INTEL471

WHITEPAPER

BLACK "FRAUD DAY" AND BEYOND

The key cyber threats facing the retail sector this holiday season in 2025

TLP:CLEAR

Key Takeaways

This white paper analyzes how cyber threat actors exploit the 2025 holiday shopping period, from Black Friday through the post-Christmas period, to target the retail sector.

- The holiday period represents a peak risk window for the retail industry. Threat actors almost certainly time operations to capitalize on this surge in transactions and promotions.
- Payment and gift card fraud are heavily commoditized. Mature underground markets support large-scale gift card and card-not-present (CNP) fraud, with specialist services advertising tens of thousands of cards and hundreds of thousands of compromised payment records.
- Phishing and fake retail brands are a primary consumer-facing threat. Seasonal lures — including Black Friday deals, delivery updates and refunds — and impersonation of major brands — especially Amazon and large U.S. retailers — have seen surges around Black Friday and Christmas in prior years, with similar patterns expected in 2025.
- Fake e-commerce sites are known to spike ahead of Black Friday. Security vendors observed a 250% increase in fake online shops ahead of Black Friday 2025, with sharp rises in sites mimicking Amazon, eBay and other brands. Underground actors sell ready-made scam pages for popular retailers, enabling rapid brand impersonation at scale.
- Ransomware pressure on retail is growing sharply. From 1 Jan to 17 Nov 2025, 466 ransomware breaches affected the retail sector, a 92% increase over the same period in 2024. The U.S. accounts for 55% of incidents, with CLOP, Qilin and Akira responsible for 44% of observed breaches.
- AI is used by threat actors as an efficiency multiplier, to generate more convincing phishing content, deepfake promotional videos and highly polished scam advertisements. It transforms previously manual fraud into scalable, industrialized operations.

*** Actors' names have been redacted for operational security purposes.**

Overview

The holiday season remains a critical time for the retail industry, marked by a significant increase in consumer spending each year. The Adobe computer software company estimates U.S. online sales alone will hit US $253.4 billion from Nov. 1, 2025, to Dec. 31, 2025 — a 5.3% increase from the same period in 2024. Further, Adobe reported "Cyber Week" — the five-day period including Thanksgiving, Black Friday and Cyber Monday — likely will drive 17.2% of overall spend this season at US $43.7 billion, up 6.3% from last year.

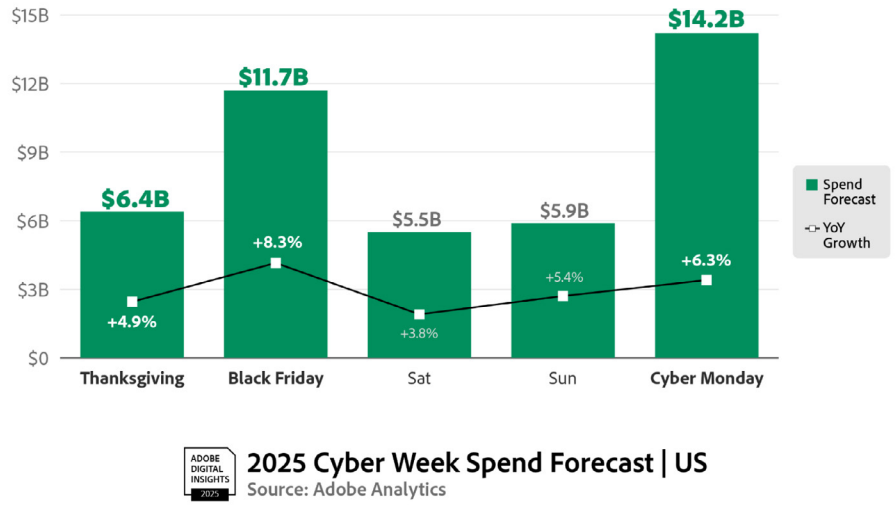

Figure 1: The image depicts Adobe's "Cyber Week" spending forecast for 2025.

This surge in engagement makes for a target-rich environment for opportunistic underground threat actors. In 2024, the chief executive of the U.K.'s GCHQ National Cyber Security Centre (NCSC) claimed the festive season had become "prime time for cybercriminals," with Black Friday becoming "Black Fraud day." The holiday season continues to expose both consumers and businesses to cyber threats such as phishing scams, e-commerce skimming and ransomware attacks. As we move through the final two months of 2025, threat actors will persist with their attempts to exploit the high volume of transactions, intricate supply chains and increasing reliance on digital platforms to compromise sensitive customer data, disrupt operations and erode trust, all in the name of illicit profits.

This report reviews the retail industry's threat landscape during the festive period, focusing on payment and transaction-related threats, including gift and payment card fraud, as well as consumer-facing threats such as phishing and fake websites. The report also addresses operational threats — specifically ransomware and its impact on business activity and consumer trust. Lastly, we discuss how the rise in artificial intelligence (AI) has augmented many of the aforementioned threats, increasing their likelihood of success.

Payment and Transaction-related Threats

Gift Card Fraud

In December 2024, the National Retail Federation reported gift cards were the third most purchased product during that year's Black Friday weekend shopping period. While gift card fraud is not synonymous to the holiday season, cybercriminals almost certainly target this peak period, taking advantage of the large volume of transactions in hopes that both businesses and consumers will have less oversight regarding the fraudulent sale or purchase of gift cards. Additionally, the ease with which threat actors can sell and/or trade gift cards within underground forums, combined with the minimal personally identifiable information (PII) required for purchases, makes tracking gift card fraud difficult and therefore more attractive to cybercriminals.

We continually observe numerous threat actors involved in gift card fraud. For example, the actor ***Red**, a long-standing member of the underground community who has been active on multiple cybercrime forums since at least 2015, operates a platform called Cytrongift that threat actors use to buy and sell unused codes, gift cards and vouchers.

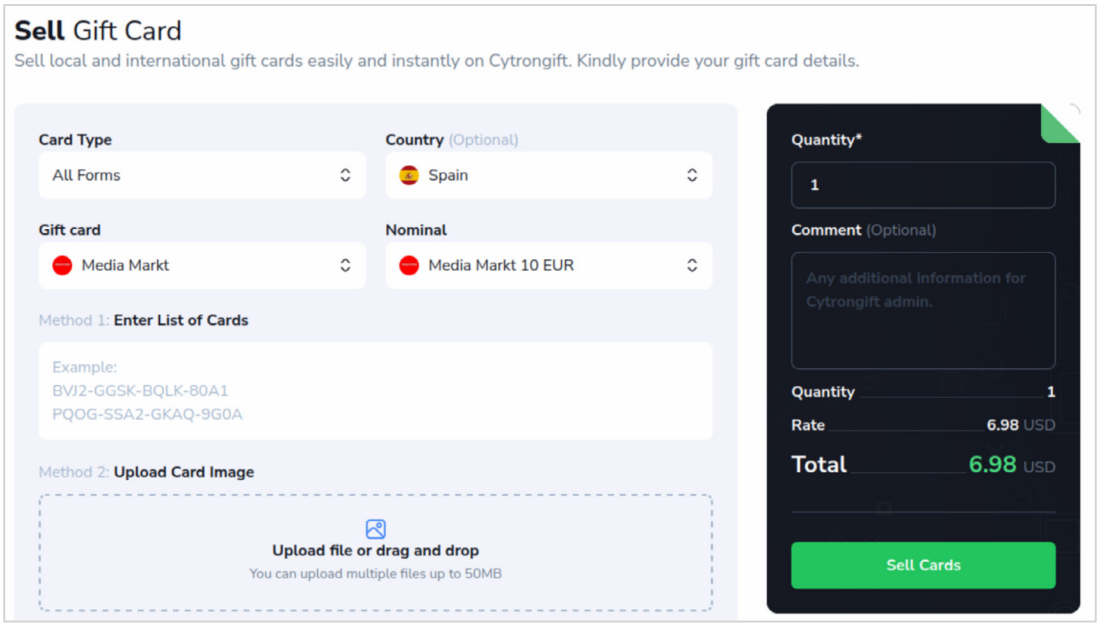

Figure 2: The image depicts a screenshot of the platform's "Sell Gift Card" page.

