CEQUENCE

2023 Holiday Season API Security Report

Cybercriminals Play the Long Game Against Retail Businesses

Introduction

Cybercrime has often been akin to physical "smash and grab" crime. Simple and straightforward crimes of opportunity that go after low-hanging fruit and deliver criminals immediate gratification. But now, they're changing up their game, investing the time and energy to be more subtle, spreading out attacks over longer periods of time to appear more legitimate and fly under the radar. This report uses the online retail industry as an example to examine this shift in behavior.

The months prior to the 2023 holidays demonstrated a change in tactics, techniques, and procedures by adversaries against prominent retailers. Attackers have shown that they are highly sophisticated and have great persistence and depth of planning. In this report, we'll dive into three major retail areas and the types of attacks they've seen leading up to the 2023 holiday season.

Application Programming Interfaces (APIs) are the communication foundation for today's infrastructure, from web apps to the cloud, making them top targets for bad actors. Organizations now need to protect APIs as well as their applications, a challenge made more difficult by the fact that APIs are designed to be used via automation. Today's cybercriminals are taking advantage of that automation, as we'll see in this report.

Methodology

The data in this report was compiled by the Cequence CQ Prime Threat Research Team which employs machine learning (ML) models and threat prediction workflows to detect and mitigate API security threats for the world's most attacked organizations comprising Fortune and Global 2000 companies. The report is sourced from the Cequence API threat intelligence database comprised of real attack data from anonymized customer production environments and is sampled from billions of transactions.

As attackers continue to gain knowledge and increase their capabilities, it is increasingly imperative to not only create and maintain a large threat intelligence database with years of data but also have an experienced team with which to interpret it. Cequence has the largest API threat intelligence database in the world and the CQ Prime Threat Research Team of API security experts and data scientists, a unique combination of resources that enables Cequence customers to stay ahead of attackers' evolving tactics.

This report focuses on Cequence Security retail industry customers in the months leading up to the 2023 holiday season. The CQ Prime team identified and categorized active threats, and the resulting threat intelligence is a foundational element of Cequence products that enable mitigation and blocking to protect customers' businesses. In the following stories, the attacks described were all mitigated or blocked by Cequence.

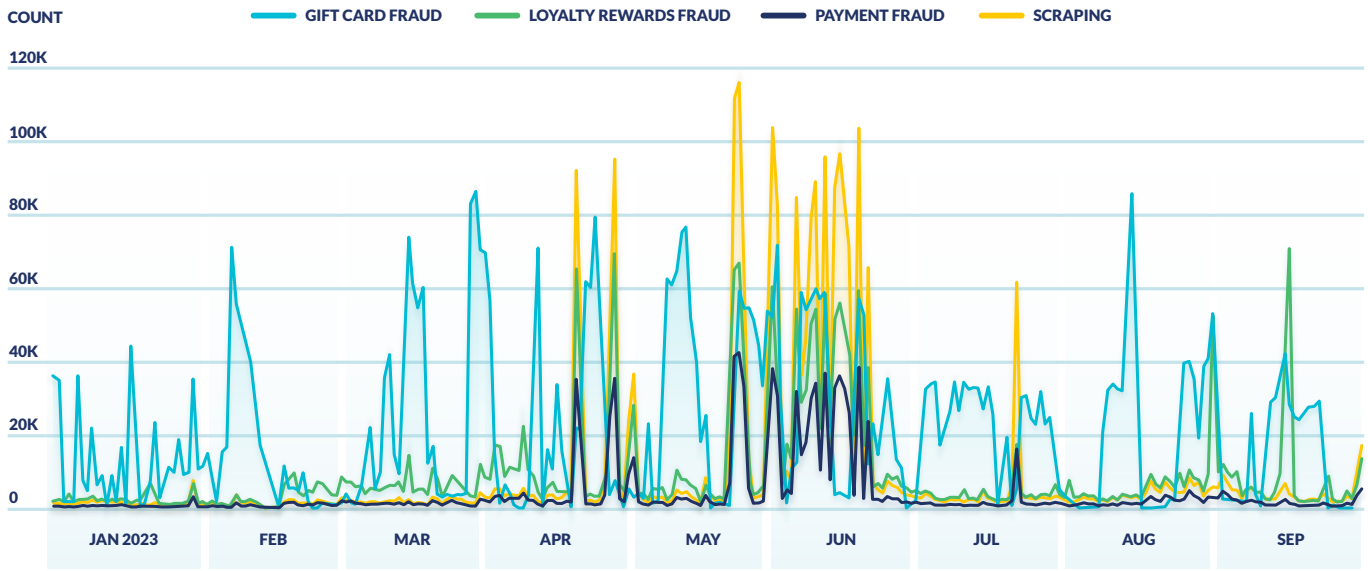
Table of Contents

Pre-Holiday Cyber Onslaught: Attackers Lay Groundwork Ahead of Retailers' Security Lockdown

Our first threat deep dive spotlights large consumer home and body product retailers. These types of companies typically experience a steady drumbeat of attacks related to gift card fraud, where attackers use botnets to perform brute force attacks on gift card websites, automatically testing large volumes of card and PIN numbers. Upon finding a successful card/PIN combination, they can drain the gift card of funds. Gift card fraud attacks happen fairly consistently throughout the year, with spikes around the time of various promotions.

