



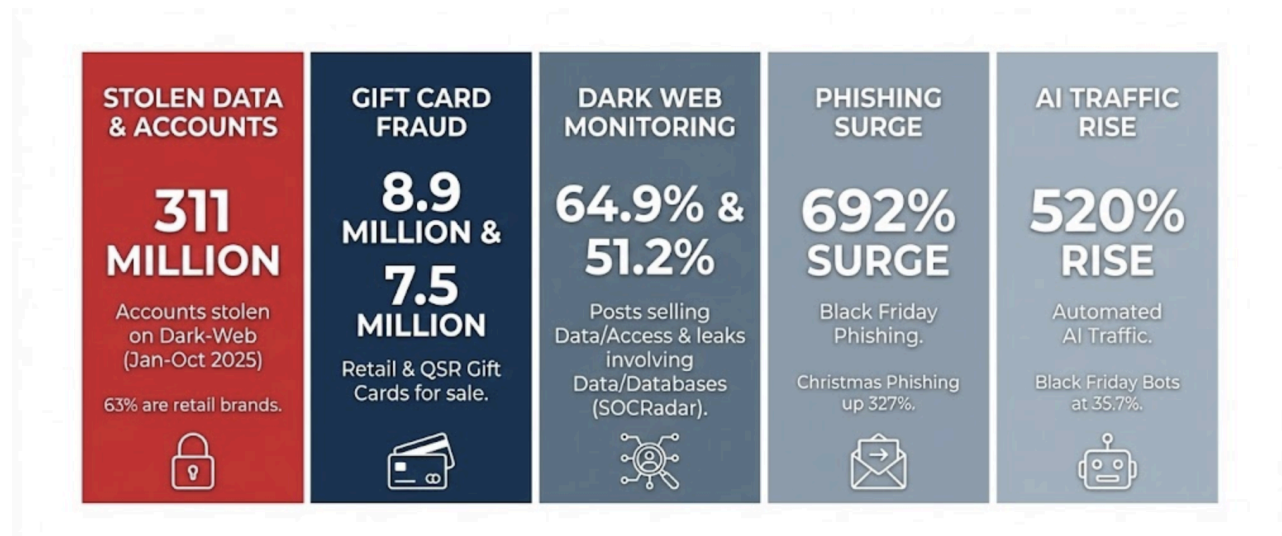
HOLIDAY SHOPPING CYBER THREATS 2025

How Criminals Exploit Retailers & Year-End Consumer Behavior

Holiday Shopping Cyber Threats 2025	1
Executive Summary	3
Introduction	4
The Holiday Threat Environment in 2025	5
Consumer Data as Seasonal Commodity	5
Peak Shopping Periods as Attack Windows	6
Dark Web Economy of Holiday Shopping Data	7
Stolen Shopper Profiles and Loyalty Accounts	8
Access Sales Against E-Commerce and Retail	9
Airline Miles, Travel Points, and BNPL Fraud	11
Gift Card Draining and Resale Markets	11
Threat Actors and Regional Targeting	13
Holiday Tooling and Campaign Infrastructure	15
Holiday Exposure Across Retail and Consumer Services	17
Which Sectors See the Most Leaks?	17
Credential Stuffing Surge in Q4	17
Streaming and Free Trial Abuse	18
Holiday Phishing and Social Engineering	20
Black Friday / Cyber Monday Scams	20
Delivery and Package-Themed Attacks	21
Fake Order Confirmations	21
Threat Actor Behavior During Holidays	23
Ransomware Slowdowns and Opportunistic Access Sales	23
Increased Stealer Logs and Credential Dumps	24
Fraud Group Collaboration Patterns	25
Threat Forecast for December 2025	26
Recommendations for CISOs and Organizations	27
Prepare Before the Season	27
Monitor During Peak Periods	27
Respond and Recover After the Season	28
Conclusion	29
References	30

Executive Summary

Cybercriminals treat the holiday season as a peak operational period. Online shopping increases, consumers sign up for temporary services, travel intensifies, and gift card purchases surge. Together, these patterns make November and December two of the most frequently exploited months for fraud, account takeovers, and phishing campaigns.



Key statistics:

- 311 million stolen accounts listed on dark-web markets in Jan-Oct 2025, 63% tied to retail brands.
- SOCRadar Dark Web Monitoring: 64.9% of retail/e-commerce/delivery posts are selling data or access; 51.2% of all posts involve data or database leaks.
- 8.9 million stolen retail gift cards and 7.5 million QSR gift cards observed for sale on underground markets.
- 692% surge in Black Friday-themed phishing during Thanksgiving week 2024; 327% increase in Christmas-themed phishing in the same period.
- 520% rise in AI-driven automated traffic to retail sites expected before Thanksgiving 2025. Also, an estimated 35.7% of Black Friday shoppers are bots or fake users.

This whitepaper examines how the dark web economy shifts toward holiday shopper data, and how sectors are exposed through identity leaks, credential dumps, and access sales. It explores the industrialization of gift card fraud, the scale of holiday-themed phishing, and changes in threat actor behavior, including ransomware groups and access brokers.

Introduction

The final weeks of the year bring predictable shifts in consumer behavior. Online shopping peaks, travel bookings rise, and digital gift exchanges become routine. Shoppers create new accounts, save payment details for faster checkout, enroll in loyalty programs, and redeem gift cards. Entertainment platforms also see a spike in subscriptions and “free trials” as families spend more time at home.

These behaviors create a dense concentration of fresh, high-value data—email addresses, phone numbers, postal addresses, loyalty identifiers, cookies, and payment metadata. They also generate many lightly secured accounts, created in a hurry and often protected with reused or weak passwords.

Threat actors track these cycles closely. As the 2025 holiday season approaches, reporting shows a steady increase in stolen accounts offered for sale, with retail consistently the most targeted sector. Data from the 2024 season illustrates how quickly attackers adapt to seasonal themes, pivoting to Black Friday- and Christmas-branded phishing as soon as retailers launch promotions. Dark-web forums and Telegram channels mirror this shift, with rising volumes of posts advertising holiday-themed phishing kits, SMS spam bots, gift card cash-out tools, and stolen shopper data. Access brokers auction control of high-volume online shops or gift-card portals, while fraud groups stockpile compromised accounts for resale during and after peak shopping days.

This report uses industry datasets, third-party research, and SOCRadar dark web observations to show:

- How consumer behavior translates into exploitable attack surfaces
- How criminals monetize exposure through data sales, access brokering, and fraud
- What concrete patterns security teams can anticipate around Black Friday, Cyber Monday, and Christmas

It concludes with actionable steps organizations can take before, during, and after the season, giving CISOs and security teams a practical, data-driven view of holiday cyber threats in 2025 and the controls that matter most.

Holiday 2025 Threat Landscape

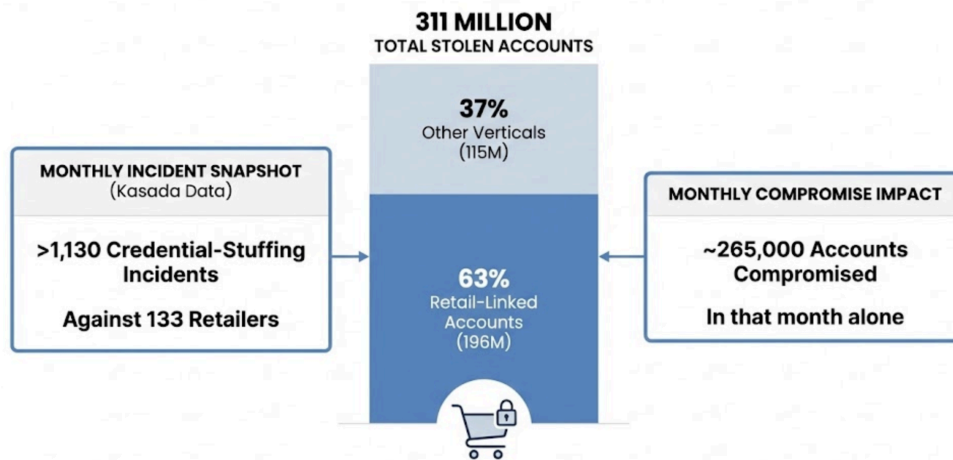
Seasonal Value of Consumer Data

During the November–December holiday shopping window, consumer data becomes more valuable across both legitimate and criminal markets. Retailers ramp up analytics, personalization, and targeted campaigns, while attackers lean on credential-stuffing kits, stealer logs, and account dumps to extract value from the same data.

