TLP: CLEAR

2023 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 2023 RH-ISAC Holiday Season Threat Trends Summary. The report is in four parts:

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

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

Associate Member Analysis: In which Akamai highlights key trends for the holiday season, including malicious bot traffic and Magecart-style attacks.

2022-2023 RH-ISAC Ransomware Threat Landscape Comparison: In which threat analysts from RH-ISAC highlight major shifts in the ransomware threats facing the community over time.

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

- Commonly familiar malware, such as Lokibot, QakBot, Emotet, and Dridex, did not rank as prevalent tools leveraged by threat actors for the 2022 holiday season, which is a divergence from previous years.
- Credential harvesting, phishing, imposter domains, Agent Tesla, and Formbook continued steadily as top threats reported by members, with specific levels fluctuating.
- 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.

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?
- 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. 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 imposter domains, in-store theft, and credential harvesting attempts, especially leveraging social engineering tactics and multifactor authentication (MFA) bypass. More detailed responses to each question are included in the following pages.

What are your primary threat focuses this season and why?

Social Engineering

Phishing remains 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. Members also reported a particular rise in threat actors leveraging MFA bypass methods.

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, minimizing 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.

Gift & Loyalty Card 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 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. 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 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 MFA.

According to members, brick-and-mortar theft and social engineering are much more brazen and overt 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.

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. 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.

Members noted a massive increase in scam campaigns leveraging imposter sites to steal personally identifiable information (PII) and payment data from consumers, which presents a difficult problem to mitigate depending on takedown resources and locations of host servers for malicious fake sites.

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.

Purchasing volume can overwhelm systems or present new anomalies (particularly due to deals and sales) that systems have not accounted for or been exposed to previously, thus slowing down the response to spot legitimate fraud and implement necessary controls.

Members also reported struggles with adequately monitoring potential security concerns with third-party vendors and supply chains.

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
- Guest profile authentication requirements
- Enhanced cybersecurity maturity
- 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