Statistics displayed on the platform claimed the service had more than 1,900 registered accounts, sold more than 23,300 cards and earned US $687,000 as of August 2025. Additionally, the website has a "Bonus" page with incentives for threat actors who sold gift cards in bulk — users who uploaded gift cards worth more than US $10,000 automatically were enrolled in a rewards program and earned 0.05% to 2% per sale depending on their participation level.

In November 2025, we reported the actor ***Blue** sought to buy digital gift cards with a primary interest in Amazon. The actor also expressed interest in purchasing digital gift cards for other U.S.-based retailers such as Gap, Home Depot, Levi's, Lowe's, Macy's, Nike, Ralph Lauren and TJ Maxx.

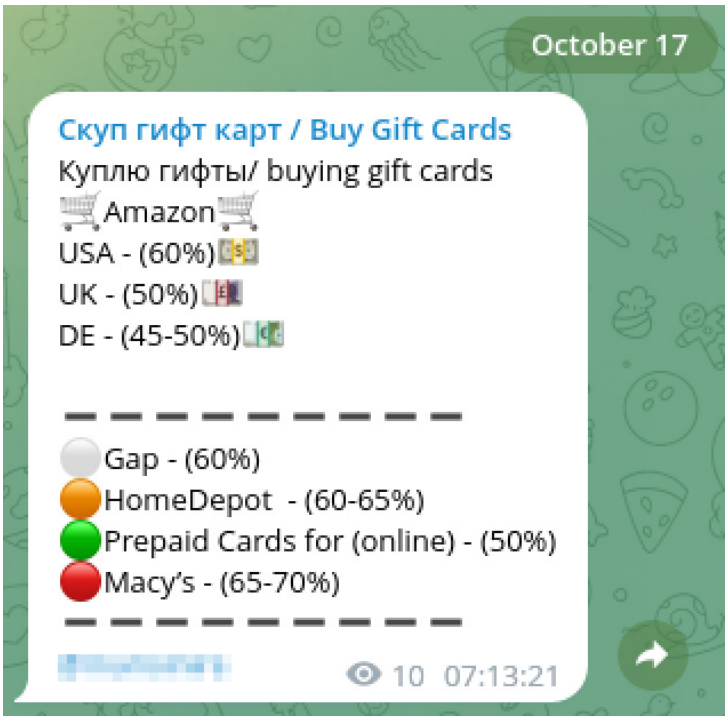

*Figure 3: The image depicts a screenshot of the actor ***Blue's** Telegram account that reveals an offer to purchase digital gift cards.*

Payment Card Fraud

While cash remains a vital part of the payment landscape, the use of payment cards has long been the preferred payment mechanism for shoppers. On the business side, the rapid influx in payment card transactions during the latter two months of the year puts increased pressure on fraud detection systems, which may struggle to quickly identify malicious activity. On the consumer side, the holiday season may leave individuals too busy or inattentive to monitor financial statements for suspicious transactions, which provides cybercriminals extended time to exploit compromised cards.

Threat actors engage in payment card fraud in several ways. Compromised payment card details often are purchased from and/or traded between other threat actors in the underground. For example, the actor ***Green** runs an underground payment card data store. The "Shop" section includes the "Cards," "Cards (NO CVV)" and "Card (NO REFUND)" subsections where users could purchase compromised card-not-present (CNP) data. The shop allegedly offered more than 750,000 compromised payment card records for multiple prices as of August 2025.

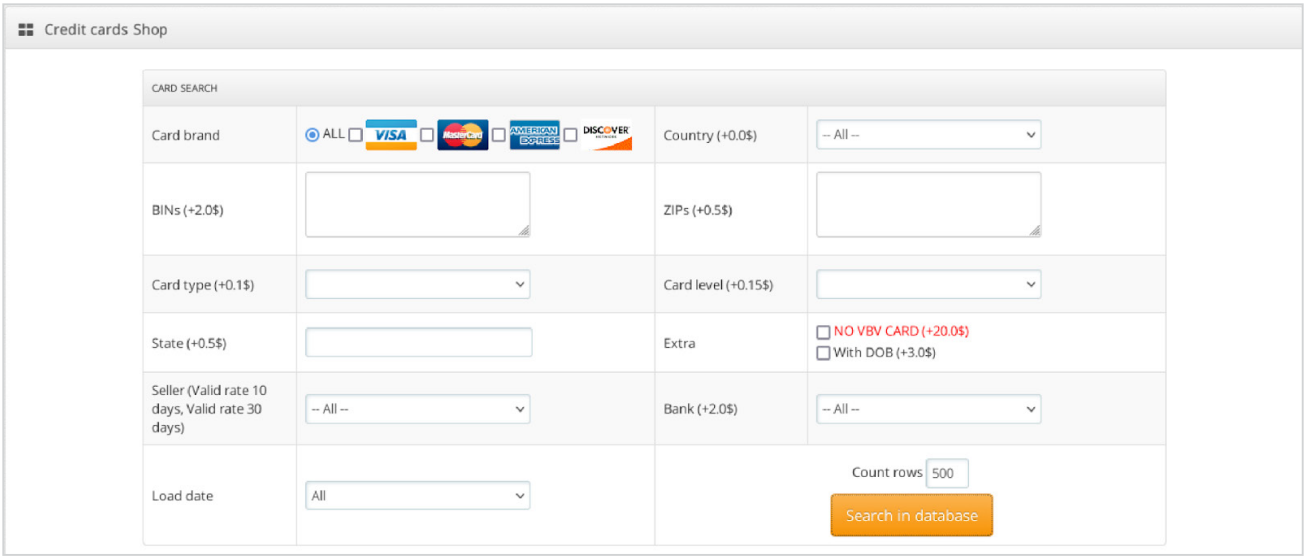

Figure 4: The image depicts a screenshot of the store's "Cards" subsection.

Cybercriminals also engage in phishing operations to obtain payment card information by sending deceptive emails or messages to victims that impersonate legitimate retailers. For example, after the cyberattack against Marks and Spencer Group PLC (M&S) in April 2025, the retailer offered legitimate e-gifts cards to some customers as an apology for the disruption. Cybercriminals were observed capitalizing on the situation, sending phishing emails impersonating M&S in hopes of making their scam more believable and therefore successful by leveraging the recent event. Threat actors almost certainly will engage in similar operations leveraging Black Friday and Cyber Monday in the coming weeks — as well as the festive period throughout December — in an attempt to increase their hit rate by blending in with the plethora of genuine emails consumers likely receive from popular retailers throughout the holiday season.

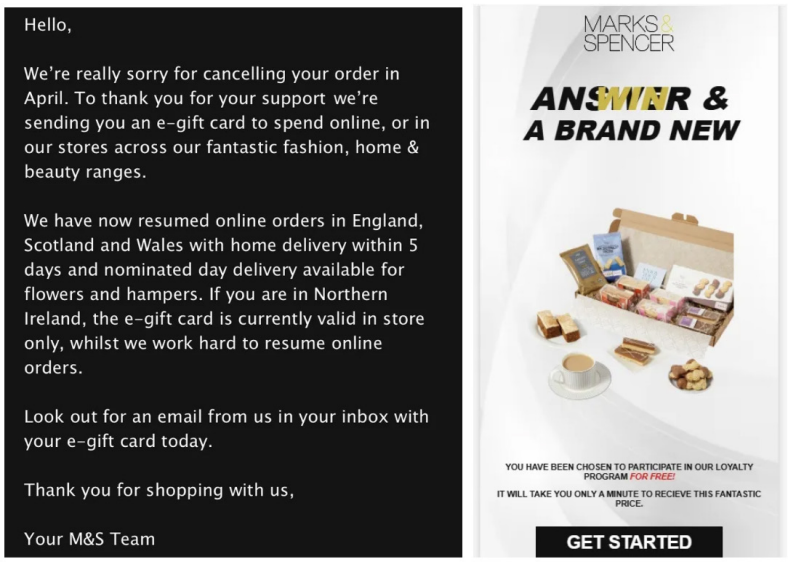

Figure 5: The images depict a legitimate email from M&S offering an e-gift card (left) and a scam email impersonating M&S (right).

