TLP: WHITE

2022 HOLIDAY SEASON CYBER THREAT TRENDS

RETAIL & HOSPITALITY ISAC

Executive Summary

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 members during the holiday season, RH-ISAC developed this report, the 2022 RH-ISAC Holiday Season Threat Trends Summary. The report is in three parts:

1. Member Perspectives: In which key subject matter experts from leading member organizations provide their insights into their current defensive preparations.

2. Threat Landscape: Where the RH-ISAC team examines the threat trends reported by the member community for the 2020 and 2021 holiday seasons from a historical and analytical perspective.

3. Associate Member Analysis: In which threat analysts from RH-ISAC associate member Flashpoint provide their perspective on the current holiday season threat landscape based on their research and data.

Key themes across data input for the current and past holiday periods include:

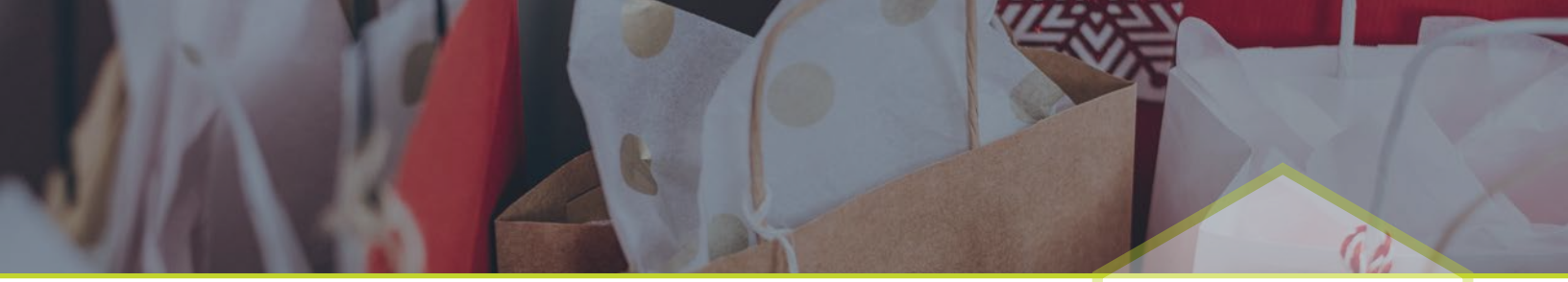
- Commonly familiar malware, such as QakBot, Emotet, Agent Tesla, and Dridex, are likely to continue as the most prevalent tools leveraged by threat actors for the 2022 holiday season.
- Phishing, credential harvesting, and various fraud variants, which are frequently the most common threats reported by members year-round, are a primary area of concern and likely focus for threat actor efforts for the season.
- Flashpoint identified the top ransomware actors targeting retailers and found 20 instances of ransomware actors leaking data of retail organizations

MEMBER PERSPECTIVE

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?**
- **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. Phishing and fraud remain critical concerns, with return fraud and gift card fraud increasing dramatically in the current period. Organizations are seeing an increase in the prevalence of credential harvesting attempts, especially leveraging social engineering tactics. More detailed responses to each question are included on the following pages.



What are your primary threat focuses this season and why?

Phishing & Credential Harvesting

Phishing remains a priority all year long as a primary intrusion vector across most cybercriminal operations. Members reported a marked increase in phishing attempts with lure themes involving popular product promotions targeting consumers for personally identifiable information (PII) harvesting. Members also reported a particular rise in threat actors leveraging the infostealers to harvest customers and have been selling them on a threat actor markets.

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 teams can expedite locking compromised accounts, minimizing the time of exposure for any fraud activity to occur.

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.

Gift & Loyalty Card Fraud

Gift cards are very popular gifts during the 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 watching 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 GC Extortion- IRS impersonation, romance scams, and lottery prize scams.

