Report

How Bots Attack Streaming Services

NETACEA

CONTENTS

INTRODUCTION

Subscription video on demand (SVOD) services are projected to generate $108.5 billion in 2024, growing to $137.7 billion in 2027[1]. Online streaming accounts for 36% of all TV usage[2], with major cable TV providers in the US losing five million subscribers in 2023[3], and 99% of US households have at least one streaming service subscription[4].

The public is now more likely to subscribe to a few select streaming services than have a cable box or satellite dish. This shift has benefited consumers with more choice, lower costs than most cable packages and easier access to the content they enjoy most.

But criminals and pirates have taken notice of this growth and are actively targeting streaming services. Using automated bot attacks, they prey on streaming user accounts and video content.

Convenience Increases Risk

One reason OTT (over-the-top) streaming*, or subscription video-on-demand (SVOD)**, has become so popular is that a wide selection of internet-based video content is easily available without additional equipment. Streaming services are ubiquitous to anyone with high-speed internet access.

This convenience comes at a cost that is often unseen by consumers but of increasing concern to streaming businesses: New opportunities for fraud and profit by criminals.

Business Drivers for Streamers

Unmitigated bot attacks directly affect the two primary sources of profit for streaming services – attracting new subscribers and retaining existing ones. The sale of stolen accounts, caused by automated account takeover, means fewer subscriptions sold, while customers locked out of their accounts damages user experience and affects renewals.

Definitions:

- ***Over-the-top (OTT) streaming:** A media service offered directly over the internet.*
- ***Subscription video-on-demand (SVOD):** A recurring fee model for streaming media services.*

Sources:

1. *https://www.statista.com/outlook/dmo/digital-media/video-on-demand/video-streaming-svod/worldwide#revenue*
2. *https://www.nielsen.com/insights/2024/colder-weather-and-nfl-playoffs-drive-increased-tv-usage-in-january/*
3. *https://www.statista.com/statistics/819243/cable-company-total-subscriber-loss/*
4. *https://www.forbes.com/home-improvement/internet/streaming-stats/*

Executive Summary

Andy Still
CTO & Co-Founder, Netacea

Netacea was born from the need to defend businesses from malicious automation. As online transactional businesses, SVOD services are especially vulnerable to automated attacks. User accounts are susceptible to account takeover via credential stuffing, welcome bonuses and free trials attract bots, and the ability to quickly create new accounts make streaming sites a target for credit card fraudsters.

The growing sophistication of bots makes stopping these attacks harder than ever. At Netacea we've witnessed bots rotate IP addresses millions of times to disguise attacks. They emulate human mouse movements and reuse valid device fingerprints. Even novices can write a successful attack script using AI coding co-pilots.

The result is a flourishing black market of stolen streaming service accounts at bargain basement prices. By undercutting the streaming sites they attack, adversaries are making huge profits, and pirates are getting free access to exclusive content.

Bots take advantage of the litany of devices that streaming services have made available for customer convenience, from smart TVs to gaming consoles of every brand and variety. Unfortunately, traditional bot defenses are largely blind to API-based bot traffic originating outside of standard web and mobile applications.

We need defenses that cover every angle of attack, without blind spots – or bots will always find and exploit a point of weakness. The swathes of stolen accounts for sale on the dark web are clear evidence of that.

In our experience, streaming businesses are very conscious of adding undue friction to user journeys. Anti-bot measures such as enforced MFA and CAPTCHA at login are very much a "last resort" due to the risk of customer drop-off and disengagement. Understandably, OTT streamers also can't risk blocking genuine customers misidentified as bots.

The information collected within this report informs Netacea's approach to protecting our streaming services customers with confidence – we hope it informs your own strategy for protecting your business against bad bots as well.