Card skimming is another method threat actors employ to obtain payment card data. Physical skimming involves devices being illicitly installed on ATMs, gas pumps or point-of-sale (PoS) systems to capture card details during legitimate transactions. Digital skimming is where threat actors embed malicious code designed to capture consumers' payment details into a retail website's payment page. While many threat actors have moved away from physical skimming due to the higher risk involved in installing a device in person, in September 2025, a surveillance video from a store in New York, U.S., showed just how quickly and covertly a skimmer could be installed.

Figure 6: The image depicts how a secondary device was attached to the card reader of a shop in New York, U.S.

We observed several actors engage in digital skimming operations. Earlier in 2025, the actor ***Yellow** offered to sell an XSniffer JavaScript (JS)-based online payment card skimmer that allegedly harvested access credentials and payment card data from e-commerce platforms and transferred stolen information to a web-based control panel.

Additionally, with the rise in contactless payments, we are seeing threat actors seek to abuse near-field communication (NFC) technology for illicit gains. For example, the actor ***Orange** offered malware designed to copy payment card data by allegedly targeting NFC transactions. The Android-based malware allegedly infected a victim's phone and used the NFC system to capture a signal from nearby cards, which allowed an attacker to use the card as their own. The actor claimed the malware included two applications that provide a command-and-control (C2) function that connected to a PoS device under ***Orange's** control and another tool deployed on an infected phone to obtain the payment card data. The actor claimed to earn US $7,000 a day with the method while working with local businesses who ***Orange** paid 10% of the funds exfiltrated from stolen cards.

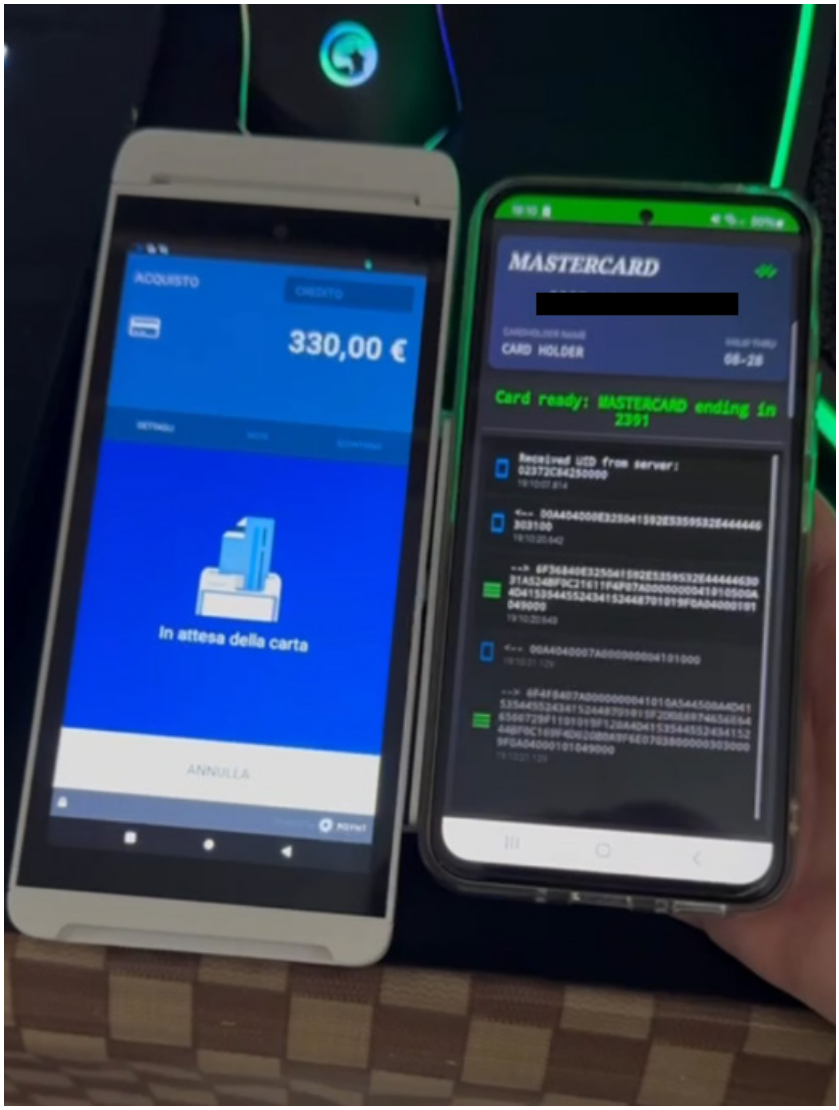

*Figure 7: The image depicts a screenshot of an attacker using **Orange's* malware to make payments to a PoS device.*

We also observed the actor ***Purple** offer NFCGate software, which allegedly was installed on two controlled Android devices. The first captured NFC data from a victim's payment card and sent it to the second device, which allegedly enabled the perpetrator to make payments using cloned contactless payment data. However, the software allegedly lacked features for covert installation or remote execution and required physical control of both smartphones involved in the transaction.

The aforementioned payment card fraud enables threat actors to execute further criminal activity, including purchasing goods from online retailers where no physical card verification is involved. Threat actors almost certainly will continue to exploit the flurry of online holiday shopping in hopes of blending in with legitimate activity to execute illicit transactions with stolen payment card data.

Consumer-facing Threats Exploiting Shopping Activity

Phishing Attacks

Phishing tactics are some of the most prevalent and harmful threats emanating from the cybercrime underground impacting both consumers and businesses during the festive period. This time of the year is synonymous with a deluge of emails, texts and social media advertisements promoting special offers, sales and deals. This provides an ideal environment for threat actors to increase current efforts or initiate operations for social-engineering activity. Shoppers expect legitimate offers from well-known retailers during this time and therefore likely are more vulnerable to these scams, which increasingly are becoming more sophisticated by closely mimicking the marketing of major brands.

After the 2024 Black Friday shopping week, the Darktrace cybersecurity company reported Christmas-themed phishing attacks increased 327% worldwide and Black Friday and Cyber Monday-themed phishing attacks soared to 692% in the final week of November 2024 compared to the beginning of the month. The company further claimed the retail industry in the U.S. displayed the largest surge in phishing emails claiming to be popular retailers and imitating promotional emails. Emails appearing to come from major brands including Best Buy, Macy's, Old Navy, Target and Walmart increased by more than 2,000% during the peak shopping period.

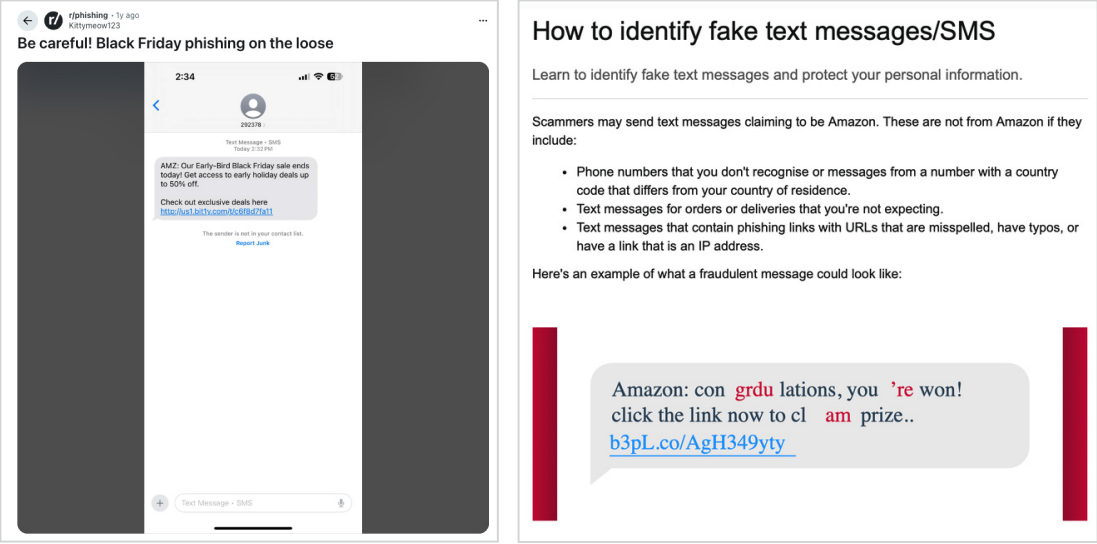

Figure 8: The image on the left depicts a screenshot of a Reddit post featuring a phishing attempt possibly trying to impersonate Amazon and leveraging the Black Friday shopping period in November 2024. The image on the right depicts a screenshot of an example of what a fraudulent Amazon-based phishing attempt could look like and tips on how to identify these messages provided by Amazon.