Return Fraud

Members also reported a significant rise in return fraud, and threat actor tactics have continued to evolve and pivot around mitigation efforts. Members reported their teams' need to prepare for insider recruiting within call centers since many companies hire temp employees or contractors during the busy season, which only elevates the risk of this type of insider behavior.

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

Members reported focusing on understanding very specific tactics 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.

Members also 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.

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

Members have 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 multifactor authentication (MFA).

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:

- 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

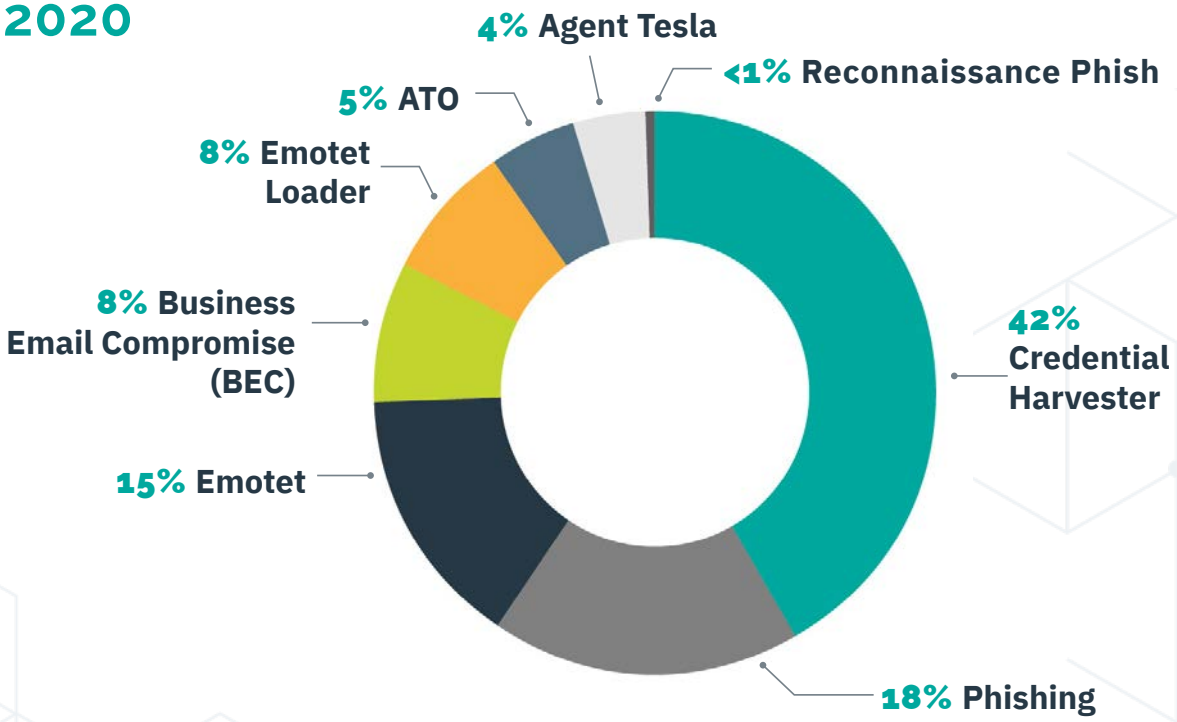
THREAT LANDSCAPE

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, 2020 and 2021. 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.

