CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

November 22, 2022

SEASON OF GIVING, SEASON OF TAKING: Heightened Fraud During Holiday Shopping

This report details the risks the holiday season presents for individuals and financial institutions, describes the tools and services that scammers can use during the holidays, and provides tips on how to avoid threats during this period. It is intended for fraud and cyber threat intelligence (CTI) teams at financial institutions and security researchers.

Executive Summary

With Black Friday and Cyber Monday soon beginning the holiday shopping season, merchants are increasing efforts to attract consumers and online shoppers are looking for discounts. Meanwhile, in the criminal underground, a parallel process is beginning as threat actors anticipate increased opportunities to commit fraud. While retailers offer discounts on the latest electronics and clothing, carding shops offer discounts on compromised payment card data. While manufacturers increase production and create innovative goods and services, threat actors release phishing and scam sites to lure in online shoppers and use the latest criminal software. And while retailers launch advertising campaigns and partner with marketing firms, threat actors prepare spam lists and partner with other threat actors to place online ads for their fraudulent websites.

This report analyzes threat actors' offerings and discussions on fraud-focused forums, carding-shop activity, and phishing and scam website activity from previous holiday seasons. Threat activity during this period involves all stages of the fraud life cycle, from the point of compromise to sale and fraudulent monetization. Historical data from the past 3 years shows that the volume of compromised payment cards offered for sale increases during the holiday season in comparison to the preceding and following 3-month periods. Ultimately, it is likely that the 2022 holiday season will follow a similar pattern, resulting in a period of heightened risk for cardholders, financial institutions, and associated service providers.

Key Judgments

- Cybercriminals are sensitive to changes in victims' purchasing habits during the holidays. As online shopping increases during the holidays, cybercriminals prepare to take advantage of expanded opportunities to defraud their victims.
- Cybercriminals exploit seasonal changes in merchants' anti-fraud measures, especially as anti-fraud measures are loosened to better handle the surge of transactions during the holidays.
- Promotions, discounts, and special offers for illicit services and stolen data increase during the holidays, encouraging more cybercriminal activity both during and after the holiday season.
- Cybercriminals are likely to take advantage of common holiday-related promotions such as Black Friday and Cyber Monday by creating themed phishing and scam pages designed to entice victims with the promise of savings.
- An increase in compromised payment cards posted for sale is likely during the holidays. This could be a result of increased shopping activity, relaxed anti-fraud measures, and increased phishing and scam activity.

Background

Payment fraud is a game of cat and mouse. The cats (financial institutions, payment card networks, merchants, payment processors, law enforcement, and payment fraud intelligence companies) continue to refine data-driven anti-fraud systems, develop more secure methods of payment, and improve payment card data storage standards. For the mice (threat actors and carding shops), the focus is adaptability. They must identify the cats' blind spots and squeeze out criminal profits for as long as they remain.

For threat actors, adaptability occurs at all stages of the fraud life cycle: the abuse of legitimate services for more persistent e-skimming and hard-to-detect card checking, bypassing security advancements like 3-D Secure (3DS), and responding to exogenous shocks to card fraud market like the brief but unexpected Russian law enforcement crackdown on cybercrime.

Threat actors view Black Friday and the holiday season as another opportunity to adapt their schemes, offerings, and activities to squeeze out additional criminal profits. Over the past 3 years, the volume of compromised card-not-present (CNP) payment cards offered for sale on carding shops during the holiday season — November through January — has typically exceeded the preceding 3 months by an average of 5% and the following 3 months by an average of 20%.

Although the past 3 years of data indicate a relationship between the holiday season and payment fraud, we identify spikes in card fraud throughout the year resulting from a host of other factors (innovations by threat actors, large-scale breaches, carding shop dynamics, and more). Therefore, the holiday season should not be interpreted as a fundamentally exceptional period of increased fraud activity, but as another prominent example of threat actors' adaptability, which in this case corresponds to a specific seasonal period.

Threat Analysis

Cybercriminals take advantage of the holidays to conduct their activities more frequently and effectively. The holidays present threat actors with enhanced opportunities to avoid detection since victims are less likely to notice fraudulent transactions due to the increased volume of sales and purchases. In part, promotional discounts on illicit services and stolen data within the threat actor community also facilitate a rise in attacks. Additionally, threat actors can attempt to directly exploit consumers' relaxed spending habits with targeted phishing attempts such as holiday-themed phishing and scam pages.