In November 2025, the Zimperium mobile security company reported more than 46% of detected phishing attacks in 2024 impersonated Amazon. These phishing attempts extended throughout the entire holiday season, with the majority taking place during Christmas and New Year with additional spikes around Amazon's fall Prime Event and Black Friday.

In addition to phishing attempts enticing victims through the facade of a sale, deal or special, threat actors also were observed leveraging delivery and/or refund phishing scams. Cybercriminals know that if individuals are shopping more during the holiday season, there likely is an increase in package deliveries and returns — almost certainly more than usual. Threat actors capitalize on this by sending an array of phishing emails and texts prompting victims to carry out actions related to a delivery or refund. In regard to the former, this includes confirming a delivery, updating a delivery address, tracking a package, investigating a delayed/redirected parcel or paying a "shipping fee."

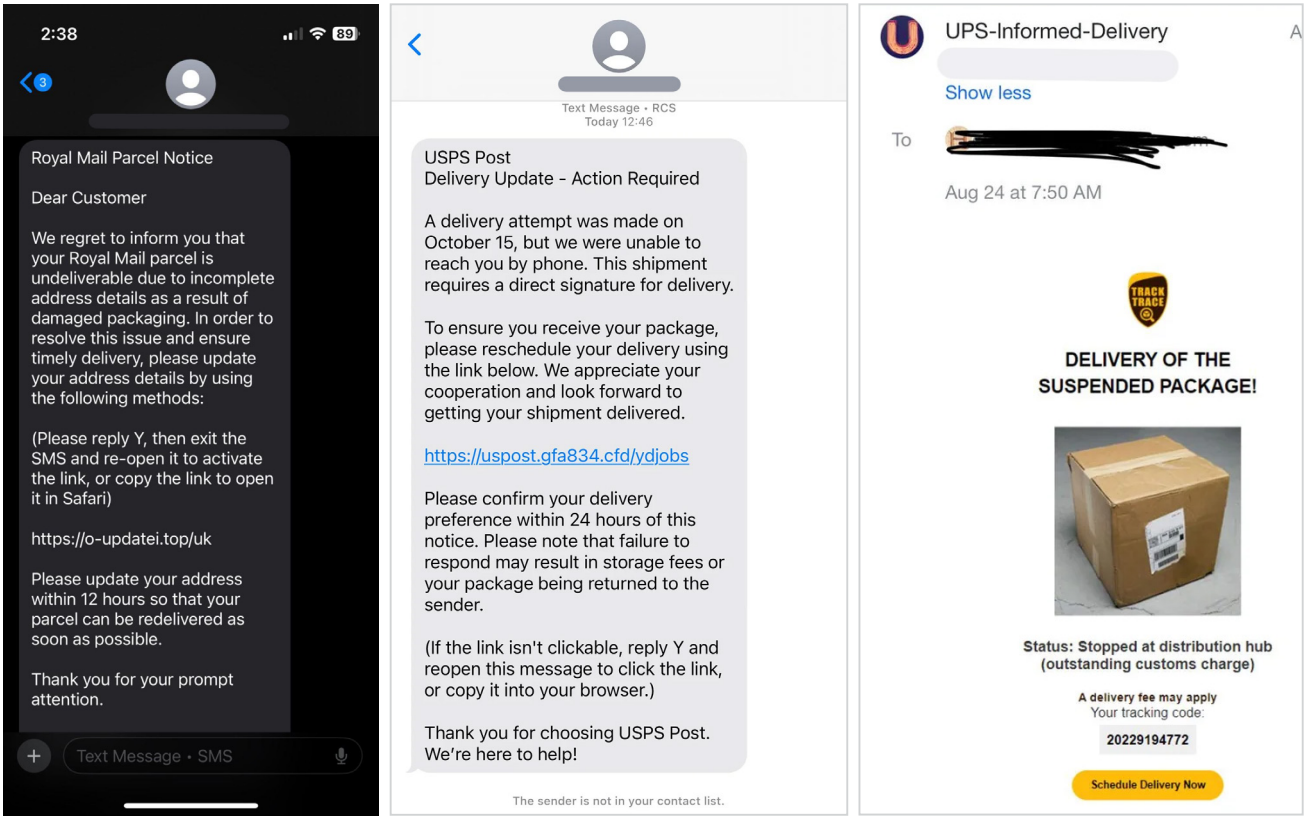

Figure 9: The images depict examples of delivery-related phishing attempts.

In regard to the latter, a threat actor might send an email or text directly asking for the victim to reply with their bank details to distribute the alleged refund or there might be a malicious link for the victim to click, which also was observed in the examples of delivery-related scams above. This tactic often sends the victim to a fake webpage that prompts them to input sensitive data, such as a username and password, bank account information and/or payment card data, allowing threat actors to record that information and gain access to a victim's account or payment card for further illicit activity.

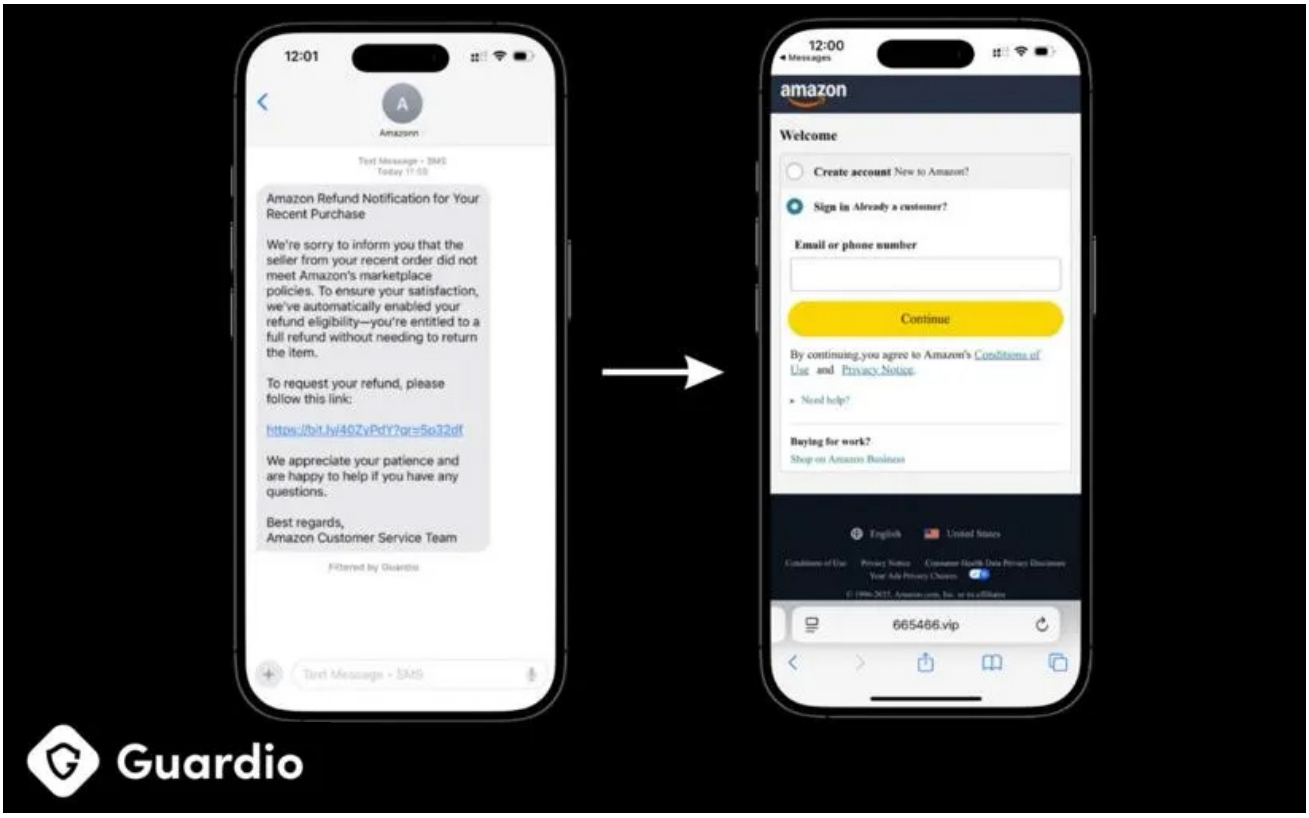

Figure 10: The image depicts a "Refund Notification" text message impersonating Amazon and the fake login page victims are redirected to.

