TLP: CLEAR

2025 HOLIDAY SEASON CYBER THREAT TRENDS

RETAIL & HOSPITALITY ISAC

Introduction

For the retail, hospitality, and travel community, the holiday season is the most intense time of year for consumers and cybersecurity professionals facing persistent threats. From the beginning of October through the end of December, cyber threats to organizations expand in both scale and intensity to match the rise in consumer traffic.

Current threat trends facing the RH-ISAC membership community includes activity related to The Com threat cluster, fraud, ransomware, and fake remote IT worker scams. While these threats are all likely to continue in prevalence for the 2025 holiday period, fraud stands out as the threat category that is most likely to expand specifically in conjunction with the increased shopping activity associated with the final quarter of the year, as has been the case in recent years. The types of fraud most likely to spike, considering historic trends, include receipt fraud, return fraud, refund fraud, bot-facilitated inventory depletion, points fraud, and loyalty fraud.

In order to examine the threat landscape facing the retail, hospitality and travel industries during the holiday season, the Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) developed this report in three parts:

Expert Perspectives: Key subject matter experts from leading RH-ISAC member organizations provide their insights into their current defensive preparations.

Threat Landscape: RH-ISAC data examines the threat trends reported by the member community for previous holiday seasons from a historical and analytical perspective.

Threat Trend Analysis: Insights about top threat trends for the holiday season, including what fraudsters want and methods they use to get it as reported by Kasada, an RH-ISAC Associate Member.

EXPERT PERSPECTIVES

RH-ISAC reached out to several key member analysts with specific expertise in fraud prevention who are currently implementing their organization's holiday season security measures. Each of these analysts was asked the following series of questions:

- What are your primary threat focuses this season and why?
- Have you observed any notable changes in the threat landscape this year from previous years?
- How is your organization preparing to handle a cybersecurity event during peak shopping days (e.g., Black Friday, Cyber Monday)?
- Are you leveraging AI-driven or automated tools to detect anomalous activity during high-traffic periods?

Q: What are your primary threat focuses this coming holiday season and why?

A: Account takeover, fraud, third-party risks, and malicious bot activity remain primary threat focuses.

Q: Have you observed any notable changes in the threat landscape this year from previous years?

A: Significant spikes in third party data extortion events, exploit development, and refund fraud activity are prevalent emerging trends as the holiday season for 2025 begins.

Q: How is your organization preparing to handle a cybersecurity event during peak shopping days (e.g., Black Friday, Cyber Monday)?

A: Common preparations include organization-wide cyber awareness campaigns, incident response plan reviews, and tabletop exercises.

Q: Are you leveraging AI-driven or automated tools to detect anomalous activity during high-traffic periods?

A: Members report finding AI and automation tools beneficial in detections for high-traffic times, with either widespread or limited deployments.

THREAT LANDSCAPE

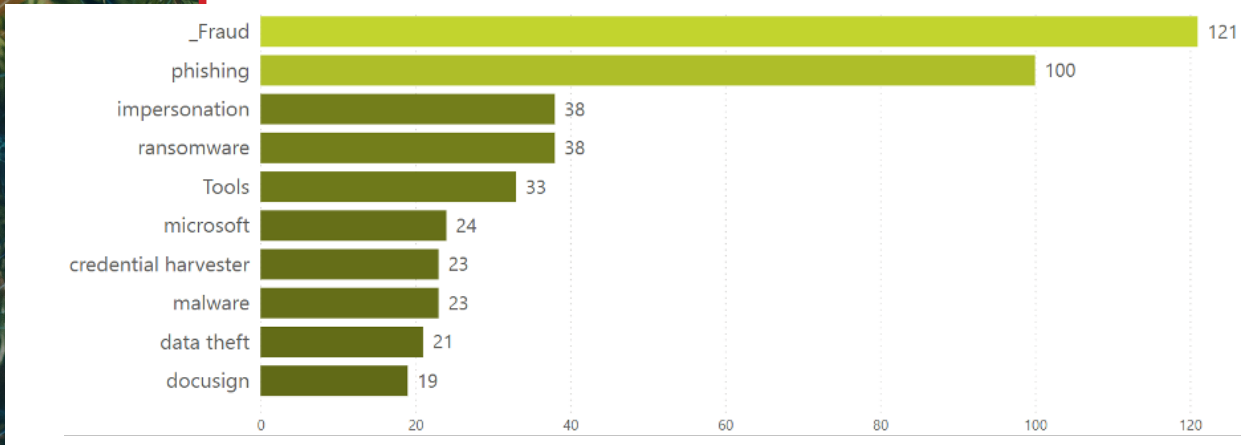
In order to establish the most likely trends in cybersecurity topics and threats shared by the RH-ISAC membership across our sharing platforms, the RH-ISAC Intelligence Team and Research, Analytics, and Education Team examined the trend data for the holiday season period for the past two years, 2024 and 2023. This historical data was used in conjunction with current quarter trends to anticipate likely threat escalations for the coming quarter.

