs is to create an online environment where all consumers are protected from online spam and abuse. Recognized by G2 as the 2023 Leader in Bot Detection and Mitigation, with the highest score in customer satisfaction and largest market presence four quarters running, Arkose Labs offers the world's first $1M warranties for credential stuffing and SMS toll fraud. With 20% of our customers being Fortune 500 companies, our AI-powered platform combines powerful risk assessments with dynamic threat response to undermine the strategy of attack, all while improving good user throughput. Headquartered in San Mateo, CA, with offices in Argentina, Australia, Costa Rica, India, and the U.K., India, Arkose Labs protects enterprises from cybercrime and abuse. For more about Arkose Labs, follow the company on LinkedIn.

Email:
demo@arkoselabs.com

REQUEST A DEMO