Fake Websites

In November 2025, Euronews reported the NordVPN cybersecurity company claimed it detected a 250% increase in the amount of fake online shops in the run-up to Black Friday — with the number of websites mimicking eBay surging 525% in October 2025 compared to September, and a 232% spike in imitations of Amazon's website. These bogus websites are designed to mimic well-known companies to trick consumers into thinking they are making purchases from legitimate retailers. However, in reality, they collect sensitive information such as login credentials, payment details and personal data from unsuspecting consumers.

Through our own research on URLs that include the term "blackfriday," we also saw a spike in possibly fake websites exploiting the holiday season in the latter two months of 2024 and observed the start of a rise in similar websites at the beginning of November 2025. If trends persist as they did in 2024, we likely will see another spike in these types of fake websites throughout the latter half of November 2025 and into December 2025. We also observed a handful of domains and websites specifically designed to impersonate well-known brands in the first two weeks of November 2025. This included the jewelry retailer Pandora and the personal care company Bath & Body Works — with similar websites impersonating other popular brands almost certain to appear closer to Black Friday and Cyber Monday.

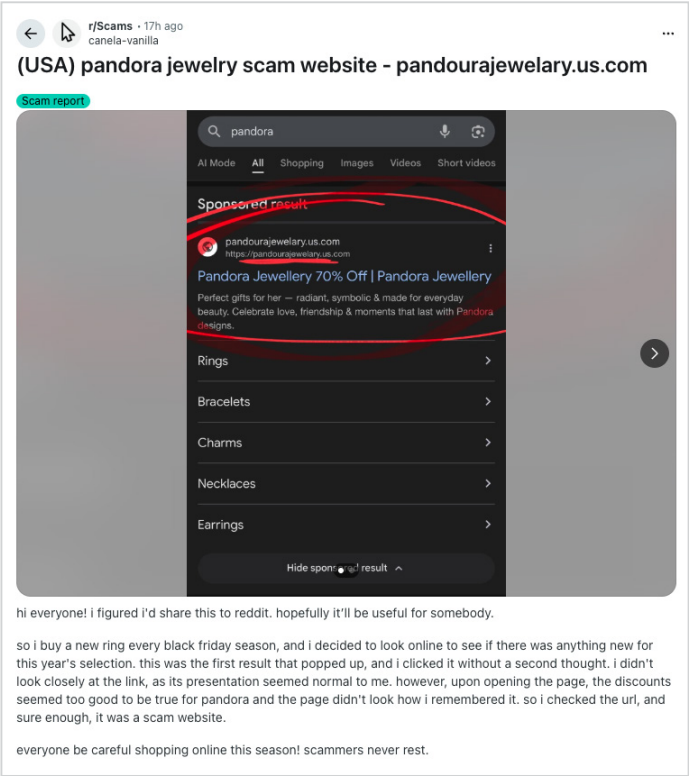

Figure 11: The image depicts a screenshot of a Reddit post featuring a likely fake website leveraging a similar domain to the popular jewelry retailer Pandora Nov. 13, 2025.

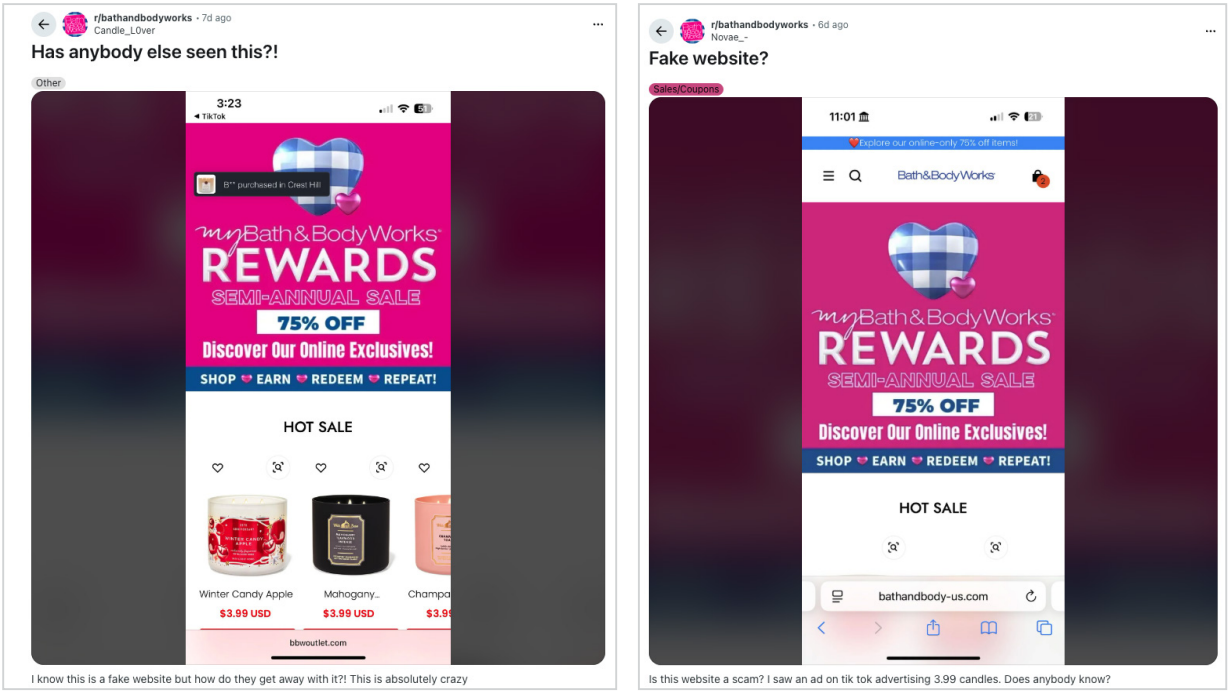

Figure 12: The images depict screenshots of Reddit posts featuring two similar examples of a fake website leveraging similar marketing and domains to the popular personal care retailer Bath & Body Works Nov. 13, 2025.

We also recently observed open source discussions about individuals possibly falling victim to social media promotions that led to a potentially fake website for Dick's Sporting Goods. One victim claimed to have made a purchase after seeing an advertisement offering a deal on UGG shoes, only to receive a confirmation email with no reference to Dick's Sporting Goods (see Figure 13). Other individuals posted similar concerns alongside images of the suspicious marketing. The advertisements appeared to appeal to both Black Friday shoppers and those looking to purchase for the December holidays.