Merchants and Anti-Fraud Measures

Threat actors presume that merchants adjust their anti-fraud measures during the holidays and seek to exploit this. Indeed, Recorded Future has previously confirmed that certain e-commerce websites disable security features such as 3DS — a protocol designed to provide additional security to online credit and debit card transactions — for purchases up to a certain threshold. Depending on the merchant, this threshold may begin in the hundreds of dollars. Cybercriminals can use experimental transactions to determine what purchase amount triggers anti-fraud measures, then keep subsequent purchases under this threshold to avoid detection.

On November 27, 2021, the threat actor "primum_leo" on the dark web forum WWH Club posted an advertisement of their "drop service". Drop services make use of hired individuals who intercept stolen packages, verify purchases, and occasionally impersonate account owners, and are vital to the success of card fraud. In the advertisement, primum_leo claimed that Black Friday and Cyber Monday are days of "open doors" in underground carding shops, stating cybercriminals can exploit surging transaction volumes and relaxed anti-fraud measures. According to the ad, threat actors may wish to use this discounted drop service in order to take advantage of relaxed anti-fraud measures.

Similarly, on August 19, 2022, the threat actor "Vyebist" on the dark web forum WWH Club commented that PayPal adjusts the rigor of its anti-fraud measures based on transaction volume and time of year. According to Vyebist, companies tighten anti-fraud measures in the summer, when demand for various products declines. However, during more profitable periods — from autumn into the winter holidays, for example — Vyebist claims companies relax anti-fraud measures. According to the threat actor, this strategy enables companies to maximize profits while simultaneously minimizing running costs and user dissatisfaction from declined legitimate transactions. In other words, companies seek to balance risk versus reward during heightened periods of purchasing activity.

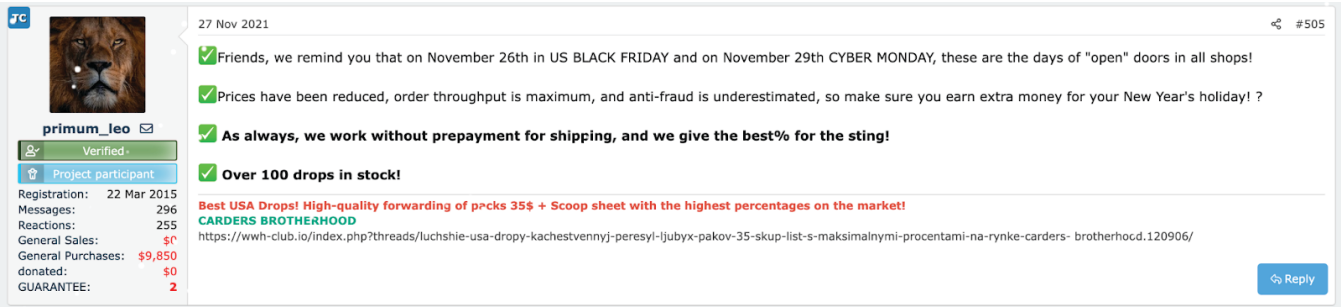

Figure 1: *(Machine translation from Russian) Threat actor primum_leo claims Black Friday and Cyber Monday are "open days" in many carding shops (Source: WWH Club forum)*

