kasada

Account Takeover Attack Trends

2025

Executive Summary

Account takeover (ATO) attacks have reached a critical inflection point. In 2024, ATO incidents surged by 250%, largely due to seasonal traffic spikes and strategic credential stuffing campaigns. Attackers retooled their methods faster than security defenses adapted, rendering traditional bot mitigation solutions ineffective.

Kasada's infiltration of 22 credential stuffing groups provided an unprecedented view into how adversaries industrialize credential abuse, with 1,027 major organizations targeted in coordinated attacks.

External research confirms the severity of stolen credentials in data breaches. Verizon's DBIR found that 31% of all breaches over the past 10 years involved stolen credentials. In addition, it takes organizations over 6 months (194 days on average) to detect a data breach.

For security and fraud leaders, these findings highlight an urgent need to rethink ATO defenses, focusing on proactive threat intelligence, continuous monitoring, and adaptive bot and fraud prevention.

Key Findings

250%
Increase in ATO Attacks

6.2 M
Accounts Compromised

85%
Had Bot Detection

Kasada observed a 250% increase in account takeover attacks in 2024. These attacks resulted in over 6 million compromised accounts, affecting large brands across several industries including retail, hospitality, travel, entertainment, and food and beverage.

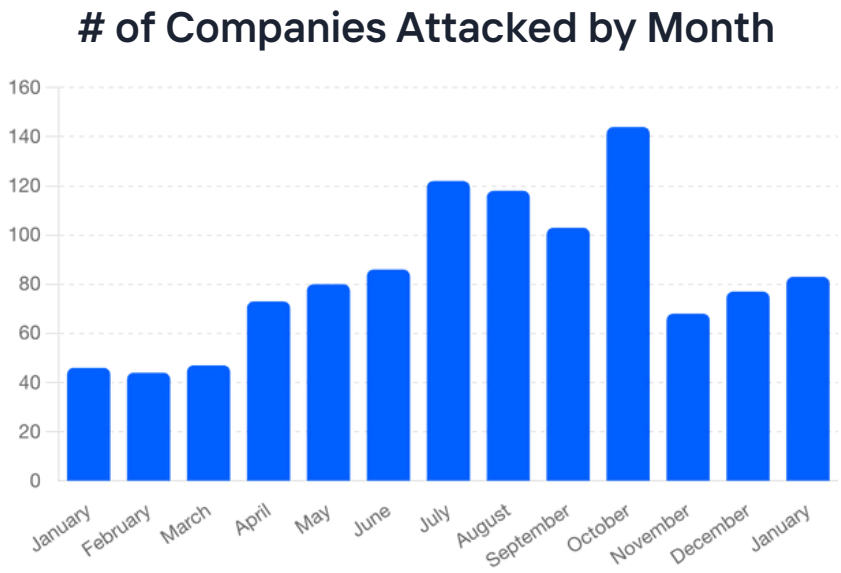
Despite 85% of targeted companies employing some form of bot detection, attackers continue to evade these defenses using sophisticated tools that bypass traditional systems.

TREND #1: ATO ATTACKS SURGE DURING SEASONAL TRAFFIC SPIKES

250% Increase in Account Takeover

Credential stuffing and account takeover attacks grew by 250% in 2024, with notable spikes during high-traffic periods.

Adversaries strategically align their attacks with peak login activity, exploiting seasonal traffic surges and promotional events to maximize success rates. This trend is expected to continue in 2025.