Historical Sharing Trends

Between the holiday seasons in 2024 and 2023, some key trends emerge:

For the 2024 holiday period, fraud reporting rose significantly and emerged as the most prevalent threat trend shared by members. This trend is likely to hold for 2025, given ongoing prevalence of fraud activity and the fraud opportunities that the holiday shopping season offers to threat actors.

For the 2023 holiday period, credential harvesting did not remain a key threat as predicted in the 2022 holiday report, while phishing and malware did remain prevalent. BlackCat's surge in 2023 reflects the increase in Scattered Spider activity, which was relatively obscure in 2022. As predicted in 2023, third-party vulnerabilities remained a key threat.



2024

2023

Holiday Season Threat Forecast

The RH-ISAC intelligence team anticipates that the key fraud trends for the 2025 holiday period will likely include:

- Continued escalation of extortion activity from threat actors claiming affiliation with The Com such as **ShinyHunters and Scattered Spider**
- A spike in **bot activity targeting high-demand items** on ecommerce platforms and targeting loyalty points for ecommerce, hospitality, and travel consumer accounts
- A spike in attempts at **account takeover and business email compromise** to further fraud activities such as payment information theft and invoice fraud
- A spike in **impersonating domains** aiming to steal customer PII and payment card data
- A spike in **holiday-branded, fraudulent ads** redirecting consumers to malicious websites
- An increase in **return fraud/abuse and "friendly fraud"/chargebacks** due to increased sales volumes

THREAT TREND ANALYSIS

RH-ISAC Associate Member Kasasa provided the following analysis for the 2025 Holiday season:

Since 2022, Kasada has consistently observed increased bad bot traffic during major sales events in the holiday period. The 2025 Holiday Period will likely be defined by an unprecedented scale of automation. With genAI traffic predicted to grow 520% in the 10 days leading up to Thanksgiving, the lines between good bot, bad bot and human will be significantly blurred. The boom in legitimate traffic and fraud during the 2025 Holiday Period creates additional challenges for staff on the floor, particularly in telling legitimate complaints and fraudulent claims apart.

Fraud Predictions for the 2025 Holiday Period

Malicious Configurations (Configs)

Key dates: November 17, 27, 28, and 29

Key industries: Retail, Accommodation

For the 2025 Holiday Period, Kasada IQ predicts that:

- Configs are pre-built scripts that contain all the settings and parameters necessary for launching an attack, like ATO. For the 2025 Holiday Period, Kasada IQ predicts that:
- Available configs will surge in the 2025 Holiday Period, particularly for accommodation and retail. Kasada IQ expects this surge will be more significant than the 2024 Holiday Period, noting significant increases in available configs for retail and accommodation throughout 2025.
- The 10 days prior to Thanksgiving and Black Friday will be a peak period for configs, with adversaries trying to get ahead of the major sales events to monetize their services.