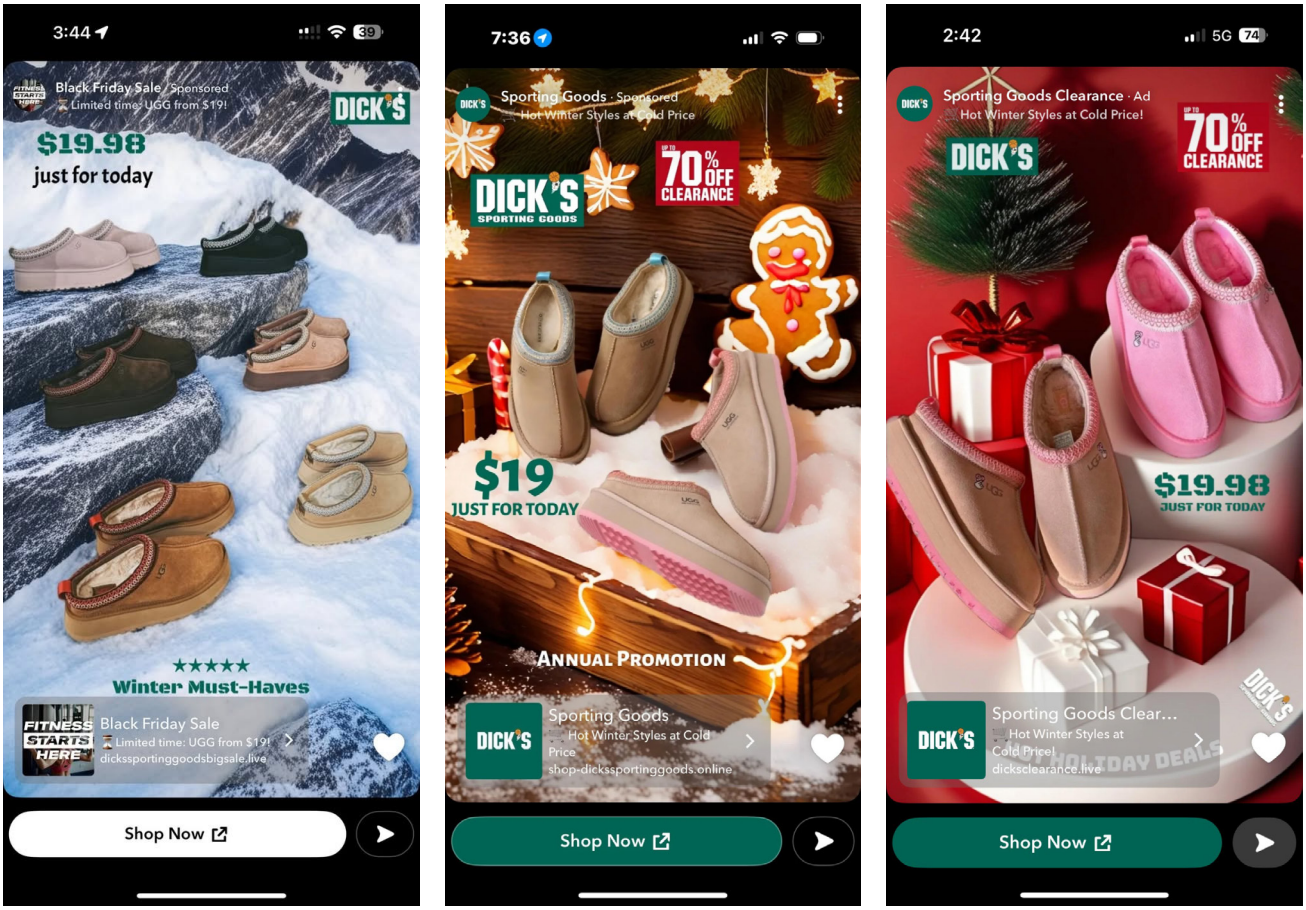

Figure 13: The images depict screenshots of advertisements from the alleged scam mimicking Dick's Sporting Goods.

Threat actors looking to engage in this type of activity can create these fake webpages themselves if they have the skill level required for such a task. However, those who do not need only look to the underground market. We continue to observe a steady supply and demand in scam pages. From April 2025 to May 2025, the actor ***Pink** offered to lease and sell scam pages via a Telegram-based bot. The actor claimed to have more than 30 scam pages that impersonated multiple legitimate companies — such as Amazon, the Brazilian department store chain Havan, the South American technology and e-commerce company Mercado Livre and the Brazilian beauty and personal care brand WePink — to capture sensitive data. The actor also allegedly developed scam pages for any store upon request.

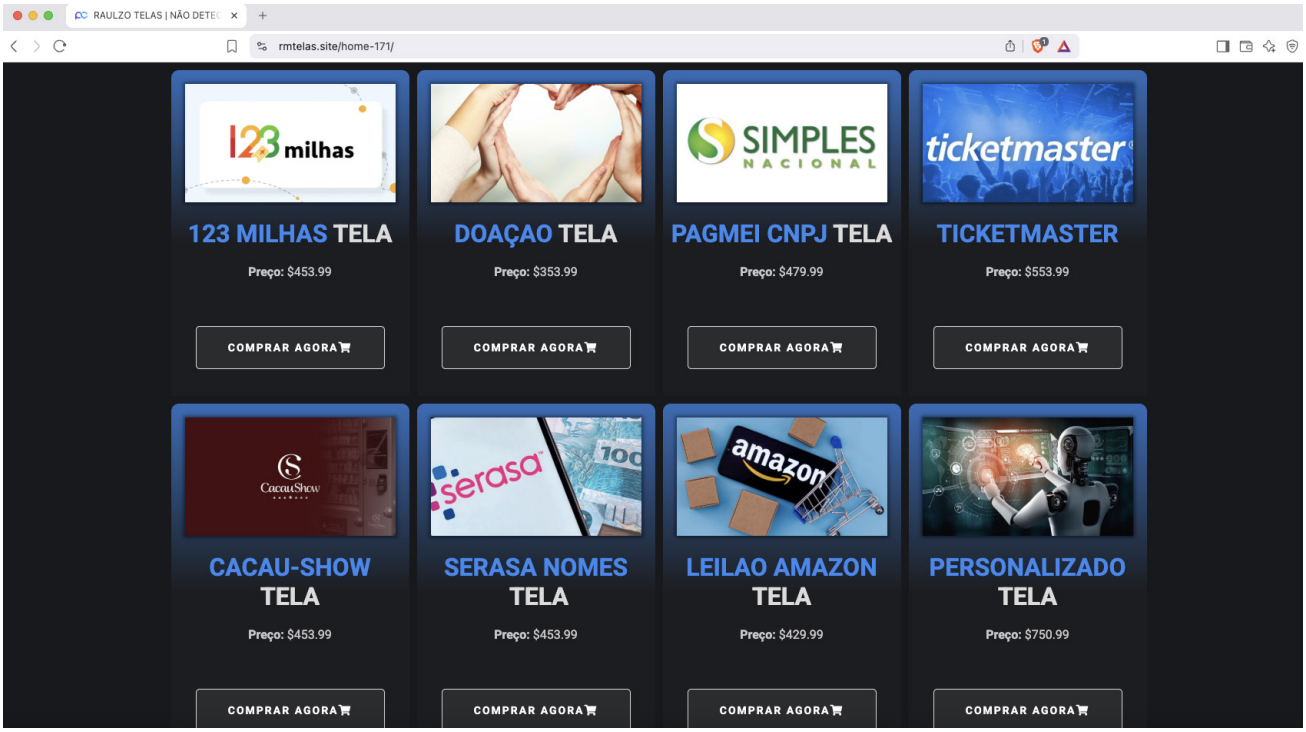

*Figure 14: The image depicts a screenshot of the actor **Pink's* scam page store.*

We also observed the actor ***Grey** offer scam pages that could be distributed via email and short message service (SMS). The actor operated a dedicated e-commerce platform where multiple malicious tools and pages were advertised and sold. The "Scam Pages" section on the website offered "ready-made scam pages" — prebuilt pages ready for deployment — and "order custom scam pages," which allowed customers to request a custom page tailored to specific needs or targets to suit different institutions or use cases.

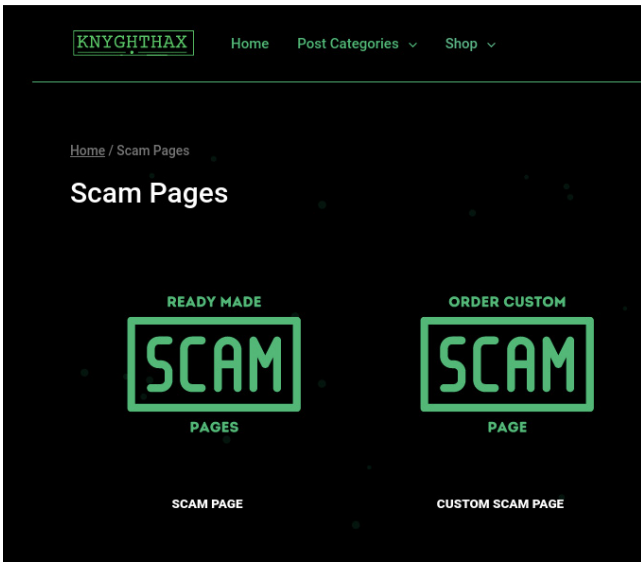

*Figure 15: The image depicts a screenshot of the actor **Grey's* e-commerce platform's "Scam Pages" section.*

Operational Threats

Ransomware Attacks

As retailers experience an increase in purchases during the holiday period, their systems likely are more vulnerable to being overloaded and therefore more susceptible to ransomware attacks. Businesses also could be more willing and/or quicker to pay ransom demands to lessen the impact of an operational disruption or outage during such a profitable season. As with the other aforementioned threats, cybercriminals are quick to take advantage of this heightened activity to execute attacks when organizations could be more vulnerable.

