New Research

Gaming Industry Threats Leveling Up: Fraud Farms and Bot Attacks Among Leading Dangers

Fresh threat intel and attack insights for gaming companies from across the Arkose Labs™ Global Network

December 2022

Arkose Labs

Summary

This timely report from across the Arkose Labs Global Network highlights and analyzes a trilogy of threats on the rise within the video game environment, presenting imminent dangers to gamers and the companies who serve them. This triumvirate of industry threats—perpetrated by fraudsters using automated basic bots, intelligent bots, and human fraud farms —strike with credential stuffing incursions, account takeovers, man-in-the-middle (MITM) phishing attacks, and fake account registrations during peak game play season (think college kids home for the holidays with lots of extra time to game!).

For example, just last week at the time of writing, we stopped a large volume attack—20 million fraudulent account creations—for one of our gaming customers. Such anecdotes demonstrate the heightened risk for account based attacks, in the gaming sector generally, and particularly at this time of year.

This report takes a closer look at locations on four continents —namely, Australia, Singapore, U.S., and U.K., — finding that they all represent hotbeds where online account-based attacks are taking place at sign-in and sign-up/ registration.

Gaming CISOs are under pressure to ensure their cybersecurity strategies improve productivity and produce a material ROI, as well as protect their systems and strengthen the online environment they create for gamers. The data presented throughout the report can be used to benchmark your company's performance and to inform your account security strategy.

Fraudsters developed basic bots to perform the most attacks in the U.S., Australia, and Singapore...but not so in the U.K.

For example, the U.S. represented the second highest percent of legitimate traffic at **84.9%**, following Australia (**86.8%**), but the U.S. has the second highest percentage of basic bot traffic with **13.6%***, behind Singapore's **17.2%***.

**As a percentage of a legit traffic*

Meanwhile, the U.K. has a higher percentage of intelligent bot traffic (**15.7%***) than other focus countries, and the highest amount of attacks overall, as a percentage of total traffic.

**As a percentage of a legit traffic*

Financially-motivated attackers target gaming companies because they are lucrative—small monetary amounts, but with massive volume. According to a survey conducted earlier this year, the average gamer spends around **$76** per month buying goods on gaming platforms, adding up to **$58,000** over a lifetime. It is estimated that in **2022**, more than **3** billion gamers exist around the world. Now consider that in the trailing **12** months we analyzed for this report, we stopped billions of account takeover attempts for gaming companies – you can see how the losses for gaming companies can amount to mind-blowing levels.

The holiday season is often when gaming companies make big announcements and/or release new game and console versions. For consumers, this time of year is busy, as gamers spend more time indoors; shop for the latest games and accessories for themselves or as gifts; and fill their downtime with countless hours of game play.

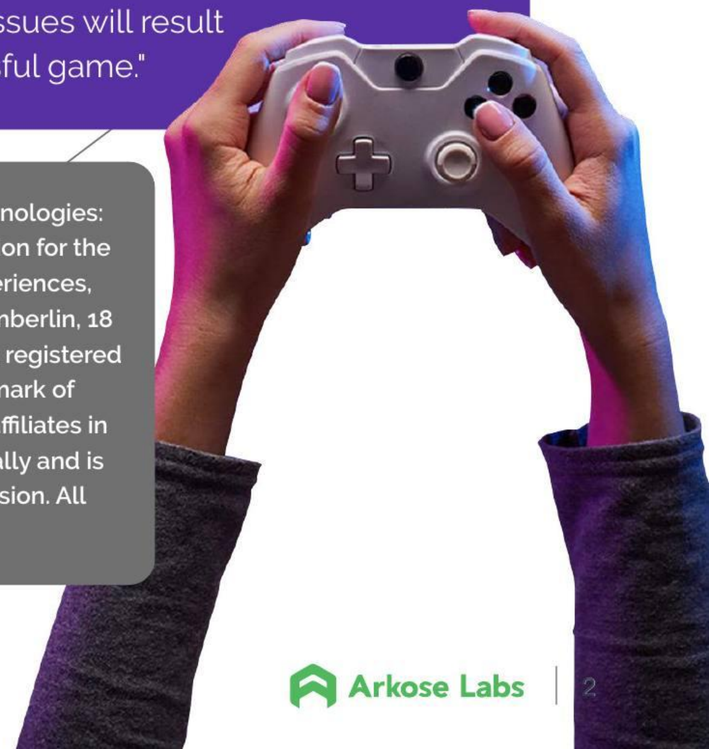
As active as gamers are during this time, so are adversaries. Online attacks don't stop, even for the holidays. As pioneers of the virtual world we increasingly inhabit as we work, shop, and transact online, gaming companies tend to be among the first to experience new sophisticated attack attempts and must adapt quickly to protect their platforms and safeguard their online consumer environments, because that's where much of their business value exists.

In this report, we will look at trailing **12** months attack trends from November **2021** to December **2022** that gaming companies are up against. These pose the greatest risk to gaming companies most important asset -- the consumer.

→ According to Gartner*:

"The video game industry at large is dedicated to the one specific value proposition: The experience of the end user is paramount. If games are not enjoyable due to design issues, poor user experience or technical flaws, the users will quickly say so. This kind of immediate and undeniable feedback forces game developers and platforms to push boundaries. In the video game industry, failure to quickly address these issues will result in an unsuccessful game."

*Gartner, Emerging Technologies: Look to Gaming Innovation for the Future of End-User Experiences, Forest Conner, Ted Chamberlin, 18 May 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved



Why Do Fraudsters Target Gaming?