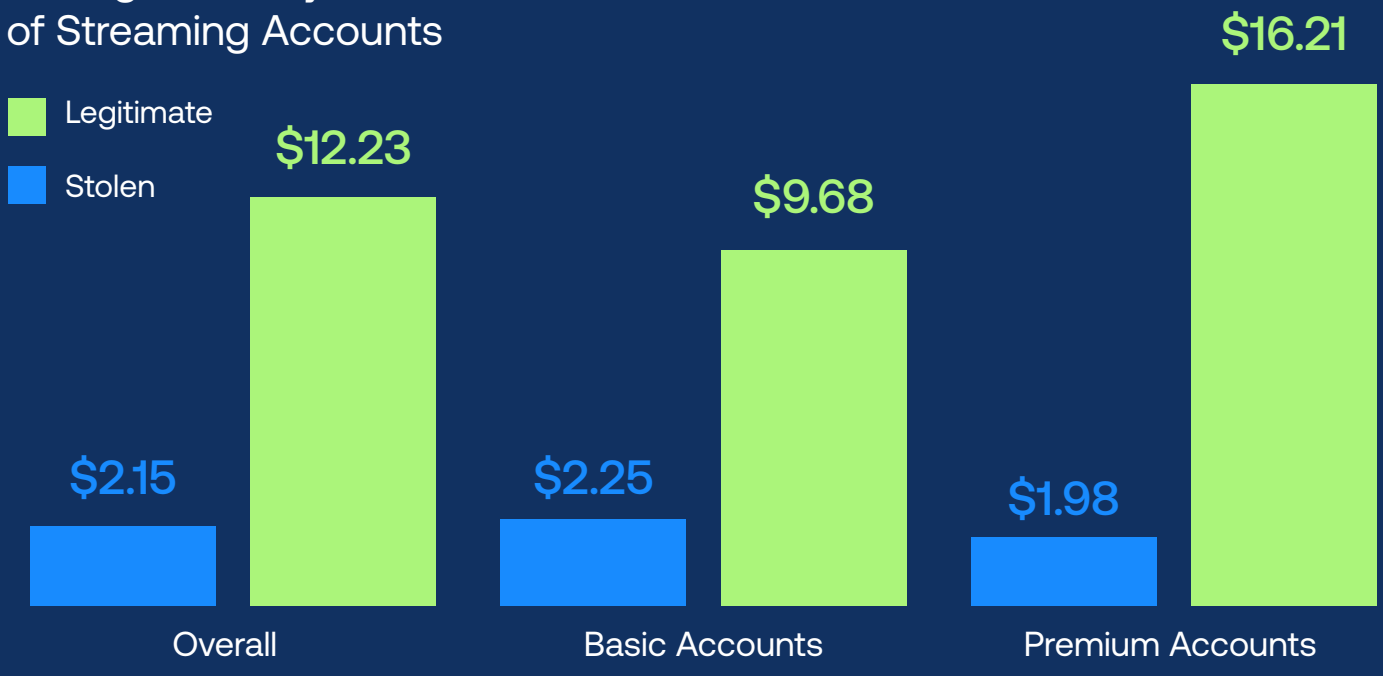
Impact of Bots on Streaming Services

Stolen Streaming Accounts Are Abundantly Available on Illicit Marketplaces

* Data collected on 14 streaming services across over 2,000 marketplaces.

Criminals Sell Stolen Streaming Accounts at 27.5% of Legitimate Price

Average Monthly Cost of Streaming Accounts



Mapping Out Threats and Defenses

As with any security concern, the first step for streaming services is to understand the size of the problem, the tactics used by their attackers and the tools needed to defend against them.

The stats on this page paint a picture of the scale of the problem. To begin addressing this, security professionals can use the BLADE Framework[5] to track the phases, tactics and techniques of business logic attacks affecting SVOD providers, such as credential stuffing and fake account creation.

The earlier in the kill chain we can identify an attack, the more effective we can be at preventing the later phases and consequences of that attack. It is vital to map out the phases and the tactics and techniques of each attack.

Stop & Act

Go to the BLADE Framework website to map your business's potential threats and better understand attacker behaviors.

5. *BLADE (Business Logic Attack Definition) Framework is an open-source project pioneered by the Netacea threat research team. Read more at* ***www.bladeframework.org***

Account Takeover & Credential Stuffing

In an account takeover attack, criminals gain unauthorized access to user accounts when seeking to steal personal information or payment details or sell access to the account to a third party.

Credential stuffing is one of the most common methods of account takeover and does not require their target platform to have suffered a data breach. Criminals use stolen credentials from any site, usually obtained via data dumps, and test them against another site by using bots. This exploits the propensity of consumers to reuse passwords across multiple online services.