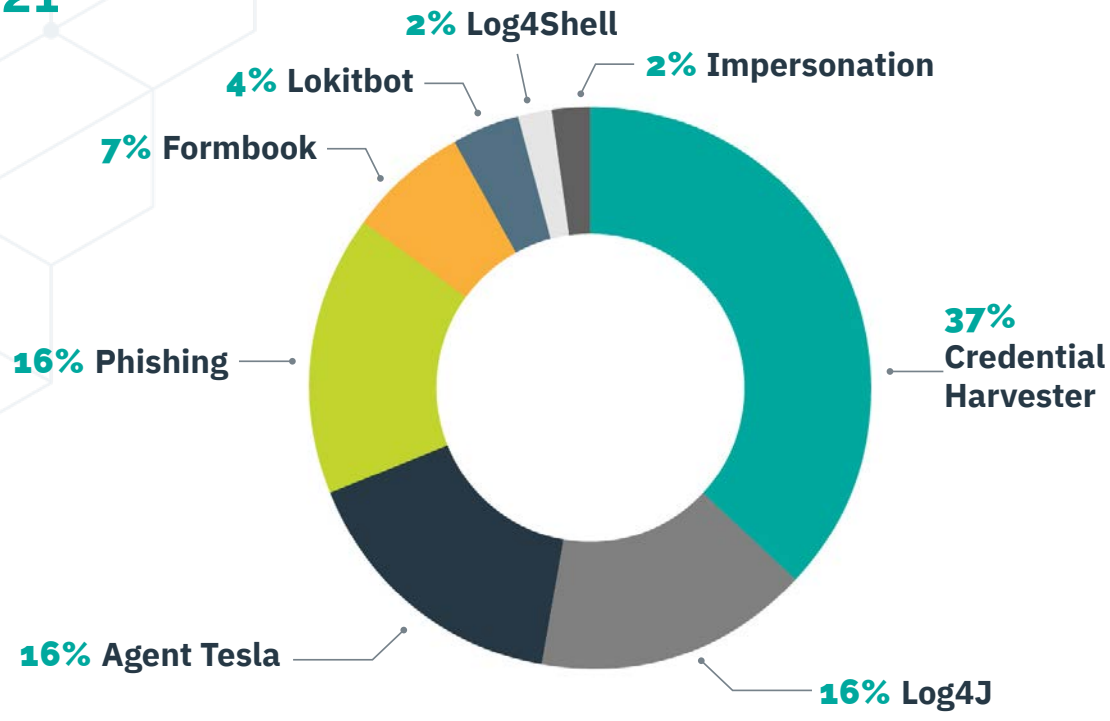
Top Holiday Season Sharing Trends

The graphs below illustrate the shared threat trends for the 2020 and 2021 holiday periods (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.