The gaming sector offers substantial potential revenue to financially-motivated bad actors. Typically, gaming websites have a large community of young users whose credentials are less likely to have been part of a data breach from other major websites. Bad actors seek to take control of high-value accounts to gain items which they can resell in the real-world, for real dollars. When an account is taken over, the entire balance is transferred to an attacker-owned account, and the attacker cashes out. Markets exist in these gaming worlds where consumers (and attackers) can convert the gaming currency into cash.

In addition, bad actors tend to register (at scale) multiple new accounts that offer bonuses, or create bogus gaming sessions for financial gain. In the iGaming sector, it's common for providers to offer promotions to entice new consumers, and bad actors may seek to abuse and monetize this opportunity, using well-tuned bots to create massive fake new accounts.

> "There are four things that cybercriminals are looking for: information, access, data, or cash."
>
> Brett Johnson,
> Chief Criminal Officer,
>
> Arkose Labs

Johnson points out that as macroeconomic conditions decline, cyber attacks will go up, and that Cybercrime-as-a-Service (CaaS) is skyrocketing. CaaS is when experienced fraudsters build automated attack tools, like malicious bots, that inexperienced bad actors can simply buy off the (dark web) shelf. These "readymade" malicious bots have democratized the use of bots to attack company websites. We expect the volume of bot-driven attacks to increase exponentially in **2023**, as our November year-over-year analysis shows a **22%** jump in basic bot attacks on gaming companies. In addition to the well-known attack tactics, such as stealing login credentials, there is also a trend towards stealing session tokens (cookies).

Why Do Fraudsters Target Gaming?

In the recent eBook titled, The Economics of Account Takeover Attacks, Arkose Labs' threat researchers examined how bad actors make a living by abusing websites and quantified their net income. Bad actors tend to harvest and sell legitimate consumers' credentials on the dark web or they orchestrate attacks or they do both. The market price of a good user's credentials varies by industry. For a skilled bad actor with a good reputation, the gaming industry offers substantial revenue potential compared with other industries, like banking and eCommerce.

For gaming sites, we differentiate between two types of accounts:

Premium accounts, which are considered high-value because they provide valuable assets to a player to progress in the game (such as powerful weapons, credits, etc.) These accounts can have a very high resale value on the dark web.

Lower-value accounts, which are sold in bulk by bad actors. They are considered lower value because the assets associated with them are unknown or limited.

The next table shows the market price and potential revenue of different types of accounts, based on the estimated credential harvested after completing an attack.

We estimate that bad actors who are new in the business (i.e. Rookie Fraudsters) with no/low reputation may sell up to **20%** of their good consumer credentials inventories, whereas more experienced bad actors who are resellers with a medium reputation may sell up to **40%** of their inventory. Long-term proven bad actors (i.e. Master Fraudsters) who are resellers with a very good reputation may sell at least **60%** of their inventory of good consumers credentials..

Industry	Average revenue / credential	Good Reputation	Medium Reputation	Bad Reputation
e-Commerce	$0.08	$7,200.00	$4,800.00	$2,400.00
Social Media	$0.10	$9,000.00	$6,000.00	$3,000.00
Fintech/ Bank	$0.40	$24,000.00	$16,000.00	$8,000.00
Gaming - Bulk Accounts	$1.70	$51,000.00	$34,000.00	$17,000.00
Gaming - Premium Accounts	$648	$29,160.00	$19,440.00	$9,720.00

Gaming Industry Threat Landscape

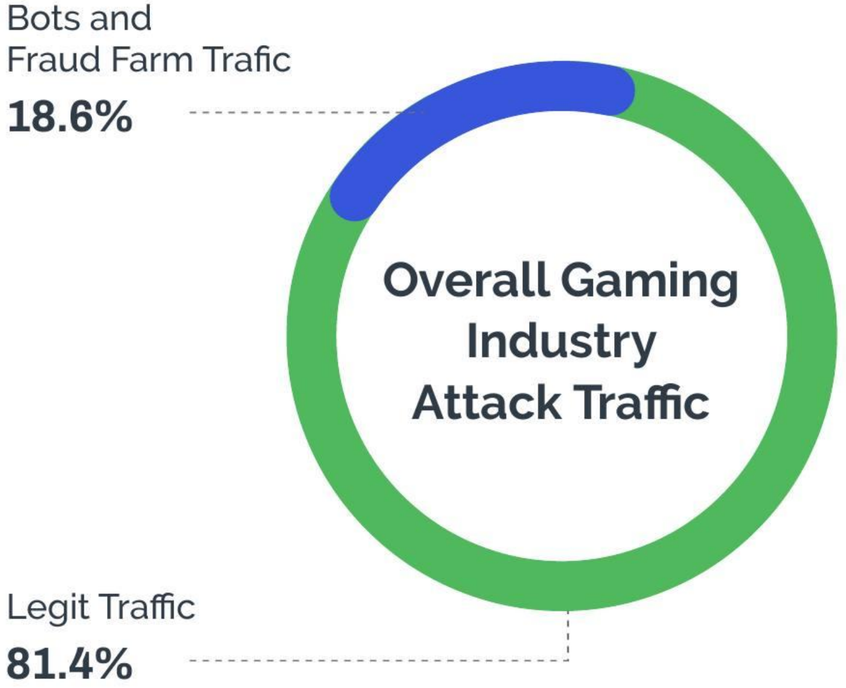
We analyzed billions of sessions from the biggest gaming companies in the world, between November 2021 and to the beginning of December 2022, and assessed four different traffic types:

Basic Bots
two or fewer rounds played, not verified

Intelligent Bots
more than two but fewer than ten rounds played, not verified

Fraud Farms
ten or more rounds played, not verified

Legit Traffic
all verified traffic

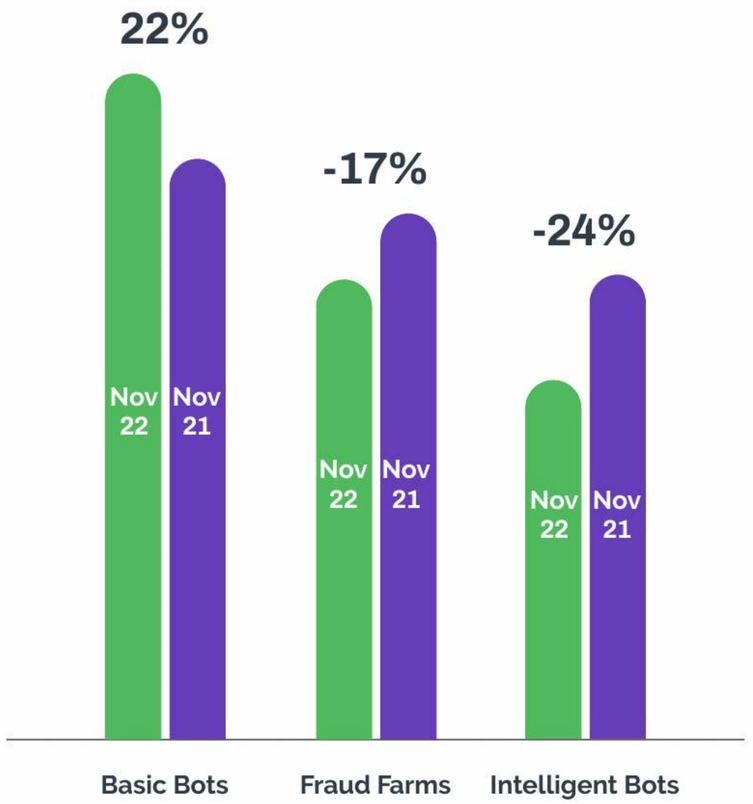


Why are basic bots the most commonly used Attack Type?

Basic bot attacks are highly scalable, providing the volumes that bad actors need in order to secure financial gains. Plus, they are an easy way for unskilled attackers to get into cybercrime. They purchase ready-made bots from an online marketpl ace on the dark web, which allows them to capture login credentials, browser fingerprints, and cookies.

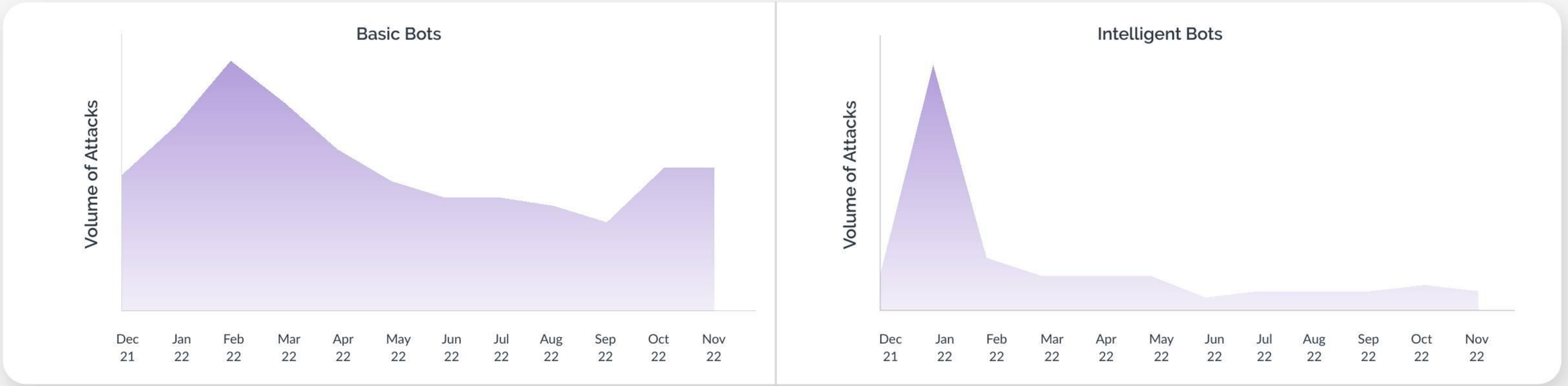
This CaaS space is growing, providing automated ways for new, unsophisticated attackers to build a lucrative career in fraud without building their own malicious bots from scratch.

A November 2022 to November 2021 assessment shows that basic bot traffic increased at a 22% clip, a faster pace than intelligent bots and fraud farms, which declined during the same time period. This finding corroborated our observation that cybercrime-as-a-service is on the rise.



Global attack volumes by month and attack type

The vast majority of attacks are carried out by basic bots. Both basic and intelligent bot attacks began rising over the 2021 holiday season and into the new year, whilst fraud farm attacks were more static.



November is typically the biggest month for video game releases. It's a month where many gamers have more time to play. And where activity and money goes, so do fraudsters. In the months following, attack volumes also rise.

