TLP: CLEAR

2024 HOLIDAY SEASON CYBER THREAT TRENDS

RETAIL & HOSPITALITY ISAC

Introduction

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

In order to examine the threat landscape facing the retail, hospitality and travel industries during the holiday season, RH-ISAC developed this report in three parts:

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

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

Threat Trend Analysis: Insights about top fraud trends for the holiday season, including what information fraudsters want and methods they use to get it as reported by Visa Payment Ecosystem Risk and Control (PERC), an RH-ISAC Associate Member.

EXPERT PERSPECTIVES

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

- What are your primary threat focuses this season and why?
- What defensive measures is your team focusing on this season? Is anything different from previous years?
- Have you noticed any notable changes in the threat landscape this year from previous years?
- What are the common gaps in defensive operations many organizations overlook as we approach the holiday season?
- Do you have any major advantages in your defensive operations this season?

The key takeaways of member analysts' answers to these questions provide critical insight into the active defensive trends in the retail sector. Social engineering and fraud remain critical concerns, with various types of fraud increasing dramatically in the current period. Organizations are seeing an increase in the prevalence of call-based social engineering, loyalty and gift card fraud, and DoS attacks. Detailed responses to each question are included in the following pages.

What are your primary threat focuses this season and why?

Social Engineering

Phishing and credential harvesting remain a priority all year long as a primary intrusion vector across most cybercriminal operations. Members report a steady prevalence in phishing attempts with lure themes involving popular product promotions targeting consumers for personally identifiable information (PII) harvesting.

ATO

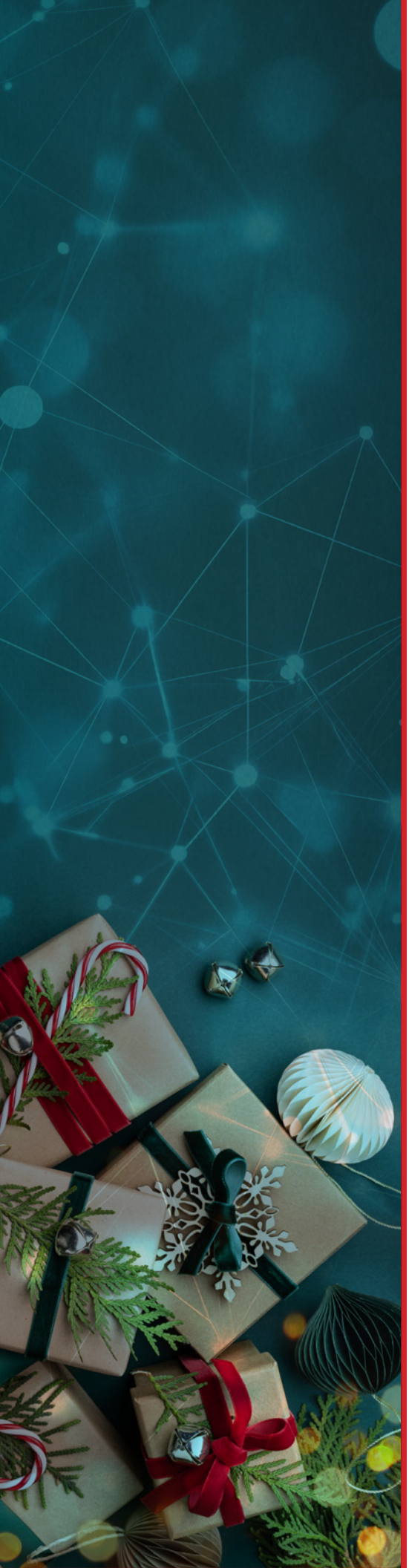
Account Takeover (ATO) typically ramps up around the holidays as fraudsters prepare for account abuse in many ways. Members report focusing more on the identification of ATO tactics and campaigns so their incident response teams can expedite locking compromised accounts, in order to minimize the time of exposure for any fraud activity to occur. Members also reported honing their intelligence collection on Telegram and other sources that frequently deal in customer credentials.

Bots

Bots have had a significant impact on online retailers, especially over the last two years as average individuals began exploring ways to earn additional income through becoming resellers of stolen information on threat actor forums. These “side hustles” support an already thriving ecosystem wherein actors have been scalping high-demand products to sell at high markups. The use of automation to support this activity causes significant negative side effects on the back end and can even lead to DDoS-like disruptions. Part of the challenge has been to distinguish this type of automated activity from other malicious attacks, like credential stuffing, and further differentiate between individuals using legitimate funds to make purchases and those attempting to engage in carding and other fraud. Oftentimes, threat actors like to hide in the increased traffic during the holiday season to avoid detection.

Fraud

Gift cards are very popular gifts during this holiday season, but they are also utilized by threat actors to stay anonymous while shopping, as well as to launder money from compromised credit cards or other payment sites. During this season, members report monitoring gift card threshold and rate limits, and movement of gift cards across accounts and tweaking their controls across different mitigation efforts. Additionally, members report focusing on raising awareness among consumers around the different types of gift card fraud tactics threat actors use, such as extortion, IRS impersonation, romance scams, and lottery prize scams. Finally, members report preparing in-store team members to look for suspicious activity related to card transactions.



What defensive measures is your team focusing on this season? Is anything different from previous years?

Members reported focusing on understanding the very specific tactics that fraudsters and threat actors are using across kill chains to enhance detection and mitigation efforts. Understanding broad trends across the threat landscape and how they work within member environments has enabled analysts to create more effective alerting, detection, and mitigation efforts.

Members also reported working closely with customer service departments, providing customer service representatives with refund-as-a-service training material, maintaining brand protection services to help take down malicious imposter sites, and kicking off internal fraud working groups for loss threats and handling.

Additionally, members reported the importance of change freezes, staffing adjustments, and operational changes in preparation for increased threats during the holiday season. Members particularly noted that an increased emphasis on improved endpoint detection and red team operations helped validate threat concerns and highlight areas for improvement. Implementing an on-call rotation for SOC staff emerged as a popular trend as well.