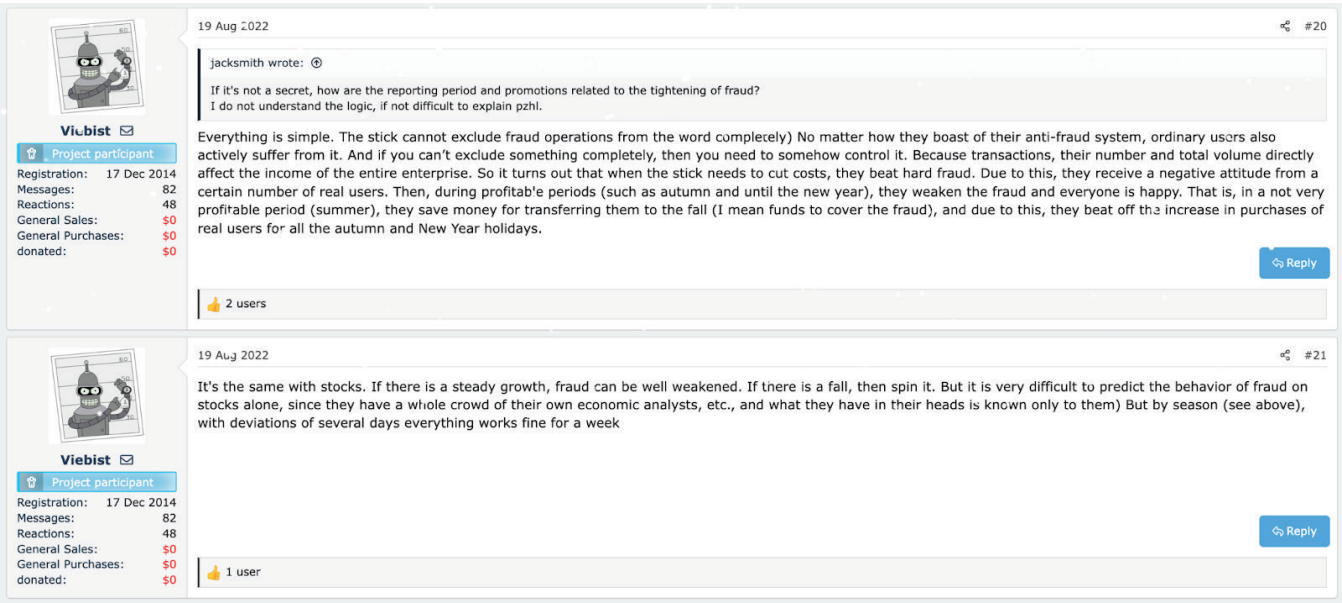

Figure 2: *(Machine translation from Russian) Threat actor Vyebist shares their opinion regarding Paypal's anti-fraud measures (Source: WWH Club forum)*

The volume and degree to which merchants actually adjust their anti-fraud measures during periods of increased transactions is less significant than the fact that threat actors like primum_leo and Vyebist at least perceive this to be true. And just as retailers may approve a greater volume of payments despite the increased risk of fraud to capitalize on surging transactions, threat actors may undertake more criminal operations despite the risk of detection to capitalize on relaxed anti-fraud measures.

Discounts and Promotions for Illicit Services and Stolen Data

The increased availability of illicit services and stolen data on dark web marketplaces during the holidays may also facilitate a rise in cybercriminal activity. As with legitimate enterprises, the holidays present an opportunity for threat actors to post discounts, promotions, and sales. Over the past 3 years, Recorded Future analysts have observed measurable increases in discounted illicit services and stolen data during the holidays. An analysis of carding shop activity revealed an uptick in both the quantity of stolen cards posted for sale from November to December and the number of holiday-related discounts for these records. Notably, the volume of cards sold slightly decreases at the end of December and significantly increases in January. This may occur because Eastern European cybercriminals frequently take extensive holidays in December before returning to "work" in January.

Holiday offers are common among vendors who provide proxy services or stolen personally identifiable information (PII). On December 3, 2021, the threat actor "CNN_News" posted an advertisement on the dark web forum WWH Club offering Black Friday discounts at CC2BTC. CC2BTC was a Russian- and English-language carding shop that opened in May 2020 and closed in spring 2022. CC2BTC operators actively advertised the shop on at least 4 forums — WWH Club, Exploit, Verified, and Omerta — and used holiday specials as a marketing ploy to attract new customers and increase loyalty among existing users. Although CC2BTC has since closed, currently active carding shops have similarly offered discounts in the past and are highly likely to do so again this holiday season.

A similar situation has arisen among other dark web vendors. Stealer logs, proxy services, bulletproof hosting (BPH), and dedicated servers are often posted for sale during the holidays, allowing threat actors to fortify their fraud infrastructure for cheaper than usual. Recorded Future analysts have previously recorded a number of promotions marketed toward threat actors coinciding with the holidays:

- In November 2021, on the dark web forum WWH Club, a fraudulent banking enrollment service used to compromise victims' banking login credentials was discounted by 30%.
- In November 2021, on the dark web forum Nulled BB, a promotional offer for web proxies which would allow cybercriminals to mask their activities was posted.
- In November 2021, on the dark web forum Exploit, a Black Friday promotion for stealer logs used to gain illicit access to victims' accounts was posted.
- From December 2021 to January 2022, on the dark web forum WWH Club, a server hosting provider offered a variety of discounts on hosting services meant for criminal activities such as brute force attacks.