2020



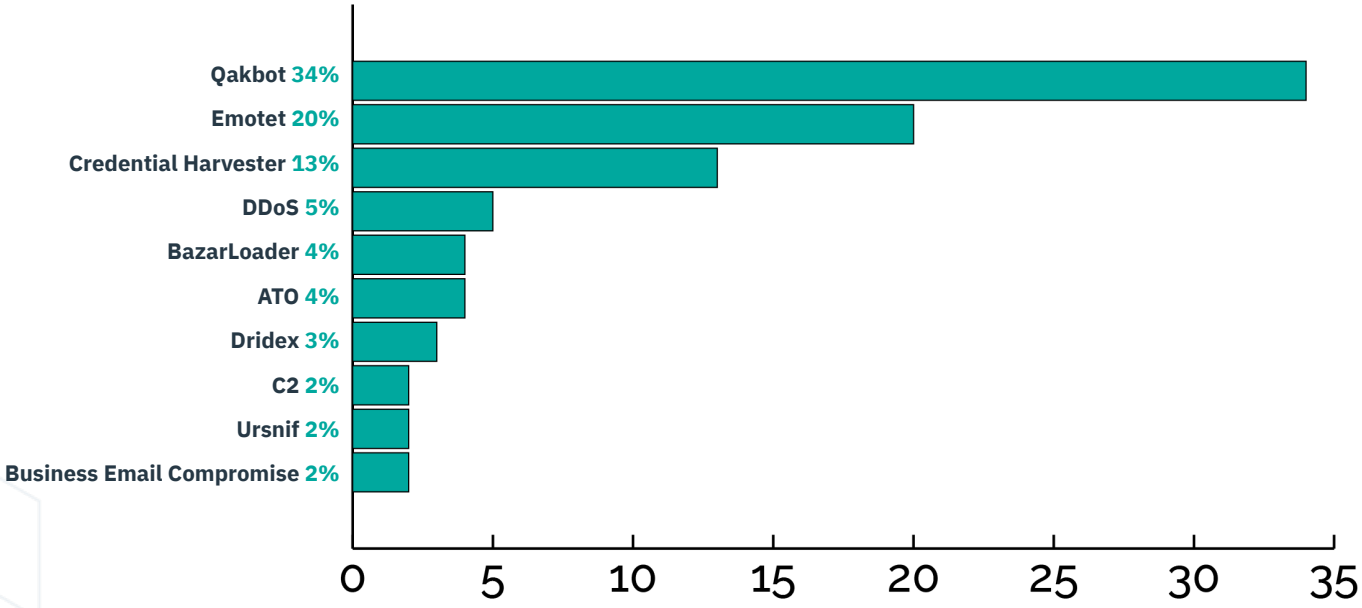
2021



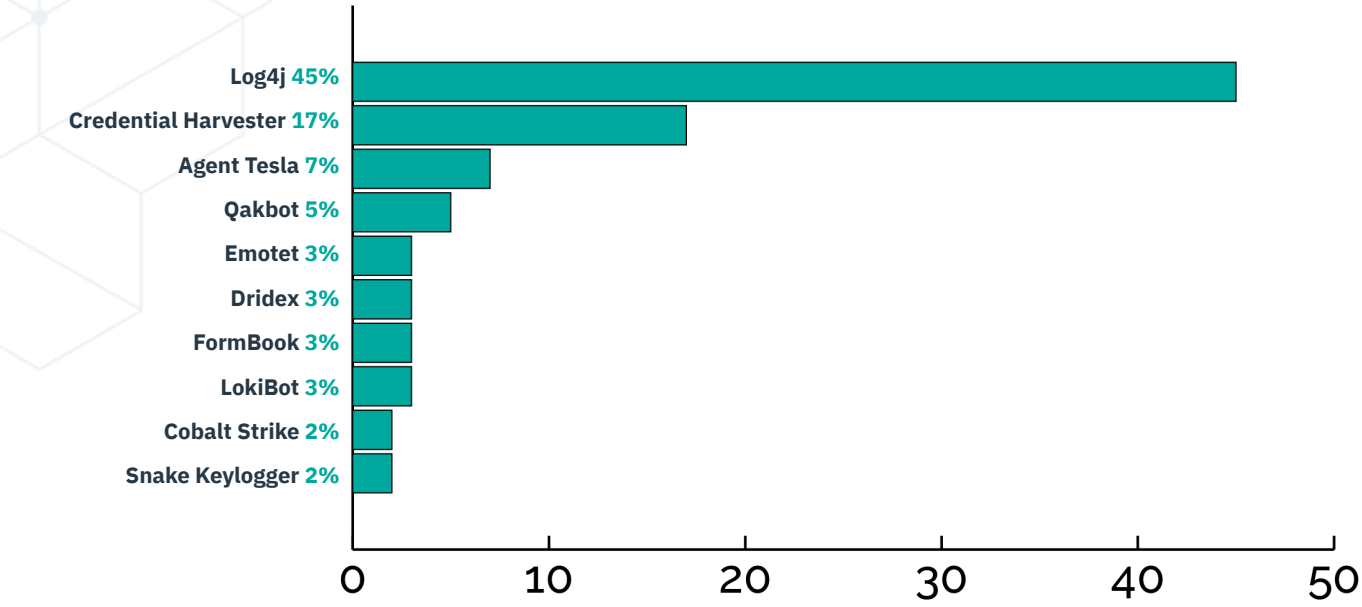
Top Holiday Season Attack Trends

The graphs below illustrate the total instances of threat indicators reported by members during the 2020 and 2021 holiday periods (October 1-December 31). Whereas the Top Shared Trends graphs on the previous page outlined the frequency of sharing regarding a threat topic, the Top Reported Threats graphs below show the volume of threat indicators shared related to a given topic.