Have you noticed any notable changes in the threat landscape this year from previous years?

Members have also reported observing increasing imposter websites, product-focused phishing attempts, and phishing attempts impersonating executives. Other member analysts indicated that they observed a greater prevalence of social engineering attacks, heavily targeted at credential harvesting or bypassing MFA. One member noted a marked increase in denial of service (DoS) attacks.

According to members, brick-and-mortar theft and social engineering are increasingly common in the current season. Social engineering in stores has recently involved more threatening and hostile behavior or attempts to involve team members in criminal activity through collusion and bribes. Social engineering by phone has also increased exponentially.

In terms of fraud tactics, members reported fraudster methods online are scrappier due to more controls being implemented to prevent and shut down activity. The activity scope is smaller and more segmented, aside from some large-scale networks. Fraud and scam operations are increasingly using legitimate infrastructure to launch campaigns.

The sophistication and ease of committing fraud has decreased, so fraudsters are doing more testing, or selling of services and methods that require more steps, operational security, and sometimes some odd steps to bypass controls.

What are the common gaps in defensive operations many organizations overlook as we approach the holiday season?

Common gaps discussed by members included poor communication between stakeholders, such as branding, legal, customer service, and public relations teams. Members also highlighted that gaps in policy or updated incident response plans could create undue burdens on defenders, and that staffing shortages could affect the ability to monitor systems around the clock. In addition to gaps in policy, members also noted a need for enhanced policy enforcement for testing and deploying changes.

Members also reported struggles with adequately monitoring potential security concerns with third-party vendors and supply chains. Additionally, tight budgets late in the year create tension for expanded security coverage.

Finally, members reported concerns with staffing, including burnout and time off balancing, as well as lowered standards for hiring new team members to fill roles for the holiday surge.

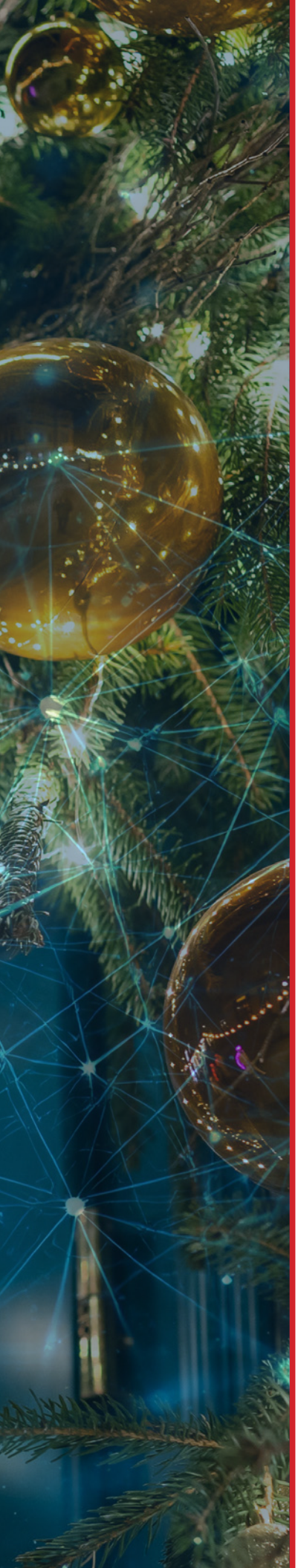
Do you have any major advantages in your defensive operations this season?

Members report finding multiple tools and practices that are particularly helpful leading up to the holiday season, including:

- Enhances security controls for various fraud types
- Updated tooling for source defense against digital skimming
- Guest profile authentication requirements
- Enhanced cybersecurity maturity, especially for eCommerce architecture
- Leading vendor threat intelligence platforms (TIPs) and Cyber Threat Intelligence (CTI) feeds
- RH-ISAC community resources and sharing platforms
- Updated policies and plans
- Bot management solutions
- Partnerships with leading cybersecurity associations and nonprofit organizations for additional threat research context
- Access to unique and insightful threat intel sources and feeds, including dark web and threat actor chat resources

THREAT LANDSCAPE

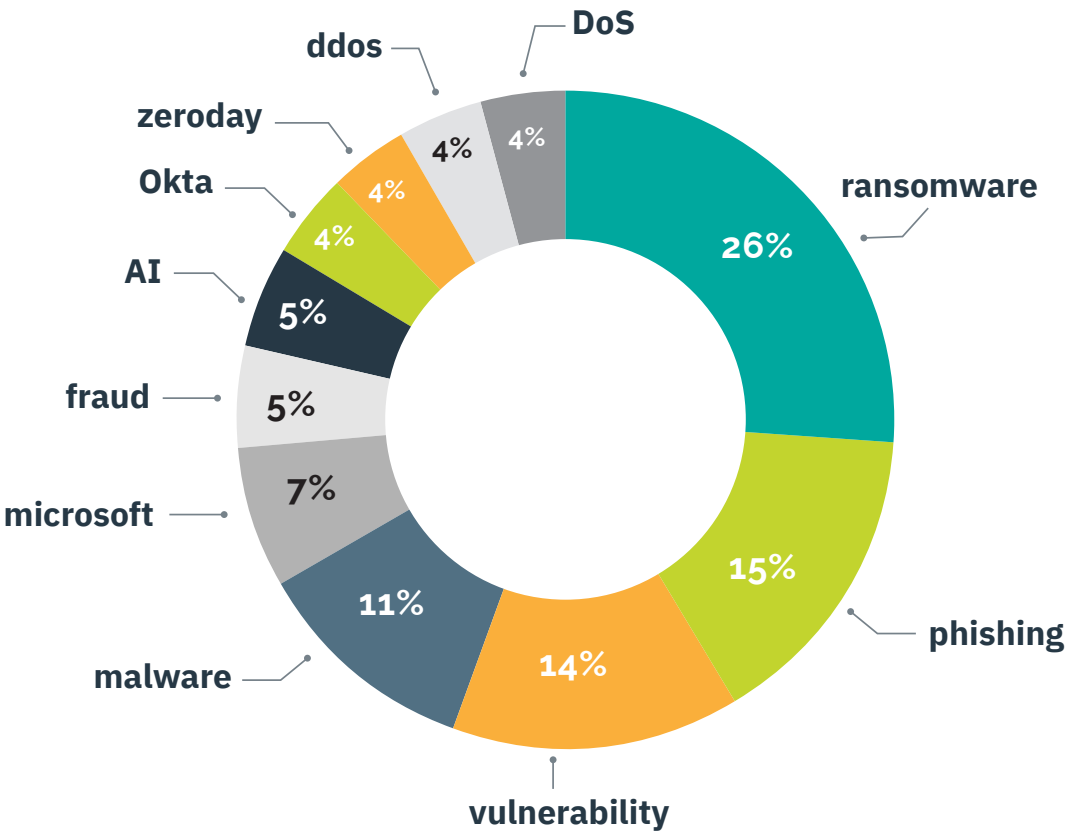
In order to establish the most likely trends in cybersecurity topics and threats as shared by the RH-ISAC membership across our sharing platforms, the RH-ISAC Intelligence Team and Research, Analytics, and Education Team examined the trend data for the holiday season period for the past two years, 2023 and 2022. While member concerns for the holiday season threat landscape largely revolve around different forms and elements of fraud, it should be noted that the trends tracked by RH-ISAC are at a more granular level, such as specific malware and attack vectors, which can ultimately enable fraud schemes through stolen data and unauthorized access.