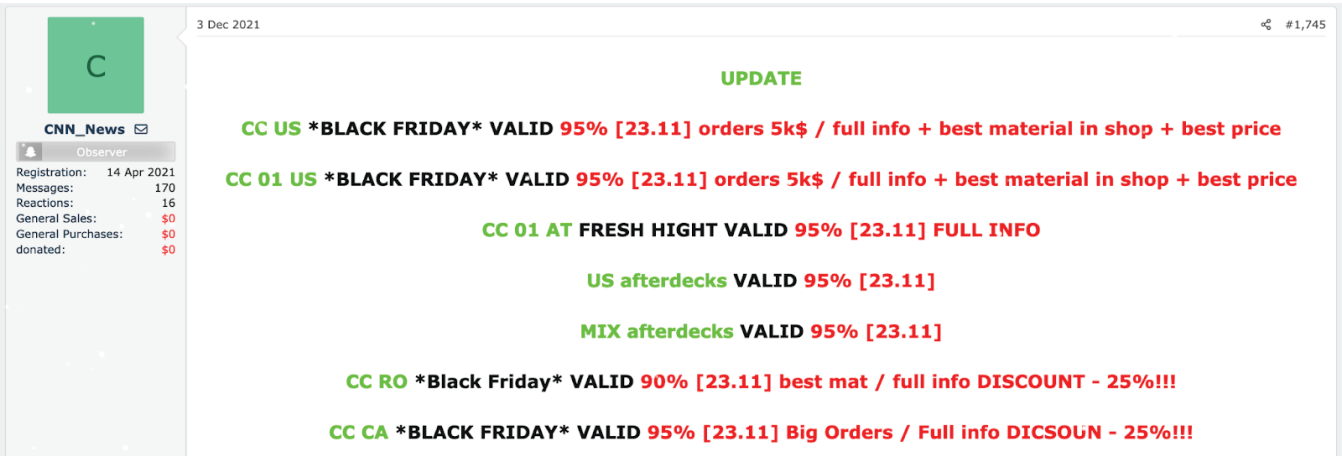

Figure 3: *Threat actor CNN_News announced Black Friday discounts on carding shop CC2BTC (Source: WWH Club forum)*