2020



2021



Threat Landscape Trend Analysis

Between the holiday seasons in 2020 and 2021, there are six key consistent trends:

- Qakbot indicators are down significantly from 34% of total reported threats in 2020 to 5% in 2021.
- Emotet indicators are also down significantly from 20% in 2020 to 3% in 2021.
- Credential Harvesting indicators are up slightly from 13% in 2020 to 17% in 2021. Credential harvesting shares are consistently at a much higher prevalence than any other threat.
- Phishing activity sharing is down slightly from 18% in 2020 to 16% in 2021. While significantly less prevalent than credential harvesting, phishing activity is consistently among the most prevalent trends in shared intelligence.
- Agent Tesla sharing is up slightly from 15% in 2020 to 16% in 2021.
- Dridex indicators are relatively stable at 3% for both periods.

Qakbot and Emotet are frequently reported by the RH-ISAC community. Credential harvesting is among the most prevalent and long-term consistent attack trends reported by the community, frequently rating as the most common threat on a weekly basis. While Dridex was seen at a significantly lower but consistent prevalence, the RH-ISAC Intelligence team has not received any indicators regarding Dridex since December 2021.

Based on the current trends the RH-ISAC Intelligence Team is tracking, these four consistent trends will almost certainly appear in the 2022 holiday season reporting period, especially in light of recent Qakbot activity and the resurgence of Emotet. Additionally, phishing activity remains extremely prevalent in the community, both in shared trends and in shared indicators, and this trend is unlikely to change for the 2022 holiday season.

It is also possible that Log4J will emerge at a low spot on the top attack trends list for the 2022 holiday season reporting period, as indicators for the vulnerability are still reported at a steady, if reduced, pace. However, Log4J is highly unlikely to emerge as a leading trend for the period.

ASSOCIATE MEMBER ANALYSIS

For the 2022 Holiday Season Threat Trends Summary, RH-ISAC invited associate member Flashpoint to provide analysis of major trends they observed during the same reporting period:

The retail sector faces a wide range of cyber challenges that will almost certainly be exacerbated during the holiday shopping season. Financially motivated actors are a continuous threat to the sector, and target retailers knowing that they may be able to steal financial information, facilitate a fraudulent refund or transaction, or hold a retail network for ransom, knowing that operational downtime could have a large impact on a retailer's profitability during the most lucrative time of year.

Since January, Flashpoint has identified 39 ransomware leaks posted to ransomware gangs' respective leak sites from retailers around the world. Victim data is leaked in the event that the ransom is not paid to the ransomer by a predetermined time.

Ransomware in the Retail Sector

The graph below illustrates the top ransomware groups year to date leaking retailer data stolen during ransomware attacks. It should be noted that Conti shut down earlier in 2022.