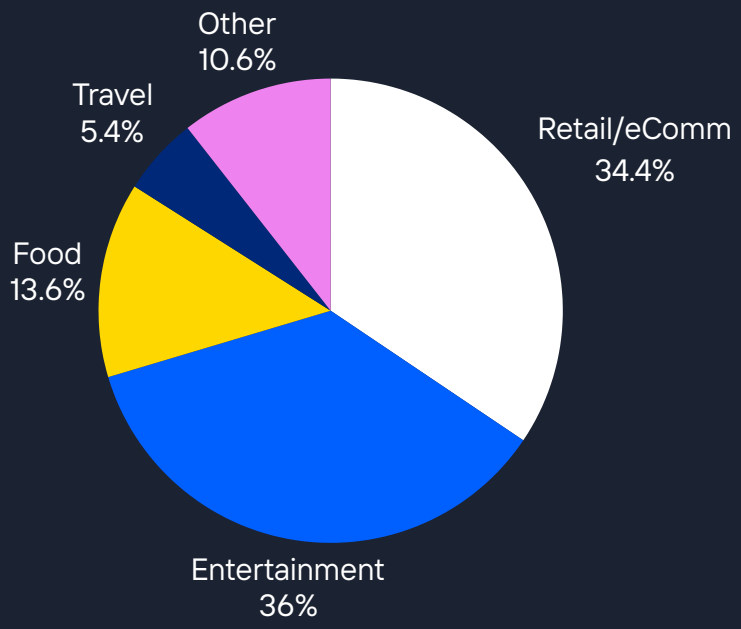


TREND #2: CREDENTIAL STUFFING ATTACKS ARE HIGHLY TARGETED

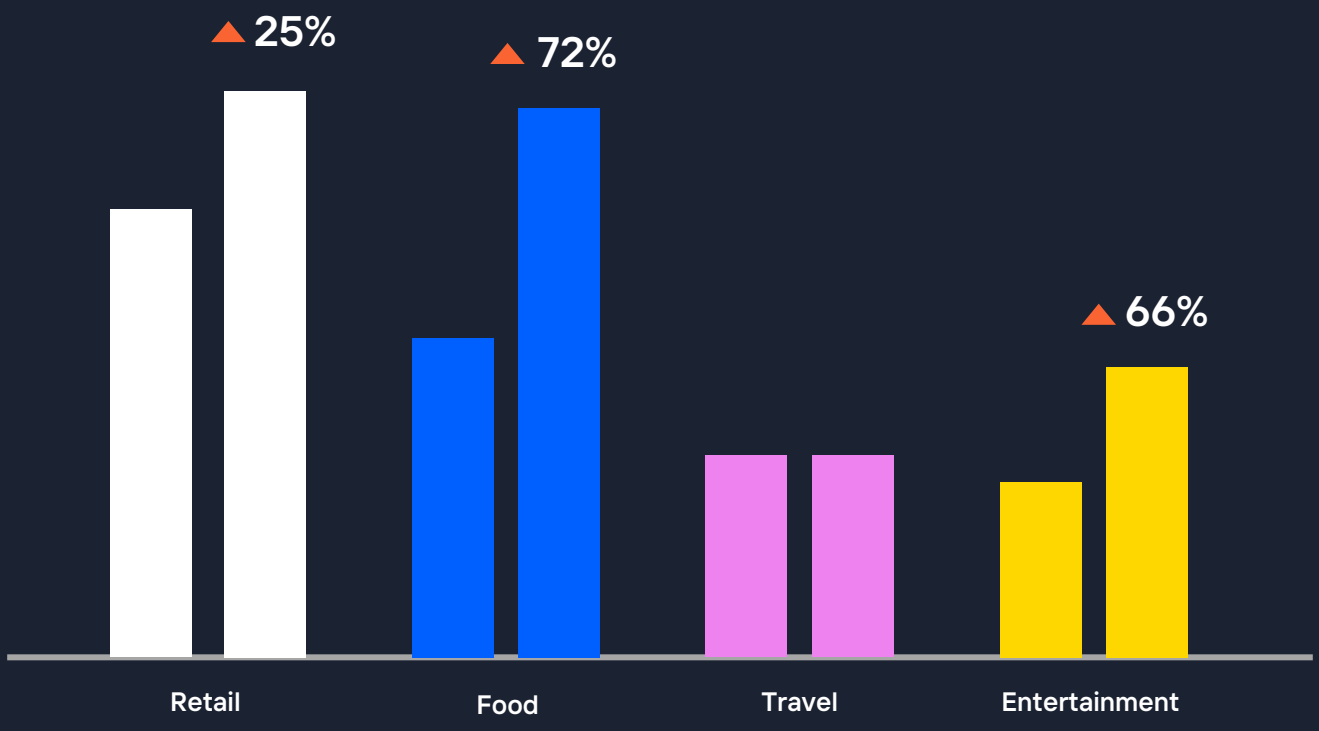
1,000+ Large Brands Targeted

The 22 credential stuffing crews we infiltrated targeted a total of 1,027 large organizations, compromising 6.2 million customer accounts.