However, in 2023 they have seen other types of attacks dramatically increase early in the second half of the year, well ahead of the holiday season. Many companies, and retailers in particular, take the holiday season as their cue to focus more on security, and begin to really lock down their networks and applications. The data suggests that sophisticated attackers began their "attack runs" earlier in the year to lay the groundwork for holiday sales to try and avoid the retailers' security lockdowns as much as possible.

Types of Fraud Attempts Change Depending on Time of Year



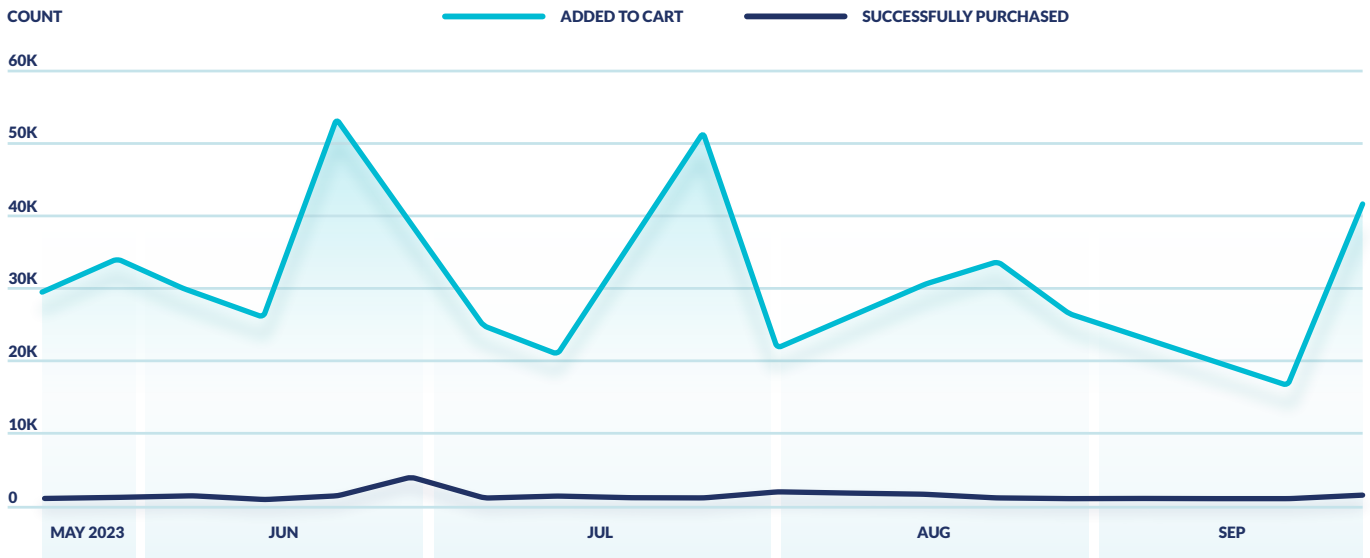
In the second half of the year, these companies noticed several types of attacks unrelated to gift card fraud happening in unison, as shown in the graph. While gift card fraud increased by 110% in the second half of the time period, scraping, loyalty card fraud, and payment card fraud increased by a collective average of over 700%. These types of attacks are correlated and spiked together because those parts of the website, applications, and associated APIs are related, especially as they pertain to attacks. This insight shows that these retailers were not experiencing simple brute force-style attacks in isolation, but sophisticated attacks from adversaries displaying highly varied tactics, techniques, and procedures.

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

Whether it's Taylor Swift concert tickets or the latest hot sneaker drops, bots are a massive problem for fans and retailers alike. The practice of using bots to "jump the line" is so pervasive and widespread that there are detailed explanatory Reddit threads, answers to Quora questions, and even readily available how-tos and "top bots" articles online.

Large sports and clothing retail companies around the world experience a common, repetitive problem during product launches such as sneaker drops. Attackers use automated tooling to volumetrically flood the system, adding large numbers of sneakers or other products to their cart in order to try and purchase as many in-demand items – either on sale or of limited availability – as possible, effectively cornering the market and preventing sales to legitimate customers. Additionally, successful attackers can then sell these items elsewhere at a high markup, adding to customer frustration.