Stop & Act

Check your authentication logs for high volumes of failed login attempts, especially at peak traffic times. This is a sign of a credential stuffing attack.

Credential Stuffing Kill Chain

Resource Development

The attacker acquires stolen credentials, proxies to disguise their attacks, and tools like OpenBullet configured to attack their intended target.

Reconnaissance

The attacker performs technical reconnaissance on the target service to learn the defenses they use and how to get past them.

Defense Bypass

Most credential stuffing tools include modules to automatically solve CAPTCHA challenges, plug in proxy lists, rotate between user agents and bypass MFA.

Attack Execution

Thousands of stolen credential pairs are entered into the target login page automatically, and data exfiltrated from accounts that are successfully accessed.

Actions on the Objective

The adversary releases or sells validated credentials on the dark or open web, usually at significantly reduced prices.

Post-attack

The attacker brokers stolen information, such as PII or payment details, either manually or via automated listings on illicit marketplaces.

The Business Impact of Account Takeover & Credential Stuffing

For such a cheap and easy attack to launch, it doesn't take a high success rate (typically 0.1%) for a credential stuffing attack to access accounts and accrue serious financial consequences on the target business.

Infrastructure Costs & Stability Risks

Credential stuffing attacks are usually high volume – in the millions of requests per hour – to test as many credentials as possible and maximize the chances of finding correct login details. Bots can account for over 90% of login attempts. This traffic is expensive to serve, has the potential to overwhelm servers, and causes stability issues.

Customer Frustration

With competition high amongst streaming services, smooth customer experience is crucial to retaining subscribers. Account lockout is a surefire way to frustrate customers, especially as they sit down to binge the next episode of the series they're hooked on, or to watch a live sporting event.

Once attackers steal accounts they lock the owners out. This not only causes frustration for customers but costs the business money in time spent on support calls, repatriating accounts.

Reputation

Any company that makes headlines for suffering a credential stuffing attack is less likely to be trusted with personal information. Credential stuffing is rarely understood by the public; customers blame the security practices of the company itself rather than their own password hygiene.

Stolen Accounts for Sale

Netacea's threat research team uncovers **hundreds of thousands** of taken-over customer accounts each month available for purchase on various hacking forums and digital marketplaces.

While stolen accounts typically sell for **27.5%** less than their legitimate prices, this depends on the type of account (e.g. premium with 4K streaming, or entry-level with adverts) and whether the reseller is offering a warranty on access to the account.

In the latter case, accounts are guaranteed to work for a certain amount of time, for example six months. If the account becomes inaccessible (the account is locked or the original owner changes their password), the reseller replaces the account with another for free – because taking over accounts is so easy for them to achieve.

Fraud Intervention Costs

The longer it takes to detect account takeover attacks, the more financial harm the attacks cause. Due to the measures attackers take to disguise their activities for as long as possible, timely intervention is incredibly difficult. It takes an average of four months for businesses to detect a bot attack has taken place on their platform[6]. Bots repeat their attacks until businesses intervene, at which point they will change tactics and bypass the new defenses with more sophisticated measures.

“The sophistication of the attack is predicated on the value of the goods that are targeted or the size of the prize. Return on investment is everything to attackers.”

Andrew Ash,
CISO at Netacea

Account takeover is a common tactic to commit fraud and so must be investigated thoroughly. By preventing credential stuffing attacks, businesses can stop accounts from being taken over and avoid costly fraud investigations.

Stop & Act

Start calculating the financial loss to your business caused by credential stuffing. Count how many users you have and how the above factors affect new subscribers and renewal figures.

6. *Death By a Billion Bots, Netacea, 2023*
https://netacea.com/reports/death-by-a-billion-bots/

Fake Account Creation

As well as stealing existing accounts, bots create fake new accounts. The only resources needed are sham personal details (which can be generated by AI or randomized). Many fake account creation bots can complete email or text verification automatically.

Multiple fake accounts are controlled by one person who can then abuse welcome offers or free trial periods, reselling them for a low cost to undermine legitimate subscription sales.

Creating fake accounts is also the first stage of carding. Carding, or card cracking, is the use of automation to test the missing details of illegally obtained credit cards until they get a successful transaction. From there they can make bigger purchases or sell the card to someone else.