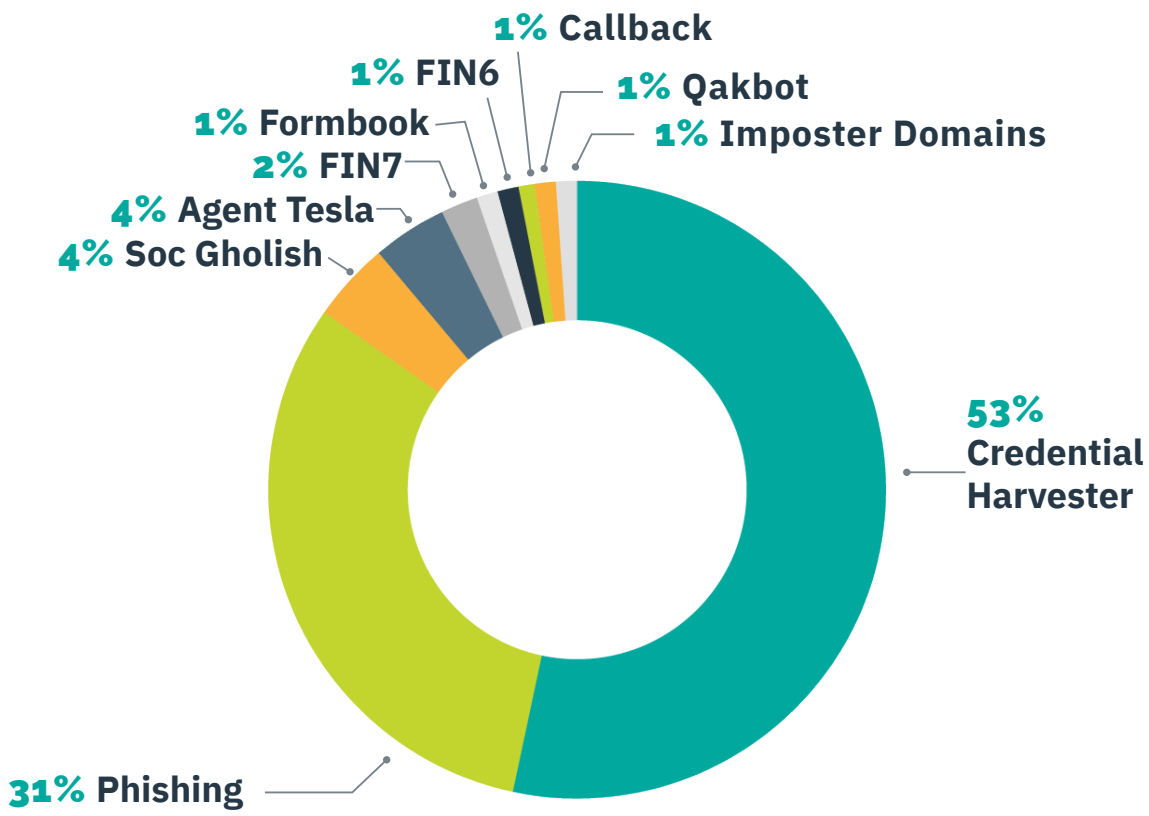
THREAT LANDSCAPE

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 three years, 2020, 2021, and 2023. 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

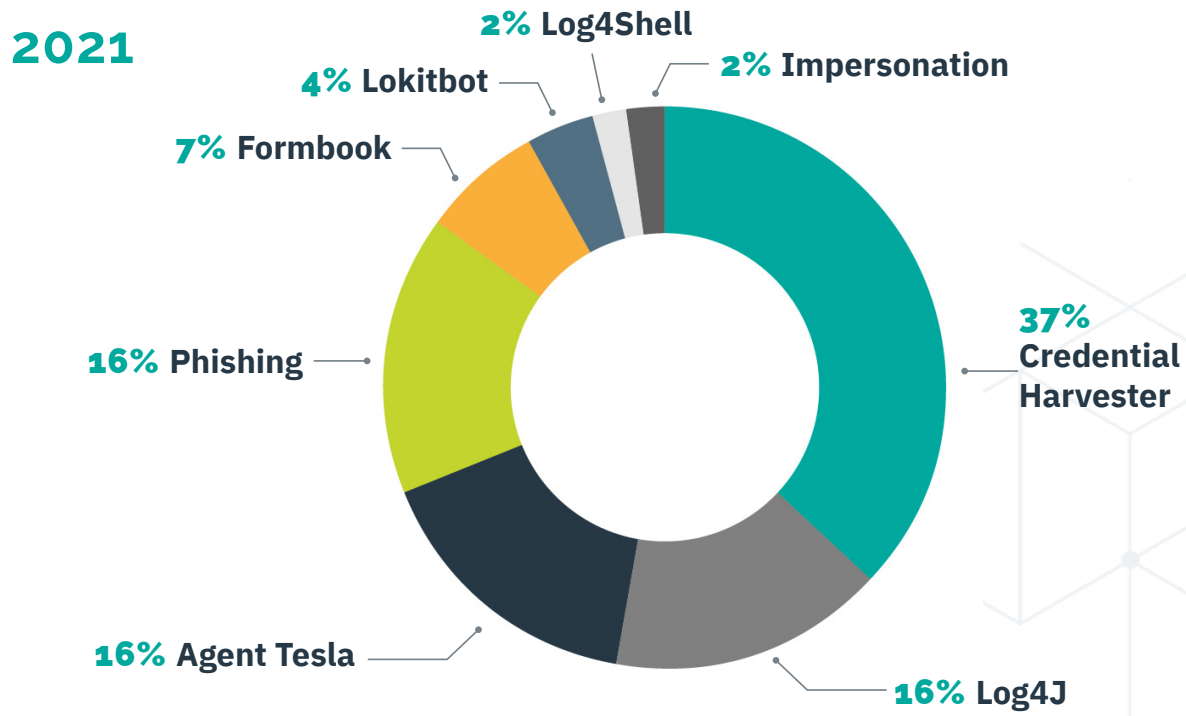
This graph illustrates the shared threat trends for the 2022 holiday period (October 1-December 31), which can be described as the frequency that threat types were shared through Member Exchange, Slack, and the Core Member Listserv:

2022

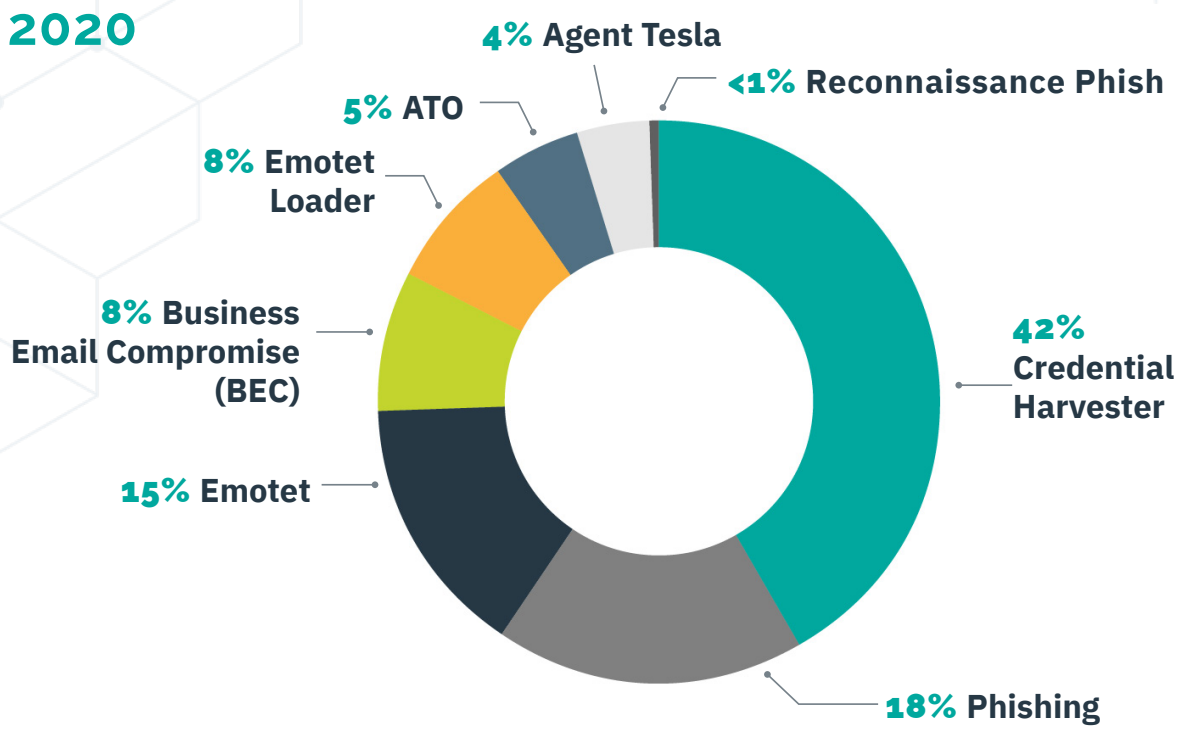


Top Holiday Season Sharing Trends (cont.)

This graph illustrates the shared threat trends for the 2021 holiday period (October 1-December 31):



The top sharing trends for the 2020 holiday season were:

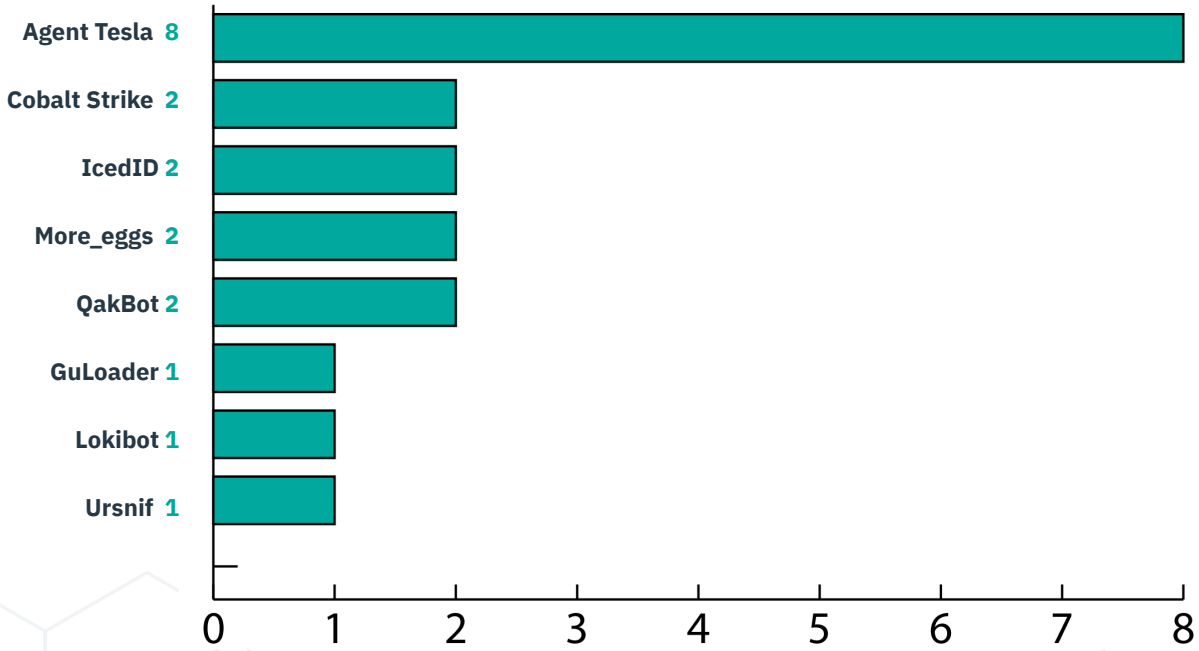


Top Holiday Season Reported Threats

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 will 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 for 2022 is more granular and focused than in previous years.

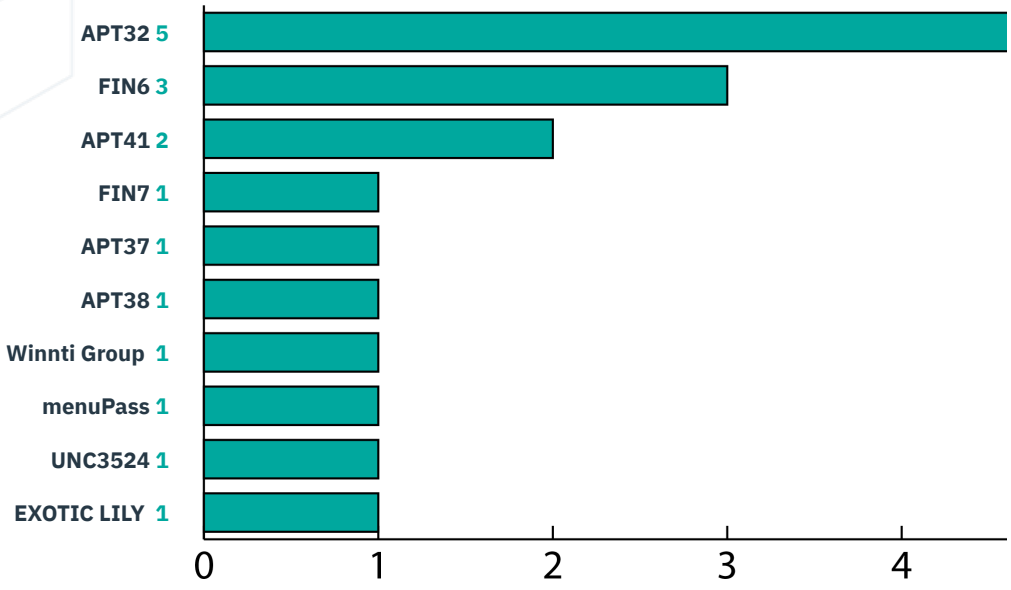
Malware

The top reported malware (MITRE ATT&CK-defined software), by total count of instances, were:



Threat Actors & Intrusion Sets

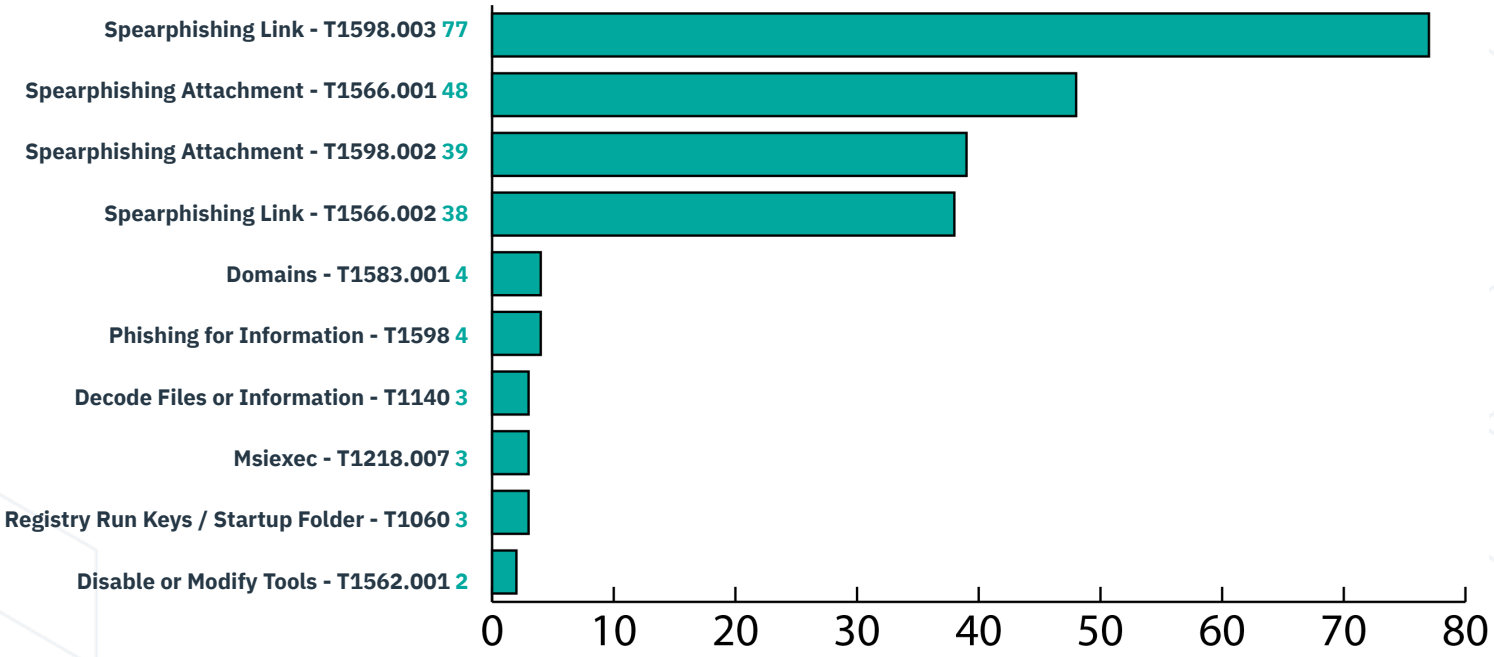
The top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) by total count of instances were:



Top Holiday Season Reported Threats (cont.)