While credential stuffing poses a cross-industry threat, certain sectors face higher attack volumes due to the high value of customer accounts, including loyalty and rewards programs, stored payment methods, and sensitive personal data.



- Retail & eCommerce: 20% of the NRF Top 100 Retailers were compromised in this campaign, with attackers targeting stored payment details, gift cards, loyalty points, and promotions.
- Restaurants & Dining: The surge in online ordering has exposed vulnerabilities in stored payment data, digital coupons, and rewards programs, making them prime targets for automated fraud.
- Travel & Hospitality: 40% of the Top 10 U.S. hotel brands suffered account takeover attacks, driven by seasonal booking spikes and the value of travel rewards and personal data, making this sector a major fraud target.

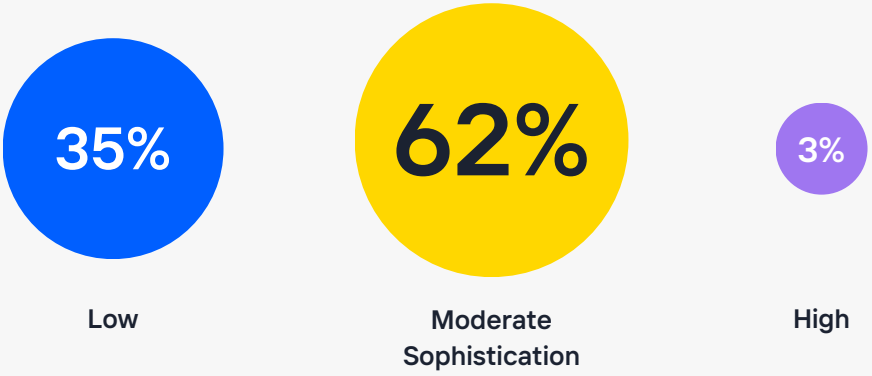


TREND #3: ATTACKERS RETOOL TO BYPASS SECURITY CONTROLS

65% of ATO Attacks are Sophisticated

Attackers are no longer relying on brute-force credential stuffing – they are customizing attacks in real-time to bypass bot mitigation.

When launching account takeover attacks, threat actors use advanced tooling like OpenBullet, which allows adversaries to configure custom scripts that evade common defenses with minimal effort.



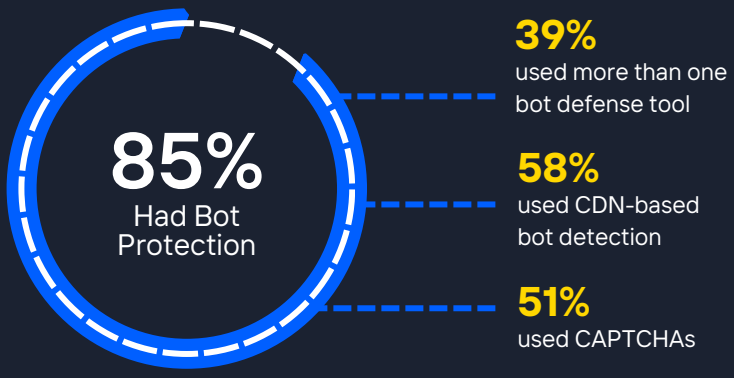
Common Evasion Tactics

BOT DETECTION BYPASS	Occurs when adversaries use automated tools called "solver services" to evade bot mitigation entirely to launch attacks.
CAPTCHA BYPASS	Enables attackers to automatically solve CAPTCHAs, enabling them to swiftly carry out attacks undetected.
PROXY ROTATION	Allows threat actors to rotate IP addresses, maintaining anonymity and avoiding detection by IP-based defenses.

TREND #4: TRADITIONAL BOT MANAGEMENT IS INEFFECTIVE

85% of Breached Brands Had Bot Detection

85% of compromised companies had bot detection in place, yet attackers successfully bypassed these defenses using common evasion tactics.