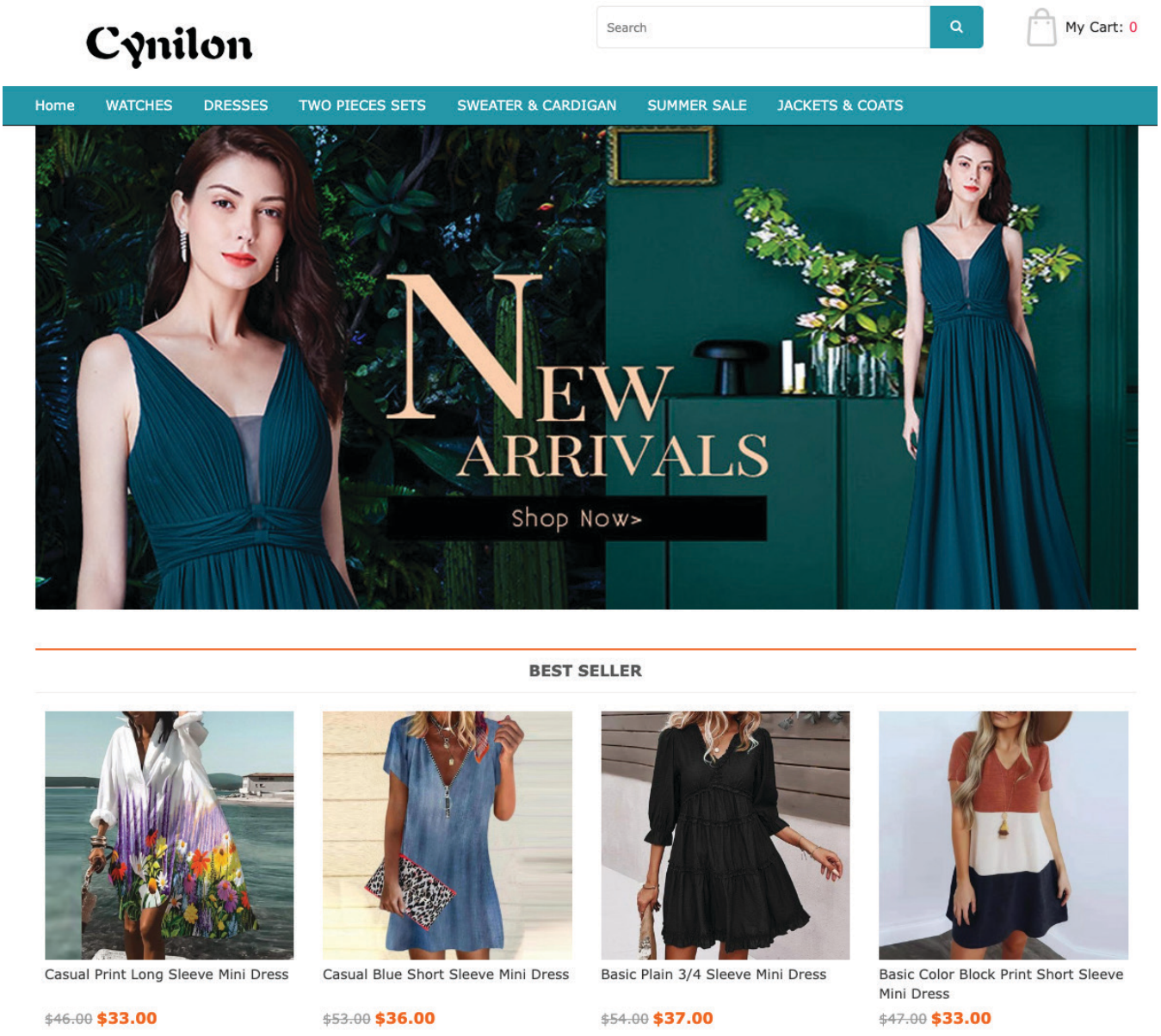

Figure 4: *Quality phishing and scam pages are often indistinguishable from legitimate e-commerce pages (Source: Recorded Future)*