Stop & Act

Investigate whether there is a correlation between new account registrations and failed card payments on your platform. This is a clear sign of fake account creation to facilitate card cracking.

Fake Account Creation Kill Chain

Resource Development

The attacker gathers tools, proxies and stolen cards (either full or partial details). They will also generate a list of personal information with which to register accounts.

Reconnaissance

The attacker investigates the registration flow of the target site to determine defenses and verification checks in place.

Defense Bypass

Bots are designed to bypass common defenses by spoofing client-side signals, such as human-like mouse movements, and rotate through proxies to disguise the attack.

Attack Execution

The bot automatically registers as many fresh accounts as the attack needs, whilst passing verification checks autonomously.

Post-attack

With many fake accounts under their control, the attacker can carry out further attacks like card cracking.

The Business Impact of Fake Account Creation

Skewed Analytics & Misinformed Business Decisions

Acquiring new members is a core business goal for all streaming sites, so having accurate data is vital to inform growth strategies. Masses of fake accounts on your platform disrupt this analysis and lead to misinformed decisions if not addressed.

Carding and Payment Fraud

Card fraudsters use streaming services to test stolen full or partial credit card details because subscription purchases are small, quick transactions with no physical stock to manage. Criminals can quickly validate whether their payment was accepted and go on to make bigger purchases elsewhere or sell the card details to a third party.

Card fraud can add significant costs to streaming service operations, even when cards are declined. Payment portals charge authorization fees per payment attempt, which adds up over time and rapidly during concentrated attacks.

Also, a sudden influx of failed payments can flag your service to the payment processor, disrupting legitimate payments from real customers. Once again, any cause of customer frustration and friction impacts the bottom line.

Free Trial Abuse

Bots generating fake accounts can rack up thousands of free trials. SVOD services offer free trials to attract new subscribers, but when these are generated by bots and used by people with no intention of buying a subscription legitimately, they become a waste of infrastructure and an operational cost.

Stop & Act

Calculate the cost per hour of your payment portal becoming unavailable due to the action of card fraud bots.

Traditional Defenses Are Failing to Protect Streaming Services

Traditional Defenses Don't Cover All Attack Surfaces

Most bot management tools, including those bundled with CDNs and WAFs as well as standalone solutions, analyze signals within individual interactions within the client.

However, 70% of Netflix content is consumed via TVs, either through a native app or via a connected set top box or console. Browser based streaming only accounts for 15% of usage. These endpoints are unprotected by client-based bot management tools. This leaves a massive "hole in the fence" for bots to login in and access accounts undetected.

Traditional Defenses Can Be Bypassed

Another consequence of bot management tools operating on the client side is that they are visible to attackers. This means the code can be reverse engineered, allowing bot operators to spoof signals and bypass detection. These bypasses can even be rented or bought and passed around to anyone who wishes to build them into their bots. Many are published each month for most major client-side vendors.

Bots are Increasingly Sophisticated

Most bot protection vendors use rule-based blocking to identify rogue IP address ranges used by bots. But bots are now far too sophisticated to be foiled by this tactic. As standard, most bots can rotate through massive lists of IP addresses and even user agents to evade detection and appear that one huge attack is many legitimate users.

Blocking IP addresses alone is often risky as bots increasingly use hired or stolen residential proxies to disguise as legitimate traffic. Hard-blocking IPs could mean blocking a real customer that also uses that IP.

Traditional Bot Defenses Risk Causing Friction to Consumers

A common anti-bot method – the increasingly convoluted CAPTCHA challenge – is not well-suited to TV screens.