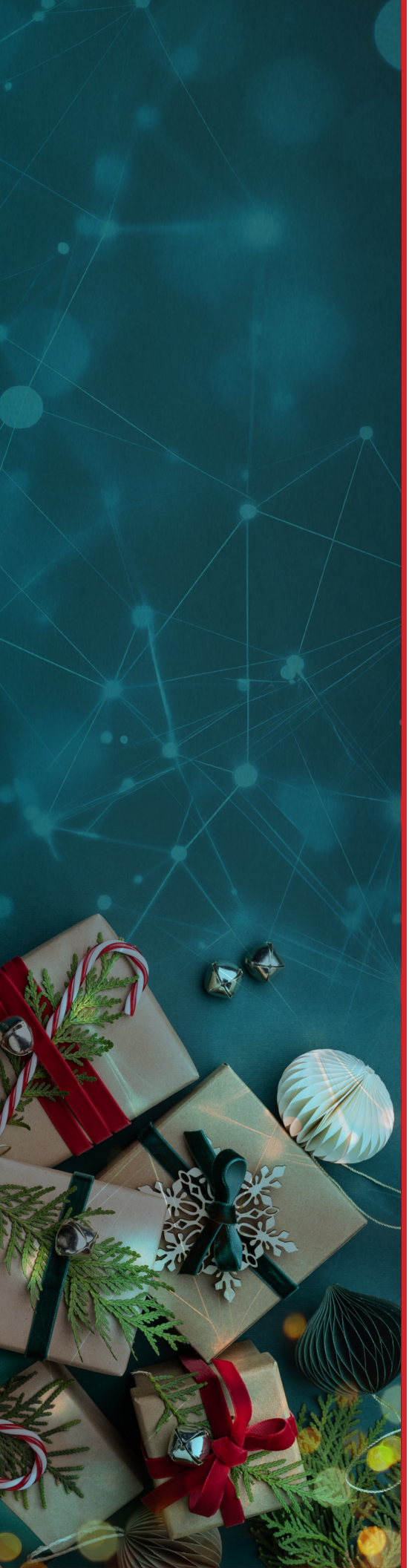
Account Takeover (ATO)

Key dates: November 23 - 29 & December 3, 9, 27

Key industries: Retail, Quick Service Restaurants (QSRs)

For the 2025 Holiday Period, Kasada IQ predicts that:

- ATO will surge, especially for retail. The surge is expected to be elevated compared to the 2024 Holiday Period due to adversary developments and AI adoption.
- The highest risk period for ATO will be the week prior to Black Friday, as adversaries secure account access for peak shopping days.
- ATO against QSRs will see a smaller rise, with the major spike occurring in the post-Christmas period.
- Retail staff will face additional challenges, particularly around fraud detection.



Gift Card Theft / Fraud

Key dates: November 17-28 & December 1-3, 13-21

Key industries: Retail, QSRs

For the 2025 Holiday Period, Kasada IQ predicts that:

- Gift card fraud will increase significantly in the 2025 Holiday Period, particularly in the retail industry, like the 2024 Holiday Period. Kasada IQ expects this to be on an elevated scale.
- For retail, gift card sales are expected to peak in the lead up and immediately after major sales events (Black Friday, Cyber Monday).
- QSR gift card sales are expected to spike throughout December, including Cyber Monday and stay elevated before dropping during Christmas.

Retail Bot Predictions

Key dates: November 17-29 & December 3, 9, 26, 27

Key industries: Retail

Retail bots are programmed to complete transactions faster than any human can. Adversaries use these bots to grab limited-edition items or bulk-buy discounted inventory, then resell it at face value or higher for profit.

For the 2025 Holiday Period, Kasada IQ predicts that:

- Fake account creation and scraping (as a precursor for retail bot activity) will increase from October.
- Peak bot activity will likely occur during the week prior to Thanksgiving and Black Friday and will continue at scale during major sales events.
- Bots are expected to target loyalty members and early access deals.
- Adversaries will engineer unwanted automation to maximise value across the entire Holiday Period, exploiting operational fatigue during the most chaotic weeks of the year.
- For the first time during a Holiday Period, traffic will be majority automated due to agentic AI. The scale of traffic will be unprecedented, with risks of excessive charges for traffic that do not convert to revenue.

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing sector-specific cybersecurity information and intelligence. The RH-ISAC connects information security teams at the strategic, operational, and tactical levels to work together on issues and challenges, share best practices and benchmark among each other – all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC serves all consumer-facing companies, including retailers, restaurants, hotels, gaming casinos, travel, food retailers, consumer products and other consumer-facing companies.

For more information, visit www.rhisac.org.

RETAIL & HOSPITALITY ISAC