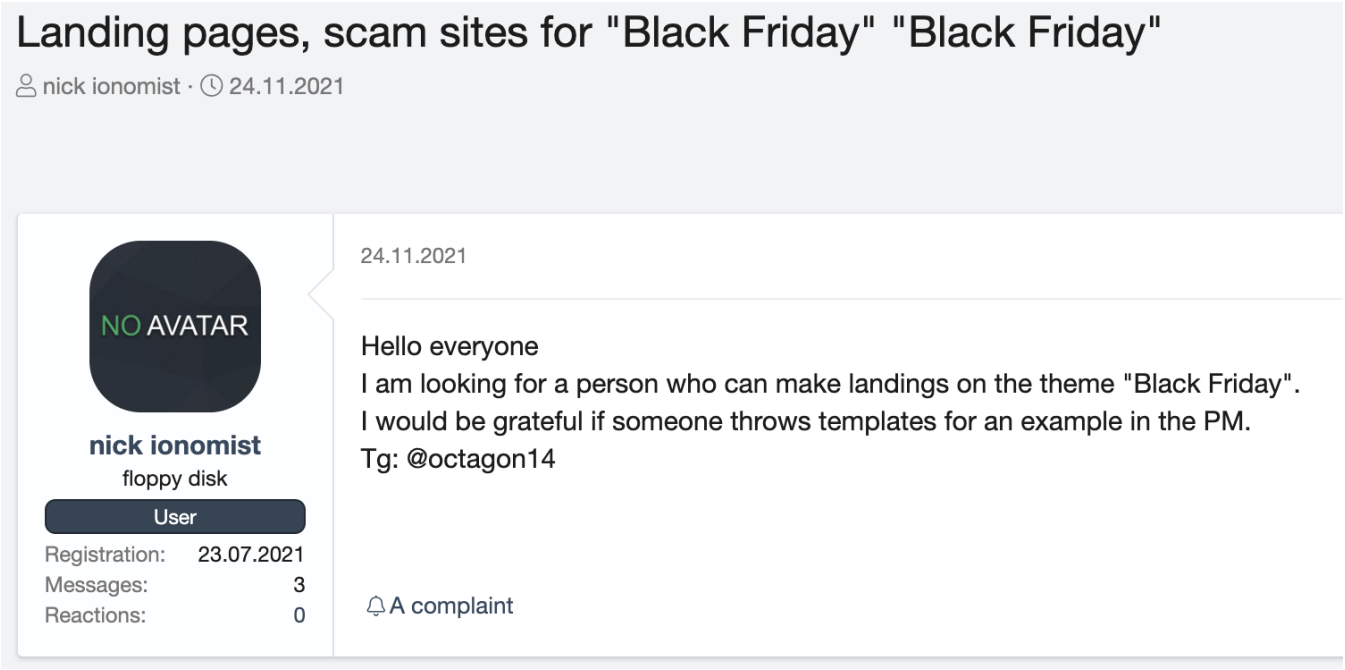

Figure 5: *(Machine translation from Russian) Threat actor nickjonom requested help creating a landing page for a scam shop for Black Friday (Source: XSS forum)*

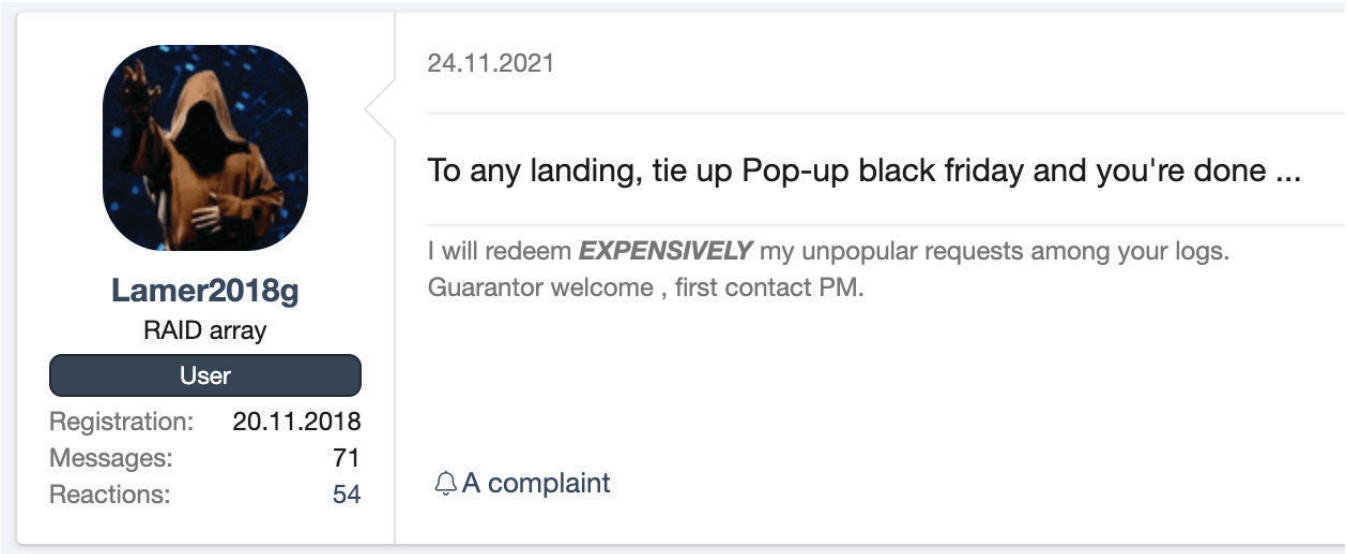

Figure 6: *(Machine translation from Russian) Replying to nickjonom, another actor Lamer2018g suggested adding a Black Friday pop-up ad to a landing page (Source: XSS forum)*

"Festive" Phishing and Scam Pages

On dark web forums, Recorded Future analysts have observed various threads and posts indicating users' interest in creating holiday-themed phishing and scam pages. Threat actors seek to take advantage of relaxed spending habits during the holidays to defraud more victims. To do this, they seek out individuals who can create holiday-themed landing pages — web pages created specifically for advertising or marketing purposes — to attract potential victims to their phishing or scam pages. Phishing pages typically mimic popular e-commerce websites and are designed to steal payment information provided by victims, whereas scam pages appear as legitimate retailers but do not actually offer any actual product, instead stealing victims' funds and payment card information after they are charged.