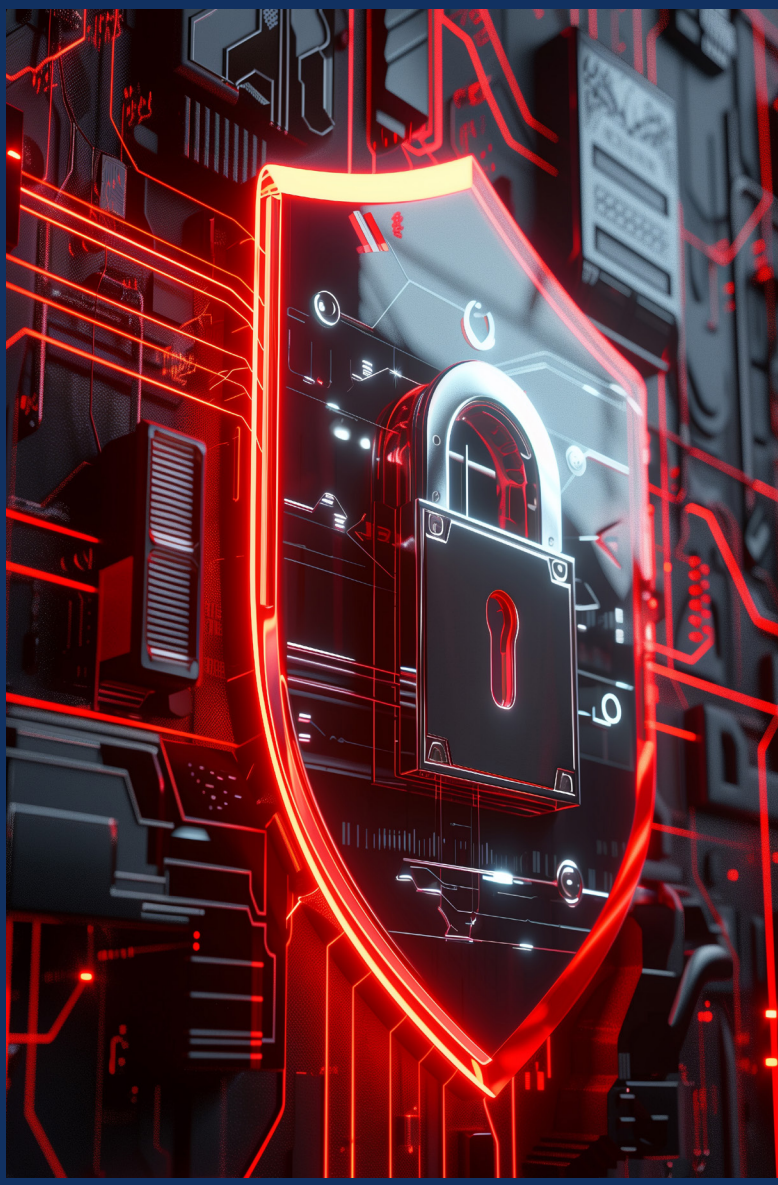
Detection accuracy is also vital. Mistakenly blocking real users may cause viewers to miss out on live events such as sports games, which would cause customer complaints and lost subscribers.

Case study: Protecting a Major Streaming Service from Bots During a Huge Live Event

A large US-based SVOD service was about to exclusively stream the biggest sporting event of the year live. The event was a big incentive for new subscribers to join and the business wanted to retain as many first-time customers as possible.

Unfortunately, they knew their existing bot protection had been unable to defend against waves of credential stuffing attacks targeting their customers. They anticipated a large attack during the event as the bots could hide their actions within the higher-than-normal number of login requests.

Crucially, the streaming service couldn't risk locking legitimate customers out as a byproduct of bot mitigations – restoring falsely blocked accounts is resource intensive, and the event might already be over by the time the issues were fixed. There was also the risk of large volumes of bots affecting the availability of the service and preventing people from watching the event – an outcome that simply could not be allowed to happen.



The Solution

Netacea protected the platform against credential stuffing and fake account creation with AI-powered bot protection, analyzing every single login and registration request worldwide across all websites, apps and APIs.