Several seasonal dynamics drive this spike:

- **More new accounts.** Shoppers create accounts across multiple platforms for discounts, free shipping, or loyalty rewards, often reusing passwords and storing payment tokens.
- **Expansion of trial services.** Entertainment, delivery subscriptions, and other “free trials” add fresh credentials and contact details into circulation.
- **Surge in travel activity.** Holiday trips generate large volumes of booking records and loyalty data, including frequent flyer numbers and hotel points.
- **Concentration of value and time pressure.** Holiday accounts tend to hold multiple saved cards, active loyalty balances, and current addresses, while rushed users are more likely to ignore prompts and reuse weak passwords.

Threat actors capitalize on this by increasing dark web listings for shopper profiles, card metadata, BNPL (Buy-Now-Pay-Later) accounts, loyalty points, and travel rewards. In parallel, the Retail & Hospitality ISAC (via Adobe Analytics) expects **AI-driven automated traffic to retail sites to grow by 520%** in the ten days before Thanksgiving 2025, and CHEQ estimates that **35.7% of Black Friday “shoppers” are bots or fake users** – evidence of sharply escalating automated abuse, from credential stuffing and account takeover to broader bot-driven fraud.



Stolen accounts & retail share, January-October 2025

Black Friday to Christmas Attack Windows

Attackers do not distribute their efforts evenly throughout the quarter. They time their operations to coincide with specific peaks in consumer and retailer activity:

- **Black Friday week** - when promotional emails, social media ads, and landing pages saturate users' attention
- **Cyber Monday** - with a focus on online-only deals
- **The pre-Christmas rush** (approximately 15-23 December) - when shipping cut-offs and inventory shortages heighten urgency

Retail forecasts indicate that U.S. holiday sales in November and December 2025 will exceed **\$1 trillion** for the first time. For criminals, this concentration of spending means:

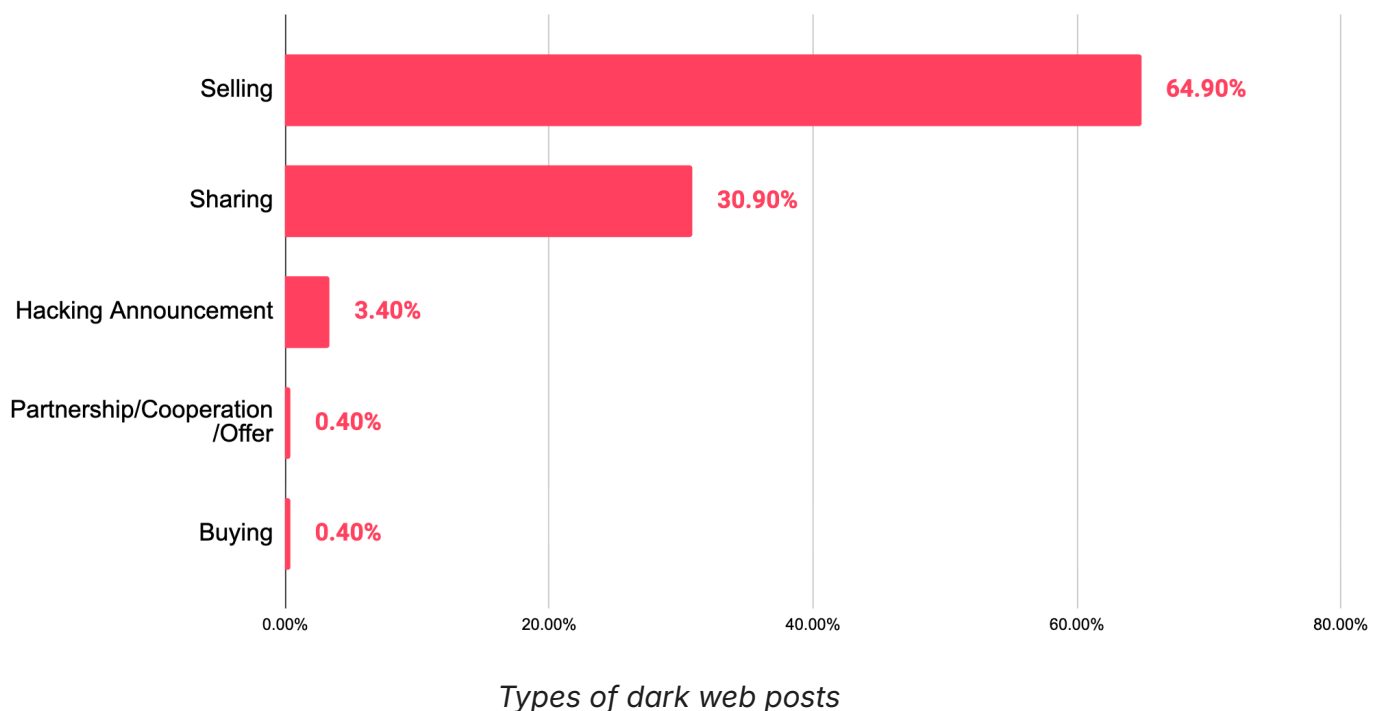
- Higher probability that a compromised account contains recent orders, active carts, or stored payment methods
- More opportunities to blend malicious traffic into legitimate volume
- Greater pressure on retailers' customer support and fraud teams, making timely detection harder

Data from 2024 showed multiple-fold spikes in Black Friday and Christmas-themed phishing during Thanksgiving week, with major U.S. retailers heavily impersonated (see Section 6.1 for details).

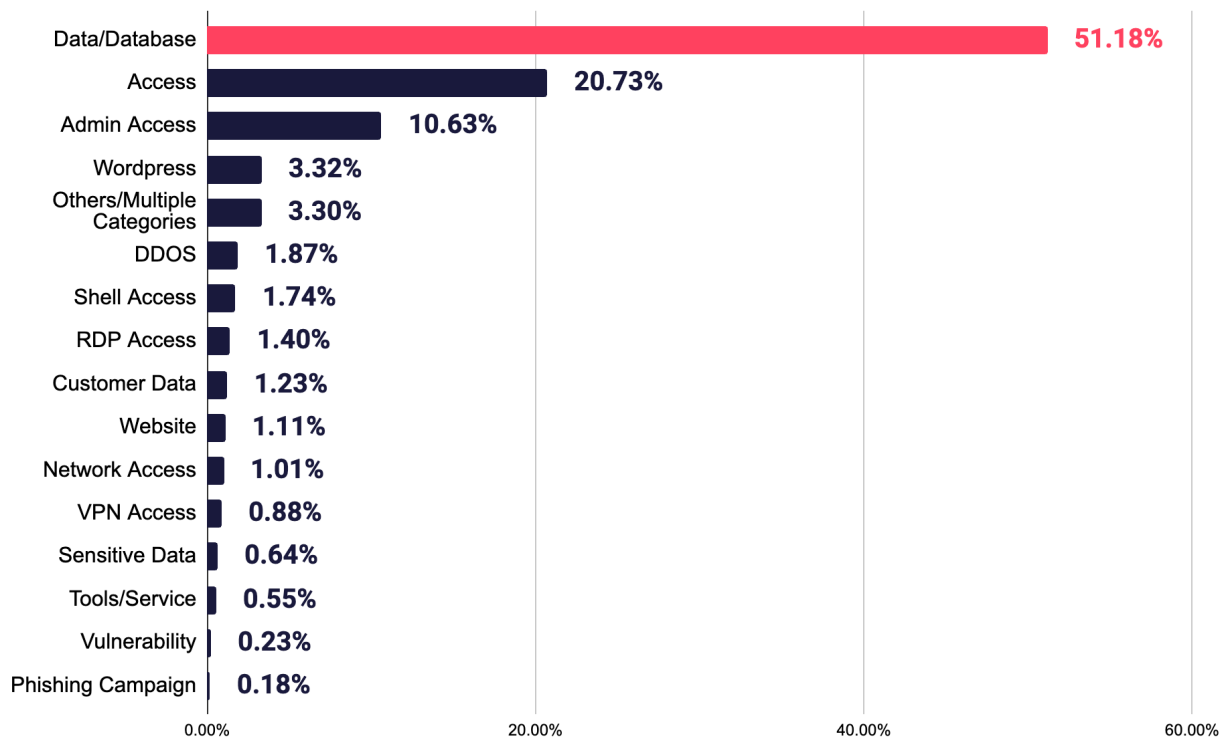
Dark Web Holiday Markets

Holiday shopping does not just change consumer behavior on legitimate platforms. It also reshapes supply and demand across dark web forums, Telegram channels, and criminal marketplaces. SOCRadar's Dark Web Monitoring shows that, across 2024-2025, posts related to sectors such as retail, e-commerce, and delivery overwhelmingly focus on monetizing access and data rather than simple discussion.

Across this dataset, **"Selling" posts account for 64.9%** of activity, followed by **"Sharing" at 30.9%**. Direct "Hacking announcements" and "Buying" or "Partnership/Cooperation" offers together make up only a few percent. In other words, most conversations appear at the commercialization stage of the attack chain rather than at initial discovery.