Top Holiday Season Sharing Trends

The graph below illustrates the shared threat trends for the 2023 holiday period (October 1 - December 31), which can be described as the frequency that threat types were shared through Member Exchange and Slack:

2023



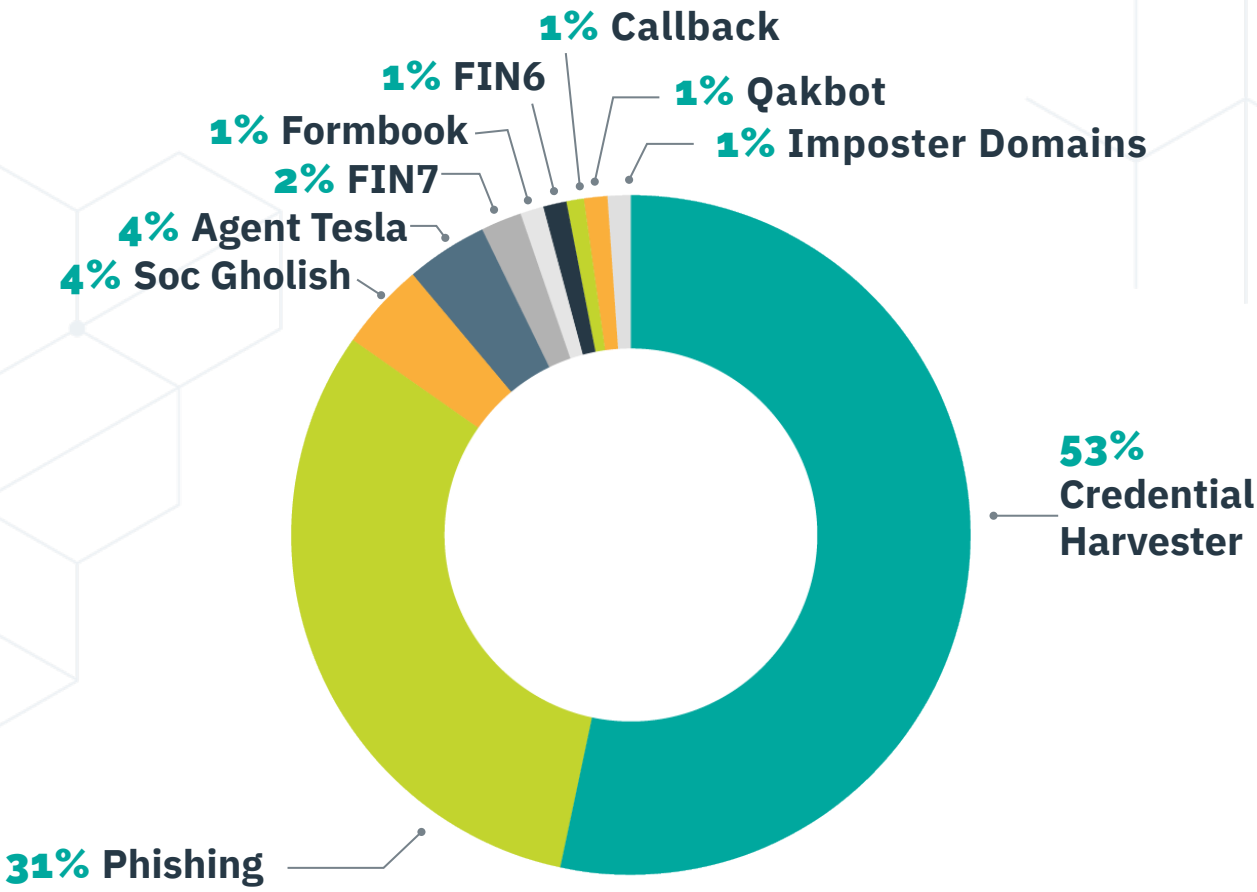
For 2023, ransomware emerged as the most common holiday threat at 26%, up significantly from 13% from the prior reporting period. Interestingly, generalized credential harvesting remained off the list entirely after it fell off the list in the prior period. This dramatic increase in ransomware reporting reflects a major global threat trend: ransomware prevalence in the threat landscape surged significantly over the last year, and the RH-ISAC member community was especially heavily targeted by ransomware actors in the second half of 2023.