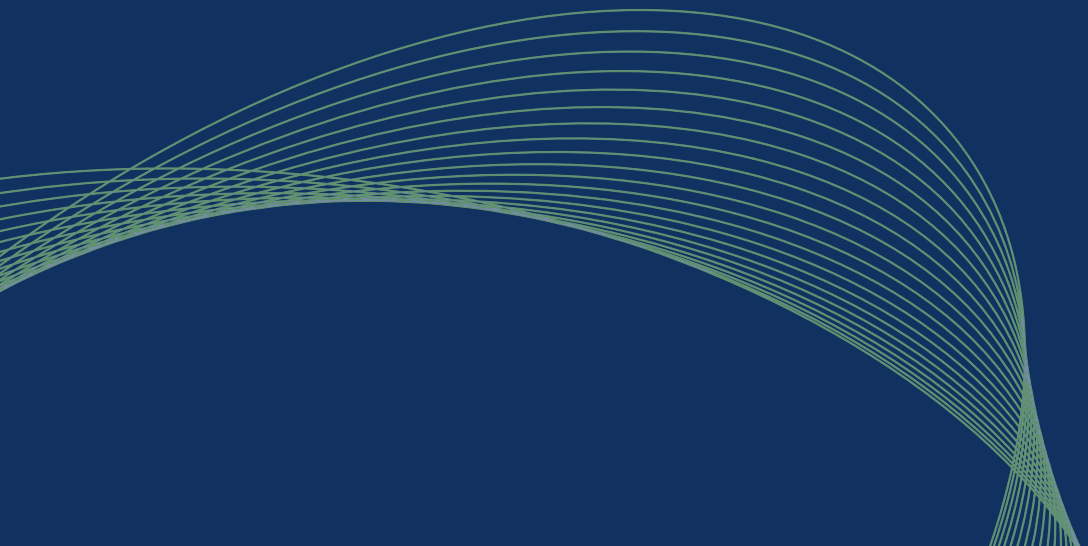
Unlike tools that rely on client-side integrations, which are complex to deploy across multiple platforms, simple to bypass and inadequate for protecting APIs, Netacea plugged straight into the customer's CDN to analyze server logs using specifically tuned machine learning models. This allowed us to analyze millions of requests concurrently and block sophisticated attacks with confidence in real-time.

The Outcome

During the lead-up, the game itself, and its aftermath, Netacea Bot Protection automatically blocked five million malicious requests attempting to access accounts or register new ones. Our solution added no latency, and no false positives were reported meaning that genuine customers were unaffected by our highly accurate mitigations.

Around 35% of all requests to the authentication API were malicious bots, with over a million disguised as requests from Xbox consoles. Inadequate protection from solutions unable to monitor APIs natively could have allowed criminals to steal 1,000 accounts.

Instead, Netacea Bot Protection allowed the streaming service to focus on serving real users during the live event without need for manual interventions from the security or infrastructure teams.



CONCLUSION

With valuable assets like premium subscriptions and exclusive video content up for grabs, streaming services are a prime target for automated attacks.

These attacks can cause significant disruption to streaming service revenues, causing would-be customers to tune out and churning existing customers whose accounts are stolen and sold wholesale on the dark web, alongside their personal information.

Bots are also complex to stop and costly to investigate. Traditional security measures like WAFs and CDN based defenses aren't designed to protect against sophisticated threats such as credential stuffing and credit card cracking. Most specialist bot defenses also don't cover all endpoints routinely served by streaming services, such as API logins via consoles and smart TVs. Without this, bots attack relentlessly and succeed with impunity.

NEXT STEPS

Netacea Bot Protection is designed to detect and stop bots accessing the services and accounts of streaming platforms with minimal maintenance and intervention.

Netacea assesses billions of web requests daily, using machine learning tuned by bot experts to categorize and block bad bot traffic rapidly. Unlike other solutions, Netacea Bot Protection looks at the full context of every visitor collectively to group traffic by its intent. This makes it much harder for attackers to disguise their malicious activities and bypass detection.

Crucially, our server-side integration with major CDNs and WAFs means that we can natively protect every access point available to bots. Netacea can detect bot traffic from any source of web traffic, including every app version or device type your customers use to log in and access content.

We also look outside of customer network traffic to see the bigger picture. Our highly regarded threat research team monitors over 3,000 illicit communities, collecting exclusive insights on attacker groups, the tools they use, who they are targeting and what they are selling, including stolen streaming accounts.

This gives Netacea the unique capability of protecting streaming sites from both high volume and low and slow bot attacks, with no disruption to genuine customers thanks to an industry-leading 0.001% typical false positive rate.

GET A DEMO OF NETACEA BOT PROTECTION

Visit **www.netacea.com/book-a-demo** to see how we could protect your streaming business from malicious bots.

NETACEA