Beneath that, the most common content categories are **Data/Database (51.18%)**, **Access (20.73%)**, and **Admin Access (10.63%)**, followed by WordPress, DDoS, shell, RDP, VPN, and other access-related tags. Together, they show a mature underground economy centered on **ready-to-use access and large volumes of consumer data** rather than raw vulnerabilities.



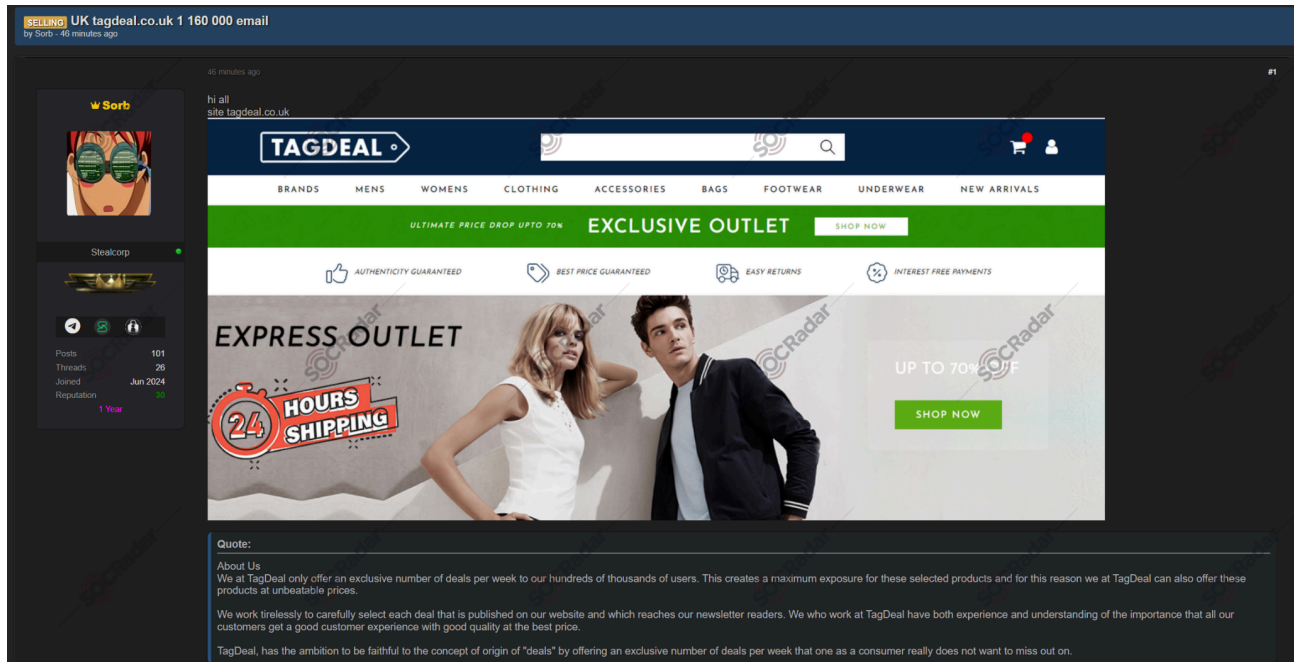
Dark web posts content categories

Stolen Shopper and Loyalty Data

On underground markets, stolen shopper profiles act as raw material for a broad set of fraud schemes. A typical profile includes an email address, username, delivery details, phone number, password (often reused), and loyalty identifiers. Many entries also include order history, giving fraudsters context on preferred brands and spending levels.

Kasada telemetry shows how strongly retail dominates this space: over **311 million stolen accounts** were identified in ten months, **63% of them tied to retail brands**. Combined with observations of over **1,100 credential-stuffing incidents** against **133 retailers** and an estimated **265,000 compromised accounts** in a single month, this indicates **industrial-scale harvesting of shopper identities** ahead of peak season.

Some listings go beyond individual accounts and offer bulk email and customer lists from specific stores. One dark-web auction advertising a UK-based fashion site, TagDeal, claims **over a million customer emails** ready for monetization. It is an example of a compromise that can feed both phishing and credential-stuffing campaigns for months.



TagDeal U.K. email database sale (SOCRadar Dark Web News)

Loyalty and travel accounts add another layer of value. Attackers favor them because:

- Points convert to flights, hotel stays, or gift cards without obvious card charges.
- Many customers do not check point balances regularly, delaying detection.
- Holiday travel concentrates point redemptions in November-January, increasing liquidity.

Account takeover campaigns during this period aim to silently drain balances, convert them into tickets or vouchers, and resell the benefits on underground markets.


Selling Access to Retail

While consumer accounts are the end-state for many fraud schemes, SOCRadar's data shows significant activity around **direct access to online shops and back-office systems**. Among all retail-related dark-web posts we analyzed, **Access** and **Admin Access** together account for more than **31%** of tagged content.

Listings commonly advertise:

- Admin logins to WordPress-based e-commerce sites.
- Full access to payment or order-management panels.
- Stores with guaranteed monthly order volumes, sometimes specifying card vs. alternative payment breakdowns.

BIG USA Shop
By **corptoday**, 3 hours ago in Auctions

corptoday
★★ If it weren't for me
★★
●●●●●

Seller
48\$
275 posts
Joined
01/18/19 (ID: 90847)
Activity
other / other
Deposit
0.000220\$
Car warranty
OK

Posted 3 hours ago (edited)
Large WordPress USA shop with admin rights.
Iframe form
8,300 orders per month , half of which are made by card (55-60%), the other half by Apple Pay
Starting price: \$25,000
Step: \$3000
Blitz: \$40,000
PPS 12h
Edited 35 minutes ago by corptoday

+ Quote

Large U.S. shop listing for WordPress admin access (SOCradar Dark Web News)



AU shop direct wp-admin form - with explicit permission to install plugins (SOCRadar Dark Web News)

These posts highlight three important points for defenders:

1. **Attackers value operational shops, not just data.** A working store with steady orders provides a platform for skimming, card testing, and malware injection.
2. **WordPress and similar CMS platforms remain frequent entry points.** The presence of "WordPress" as a distinct tag and the emphasis on wp-admin access underline how often unpatched plugins and weak admin hygiene drive compromise.
3. **Regional targeting is deliberate.** Many listings specify geography (for example, "USA shop," ".AU shop," or local TLDs) to appeal to buyers focusing on certain card issuers, currencies, or shipping networks.

Travel and BNPL Fraud

Holiday travel and last-minute gift purchases also increase the value of **airline, hotel, and BNPL accounts**. On the dark web, these rarely sit in their own category; instead, they appear inside larger “data/database” or “access” listings, but the monetization pattern is consistent:

- **Compromised airline and hotel logins** let attackers turn miles and points into flights, upgrades, or hotel stays that can be resold.
- **Refund-as-a-service offers** target travel agencies and booking platforms, using social engineering or stolen internal credentials to secure refunds while trips proceed as planned.
- **BNPL portals** face the same credential-stuffing pressure as retail logins; any account that passes basic verification can be used to order high-value goods and disappear before chargebacks catch up.

Holiday timing amplifies all of this: goods and bookings move quickly, dispute windows often lag purchases, and fraud blends into heavy seasonal traffic. Together with gift cards, these programs form a parallel currency layer that attackers can drain and resell throughout the November-January peak.

Gift Card Fraud at Scale

Gift cards are one of the most liquid assets in the holiday cybercrime economy. They are purchased in large volumes, treated much like cash by many retailers, and easy to convert through peer-to-peer sales.

2025 KasadaQ data identified **8.9 million stolen retail gift cards** and **7.5 million QSR gift cards** for sale on underground markets, confirming that cards are now a standardized commodity alongside card numbers and account credentials.

Microsoft’s reporting on the Moroccan group **Storm-0539 (Atlas Lion)** shows the upper bound of this fraud model: in some cases, the group stole **up to \$100,000 per day** from individual companies by targeting corporate gift card portals, with activity rising sharply around Black Friday and Christmas.