The late 2021 and early 2022 spike our threat research team observed was a massive attack by CAPTCHA solvers—deployed by fraudsters who were active in other industries but turned their attention and started to test the financial gains that could be generated in the gaming sector.

(Source: https://gamerant.com/new-video-game-releases-november-2022/_

Fraud farms tend to be low and slow (but equally impactful) human-led attacks.

We also analyzed the data to better understand patterns in the following use cases:

Fake Account Creation

Attacks connected with initial sign-up for an online account

ATO Attacks

Attacks connected with signing into an account

Payment/Monetization

Buying digital goods or trading game-specific payment cards, or credit cards

In-product abuse

Odd or anonymous behavior like joining lobbies, trading cards for purchases, etc.

password changes

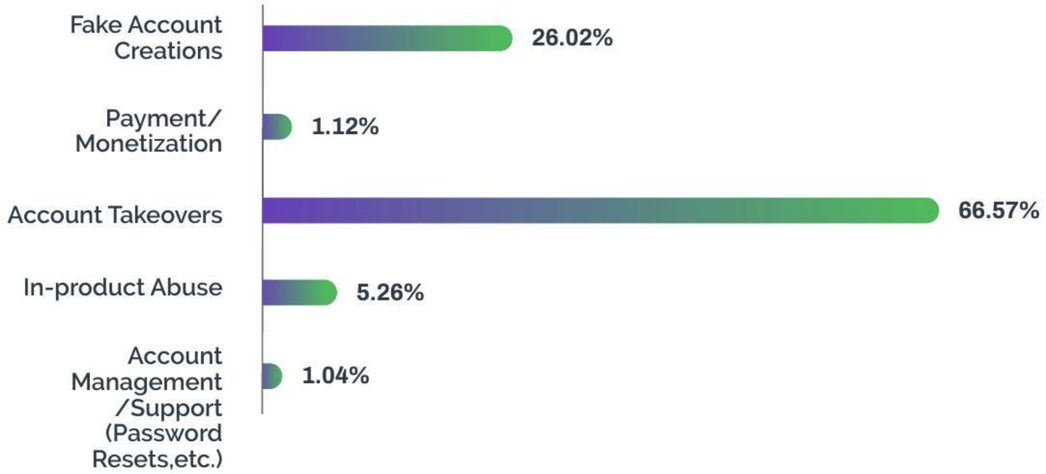
Bots that send over multiple requests for assistance to saturate the help center and disrupt the consumer experience

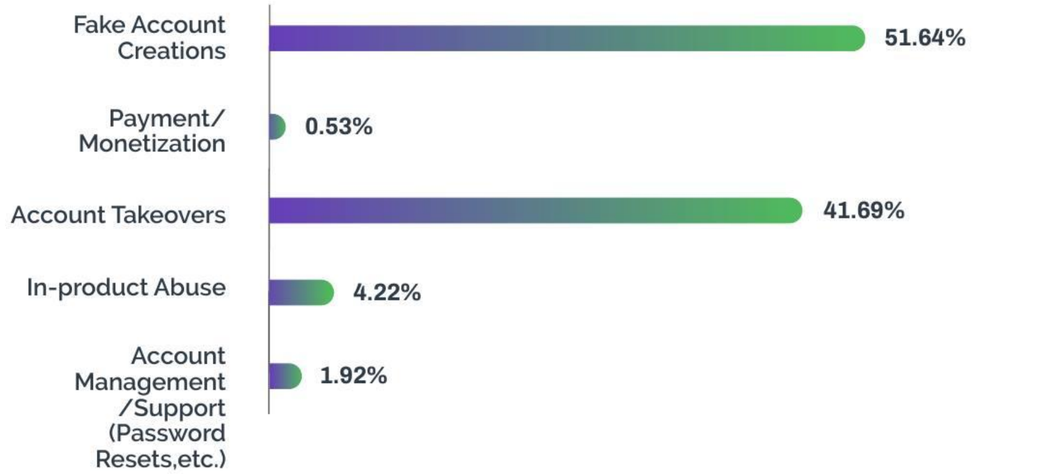
Basic Bots Attacks by Use Case

The vast majority of attacks carried out by basic bots are account takeovers and fake account creations, which take place at sign-in/log-in and sign-up/ registration.

Intelligent Bots by Use Case

Registration or fake account creation attacks are the most commonly used attack type, followed by account takeovers.