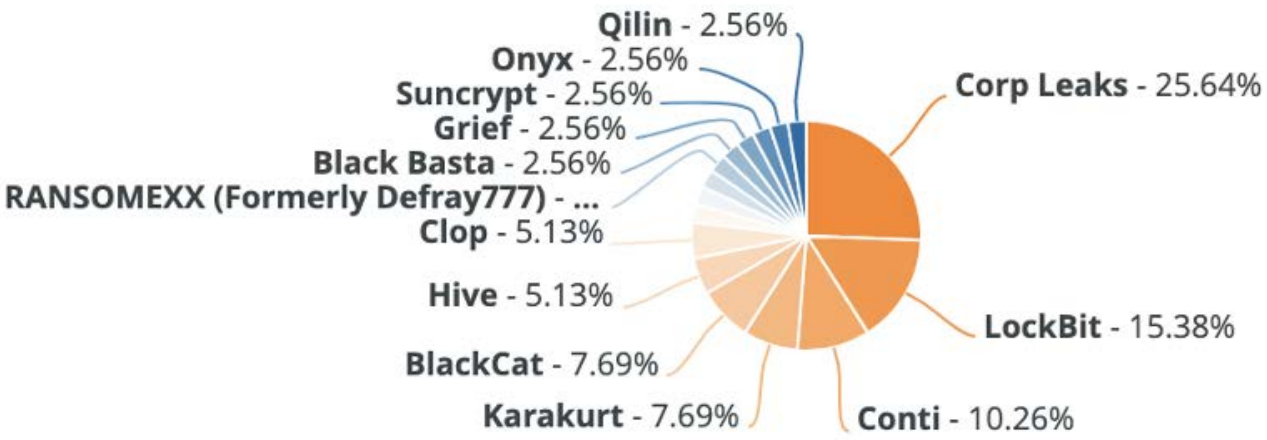
It is important to note that this graphic illustrates only instances where the ransomers' demands were not met. It is highly likely that other retailers had been targeted by ransomware attacks and paid the ransom to avoid threat actors leaking information.

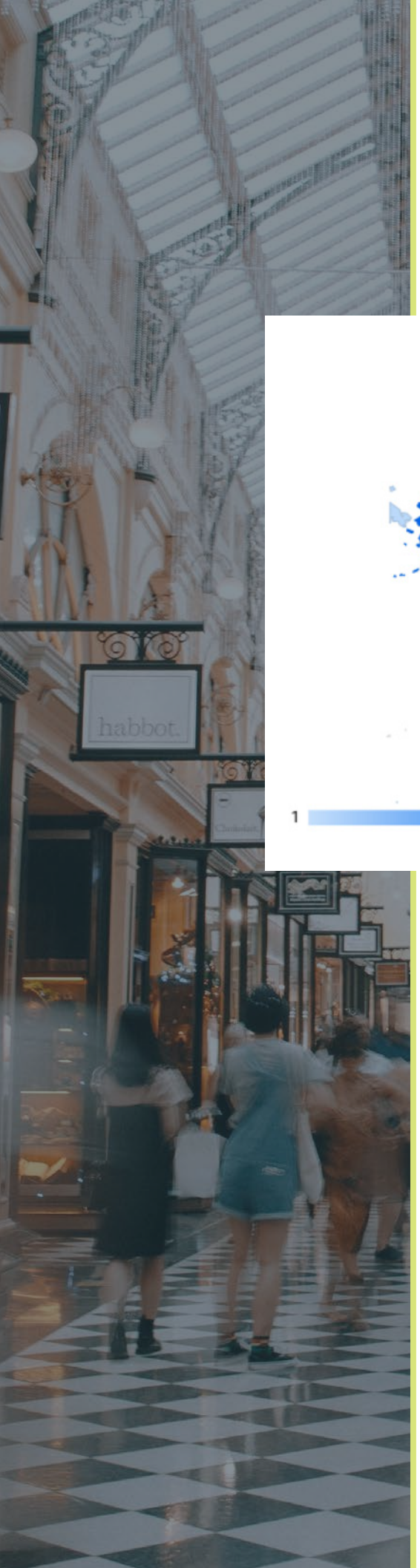
During last year's holiday shopping season, which Flashpoint typically defines as the period between October and January, there were a total of 20 leaks originating from retail organizations. Conti and LockBit were the largest perpetrators.