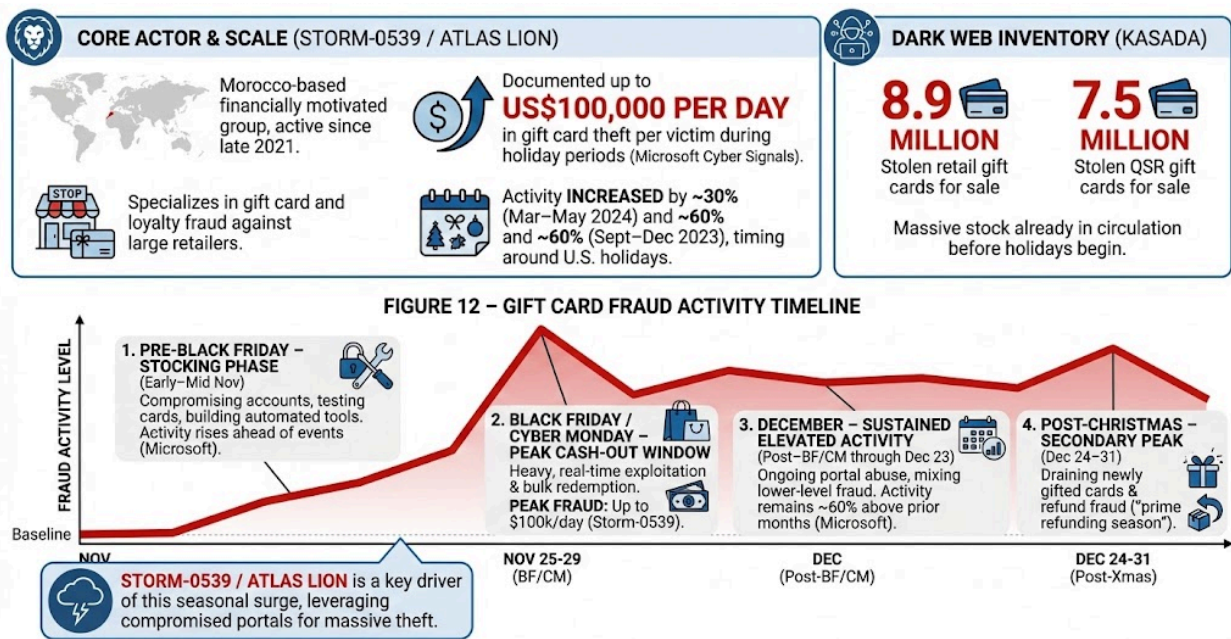
A related campaign, dubbed **"Jingle Thief"** in 2025 reporting, illustrates how far this has evolved. Instead of relying only on direct portal abuse, Storm-0539 compromised cloud productivity and order-management platforms (such as collaboration and file-sharing services), then spent months studying internal spreadsheets, exports, and workflows tied to gift card issuance. In some victims, the group reportedly maintained access for up to a year and compromised dozens of accounts before launching large-scale theft during peak holiday weeks.

In summary, the associated fraud lifecycle follows a seasonal pattern:

- **Pre-Black Friday:** actors stockpile cards by breaching portals and enumerating vulnerable systems
- **Black Friday / Cyber Monday:** fraud peaks as criminals rapidly cash out balances while transaction volumes are highest
- **December:** elevated but more targeted activity continues, especially around electronics and gaming
- **Post-Christmas:** a second spike occurs as criminals drain newly gifted cards before recipients attempt to redeem them

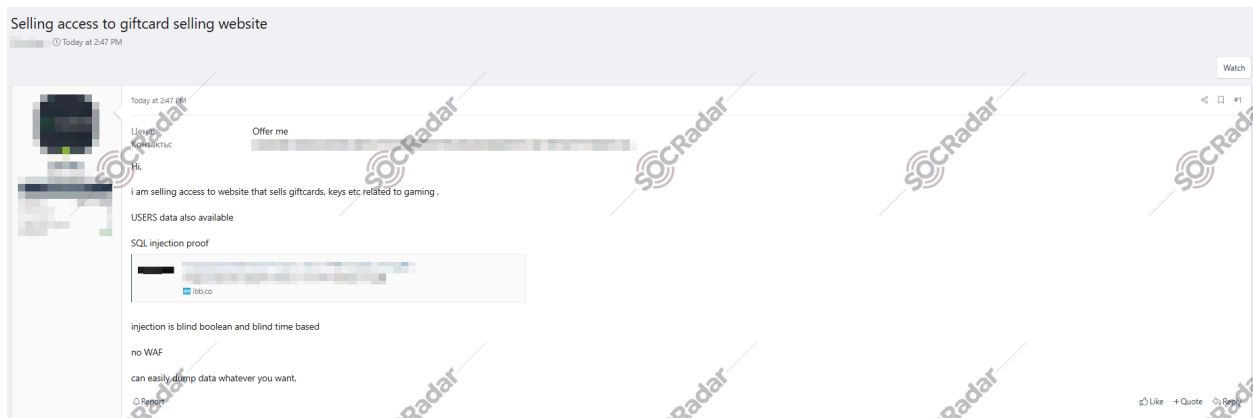
Common tactics across these operations include:

- Compromising employee accounts to reach internal gift card management tools
- Inflating balances or issuing new cards in bulk
- Draining existing cards through automated balance checkers and scripted purchases
- Reselling codes on dark-web forums and encrypted channels



Storm-0539 gift card fraud activity: key details & seasonal timeline

SOCRadar's Dark Web Monitoring captures both low-barrier tools and higher-impact access listings within the gift card fraud ecosystem.



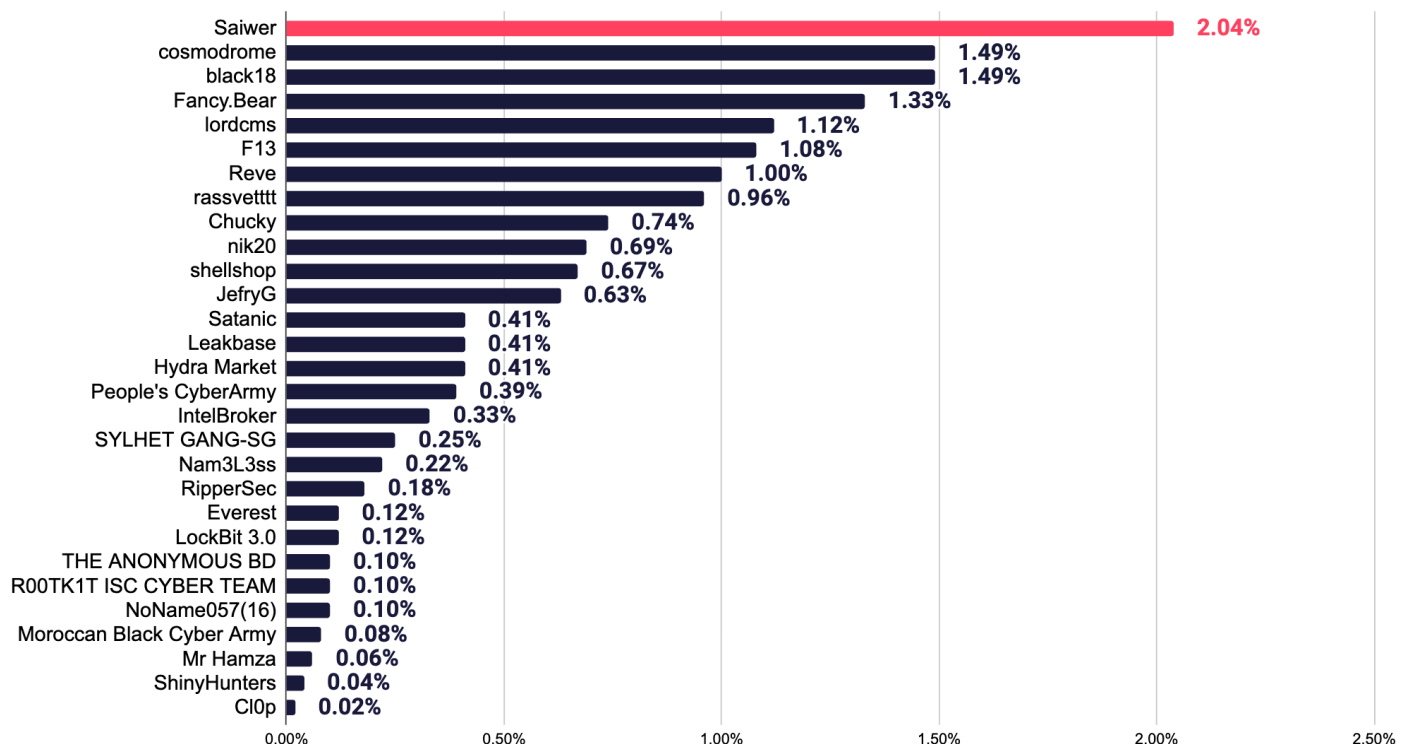
Listing selling access to a gift-card selling website via SQL injection - shows a more advanced case where the actor advertises database access, confirms the vulnerability type, and notes the absence of a WAF. (SOCRadAr Dark Web News)

Threat Actors and Regional Targeting

The dark-web activity behind these trends is not dominated by a single group. Instead, SOCRadar telemetry reveals a **long tail of actors**, ranging from well-known ransomware and data-leak brands to smaller brokers and carding crews.