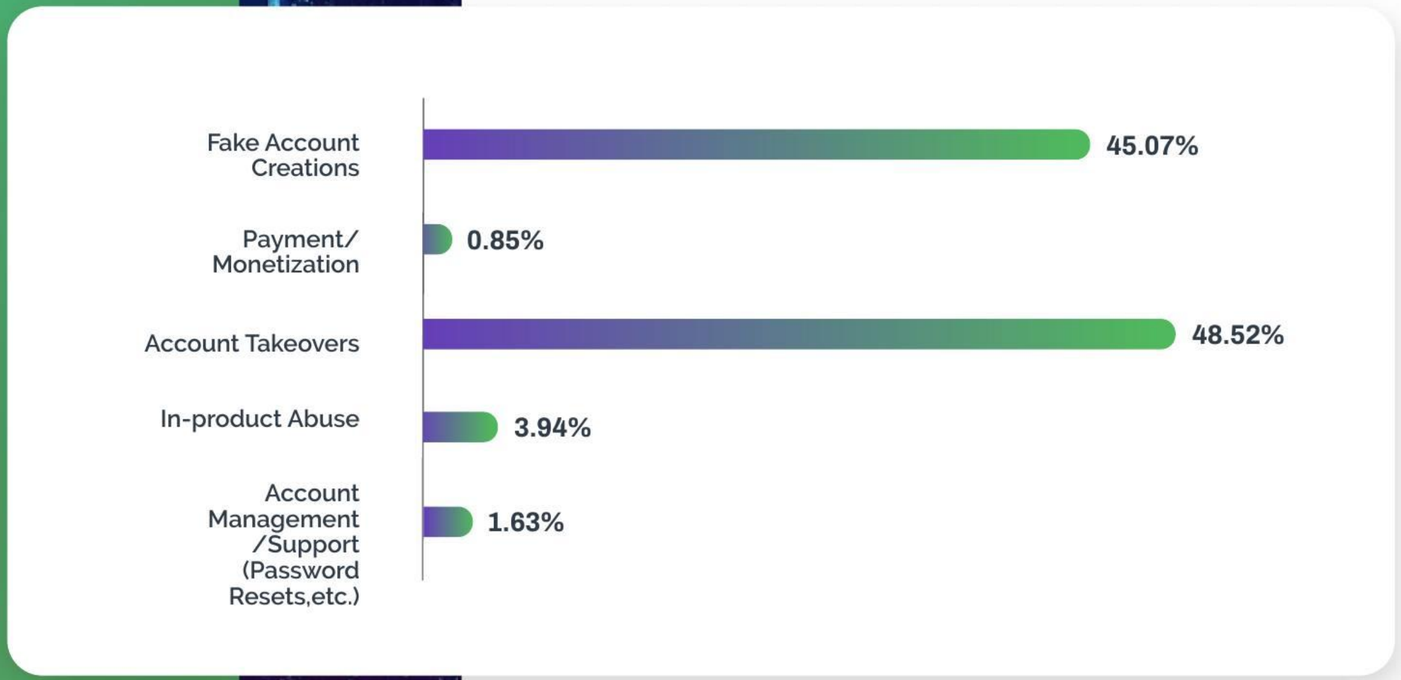


Attackers tend to register for new accounts and sell them on the dark web—after taking the benefits from the trial and getting the gaming account to a higher level to make it attractive to other gamers. Once a legitimate buyer purchases the attacker's existing account, the account will most liely get flagged and then banned. The result is that the end consumer loses money and has no recourse. The consumer tends to get frustrated with the gaming company, not the attacker, about the banned the account, jeopardizing the gaming company's brand reputation.

The percentages are calculated to the nearest .01%.

Fraud Farm Attacks by Use Case

As with basic and intelligent bots, fake account creations and account takeovers remain the most common use case perpetrated by human-driven fraud farm attacks .



Countries in Focus

Of the four countries studied in the report, the U.K. has both the highest percentage of intelligent bot traffic, and the highest amount of attacks overall (as a percentage of total traffic)

Driving this insight is that several known and suspicious ISPs are open and have a presence in the UK.

Country	Basic bots	Fraud farms	Intelligent bots	Legit traffic
USA	13.58%	0.31%	1.19%	84.92%
Australia	12.45%	0.15%	0.64%	86.76%
UK	12.25%	0.19%	15.67%	71.89%
Singapore	17.24%	0.54%	2.51%	79.71%

Attacks by Use Case:

When examining attacks by type of attacker and use case for the four focus countries, we found that login-based account takeovers comprised the majority of attacks in the US, Singapore, and Australia, with most of the attacks being performed by basic bots. In the U.K., fake new account creation was the most common use case for adversaries.

US OVERVIEW

Use case	Basic bots	Fraud farms	Intelligent bots	Total
Account Management / Support	1.70%	0.02%	0.08%	1.80%
In-product Abuse	5.92%	0.08%	0.43%	6.43%
Account Takeovers	59.92%	0.98%	5.26%	66.16%
Payment/Monetization	2.97%	0.04%	0.12%	3.13%
Fake Account Creations	19.54%	0.92%	2.00%	22.46%
Grand Total	90.05%	2.04%	7.89%	

The percentages are calculated to the nearest .01%.

Attacks by Use Case

AUSTRALIA ATTACK PATTERNS

Use case	Basic bots	Fraud farms	Intelligent bots	Total
Account Management / Support	1.42%	0.01%	0.10%	1.53%
In-product Abuse	6.14%	0.06%	0.41%	6.61%
Account Takeovers	68.20%	0.61%	3.11%	71.92%
Payment/Monetization	2.30%	0.04%	0.11%	2.45%
Fake Account Creations	15.97%	0.41%	1.13%	17.51%
Grand Total	94.03%	1.13%	4.86%	

UK ATTACK PATTERNS

Use case	Basic bots	Fraud farms	Intelligent bots	Total
Account Management / Support	0.57%	0.01%	0.03%	0.61%
In-product Abuse	3.50%	0.05%	0.28%	3.83%
Account Takeovers	27.69%	0.35%	1.49%	29.53%
Payment/Monetization	0.93%	0.01%	0.04%	0.98%
Fake Account Creations	10.90%	0.25%	53.91%	65.06%
Grand Total	43.59%	0.67%	55.75%	

SINGAPORE ATTTACK PATTERNS

Use case	Basic bots	Fraud farms	Intelligent bots	Total
Account Management / Support	1.22%	0.02%	0.15%	1.39%
In-product Abuse	4.20%	0.06%	0.48%	4.74%
Account Takeovers	62.68%	1.09%	6.17%	69.94%
Payment/Monetization	0.62%	0.02%	0.06%	0.70%
Fake Account Creations	16.24%	1.49%	5.49%	23.22%
Grand Total	84.96%	2.68%	12.35%	

The percentages are calculated to the nearest .01%.