Number of Items Added to Cart vs. Purchased



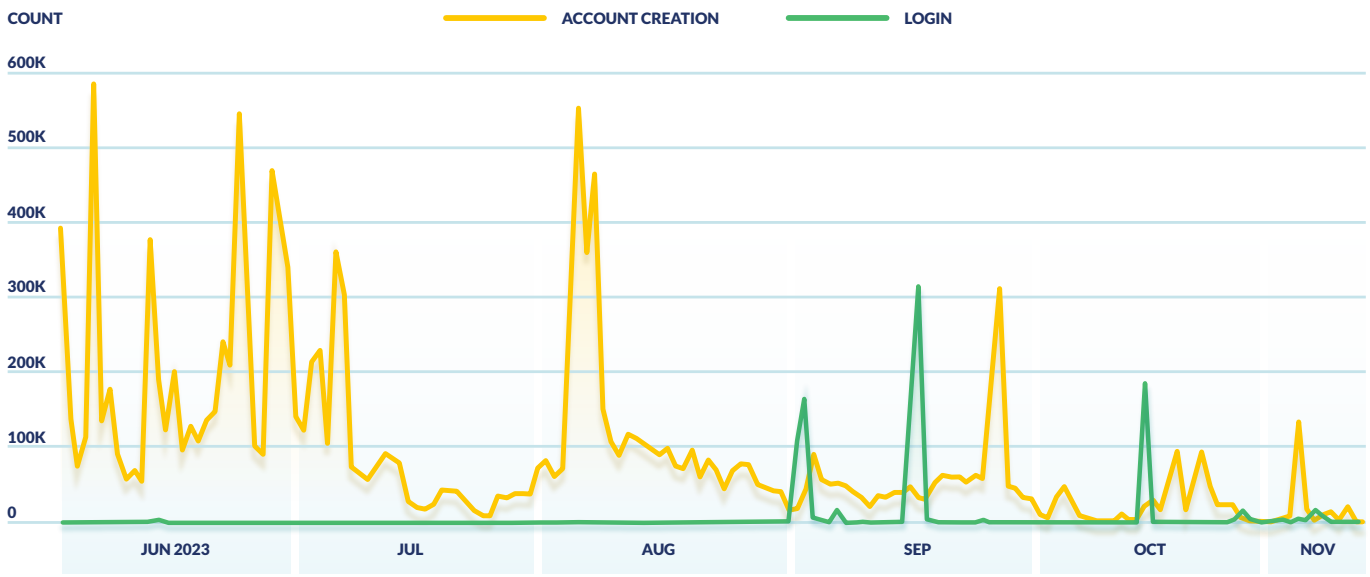
The data shows that large numbers of products were added to carts, but very few comparative purchases as the fraudsters were identified and blocked from making their purchases. Add-to-cart spikes are correlated with product launches, as attackers attempt to monopolize limited-availability items. While these drops or flash sales happen periodically over the course of the year, the frequency typically increases around the holidays.

Playing the Long Game: The Rising Threat of Trust-Building Account Takeovers

This threat example is another that employs the "long game" of low and slow attacks over time. "Social commerce" retailers combine ecommerce with social media, leveraging user contributions to build community. Most online retailers encounter attacks that employ standard well-known account takeover (ATO) tactics that peak during the holidays. ATO is an attack on legitimate existing online customer accounts, where criminals take ownership of the accounts for their own nefarious purposes. However, social commerce companies often see a different type of attack well before the holiday season begins.

In this example, attackers attempted to create high volumes of valid accounts via standard APIs earlier in the year, hoping to use the time to build trust and cred in the market to increase social sharing and extend their reach, increasing the visibility of the products they're selling over others'. The attackers tooling and automation enables them to perform regular user operations such as account creation, likes, subscribes, and communication with other accounts to increase influence – but much faster and at a larger scale than legitimate humans could. This has the effect of crowding out legitimate users and impugning the integrity of the company and its marketplace. This type of attack shows the high level of planning and persistence that goes into modern retail attacks.

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



Interestingly, fraudulent account creation attempts often decline towards the holidays, while basic account takeover tactics begin to rise. While fraudulent account creation dropped 72% from the first half of the time period, account takeovers (ATOs) increased a staggering 410 times in the second half! Given the short runway before the holidays and the amount of time it takes to build influence for each account, at this point it's more advantageous for the attacker to take over established accounts than create new ones. These basic account takeover attempts occur throughout the year but really pick up steam in the second half of the year.

The Current API Threat Landscape

Cequence is in a unique position to report on real customer traffic across a large number of customers, industries, and geographies comprising Fortune and Global 2000 companies. The CQ Prime Threat Research Team and Cequence's unique API threat intelligence database enables us to learn a great deal about the types and scale of today's attacks with historical context. The data points below are based on six months of traffic across all Cequence customers from June through November 2023.

719 million

Malicious traffic came from 719 million unique IP addresses.

