CEQUENCE

RETAILERS!
FRAUD IS UP NEARLY
700%

2023 Holiday Season API Security Report

Retail cybercriminals have graduated from quick, unsophisticated smash and grab-style attacks to playing the long game, spreading attacks out over the course of the year in preparation for a holiday season bonanza. Organizations now must extend their holiday vigilance throughout the year.

DOWNLOAD NOW

The State of Threats and Bot Management Today

The data below are based on six months of anonymized traffic across all Cequence customers from June through November 2023.

Malicious traffic came from **719M** unique IP addresses

Out of **154B** requests...

19B were confirmed malicious requests — **12%**

22B were automated (bot) requests — **14%**

216M requests were blocked in a single day

325M account takeover attempts

ATOs remain one of the main tactics for adversaries, increasing more than 50% from the previous six-month period.

148M different user agents observed

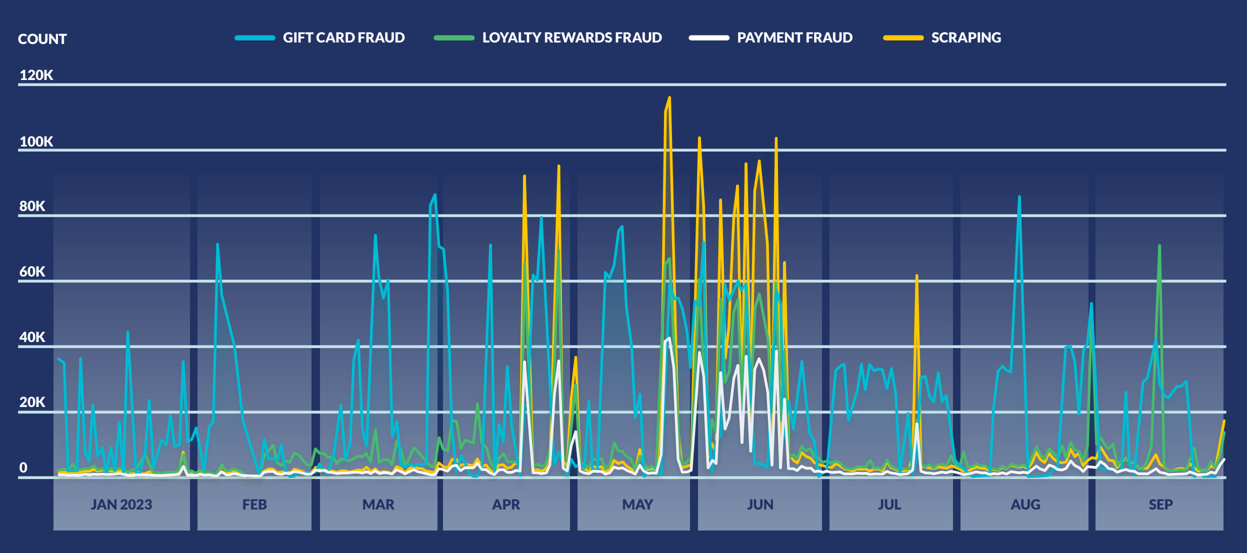
Attackers Lay Groundwork Ahead of Retailers' Security Lockdown

In 2023, Cequence noticed that attacks other than standard gift card fraud occured at high volume starting early in the year. Since retailers are well known to lock down their networks during the holiday season as well as the fact that "Black Friday" can comprise a month's worth of promotions for some retailers, the data suggest that attackers are laying the groundwork for their holiday attacks well in advance of the holidays.

700%

Growth in Scraping, Loyalty Card, and Payment Card Fraud
in the second half of 2023

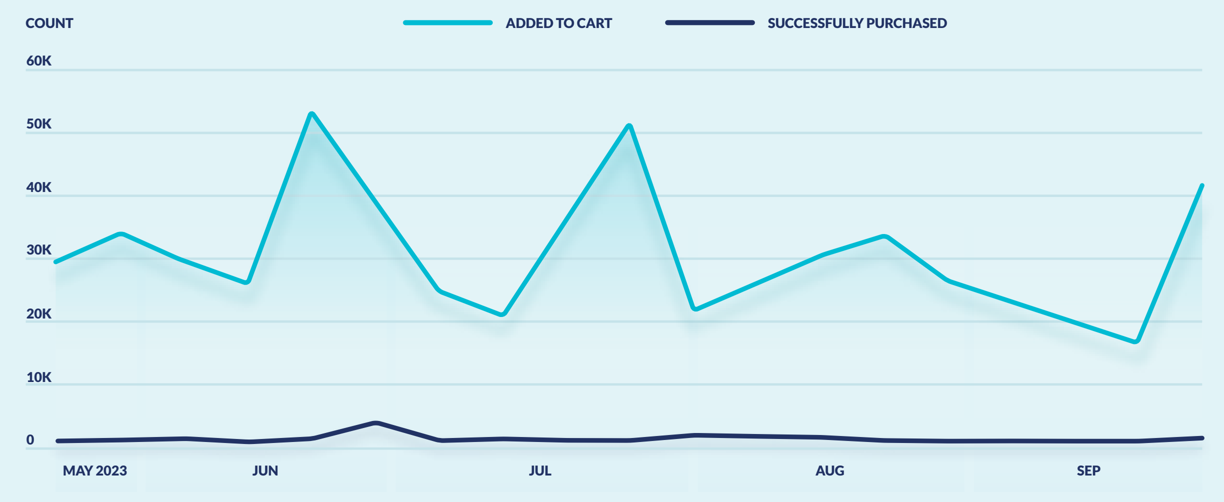
Types of Fraud Attempts Change Depending on Time of Year



Combatting the Surge of Automated Line-Jumpers in High-Demand Retail Drops

From Taylor Swift tickets to the latest sneakers, limited availability sales are a frequent target for cyber-criminals. This year, Cequence observed large numbers of products added to carts, but few comparative purchases as the fraudsters were identified and prevented from purchasing. Add-to-cart spikes are correlated with product launches, as attackers attempt to monopolize limited-availability items.