Across the holiday-related dataset:

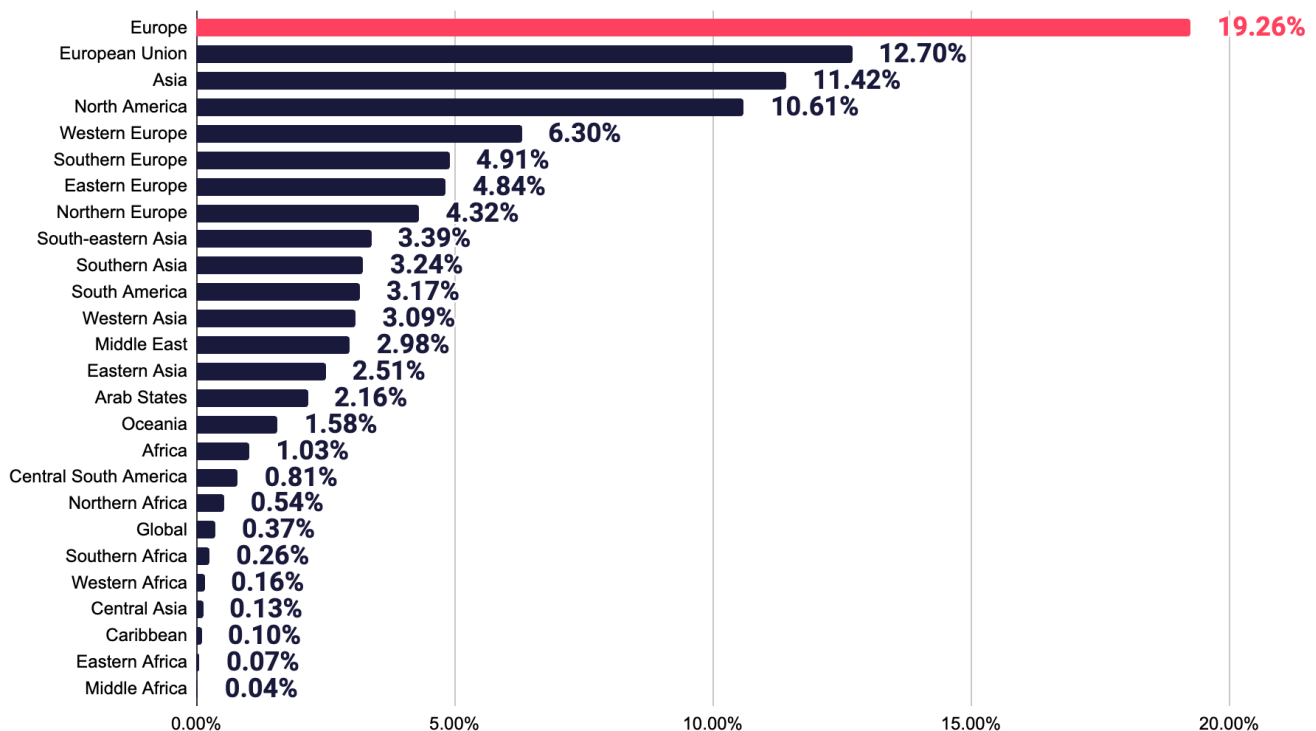
- Handles such as **Saiwer**, **cosmodrome**, **black18**, **Fancy.Bear**, **lordcms**, **F13**, and **Reve** appear among the most active in dark web forum postings. Well-known names like **Leakbase**, **Hydra Market**, **IntelBroker**, **NoName057(16)**, **ShinyHunters**, **CI0p**, and **LockBit 3.0** also surface, alongside a long tail of smaller brokers and carding crews.



Most active threat actors

Geographically, the posts reference a broad set of targets, but **Europe and North America dominate**:

- **Europe (19.26%)** and the **European Union (12.70%)** together account for nearly one-third of all region mentions.
- **Asia (11.42%)** and **North America (10.61%)** follow, with more granular references to Western, Southern, Eastern, and Northern Europe, South-eastern and Southern Asia, and the Middle East.
- Regions such as **Oceania (1.58%)**, **Africa (1.03%)**, and Latin American subregions appear less frequently but still represent consistent targeting.



Distribution of targeted regions

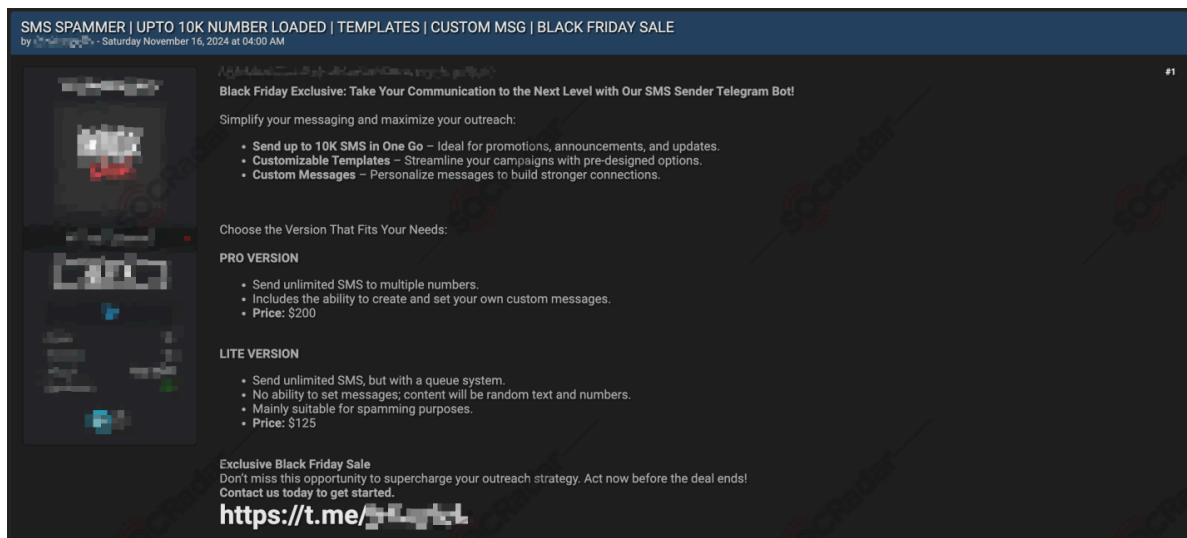
These distributions align with where online shopping volumes, card usage, and mature e-commerce infrastructures are highest - precisely the environments where stolen accounts, gift cards, and access to busy shops yield the greatest returns.

Holiday Attack Tooling

Finally, a smaller but significant portion of dark-web posts in this dataset concerns **tools and services** that make it easier to run seasonal campaigns. Although “Tools/Service” and “Phishing Campaign” tags together account for **less than 1%** of all posts, their impact is outsized because a single tool can support many operators.

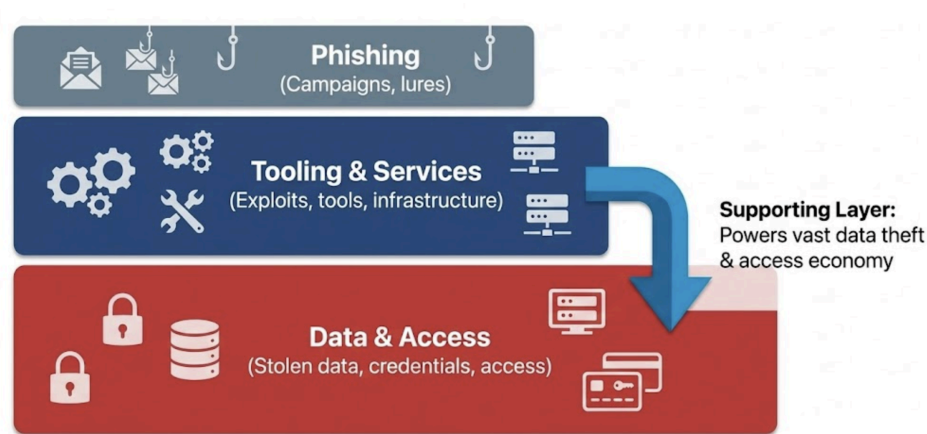
SOCRadar identified, for example:

- A **Black Friday-branded SMS spammer bot** that promises up to 10,000 SMS messages in one run, customizable templates, and separate “pro” and “lite” versions priced for different use cases. This kind of tool lowers the barrier for running large-scale smishing campaigns impersonating retailers, delivery firms, or payment providers around peak shopping days.



SMS spammer Black Friday sale (SOCRadar Dark Web News)

These offerings show how threat actors productize their operations around the same calendar that legitimate retailers use. As soon as mass-marketing teams schedule Black Friday and Christmas campaigns, a parallel ecosystem sells the infrastructure to spoof them at scale.