Emerging Threats for the Gaming Sector

Adversaries constantly innovate their attacks. Here are some of the most recent trends targeting the gaming industry

Reverse proxy phishing attacks

These attacks, also known as Man- in-the-Middle (MITM) attacks, were the fastest growing type of internet crime from **2019-2021**, a problem our customers say has intensified over the summer of **2022**. Enterprises cannot block these attacks because adversaries are always changing the companies' domains. In fact, attackers also register dozens of domains to avoid being detected by WAF-deny lists and spam filters. In these cases, we alert consumers of the issue to warn them of a potential phishing scam. Phony websites and emails coming from well-known people or organizations, such as the victim's bank, place of employment, or other institution, are the workhorse of this type of phishing expedition. Get more details on page **16**.

Volumetric attacks

We're seeing a mixture of attacks from both basic bots and intelligent ones on login and signup, trying to collapse the servers without impacting consumers. Only last week at the time of writing, we stopped nearly **20** million fake new account registrations for just one of our customers.

Use of Discord for communications

Discord, a VoIP and instant messaging social platform, appeals to gamers. It is mostly used for legitimate purposes, but it can also be a meeting place for attackers to socialize, work together, share and exchange exploits and tools, and refine existing techniques while working together to establish new ones.

> Some of these attackers really don't see that they are doing anything wrong—they are just playing around, tinkering with bots, hacks, exploits, work-arounds, etc. That's a much bigger idea than it seems. Those attackers aren't looking to harm, per se, they are just messing with stuff. But that causes a lot of issues in those gaming environments and disrupts the intended user experience for everyone. That's where we come in.
>
> Brett Johnson,
> Chief Criminal Officer,
>
> Arkose Labs