Phishing fell from first to second most prevalent threat, from 16% to 15%, being overtaken by the sheer volume of ransomware-related shares. Microsoft-related threats fell from 16% to 7%, returning to previous low levels of reporting after a surge during the May-August 2023 period. General vulnerabilities (14%), general malware (11%), and fraud (5%) rounded out the remaining threats for the top list.

Top Holiday Season Sharing Trends (cont.)

The graph below illustrates the shared threat trends for the 2022 holiday period (October 1 - December 31), which can be described as the frequency that threat types were shared through Member Exchange, Slack, and the Core Member Listserv.

2022



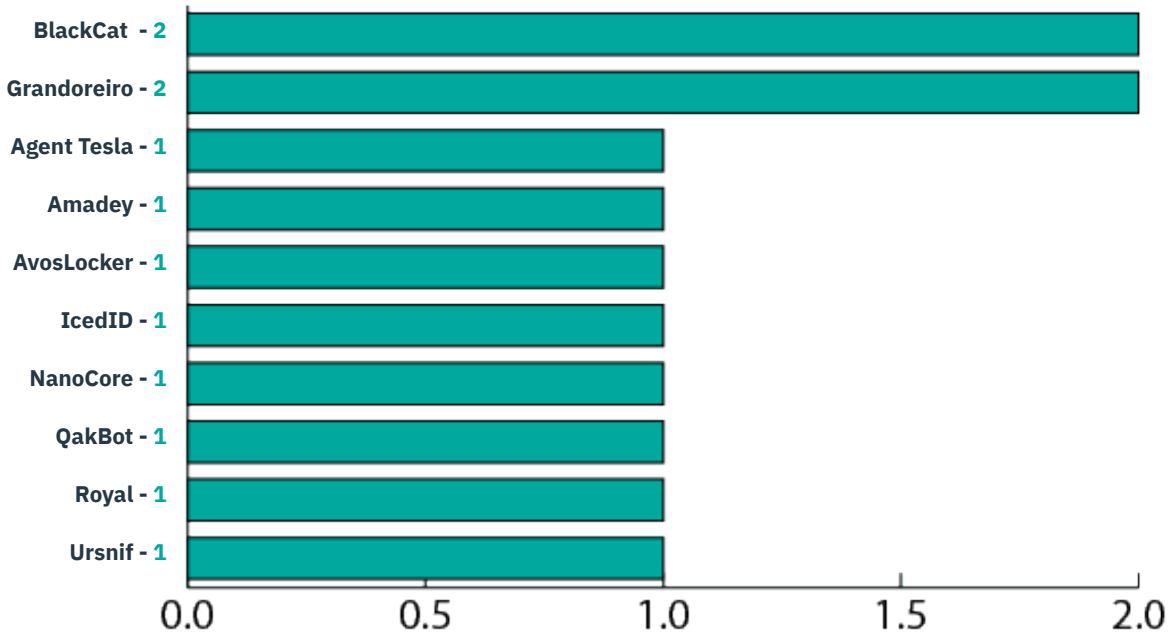
Top Holiday Season Reported Threats

After the launch of the RH-ISAC Malware Information Sharing Platform MISP instance in January 2022, threat trends are now tracked via the RH-ISAC MISP instance, which change the way data is presented for threat trends, including in this report. Tracked data on member-reported threat trends includes prevalent malware, threat actors, intrusion sets, MITRE ATT&CK Techniques, and attribute types. This level of data tracking since 2022 is more granular and focused than in previous years as a result of enhancements to the RH-ISAC MISP instance.

2023 Holiday Season Reported Threats

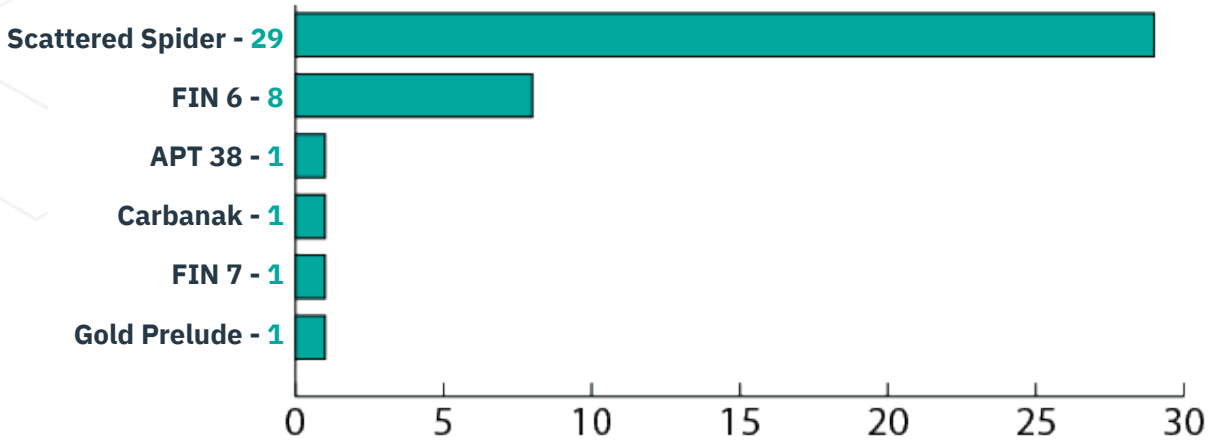
Malware

The graph below shows top reported malware (MITRE ATT&CK-defined software), by total count of instances for October - December 2023:



Threat Actors & Intrusion Sets

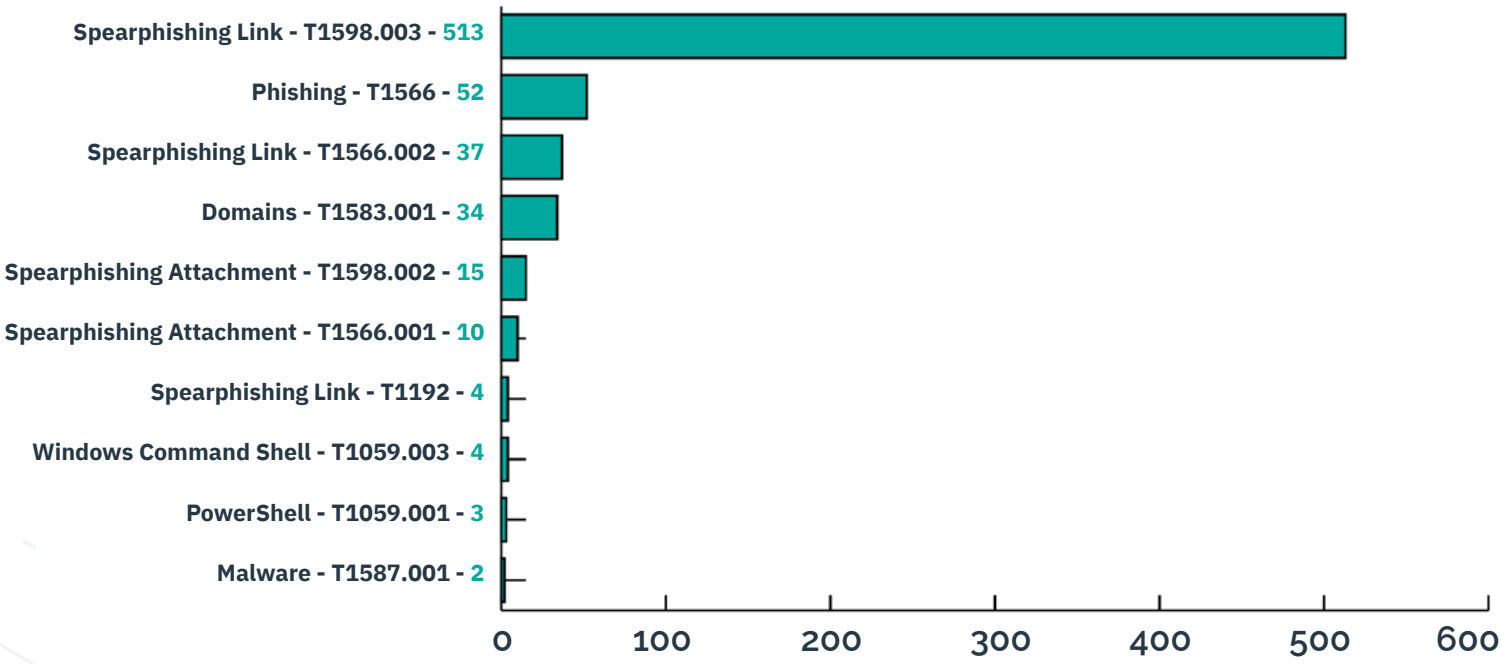
The top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) by total count of instances for October - December 2023:



Top Holiday Season Reported Threats (cont.)

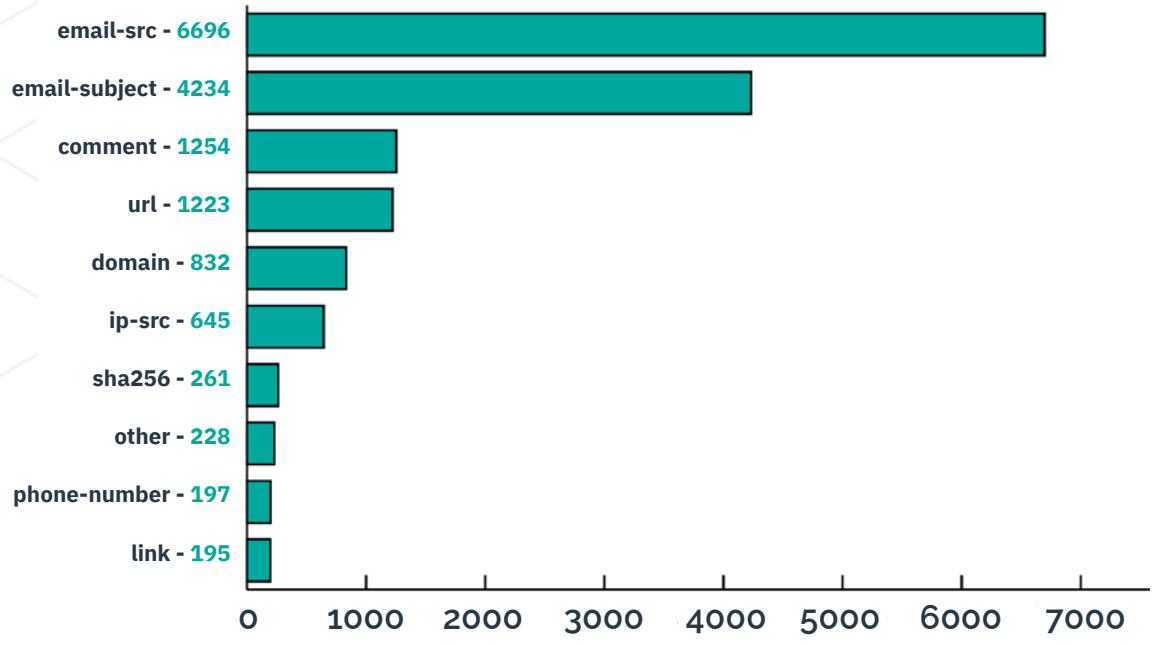
MITRE ATT&CK Techniques

The graph below shows the top reported MITRE ATT&CK techniques by total count of instances for October - December 2023:



Attribute Types

The graph below shows top reported attribute types (categories of technical intelligence shared by members) by total count of instances for October - December 2023:

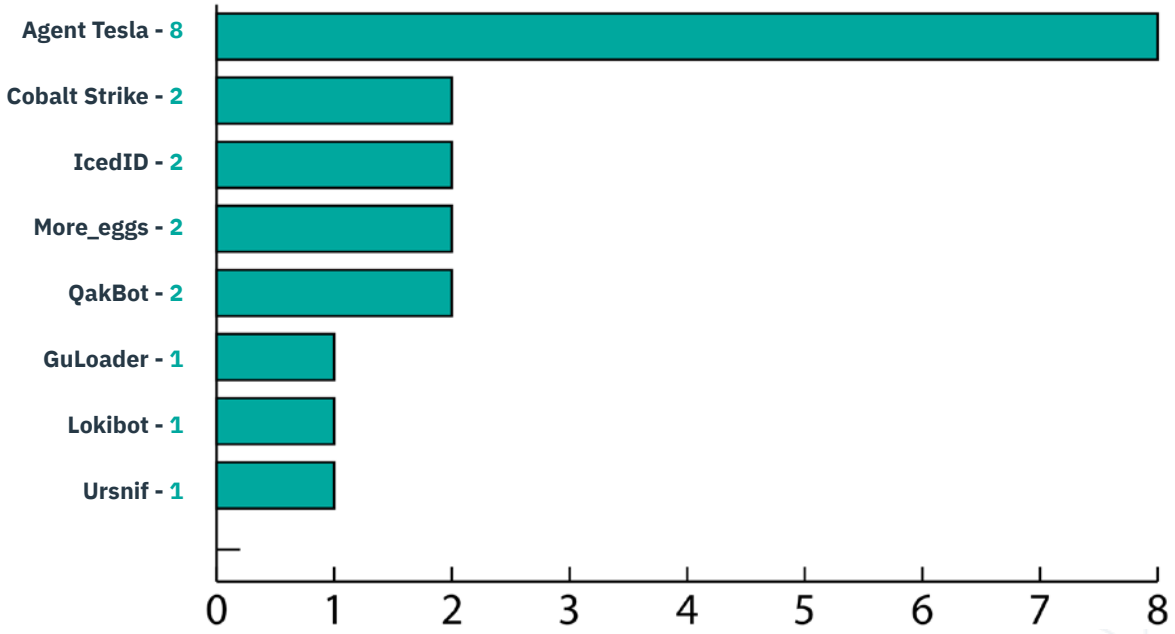


Top Holiday Season Reported Threats (cont.)

2022 Holiday Season Reported Threats

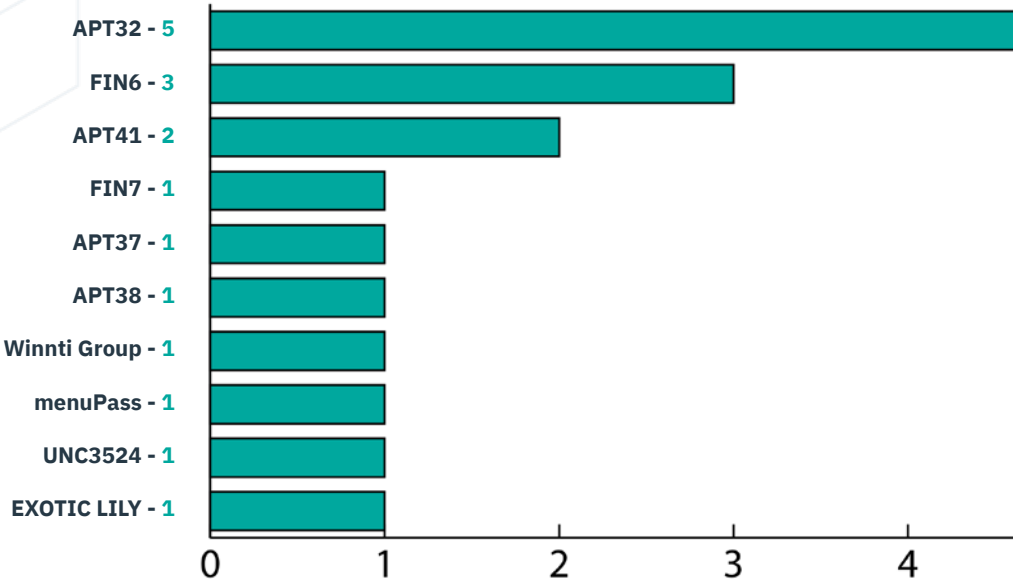
Malware

The graph below shows top reported malware (MITRE ATT&CK-defined software), by total count of instances for October - December 2022:



Threat Actors & Intrusion Sets

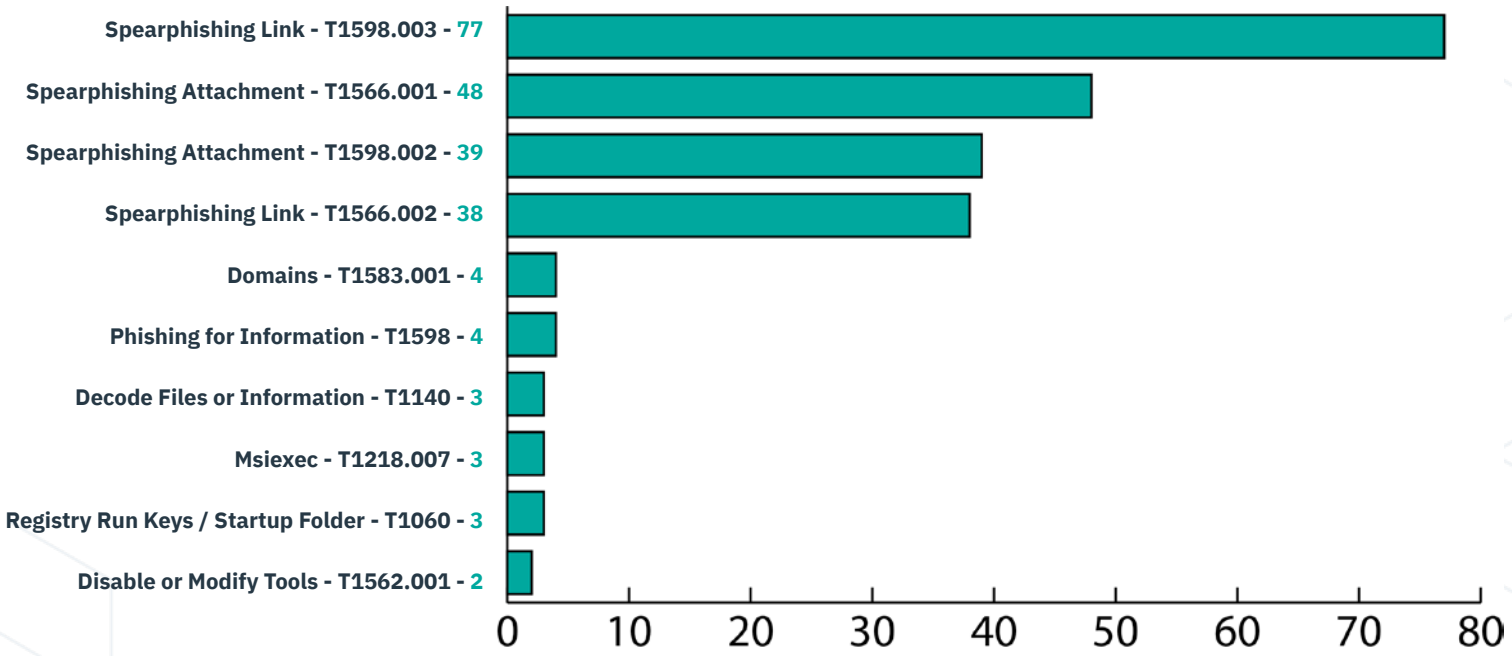
The top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) by total count of instances for October - December 2022:



Top Holiday Season Reported Threats (cont.)

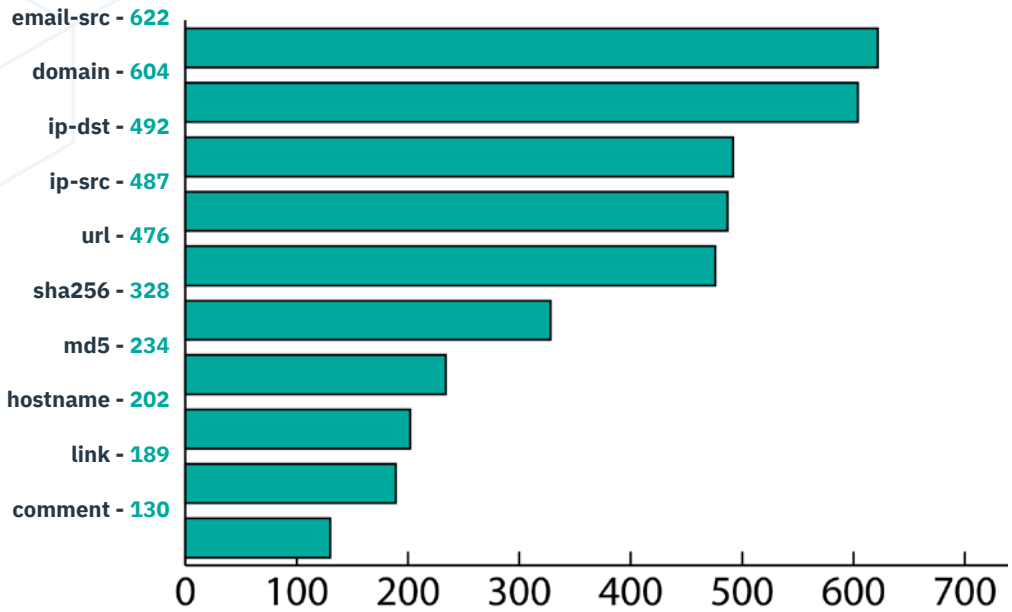
MITRE ATT&CK Techniques

The graph below shows the top reported MITRE ATT&CK techniques by total count of instances for October - December 2022:



Attribute Types

The graph below shows top reported attribute types (categories of technical intelligence shared by members) by total count of instances for October - December 2022:



Threat Landscape Trend Analysis

Between the holiday seasons in 2023 and 2021, there were six key trends:

- **Ransomware** overtook credential harvesting and phishing at the most prevalent threat reported by RH-ISAC members
- **Credential harvesting reporting fell** significantly in 2023, overtaken by vulnerability concerns and malware reporting
- **Malware** families and **phishing** remained among the top threats
- The **BlackCat** ransomware strain and **Cobalt Strike** emerged as the top malware for 2023, overtaking Agent Tesla and IcedID.
- **Spearphishing** techniques and **malicious domains** remained the most prevalent TTPs leveraged by threat actors across both years.
- **Scattered Spider** overtook APT32 as the most prevalent threat actor reported by the RH-ISAC member community, while FIN6 remained in second place.

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

For the 2024 period, social engineering, ransomware, and Scattered Spider activity are likely to remain key threats to members. Malware trends may fluctuate slightly, and major zero-day vulnerabilities that emerged throughout 2023 and 2024 (and those that have yet to emerge) are also likely to continue to rank among key threats to member holiday operations.

THREAT TREND ANALYSIS

RH-ISAC Associate Member VISA provided the following analysis for the 2024 Holiday season:

For the upcoming 2024 holiday season, Visa Payment Ecosystem Risk and Control (PERC) anticipates fraudsters will take advantage of holiday season-specific commerce, such as an increase in travel and in-demand goods/services, to conduct a variety of old and new scams. The following report identifies the top five fraud schemes consumers should watch out for during the 2024 holiday season.