How phishing and tools fuel the holiday cybercrime economy

Holiday Exposure by Sector

High-Risk Retail Segments

Retail is not a single risk profile. Some segments consistently attract more attention from threat actors, especially in Q4 when volumes spike and downtime is costly. Thales reported **837 cyber incidents** and **419 confirmed breaches** affecting retail in **Q2 2025**, with **ransomware present in 44%** of those breaches and a **median ransom demand of around \$2 million**, nearly double the previous year.

Within retail, several verticals stand out as high-value targets during the holiday period:

- **Electronics and gaming** - high resale value, strong demand, and frequent financing/BNPL use.
- **Apparel and fashion** - dense transaction volumes, aggressive discounting, and high marketing activity.
- **Cosmetics and personal care** - subscription models and rich loyalty data tied to recurring purchases.
- **Food delivery and grocery** - always-on services linked to saved payment methods and location data.
- **Online marketplaces** - large customer bases, third-party sellers, and complex payment workflows.

These segments are attractive because they combine **high transaction volume, stored payment and loyalty data**, and **tight operating margins** that make disruption during peak season especially painful, raising the leverage of both ransomware operators and fraud groups.

Q4 Credential Stuffing Spike

Credential stuffing and account takeover (ATO) follow the same seasonal curve as consumer activity. Reports from Arkose Labs indicate that ATO attacks are expected to rise by **at least 47%** during the peak holiday season, while Kasada's automated threat reporting shows that the average retailer faces **2.5-3× more bot-driven login traffic** in holiday months than during the rest of the year.

During Black Friday weekend specifically, some studies have observed **more than a 200% increase** in credential-stuffing attempts compared with normal traffic levels, even if precise figures vary by year and vertical.

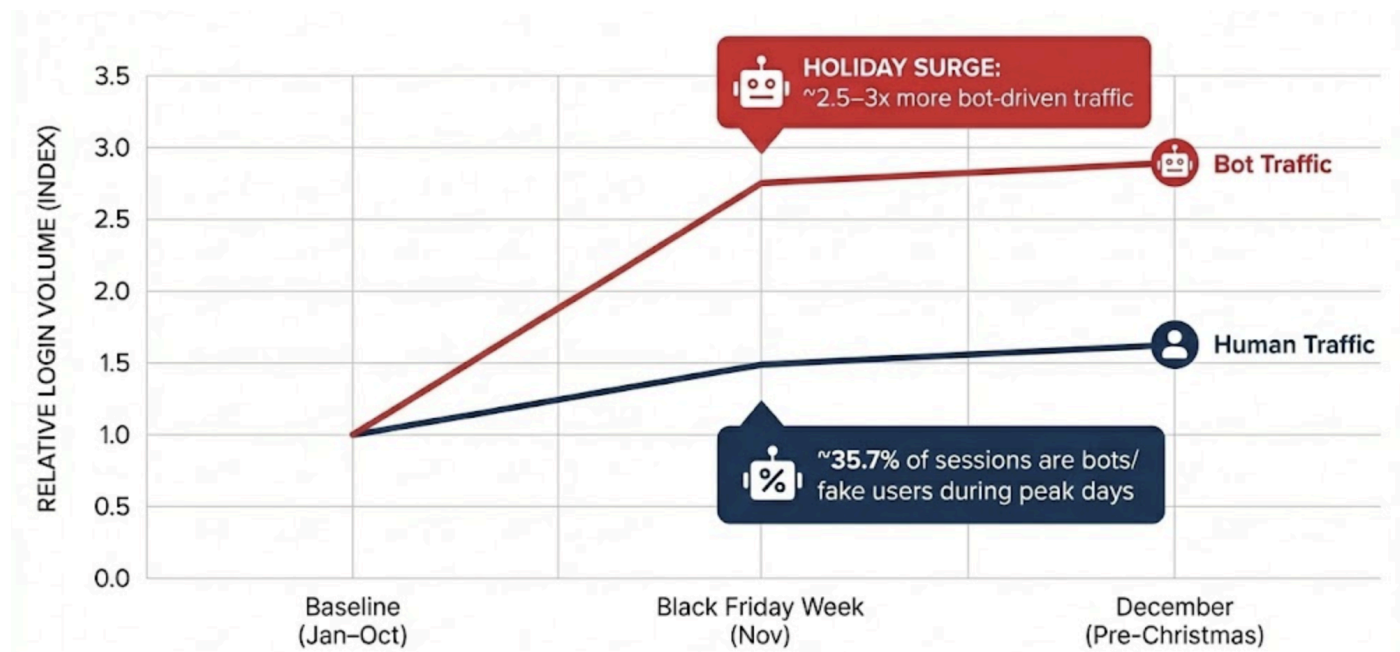
Attackers typically combine:

- Large credential dumps from prior breaches
- Fresh stealer logs collected by infostealer malware
- Botnets and "human-like" agentic bots that mimic realistic delays and mouse movements

Primary targets include:

- Customer login portals for online shops
- BNPL and digital-wallet platforms
- Loyalty program portals
- Gift card balance-check pages

Once attackers compromise accounts, they test stored cards, drain loyalty points, and sometimes pivot into refund fraud or social engineering of customer-service teams.



Bot vs human login traffic during the holiday

Streaming and Free Trial Abuse

Entertainment and streaming platforms experience their own holiday effect. Families subscribe to new services, redeem promotional gift cards, or activate “free trial” offers around Christmas and New Year.

Although precise December-only datasets are limited, threat intelligence feeds show:

- Consistent listings for compromised accounts on platforms such as Netflix, Disney+, Hulu, and Spotify
- A slight drop in streaming-account sales around Black Friday and Cyber Monday, likely because criminals stockpile access beforehand and use or distribute it off-platform
- A post-Christmas surge in account sales between **24-26 December**, coinciding with new subscriptions and gift redemptions



Streaming account sales timeline: Black Friday to post-Christmas

For attackers, streaming and other entertainment accounts offer:

- Reusable access that can be resold several times until the owner notices
- A low-risk way to monetize stolen credentials (without immediately triggering fraud controls on bank or card systems)
- A convenient testing ground for credential pairs that may also work on higher-value services

Additionally, bots abuse free-trial systems by creating large numbers of disposable accounts, which are then rented, bundled as “holiday trial” packages, or used to mask other fraudulent activity.

Holiday Phishing Tactics

Black Friday / Cyber Monday Scams

Phishing remains one of the most efficient channels for holiday fraud. Darktrace's 2024 analysis showed that, during Thanksgiving week, Black Friday-themed phishing increased by **692%** and Christmas-themed phishing by **327%** compared with early November. Impersonation of major U.S. retail brands, such as Walmart, Target, and Best Buy, rose by more than **2,000%**, and global telemetry from APWG recorded **989,123 phishing attacks** in Q4 2024.

These peaks are not limited to email. Visa's Payment Fraud Disruption team reported a **284% increase** in fake or spoofed merchant websites around Black Friday and Cyber Monday, while other sources saw a **41% rise** in malvertising campaigns and a **65% increase** in phishing attacks on e-commerce platforms.



Black Friday and Christmas-themed phishing growth, according to 2024 data (Source: Darktrace analysis of 626 customer environments)

Common characteristics of holiday phishing campaigns include:

- Subject lines referencing **limited-time deals**, **exclusive coupons**, or **order updates**
- Look-and-feel cloning of major retailers' email templates and landing pages
- Use of newly registered domains that resemble legitimate brand URLs
- Integration with malicious browser extensions or fake coupon tools

As AI-generated content becomes more accessible, attackers increasingly rely on generative models to craft emails, social posts, and even entire cloned websites that avoid obvious grammatical errors and appear more convincing. McAfee's 2025 consumer research found that **46% of Americans reported encountering AI-powered scams** while shopping, covering fake product reviews, impersonated support chats, and synthetic voices on support hotlines.