Number of Items Added to Cart vs. Purchased



The Rising Threat of Influencer Account Takeovers

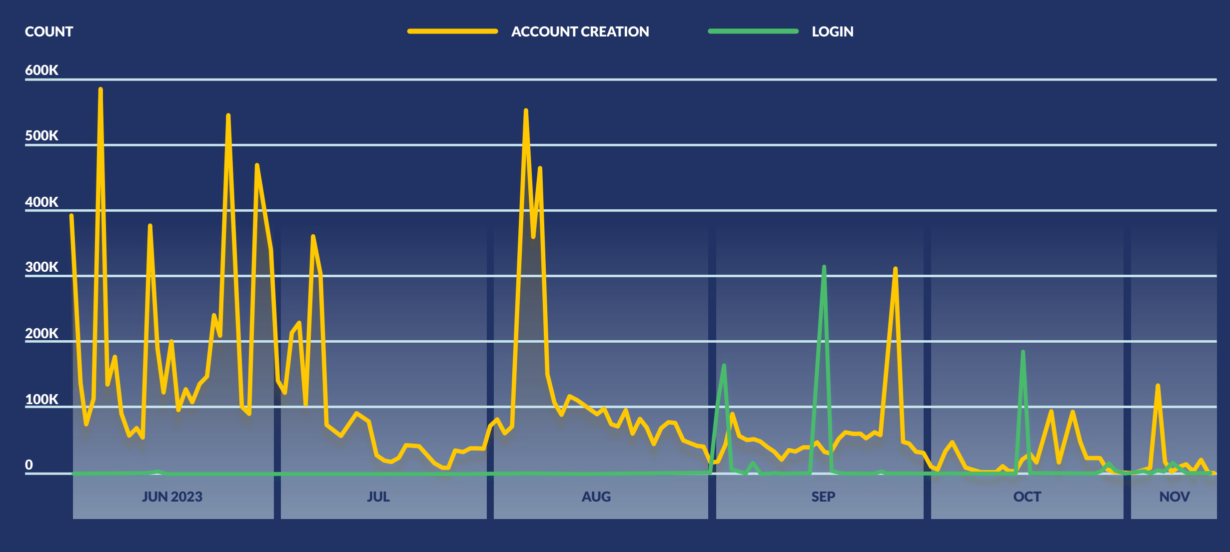
Social commerce retailers combine ecommerce with social media, leveraging user contributions to build community. Attackers are taking advantage and creating high volumes of valid accounts via standard APIs earlier in the year. The attacker's automated tools enable them to create accounts and generate likes and subscribes to increase influence – but much faster and at a larger scale than legitimate humans could, crowding out the sales of legitimate users.

410x

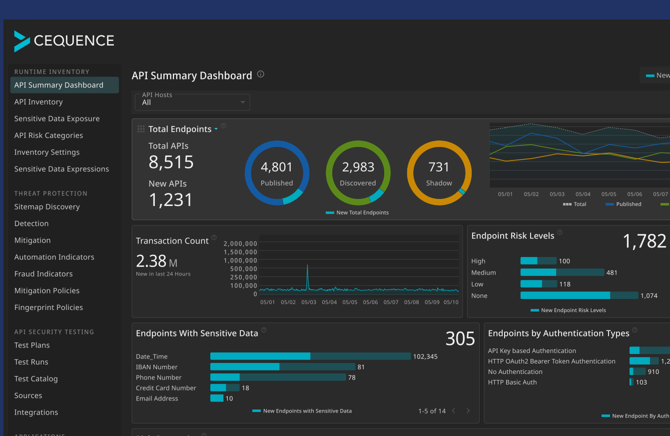
Growth in Account Take Overs
and 50% growth compared to the previous 6 months

Fraudulent account creation attempts declined nearing the holidays, while basic account takeover tactics rose. While fraudulent account creation dropped 72% from the first half to the second half of the time period, account takeovers (ATOs) increased a staggering 410 times! This is due to the attacker changing tactics to those that require less runway and planning, like ATOs.

Types of Fraud Attempts Are Concentrated at Different Times of the Year



API attacks contine to evolve, with new tactics and techniques designed to evade improving defenses. To protect against API threats like these, organizations need to adopt a comprehensive approach to their API security. They must discover and inventory all their APIs, ensure they're in compliance with API specifications, and then identify and block attacks as they happen. Cequence can be your partner throughout the API security lifecycle and help protect your organization from existing and emerging threats.



Try a free API security assessment today:

www.cequence.ai/assessment/

CEQUENCE

100 S Murphy Avenue, Suite 300, Sunnyvale, CA 94086 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai

Cequence-HolidayThreatReportInfographic-20240116