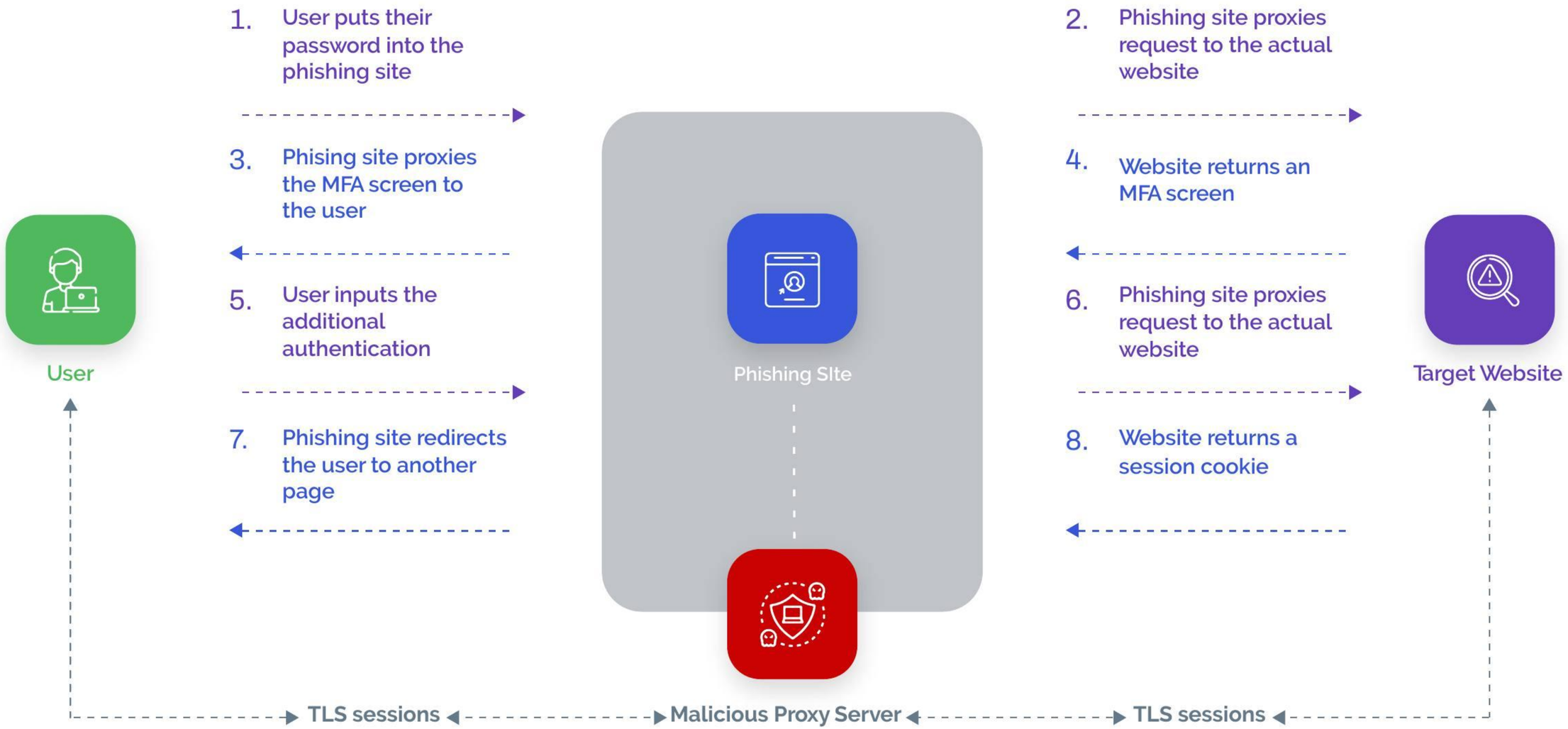
Reverse Proxy Phishing Attacks

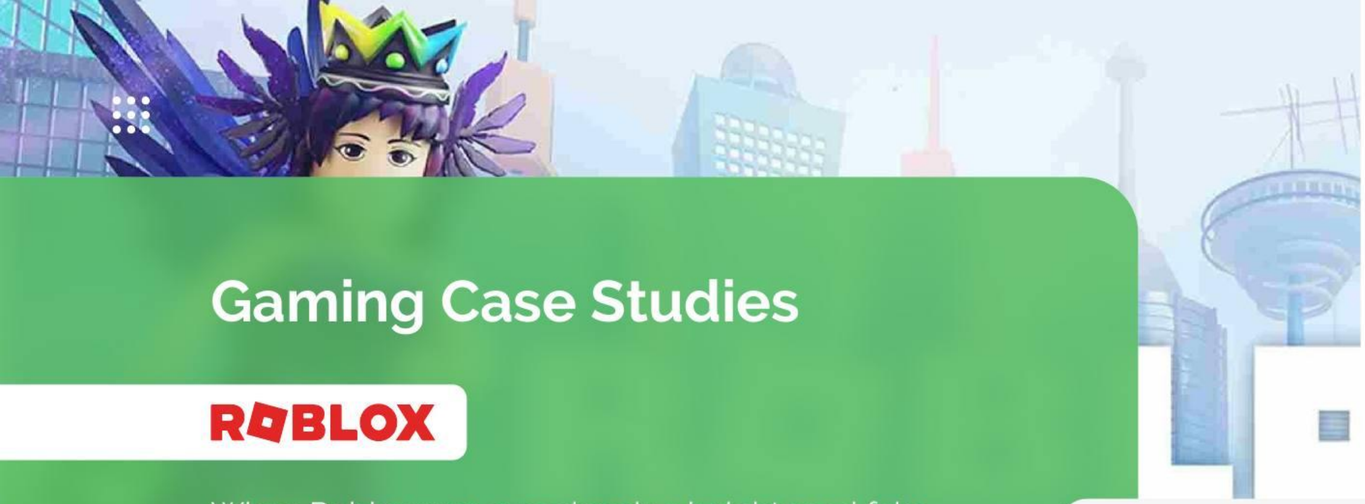
MITM attacks are the latest phishing attack evolution targeting gaming companies. These attacks act as malicious reverse proxy servers of online services and mirror the targeted website's content to consumers, while extracting credentials like MFA tokens and session cookies in transit. These MITM phishing kits also automate the harvesting of two factor authentication (2FA) sessions. The latest phishing attack, EvilProxy, employs the same "reverse-proxy" approach to allow inexperienced criminals to use reverse proxy and cookie-injection methods to circumvent 2FA sessions on a large scale. Fraudsters can then lure victims to phishing sites and sniff out the traffic from which they can extract credentials and MFA tokens.

Another Phishing-as-a-Service platform, Caffeine, streamlines the process of carrying out phishing attacks with advanced features for customizing dynamic URL schemas to generate victimspecific pages and IP blocking options for geo-blocking. Attackers can register for an account that provides immediate access to the "store," where they can find phishing campaign creation tools, an overview dashboard, and a way to purchase a subscription license. When a site implements security measures that cannot be proxied and don't require user interaction, this approach becomes hard to automate.

Our adaptive challenge responses, as part of Arkose Protect™, cannot be automated by the MITM reverse proxies. We combine highly-transparent detection with targeted attack response to catch fraud early in the customer journey, without impacting the good user experience. Our solution is configured on the login and registration pages of the website prior to the MFA step. These workflows can be resolved, provided the web server receives the token upon successful completion of the challenge response process. This new approach to phishing detection not only requires a token to protect from MITM attacks, but it also alerts the end-user of the threat. This unique positioning on the login/ registration workflow, combined with advanced phishing detection and challenge capabilities, means our technology offers potent defense against reverse-proxy-based MITM phishing attacks.