On November 24, 2021, the threat actor "nickjonom" on the dark web forum XSS requested assistance creating a holiday-themed landing page for a scam shop for Black Friday.

Replying to nickjonom's request, threat actor "Lamer2018g" suggested simply adding a fraudulent Black Friday pop-up ad to an existing landing page.

An increase in phishing and scam pages would likely contribute to a surge in compromised payment cards and PII. Scammers typically monetize stolen payment card and PII data obtained from their phishing websites through resale on dark web marketplaces and forums, or for personal use to commit payment card fraud.

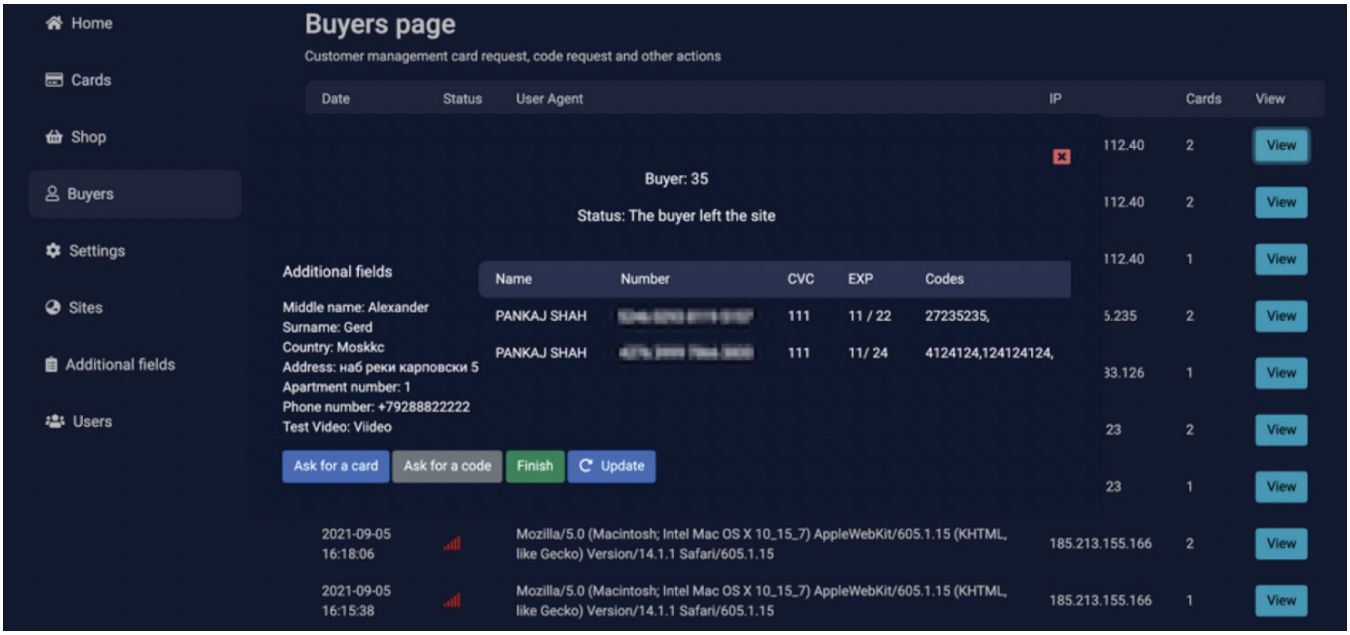

Figure 7: *The phishing panel "FishPanel" includes phished card data, a browser fingerprint, and the "Ask for a code" prompt to phish victims' 3DS verification codes (Source: XSS Forum)*

Phishing Panels

With a rise in phishing and scam pages likely, tools and services like phishing panels are also likely to see greater use. Phishing panels dramatically simplify phishing operations and provide threat actors who commit fraud the means to bypass verification tools like 3DS. In the wake of the massive adoption of 3DS in Europe and its growing popularity in the US, 3DS bypass has become increasingly necessary to compromise victims' payment cards. Consequently, phishing panels have also become widespread.