Why it Matters: Consequences of Credential Stuffing and ATO

Impact for Brands

The financial and reputational costs of credential stuffing are significant. Compromised customer accounts lead to:

FINANCIAL FRAUD	Attackers exploit accounts to make unauthorized purchases, withdraw or transfer funds, steal loyalty points, and commit fraud.
OPERATIONAL STRAIN	Businesses must allocate resources to customer support, call centers, incident management, and more following an account takeover attack, often resulting in downtime or reduced quality in their customer service.
REGULATORY RISKS	Companies may face fines and legal repercussions for failing to protect customer accounts, especially if personally identifiable information (PII) is compromised.

Impact for Consumers

Credential stuffing and account takoever attacks lead to:

- Consumer Security and Privacy Risks: Stolen personal information, loyalty points, unauthorized transactions, and identity theft, jeopardizing consumers' financial security and privacy.
- Consumer Loss of Trust: The hassle of resolving fraud and recovering compromised accounts negatively impacts the customer experience.

Strategic Recommendations

To effectively counter credential stuffing and account takeover, companies should adopt a proactive, multi-layered approach.

Here are key actions to take:

1. SHIFT LEFT IN YOUR SECURITY PRACTICES	Detect and prevent account takeover by monitoring key signals like increased login failures, unusual geographic access, and spikes in login attempts. These indicators of credential stuffing must be addressed early in the attack chain to effectively safeguard customer accounts.
2. STAY UPDATED ON ADVERSARY TRENDS	Keep an eye on underground markets and threat intelligence sources for new attack methods and tools. Use these insights from adversary trends to adjust defenses and make it harder for attackers to succeed.
3. INTEGRATE SIGNALS ACROSS DEPARTMENTS	Cross-functional collaboration allows for quicker detection and response to ATO attempts. Security may own authentication, loyalty might handle browsing data, and commercial teams manage redemptions. Many organizations discover valuable, previously overlooked signals that enhance security when they integrate data across departments. Break down silos and collaborate with other teams to combine these insights and provide a comprehensive view of the threats you face.
4. MAKE THE ADVERSARY'S JOB MORE DIFFICULT	Static, rule-based bot defenses are outdated and insufficient. To counter advanced tools like OpenBullet, organizations need adaptive bot defenses that can detect and dynamically respond to automated attacks, effectively disrupting advanced adversarial tactics and techniques.

Conclusion

The 2025 Account Takeover Attack Trends report highlights a stark reality: attackers are more collaborative and persistent, and the stakes for businesses have never been higher.

As credential stuffing and ATO attacks continue to escalate this year and beyond, companies cannot afford to rely on traditional security measures alone.

Good bot defense is the bedrock of successful fraud prevention, as it blocks the automated attacks that lead to fraud downstream. By prioritizing advanced threat intelligence, monitoring for emerging attack vectors, and breaking down internal silos, companies can safeguard their customer accounts and maintain trust.

The future may bring heightened challenges, but with the right strategies in place, businesses can protect their customers, their reputation, and their bottom line.

For more insights on defending your organization against credential stuffing and account takeover, visit kasada.io to explore our latest resources on how you can achieve robust bot defense and fraud prevention.

See how Kasada defeats automated threats by understanding the human minds behind them.

Learn more

Kasada Bot Defense

Invisible, resilient defenses keep your site safe from bot attacks and automated fraud.

KasadaIQ for Fraud

A fraud prevention service that gives you early warning signs of abuse with actionable insights and dedicated analysts.

About Kasada

Kasada has developed a radical approach to defeating automated cyber threats based on its unmatched understanding of the human minds behind them. The Kasada platform overcomes the shortcomings of traditional bot management to provide immediate and enduring protection for web, mobile, and API channels. Its invisible, dynamic defenses provide a seamless user experience and eliminate the need for ineffective, annoying CAPTCHAs. Our team handles the bots so clients have freedom to focus on growing their businesses, not defending it. Kasada is based in New York and Sydney, with hubs in Melbourne, Boston, and San Francisco.

kasada

For more information, please visit our site.

See More