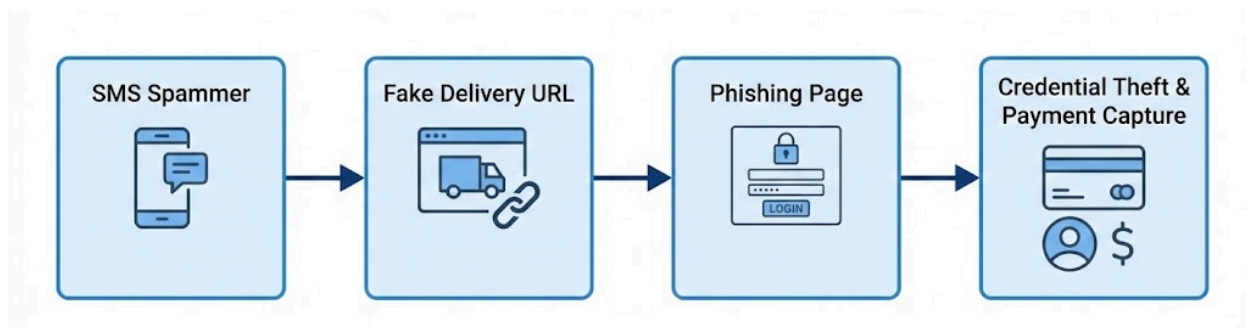
Delivery-Themed Scams

As parcel volumes spike, attackers shift to delivery and logistics lures. The Federal Trade Commission (FTC) estimated that text-based scams cost U.S. consumers around **\$470 million** in 2024, with package-delivery notifications among the most commonly reported themes.

Typical attack patterns include:

- SMS messages claiming a **missed delivery** or **address confirmation**
- Links to fake tracking portals that mimic USPS, FedEx, UPS, DHL, or regional carriers
- Requests for **small "re-delivery" or customs fees** paid via card
- Phishing pages that harvest email credentials or card details

Because many recipients genuinely expect packages during this period, they are more likely to respond quickly and overlook red flags. Stolen credentials collected through these fake portals can then be used to access email accounts, reset passwords for other services, or conduct further phishing.



Delivery-themed scams

Fake Order Scams

Fake order confirmation emails and messages exploit a different aspect of consumer psychology: fear of unauthorized purchases or anxiety about delayed gifts. These lures often claim:

- An expensive order has shipped to an unfamiliar address
- A subscription has renewed at a high price
- An order cannot be processed without additional information

Victims are directed to:

- Call a fraudulent “support” line, where social engineers attempt to gather card data or convince them to install remote-access software
- Visit a phishing site to “cancel” the order, entering login credentials and payment details
- Download attached invoices that deliver malware

Using AI tools, attackers generate realistic invoices, branded email templates, and localized copy in bulk, enabling hundreds of slightly varied lures tailored to different brands and regions.

Threat Actor Behavior During Holidays

Ransomware Slowdowns and Opportunistic Access Sales

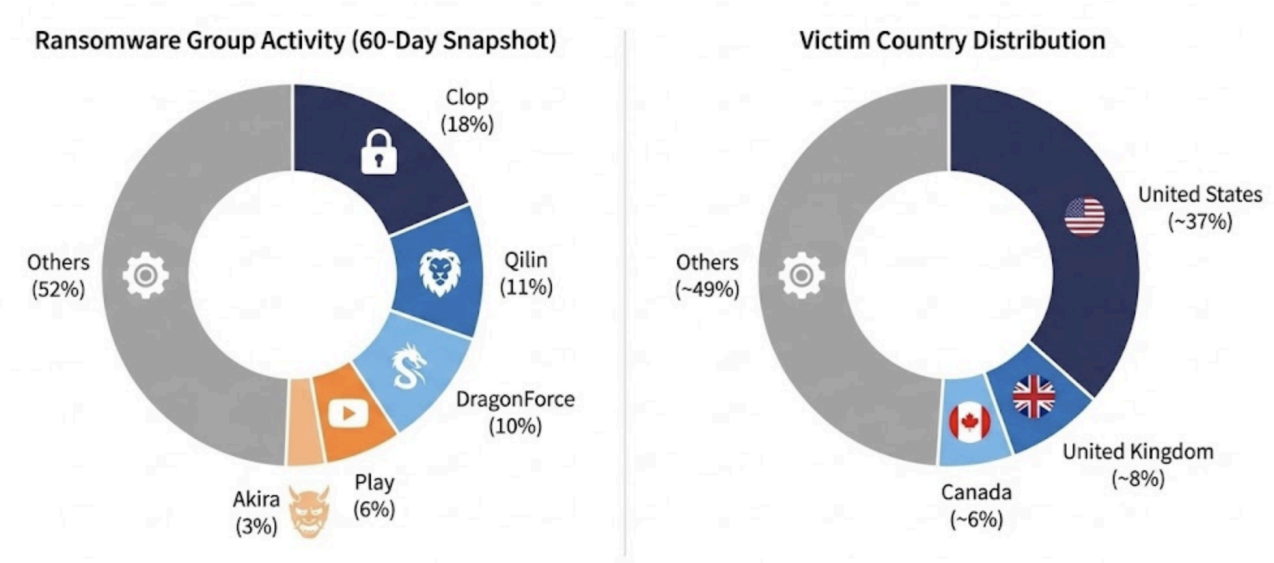
Ransomware activity around major holidays has become more nuanced than a simple “on” or “off” pattern. Historically, some groups slowed large-scale encryption operations during public holidays to avoid complex negotiations and high-profile scrutiny. Today, many actors instead **shift focus rather than fully pause**.

Evidence from recent Q4 reporting and incident trends suggests that:

- Some crews reduce visible, high-impact encryption campaigns around major holidays, especially on peak shopping days.
- At the same time, ransomware-aligned actors and access brokers **intensify initial access work** - credential theft, lateral movement, and data collection - while defenders are distracted or operating with reduced staffing.
- Stolen access is then sold on dark-web markets with details such as sector, geography, and estimated revenue, allowing other groups to stage full ransomware or data-extortion attacks in January and beyond.

Recent 60-day SOCRadar observations illustrate the broader ecosystem behind these holiday patterns. In that period, groups such as **Clop (18% of observed incidents)**, **Qilin (11%)**, **DragonForce (10%)**, **Play (6%)**, and **Akira (3%)** remained active, with victims concentrated in countries like the **United States (~37% of incidents)**, the **United Kingdom (~8%)**, and **Canada (~6%)**.

While this snapshot is not limited to holiday weeks or to retail alone, it shows that **well-known ransomware brands and their affiliates continue to operate at scale** as organizations enter the peak shopping season - often using Q4 to quietly prepare access that will be monetized in early 2026.



SOCRadar Ransomware Intelligence: 60-day ransomware snapshot and victim distribution

Increased Stealer Logs and Credential Dumps

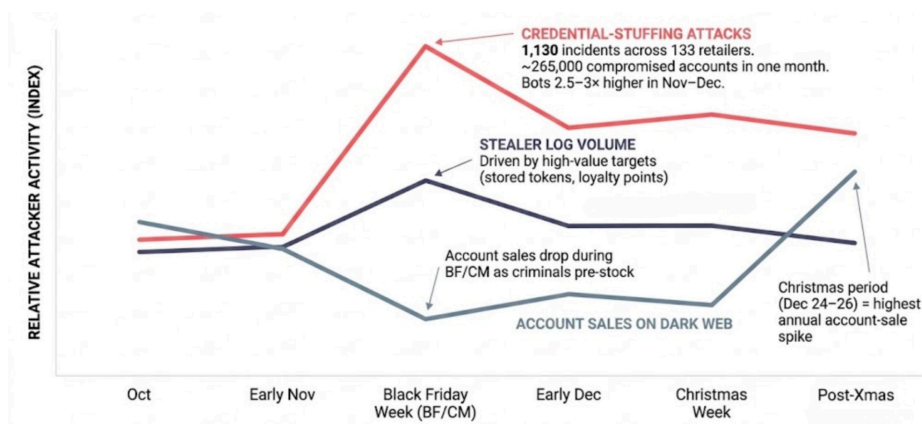
Stealer malware families such as RedLine, Lumma, and Raccoon operate continuously, but the value of their output rises during the holiday period. Logs collected from infected systems often contain:

- Browser-saved passwords for retail, banking, and email sites
- Autofill data, including postal addresses and phone numbers
- Session cookies that may bypass multi-factor authentication

Threat intelligence reporting from multiple vendors shows that as credential-stuffing and account takeover (ATO) attacks accelerate in Q4, underground marketplaces see a corresponding uptick in the sale of **fresh stealer logs**. Bot traffic against login pages climbs to several times normal levels for many retailers, and security teams observe a disproportionate rise in suspicious logins from new locations or device fingerprints.

These dynamics are reflected in account-sale patterns observed across recent holiday seasons:

- Access to many accounts is harvested in the week before Black Friday, when they contain saved carts, coupons, and loaded payment methods.
- During Black Friday and Cyber Monday, account sale volume on some markets temporarily dips, suggesting criminals are actively **using** previously acquired access rather than selling it.
- Between **24-26 December**, listings surge to their highest levels, as fraudsters convert newly created holiday accounts and gifted subscriptions into cash.