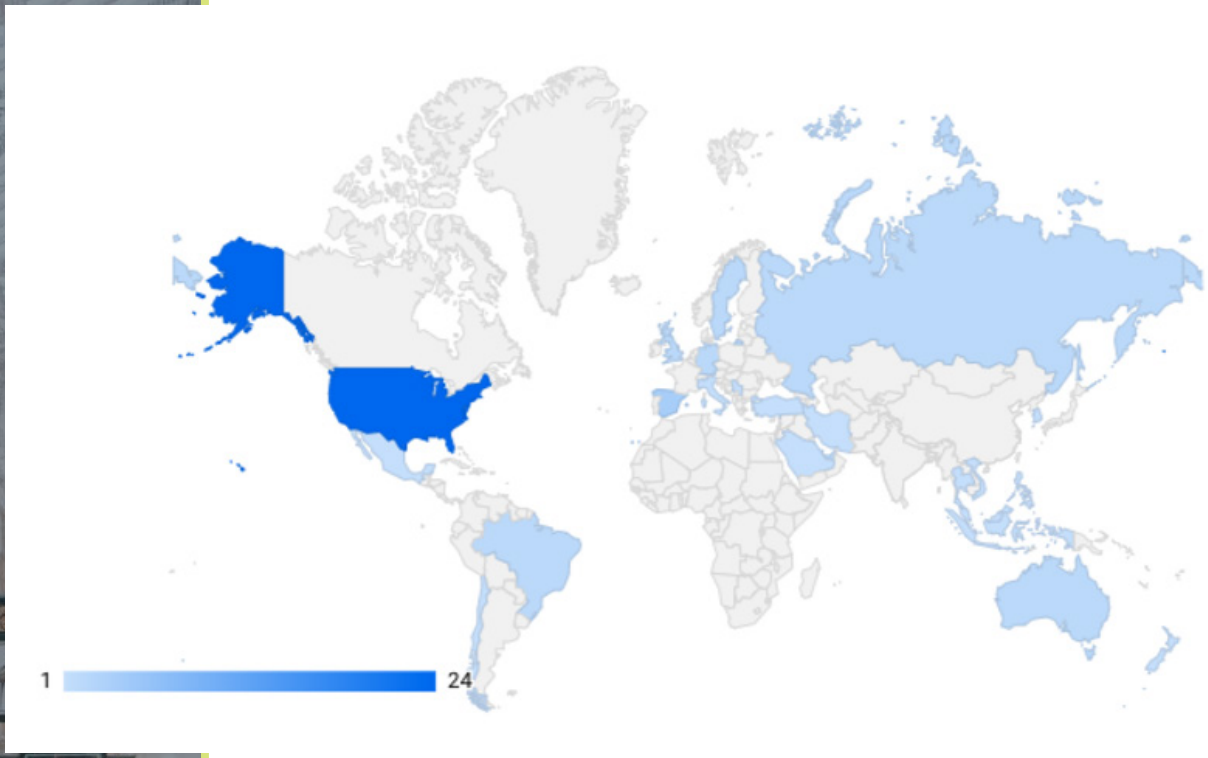
Based on this trend, it is likely that retailers will experience an increased threat of ransomware attacks during this period. Ransomware gangs and affiliates will be targeting retailers assuming that their victims will be more apt to pay a ransom to minimize downtime and to keep their names off leak sites. The impact of ransomware attacks could negatively affect overall profitability, whether it be due to operational downtime or a damaged brand reputation.

So far, in 2022, U.S.-based retail entities are the most heavily targeted industry, based on a review of Flashpoint reporting of advertisements for data and access within illicit communities. The United States has consistently been one of the most impacted countries by retail-related fraud over the past two years.

Ransomware Groups by % of Public Victims







This map shows the volume of retail-related advertisements of data and network access advertisements within illicit communities.

Going into the 2022 holiday shopping season, it is highly likely that this trend of targeting U.S.-based retailers will continue. Attacks against these retailers have previously included refund fraud, gift card fraud, and curbside pickup fraud. Threat actors are also likely to target the content management systems of online shops to exfiltrate financial information.

Across Flashpoint's reporting of all sectors, phishing has been identified as the most popular hacking services advertised within illicit communities for the year. These phishing services can come in the form of bespoke scam pages, SMS phishing (smishing), and emails with malicious attachments. Traditionally, during the holiday shopping season, these phishing messages have taken the form of fake coupons or discount codes.

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