In 2024, we detected 51 ransomware breaches impacting the retail industry during November and December, which accounted for 18% of the total breaches for the year. Within those two months, 36% of breaches were attributed to the activity of four ransomware groups — **LockBit**, **RansomHub**, **Play** and **Akira**.

Since the start of 2025, we reported 462 ransomware breaches impacting the retail industry, representing an almost 91% increase from the same period in 2024. The U.S. experienced the highest number of incidents, accounting for 55% of events, followed by Canada and Spain at almost 9% and 3%, respectively. The most impactful ransomware groups during this period — **CLOP**, **Qilin** and **Akira** in descending order — were responsible for 44% of all breaches targeting the industry.

Moreover, in the first two weeks of November 2025, we identified 15 breaches impacting the retail industry. If this cadence continues, we could see a slight increase in attacks against the industry for November and December 2025 versus the same time period in 2024.

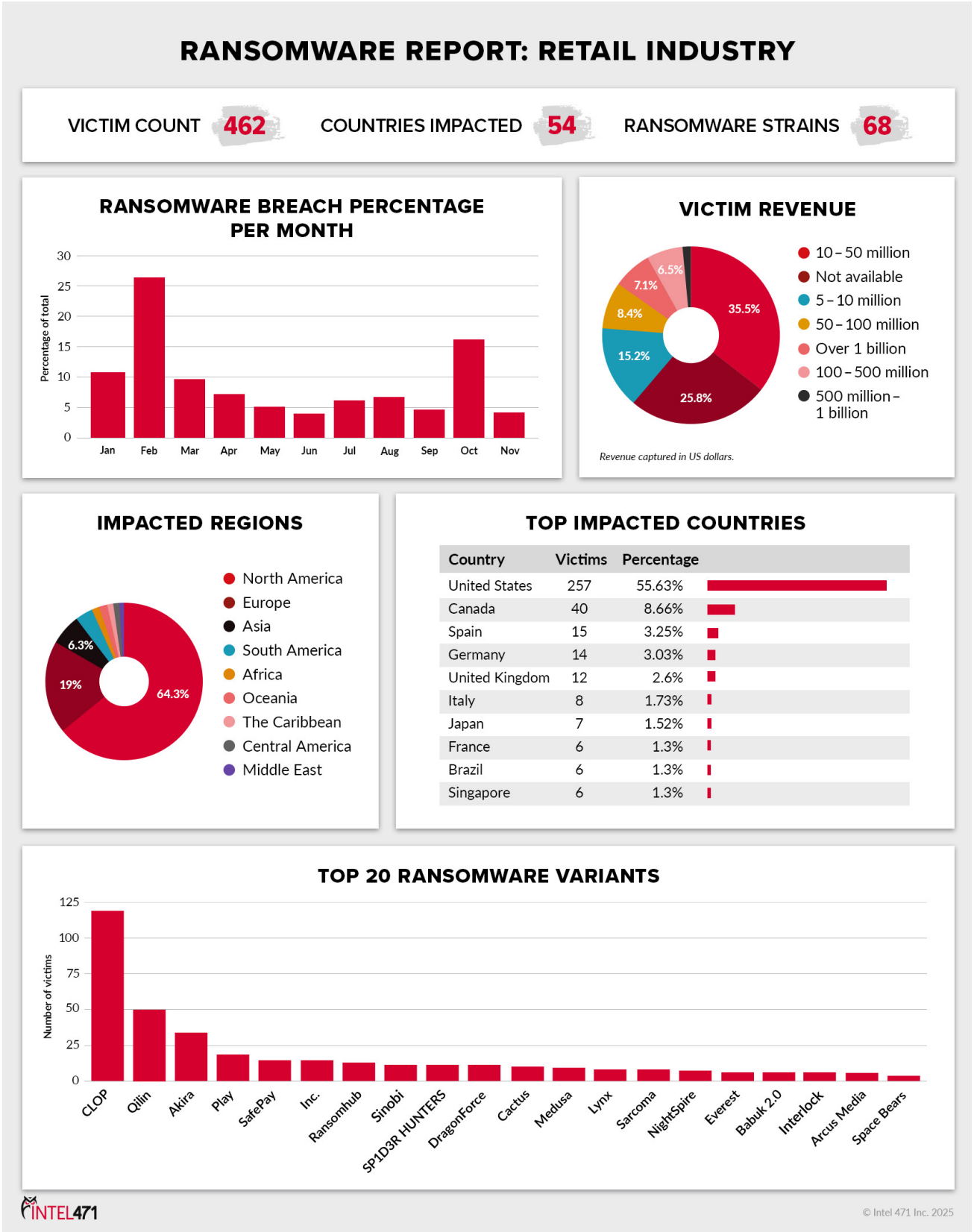

Figure 16: This graphic depicts an overview of ransomware attacks impacting the Retail industry from Jan. 1, 2025 to Nov. 17, 2025.

Rise of Artificial Intelligence

We continue to report on the rise of AI and how it has been reflected in the cybercrime underground. We previously assessed AI improves methods cybercriminals already leverage, with threat actors finding new ways to use the technology to increase their potential rather than treating it as a stand-alone capability. It likely also has enticed and enabled both newcomers to and novices of the underground marketplace to carry out cybercriminal activity by lowering the barrier of entry. Moreover, AI's rapid evolution presents a significant and escalating threat to online trust and security, of which retailers and their customers are not immune.

One of the main use cases of AI within the underground that we consistently observe is its enhancement to social-engineering activity. Social engineering touches many of the threats prevalent during the holiday season, and AI significantly has increased its efficiency and authenticity and therefore its effectiveness. Threat actors now are able to rapidly create curated phishing content — such as fake webpages, texts and emails in non-native languages, impersonation attempts and other synthetic media — with much less effort. Consequently, we have seen a shift from broad opportunistic scams to more targeted and personalized campaigns that mimic legitimate business and organizations with increasing accuracy.

AI improves methods cybercriminals already leverage, with threat actors finding new ways to use the technology to increase their potential rather than treating it as a stand-alone capability

This year we reported the actor ***Black** offers deepfake videos using lip-sync and face-swap technologies, which can be leveraged for fake promotional videos, Google Ads and more. The actor's team members allegedly have more than two years of experience producing high-quality deepfakes and allegedly employ AI-powered tools to enhance overall visual quality. Additionally, if a customer lacked a source video or ideas for a scenario, the actor's team would provide several options. We also observed the actor ***White** offer a service creating AI-driven images. The actor claimed to be on a team whose members specialize in graphic design and motion graphics and offered a wide range of services including images and videos for advertisements as well as screen mock-ups for custom content.

We also recently observed open source discussions about potentially fake AI-generated family jewelry store webpages. One user claimed a website called Anna & Felix appeared upon first glance to be a small family business where a mother and her son sold their handcrafted jewelry. The user then stated several other websites exist under other parent/child names and display very similar images and almost identical wording. We input the names into URLScan and confirmed the existence of these possibly fraudulent webpages — one of which appears to offer an "exclusive autumn sale." The screenshots below reveal the websites display nearly identical images and messages alongside the same offer of an 80% discount.