Stealer logs, credential stuffing & account sales (October-December)

Fraud Group Collaboration Patterns

Carding forums, refund-fraud communities, and Telegram channels form an ecosystem that behaves differently during the holidays. Observed patterns include:

- **Shared infrastructure.** Multiple groups reuse the same SMS spamming tools, phishing kits, or compromised panels.
- **Seasonal playbooks.** Channels circulate scripts and instructions for "holiday refunding," package-delivery scams, and gift card fraud, tuned to specific retailers.
- **Access trading.** Access brokers exchange or auction admin logins for online shops and backend systems, as illustrated by the "Big USA Shop" and ".AU Shop direct wp-admin form" auctions.

These collaborative dynamics mean that a single security lapse by one retailer or service provider can fuel multiple parallel fraud campaigns.

Holiday 2025 Threat Outlook

Based on historical Q4 patterns, 2024 attack data, and current SOCRadar intelligence, several threat categories are likely to intensify as the 2025 holiday period progresses:

- **Automated and AI-driven abuse.** With AI-generated traffic projected to rise by 520% before Thanksgiving, retailers should expect more human-like bots targeting logins, checkouts, and promo engines across web, mobile, and API channels.
- **Package-delivery and multi-channel scams.** Fake shipping alerts will peak during the December 15-23 pre-Christmas rush, using highly convincing USPS/FedEx/UPS look-alike pages and SMS spam tools to harvest credentials and payment data.
- **BNPL and alternative payment fraud.** Last-minute shoppers seeking instant credit for high-value gifts will make BNPL services and digital wallets prime targets. Criminals will abuse streamlined approvals and stolen identities to conduct “buy and disappear” fraud.
- **Gift card and loyalty exploitation.** With at least 8.9 million retail and 7.5 million QSR gift cards already circulating on dark web markets, groups such as Storm-0539 and its “Jingle Thief” campaign are likely to intensify portal compromises, generator-tool distribution, and post-Christmas balance draining, often after spending months embedded in cloud-based gift card workflows before launching large-scale theft during peak shopping weeks.
- **Travel account resale and refund abuse.** As holiday travel surges, compromised airline and hotel loyalty accounts with large balances or elite status will command premium prices. Immediately after Christmas, attackers will pivot to “prime refunding season,” abusing overwhelmed support teams to claim non-delivery or fraudulent returns.
- **Access staging and January ransomware campaigns.** While not December activity, it's worth noting that January consistently sees elevated sales of network access and credentials harvested during Q4. Ransomware groups that maintained operational silence during December holidays will likely resume active encryption campaigns in early January, leveraging access obtained during the holiday period.

Organizations should treat these developments as components of a single seasonal attack economy, aligning monitoring, customer protection, and incident response plans around the full November-January lifecycle.

Recommendations for CISOs and Organizations

This section translates the preceding analysis into practical actions for security and fraud teams. The recommendations focus on the period from early November through mid-January, when holiday activity and post-holiday refund fraud are most intense.

Before the Season

- **Map your holiday attack surface.**
Identify high-load systems - e-commerce portals, mobile apps, loyalty platforms, streaming services, BNPL/payment integrations, and gift card portals - along with the third parties behind them (processors, marketing tools, support vendors). Solutions like SOCRadar's Attack Surface Management (ASM) can help enumerate exposed domains, subdomains, and services before traffic spikes.
- **Harden authentication and sessions.**
Enforce MFA for admin and privileged customer actions, use risk-based authentication (device, IP reputation, geo), and shorten session lifetimes for sensitive tasks such as gift card management and high-value redemptions.
- **Raise the bar for bots and credential stuffing.**
Deploy behavior-based bot detection, and monitor for login anomalies such as sudden spikes in failed attempts, new ASNs, or uniform user-agent strings. Feed dark web and breach intelligence (e.g., from SOCRadar's Threat Intelligence and Identity modules) into password-breach checks and risk scoring to flag accounts using known compromised credentials.
- **Lock down gift card and loyalty workflows.**
Limit who can create/adjust balances, require strong auth for bulk issuance and high-value redemptions, and set alerts for unusual patterns (e.g., rapid small card creation or repeated balance checks from the same IP).

During Peak Weeks

- **Run targeted holiday threat monitoring.**

Task internal or external intelligence teams to track brand impersonation, phishing kits, and dark web discussions mentioning your organization. SOCRadar's Dark Web Monitoring and Brand Protection / Phishing Radar modules can surface listings that advertise access to your domains, admin panels, or customer databases, similar to the "Big USA Shop" and ".AU shop" examples in this report.

- **Instrument gift card and BNPL analytics.**

Monitor rapid balance checks from single IPs, sequences of high-value BNPL purchases from new accounts, and repeated failed gift card redemptions. Tune rules with fraud teams for Black Friday and pre-Christmas without overwhelming analysts.

- **Prepare for SMS and email surges.**

Proactively inform customers how you actually send delivery updates, password resets, and promos; share examples of legitimate URLs and state that you will never request full card numbers or login details via SMS/email. Ensure SPF/DKIM/DMARC and SMS sender registration are in place; use SOCRadar Brand Protection findings to quickly spot spoofed domains, fake shops, or look-alike "support" sites piggybacking on your name.

- **Keep incident response ready.**

Confirm on-call coverage and escalation paths, and have playbooks for ATO, gift card fraud, phishing-site takedowns, and mass password resets. A short tabletop exercise simulating a Black Friday phishing wave or gift card portal compromise can expose gaps.

After the Season

- **Audit post-holiday activity.**

In January, review logs for unusual refund volumes, chargebacks, and gift card redemptions. Look for clusters of accounts, devices, or IPs that point to organized refund fraud or account resale. Cross-check with SOCRadar Dark Web Monitoring and Identity Intelligence to see whether affected accounts, emails, or loyalty IDs appear in recent dumps.

- **Update detection and risk models.**

Incorporate newly observed phishing templates, domains, and infrastructure into blocklists, and update SIEM/SOAR rules with indicators linked to tools like SMS spammers and gift card generators. Threat intelligence from platforms such as SOCRadar can help correlate these indicators with specific threat actors and campaigns.

- **Communicate clearly with customers.**

If incidents occur, explain what happened, what you've done, and what customers should do (e.g., reset passwords, enable MFA). Use the post-season period to reinforce basic hygiene and to promote safer login and payment habits ahead of the next holiday cycle.

- **Review vendors and partners.**

Assess whether third-party providers contributed to incidents or near misses. Update contractual requirements for logging, incident reporting, and control baselines. You can achieve visibility into vendor exposure through SOCRadar's Supply Chain Intelligence.

Conclusion

The holiday season concentrates both opportunity and risk. As more shopping, travel planning, and entertainment move online, the volume of valuable data and transactions rises sharply — and threat actors align their operations with Black Friday, Cyber Monday, and Christmas timelines.

Data from 2023-2025 shows a clear pattern: stolen retail accounts number in the hundreds of millions, most dark-web listings tie back to commerce and loyalty platforms, and gift card fraud has become industrialized, with some groups stealing up to \$100,000 per day from compromised systems. Phishing volumes spike around key dates, and AI-assisted tooling makes scams harder to distinguish from legitimate activity. At the same time, access itself has become a tradable commodity, with admin logins, SQL injection access to gift-card sites, and curated retailer mailing lists bought and sold as standard inventory.

The advantage for defenders is that these patterns are predictable. Organizations that understand how seasonal consumer behavior shapes attack surfaces (and which tactics spike when) can adjust their defenses accordingly. By hardening authentication, monitoring for automated abuse, tightening controls around gift cards and loyalty systems, and integrating dark web intelligence into security operations, they can reduce both the likelihood and impact of holiday-driven attacks and better protect customers at the time of year when they are most active and most vulnerable online.

References

1. <https://www.kasada.io/top-holiday-fraud-trends-2025/>
2. <https://www.darktrace.com/blog/phishing-attacks-surge-in-buildup-to-black-friday>
3. <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/>
4. <https://unit42.paloaltonetworks.com/jingle-thief-cloud-based-gift-card-fraud-campaign>
5. <https://www.globenewswire.com/news-release/2025/11/03/3179482/0/en/>
6. <https://cpl.thalesgroup.com/blog/data-security/changing-retail-cybersecurity-threat-landscape>
7. <https://www.esecurityplanet.com/threats/holiday-fraud-trends-2025-the-top-cyber-threats-to-watch-this-season/>
8. <https://www.mcafee.com/blogs/internet-security/how-to-protect-yourself-from-black-friday-and-cyber-monday-ai-scams/>
9. <https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>
10. <https://rhisac.org/wp-content/uploads/Holiday-Trends-Report-2024-Clear.pdf>
11. https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf
12. <https://www.arkoselabs.com/resource/2024-holiday-fraud-prevention-report/>
13. <https://cheq.ai/blog/cyber-threats-retail-black-friday-cyber-monday/>
14. <https://gbhackers.com/ransomware-attacks-2/>