What Fraudsters Want

Visa PERC anticipates scammers will use various methods to steal cardholder information and money due to increased eCommerce and in-person shopping during the upcoming holiday season. Fraudsters' main goals are typically:

- **Account Takeover:** Scammers take over accounts by convincing victims to hand over data, such as one-time passcodes (OTPs), that allows them to bypass account authentication. They often use phishing and social engineering to trick victims into providing OTPs.
- **Theft of Data:** Scammers steal payment data and personal information through social engineering and malware. Tactics include phishing, fake websites, and infecting victims' devices with malware.
- **Theft of Funds:** Scammers use stolen data and account takeover to withdraw funds, buy goods to resell, or transfer money. They also create fake online stores and websites to steal money from victims.

Top 5 Ways Fraudsters Will Try to Get What They Want This Holiday Season

Here are the top five ways Visa PERC expects fraudsters will attempt to take over accounts or steal data or funds this holiday season:

- Phishing and Social Engineering
- Scam Merchants
- Holiday Travel Scams
- Malicious Holiday Apps
- Physical Theft

Phishing and Social Engineering

Phishing and social engineering involve scammers pretending to be trustworthy entities to steal sensitive information. Visa PERC anticipates an increase in these attacks during the holiday season.

Phishing

There are three main types of phishing to watch out for:

Email Phishing: Scammers send emails that look like they're from trusted organizations. Be cautious of emails asking for personal info, containing suspicious links, or creating urgency about financial matters. Common holiday scams include discounted goods/shopping deals or fake Black Friday deals, heavily discounted travel deals, and spoofed merchant emails from well-known and in-demand brands.

Phone Phishing: Phishing over the phone, also called "vishing," occurs when scammers call pretending to be from financial institutions or other trusted services to trick victims into giving sensitive information. Common holiday phone scams include bank impersonation scams, utility/services impersonation scams, and charity/donation scams.

Text Message Phishing: Also known as "smishing," text message phishing involves scammers sending text messages to ask for account information or direct victims to malicious links or spoofed sites. Common holiday scams include package delivery scams, prize or free giveaway scams, and financial/account problem text messages.

Social Engineering

Scammers have additional tricks up their sleeves during the holiday season and will look to specific seasonal topics to carry out additional social engineering scams, including seasonal job scams, fake charities, and donation scams, and year-end flexible spending account schemes.

Seasonal job scams: Scammers are likely to exploit seasonal holiday job seekers. Last year, reports of employment scams increased by 545% during the holiday season. Scammers use legitimate job boards to post fake listings, spoof real company websites, or pose as recruiters. Once a job seeker is "hired," scammers request sensitive personal information or payments for things like office equipment or background checks. This can lead to identity theft, account takeover, or the victim becoming an unwitting money mule.

Donation scams and fake charities: Scammers exploit the holiday spirit by setting up fake charities to steal donations. They create websites that mimic real charities and use social media to ask for donations via cryptocurrency wallets or peer-to-peer accounts. Some sites even have fake testimonials to build credibility. To avoid these scams, research charities on trusted websites like the IRS, UK Charity Register, or BBB's Wise Giving Alliance.

FSA Account Takeover Scams: As the year ends, people with Flexible Spending Accounts (FSA) may get reminders about the "use it or lose it" rule, which forfeits unused funds at the end of the year. Scammers exploit this by sending fake emails pretending to be healthcare providers, offering ways to extend fund availability, in attempts to steal login credentials and drain spending accounts.

Scam Merchants

Scammers create fake merchants and advertise heavily discounted popular or luxury items on social media and other platforms to lure shoppers to their websites. In the past four months, Visa PERC identified a 284% increase in fake and spoofed merchant websites as compared to the prior 4 months. When shoppers make purchases on these fake sites, scammers steal payment data and personal information, receiving funds into their accounts. During the holiday season, these fake sites are expected to increase due to more online shopping. Scammers also spoof well-known brand websites and use search engine optimization (SEO) techniques to appear higher in search results, tricking shoppers into believing they are making legitimate purchases. This results in stolen data and payments for orders that are never fulfilled. Researchers polled holiday shoppers after the 2023 holiday season and found that one-third of respondents in the 18-44 age group said they experienced fraud from purchasing a product they found by clicking a social media advertisement.

Holiday Travel Scams

With millions traveling during the holidays, scammers target hotel, holiday rental, and airline industries. They create fake travel websites, send phishing emails about flight cancellations, and list non-existent holiday rentals to steal data and money. Common scams include:

Fake Travel Websites: Pretending to offer travel services or spoofing major airlines to lure customers with low prices. Scammers then upcharge for amenities and cut off communication.

Phishing Emails: Impersonating airline officials to send fake flight cancellation emails, asking for payment information to rebook flights.

Call Center Scams: Using malicious advertising or SEO to promote fake sites, leading victims to chat with fake customer service reps who steal payment details or charge high fees to "change bookings."

Fake Rental Listings: Posting fake accommodation listings with stolen photos and descriptions, often at below-market prices. Victims pay for non-existent rentals or are advised to pay outside legitimate platforms.

Malicious Holiday Apps

Scammers use holiday-themed apps to deliver malware to victims' devices. That adorable Santa tracking app that you see advertised on social media that has few or no reviews and requires you to download it by clicking a link rather than visiting a known and trusted app store... Beware! Scammers create new apps or imitate legitimate apps that, when downloaded, infect devices and steal sensitive data like login credentials and payment information. Visa PERC expects an increase in these malicious apps during the holiday season and advises consumers to be careful when downloading unknown apps.

Physical Theft

During the holiday season, scammers may physically steal payment cards or phones from consumers in crowded stores, malls, or parking lots. They often target unattended bags or wait for shoppers to exit stores to steal their cards and make purchases. Scammers also steal card data by targeting ATMs and POS terminals with skimming attacks due to increased shopping. They place devices called "skimmers" on terminals to steal payment card data. In crowded stores, scammers can install skimmers unnoticed, hiding the installation behind large items or distractions. Another method used to steal money is "digital pickpocketing," where scammers use mobile point-of-sale (MPOS) devices to conduct fraudulent contactless transactions by tapping against a victim's purse, wallet, or pocket.

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

For more information, visit www.rhisac.org.

RETAIL & HOSPITALITY ISAC