Anatomy of a Reverse Proxy Phishing Attack





Gaming Case Studies

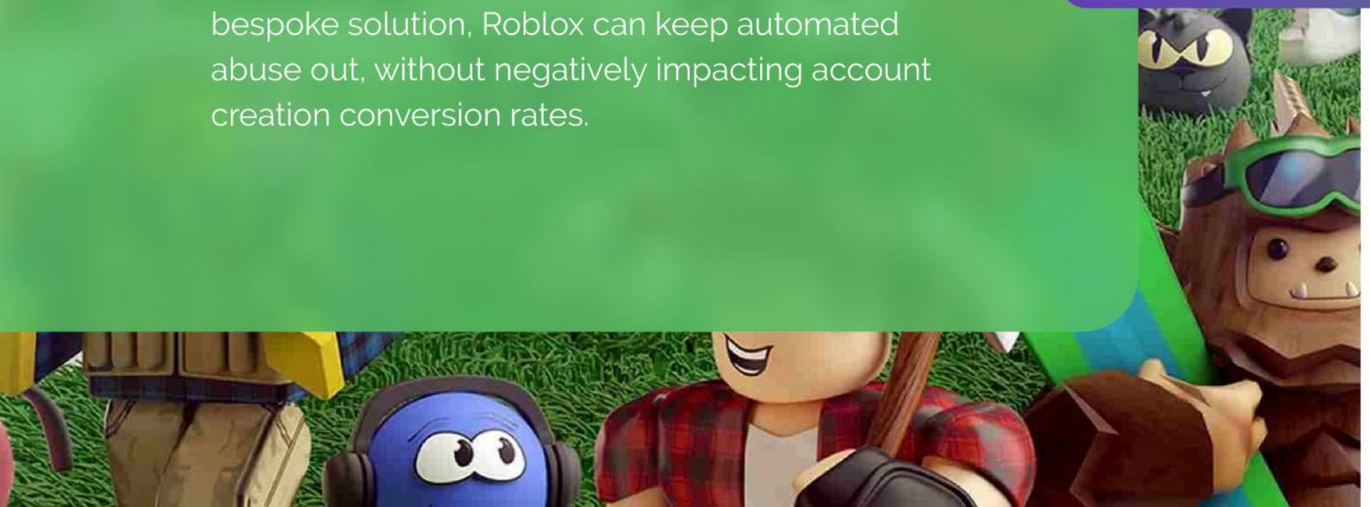
ROBLOX

When Roblox was experiencing heightened fake account creations, it turned to Arkose Labs for help. We worked with Roblox to significantly reduce platform abuse from automated bots, whilst keeping the experience positive for genuine users.

The Arkose Enforce challenges replaced stock pictures with Roblox's unique imagery. By blending with the platform's design, we helped Roblox deliver a seamless user experience. Thanks to this bespoke solution, Roblox can keep automated abuse out, without negatively impacting account creation conversion rates.

> The difference between our past solution and Arkose Labs is night and day for us. Previous solutions created a bad user experience, while Arkose solves our problem with no added friction, and makes it fun for our users.

– Software Engineer at Roblox



GAMING INDUSTRY GIANT

Arkose Labs eliminated in-game auction house and virtual currency abuse and saved this gaming giant millions of dollars.

Another gaming company turned to Arkose Labs for help with preventing in-game currency abuse. Account takeovers targeted genuine users, draining or transferring their assets, and the company needed help to provide a safe experience for their valued customers.

By deploying custom in-game enforcement challenges, we accurately filtered out bots and other organized attacks. The result was a fifteen-fold reduction in fraudulent activity, and millions of dollars saved for the company.

> We had very specific requirements as to how we wanted Arkose Labs to approach stopping the attacks. They are very flexible in tailoring attack mitigation techniques that align with our own unique security strategy.
>
> – Manager, Fraud and Data Science

The $1 Million Credential Stuffing Warranty

Bot attacks and account-focused threats present significant risks to gaming companies' revenue and brand reputation.

The investment in fortifying the consumer experience is mandatory. Cybersecurity is a "before-the-fact" investment, meaning you pay upfront in hopes of saving costs in the long run, but there's no guarantee or certainty that the technology you're contracting for will work.

That's why we pioneered the industry's only $1 Million Credential Stuffing Warranty. CISOs have a guaranteed outcome: either Arkose Labs stops the attack, or we cover the loss.

Expert Insight:
Brett Johnson,
Chief Criminal Officer

Many industries work in security silos. But Johnson says banks, retail merchants, and other businesses should look to the attacks in the gaming space to predict what is coming their way. Now, we're seeing criminals consider where they can use automated attacks (bot-based attacks) in other verticals.

"Pay attention to the gaming industry. That is the playground, the proving ground for most automated types of attacks. Because the dollar amounts are not very high on the returns, criminals are looking for automated ways to commit the types of fraud that manual humans are doing in other verticals. Once those automated ways are proven effective in that testing ground, then they'll start deploying them in other verticals."

How Can Arkose Labs Help?

Financial incentive fuels all fraud. Arkose Labs delivers long-term bot mitigation and account security by undermining the economic drivers behind attacks. We help gaming companies defend the most targeted user touch-points by uncovering hidden attack signals and sabotaging attackers' ROI without sacrificing good user throughput.

We protect global gaming companies from evolving attacks; block automated activity aimed at monetizing stolen data; and secure the in-game experience from match-fixing. Arkose Labs' unique detection and mitigation platform analyzes data from user sessions to determine the context, behavior, and past reputation of every request. We classify traffic based on its risk profile and present suspicious traffic with enforcement challenges to differentiate between true users and fraudsters.

We give businesses the advantage over adversaries, resulting in:

$Millions Saved in Costs Associated with Fraud Attacks

80% Reduction in Good User Friction

98% Reduction in Bot Attacks

Arkose Labs

Arkose Labs' mission is to create an online environment where all consumers are protected from malicious activity. Its AI-based platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks while improving good user throughput. The company offers the world's first and only $1 Million Credential Stuffing Warranty™. Headquartered in San Mateo, CA with offices in Brisbane and Sydney, Australia, San Jose, Costa Rica, and London, UK, the company ranked as the 106th fastest-growing company in North America on the 2022 Deloitte Fast500 list.

O ces

San Francisco
2 W5th Ave 3rd floor, San Mateo, CA 94402

Brisbane
315 Brunswick St, Brisbane, Queensland AU

United Kingdom
167-169 Great Portland Street, 5th Floor, London, W1W 5PF

Australia
San Jose, Costa Rica
Tokyo

Schedule Demo