154 billion requests

Of 154 billion requests, 22 billion (14%) were automated (bot) requests and 19 billion (12%) were confirmed malicious requests.

While these percentages may seem low compared to some seen in the news, they are predicated on the scope of traffic the numbers are sampled from. Cequence typically processes all API traffic for its customers, so the breadth of traffic is much larger than products that only examine login traffic to a particular instrumented web app, for example.

216 million

The highest number of blocked requests in a single day was 216 million.

325 million

There were 325 million malicious login or ATO attempts.

148 million

More than 148 million different browser types (user agents) were observed.

A relatively small percentage can be accounted for by operating system, device, and browser combinations – the overwhelming majority of the number represents attackers generating massive numbers of unique browser user agents as part of their schemes.

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

API Security is a Key Element of a Successful Security Strategy

Cequence is the only vendor offering a comprehensive Unified API Protection platform offering discovery, compliance, and protection across all internal and external APIs. The platform secures more than 8 billion daily API calls and protects more than 3 billion user accounts across its customer base, including Fortune and Global 2000 businesses. Customers can start with a single product or the whole platform and deploy it however they like – on-premises, SaaS, or hybrid.

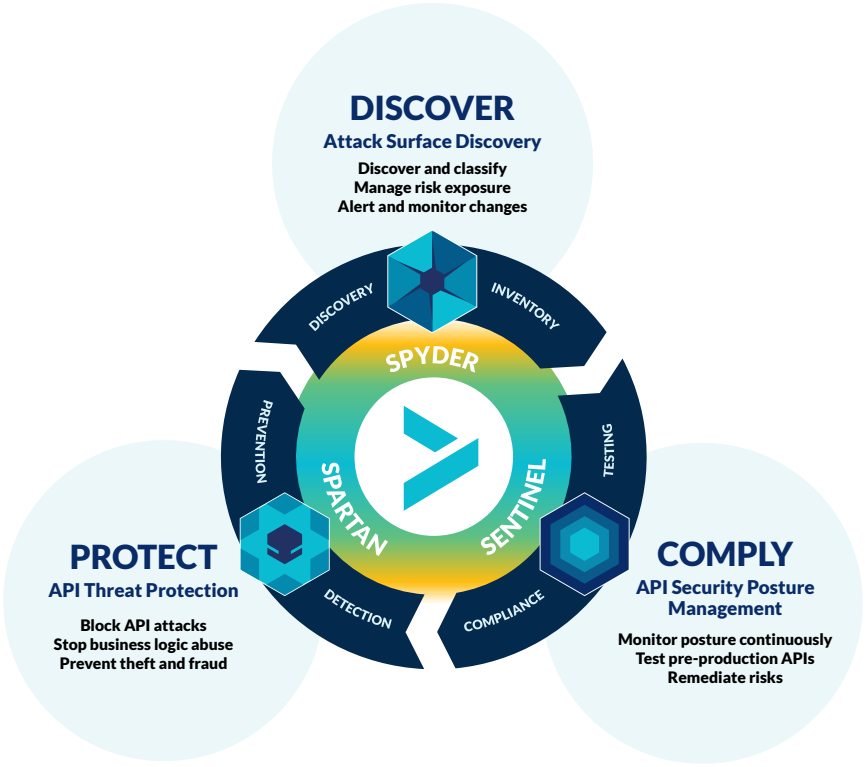
The Cequence Unified API Protection (UAP) platform is the only API security offering that addresses all phases of the API protection lifecycle – discovering the entire API attack surface, eliminating unknown and unmitigated API security risks, and natively protecting APIs from cyber attacks that lead to data loss, fraud, and business disruption.

DISCOVER
Identify all internal and external APIs, including known and unknown APIs, providing complete visibility into the API attack surface of an organization.

COMPLY
Ensure that APIs comply with API specifications, security test requirements, and governance best practices.

PROTECT
Detect and block API threats that target API applications, in real time, with minimal false positives.

The Cequence UAP platform is supported by the globally distributed CQ Prime Threat Research Team of data scientists and cybersecurity experts that provide our customers with supplementary assistance ranging from ongoing research to fully managed threat detection and response.



Conclusions and Recommendations

This year's lead up to the 2023 holidays unveiled some unique tactics, techniques, and procedures used by attackers against large, global retailers. The data shows that adversaries will plan well in advance with the knowledge that systems will be locked down during the holidays becoming much harder to penetrate. Also apparent is the brute force tactics utilized to try and corner the market around flash sale items. And they play the long game, busily working well in advance of the holiday season to be prepared to take maximum advantage of unprepared retailers and unsuspecting customers.

To protect against these kinds of threats and many others, it's critical for companies to adopt a comprehensive approach to API security that focuses on the entire API security lifecycle. 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 help throughout the API security lifecycle and ensure your organization is protected from both existing and emerging threats.