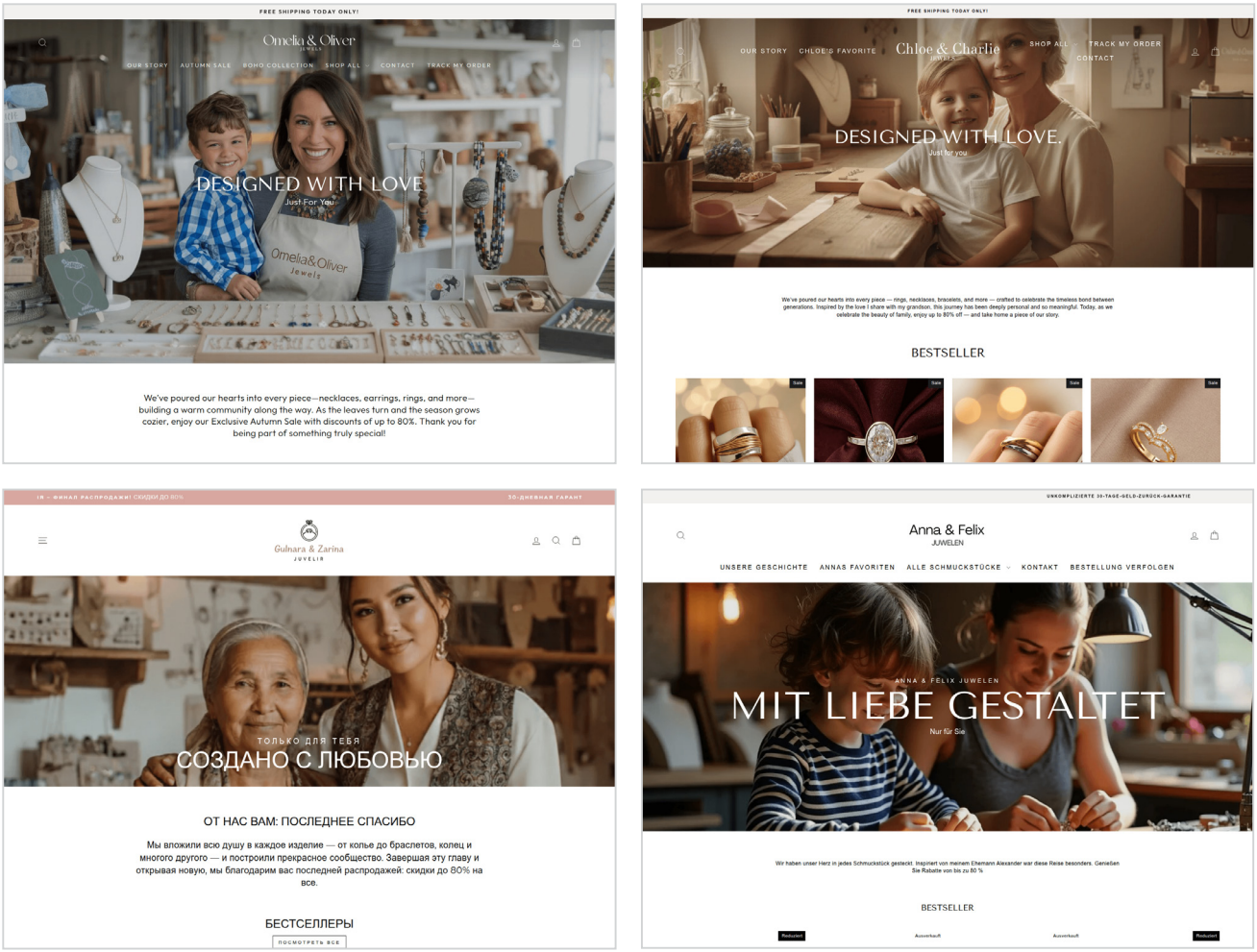

Figure 17: The images depict screenshots provided by URLScan when queried with omeliaoliverjewels, chloecharliejewels, gulnarazarina-juvelir and annafelixjuwelen.

Assessment

History continues to provide us with evidence that as the festive period approaches, we almost certainly will see a rise in various cyber threats. Payment and gift card fraud likely will surge during the holiday season as threat actors seek to exploit the increase in transaction volume and retailer promotions. This almost certainly will coincide with phishing campaigns leveraging holiday-themed lures such as Black Friday discounts, spoofed delivery notifications and fabricated refund claims. Simultaneously, sham e-commerce websites and malicious advertisements almost certainly will proliferate as threat actors target consumers seeking the best deal. Ransomware operators also may escalate activity, taking advantage of retailers' limited tolerance for operational disruptions or outages during peak sale periods.

Further, AI almost certainly will continue to amplify the sophistication and efficiency of various festive-period cyber threats targeting both retailers and consumers. It has the ability to enable threat actors to produce customized phishing lures, more convincing fake customer service messages and fraudulent branded delivery notifications that more accurately impersonate legitimate retailer communications. Moreover, while individuals and organizations alike previously could identify these scams through grammatical and formatting errors, AI has greatly compromised that detection method. This technology also is being used to automate and/or streamline the creation of bogus e-commerce websites, advertisements and social media promotions at scale, making it harder to distinguish fake listings from real ones. As a result, AI has transformed what used to be a more manual threat into one of greater volume and authenticity, increasing overall risk during the holiday shopping period. Nevertheless, we continue to assess AI's impact on cybercrime functions more as an efficiency upgrade rather than a fundamentally new threat, with threat actors seeking methods to leverage AI more effectively — focusing on enablement and scaling as opposed to the implementation of fully automated attack chains.

Recommendations

Prevention Strategies

- **Implement multifactor authentication (MFA):** Enforce MFA across all employee and customer accounts to add an extra layer of security against unauthorized access due to compromised credentials.
- **Regularly train employees:** Provide comprehensive cybersecurity awareness training for all staff, including seasonal and temporary employees. Focus on recognizing phishing attempts and social-engineering tactics and proper handling of sensitive information.
- **Strengthen network security:** Implement robust firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), and network segmentation to protect sensitive data and systems. Regularly update and patch all software and hardware to address known vulnerabilities.
- **Monitor for fake websites and brand misuse:** Use brand monitoring services to detect and take down fraudulent websites and ads impersonating your business.
- **Develop an incident response plan:** Create and regularly update an incident response plan tailored to holiday-specific threats.
- **Leverage customer awareness initiatives:** Inform customers about prevalent scams during the holiday season.

Detection Strategies

- **Continuous network monitoring:** Implement security information and event management (SIEM) systems to monitor network traffic and system logs for suspicious activities in real time.
- **Threat intelligence integration:** Use threat intelligence feeds to stay informed about emerging threats and indicators of compromise (IoCs) relevant to your industry.
- **Endpoint detection and response (EDR):** Use EDR solutions on all endpoints to detect and respond to threats at the device level, including malware infections and unauthorized access attempts.
- **Employee reporting mechanisms:** Establish clear channels for employees to report suspicious emails, calls or activities.

Intel 471's General Intelligence Requirements (GIRs)

1.1.1 Ransomware malware
1.1.9 Point-of-sale (PoS) malware
2.1 Vulnerabilities
4.1.5 Prepaid or gift card fraud
4.2.1 Payment card fraud
4.2.1.1 Online payment card skimming
4.2.2 Compromised credentials
4.2.3 Compromised personally identifiable information (PII)
4.3.2 Account checking and credential stuffing
4.3.3 Account brute forcing
4.4.1 Phishing
4.4.4 Social media scams
4.4.5 Smishing
4.6 Artificial intelligence (AI) fraud
5.3.2 Physical point-of-sale (PoS) system attack techniques
6.1.1.7 Retail, wholesale and distribution industry

About Intel 471

Intel 471 equips enterprises and government agencies with intelligence-driven security offerings powered by real-time insights into cyber adversaries, threat patterns, and potential attacks relevant to their operations. By integrating human-sourced intelligence with advanced automation and curation, the company's platform enhances security measures and enables teams to bolster their security posture by prioritizing controls and detections based on real-time cyber threats. Organizations are empowered to neutralize and mitigate digital risks across dozens of use cases across our solution portfolios: Cyber Threat Exposure, Cyber Threat Intelligence, and Cyber Threat Hunting. Learn more at intel471.com.

Our customers' eyes and ears outside the wire.