To effectively employ phishing panels, cybercriminals must first link their phishing page to their phishing panel. After a victim arrives on the phishing page, live data from the victim's browsing session populates the threat actor's phishing panel. After the phishing website prompts the user for payment, the victim enters their payment information, which again automatically populates the threat actor's phishing panel.

The threat actor then initiates a prompt for 3DS verification on the phishing page. As the victim waits to receive their 3DS verification code — an actual code has not yet been sent — the cybercriminal uses payment card data gleaned from the victim using the phishing panel to initiate a real purchase on another e-commerce website. This fraudulent transaction triggers the 3DS protocol, sending a real 3DS verification code to the victim. Once the victim receives and inputs this code into the prompt on the phishing website, the real code populates the cybercriminal's phishing panel. The cybercriminal can then collect the phished code and use it to complete their fraudulent transaction.

Obstacles and Challenges for Scam Pages

Depending on how scam pages are executed, barriers to entry may exist. On popular social media platforms, cybercriminals can claim to sell goods under the guise of a fake retailer, but they face challenges monetizing fraudulent transactions or phishing victims' payment card information. Major payment gateways frequently used to process payments on social media rarely share victims' payment card information with the merchant. Many payment gateways also allow fraud victims to contest fraudulent transactions, which may result in frozen payments or chargebacks.

One common solution is to redirect victims from cybercriminals' social media pages to their own scam pages, where they may have more freedom to process fraudulent transactions and conduct phishing attacks. However, creating their own online scam pages presents additional challenges:

- To receive payment, cybercriminals must either open merchant accounts or compromise legitimate merchant accounts, or use services on dark web forums which provide access to such merchant accounts.
- As with social media scam pages, payment gateways on independent scam pages do not always share victims' payment card information, and they may allow fraud victims to contest payments.
- To fully exploit online scam pages, cybercriminals must organize a bare minimum of advertising, which requires additional time and resources.

None of these challenges are insurmountable, and they should certainly not be taken to mean phishing or scam pages pose less of a threat than other items in this report. Cybercriminals are adaptable and may employ rudimentary "customer service" to deter fraud victims from contesting purchases. For example, scam pages frequently indicate long shipping delays may occur with their products. Once payments have cleared, the scammer may simply ignore complaints from their defrauded victims. Alternatively, if many complaints have been made against the scam page, the scammer can simply close down their old page and reopen a new one. Scam pages have a short life cycle, typically operating from 30 to 60 days.

Mitigations

- Practice good cybersecurity hygiene, verify buyers and sellers, and be discriminating of holiday purchases.
- Maintain or increase the rigor of anti-fraud measures during the holidays to prevent fraudulent transactions. For merchants, consider requiring additional verification for all transactions. For financial institutions, consider adjusting fraud score calculations or lowering the threshold necessary to deny a transaction.
- Use Recorded Future's Payment Fraud Intelligence to better anticipate and mitigate payment card fraud. Recorded Future tracks compromised payment cards posted for sale on dark web sources, allowing financial institutions to act on compromised cards before fraud occurs. Likewise, Recorded Future's macro-level intelligence allows financial institutions to identify demand for their portfolios, forecast strategic threats, and improve anti-fraud controls.

Outlook

Analysis of historical data suggests cybercrime increases during the holidays due to a convergence of factors, and the 2022 holiday season will likely be no different. Relaxed spending habits and increases in retailers' seasonal promotions bolster online sales but also expands the pool of opportunity for threat actors. This effect is exacerbated by cybercriminals' perception that merchants relax anti-fraud measures during periods of high-volume sales, opening them up to attack. Holiday-related promotions on dark web forums also allow cybercriminals to scale up their infrastructure at a discount, encouraging them to intensify their activities. Holiday-related promotions such as Black Friday provide additional openings for cybercriminals to defraud victims through the creation of themed phishing and scam pages.

Taken together with data that demonstrates a historical end-of-the-year bump in the number of stolen card records posted for sale, these factors suggest a period of heightened risk for cardholders, financial institutions, and associated service providers is likely in the coming months.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.