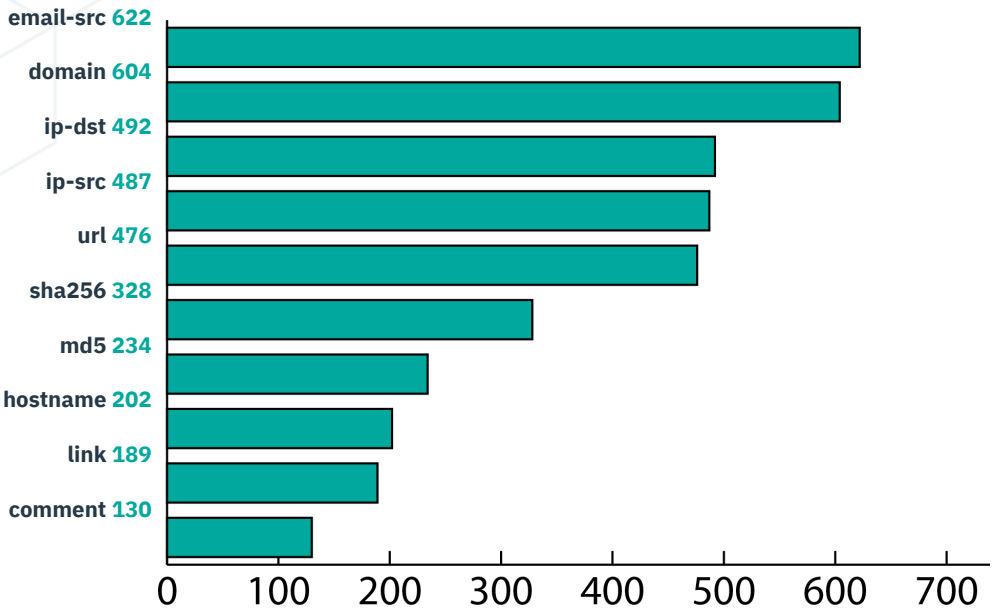
MITRE ATT&CK Techniques

The top reported MITRE ATT&CK techniques by total count of instances were:



Attribute Types

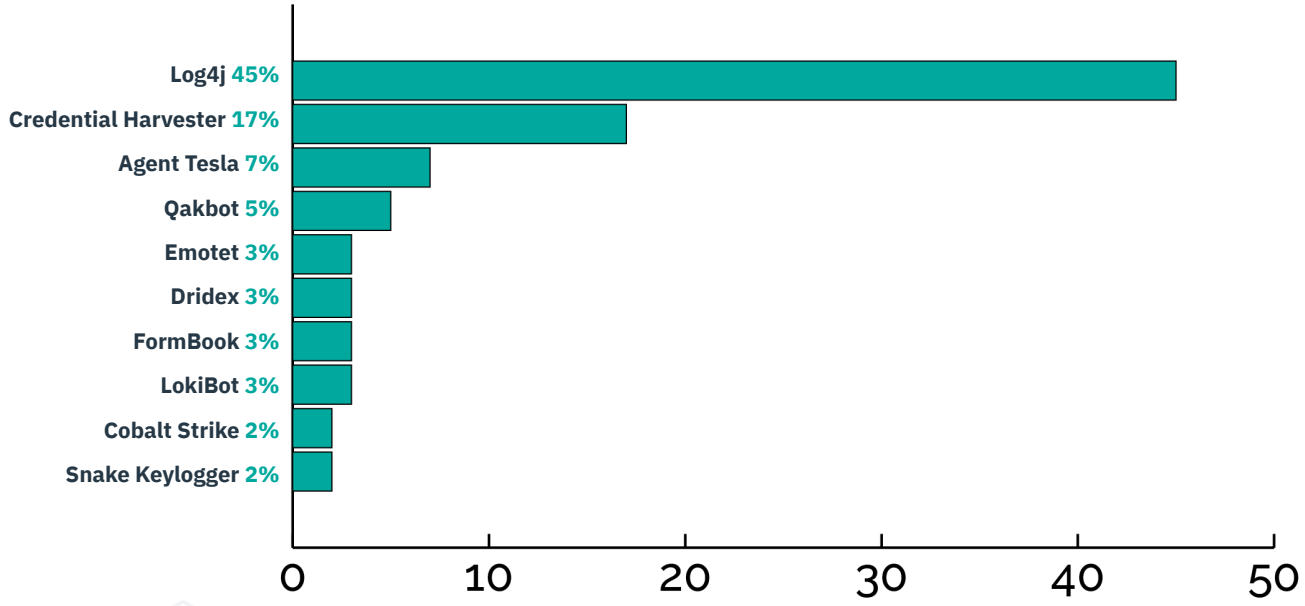
The top reported attribute types (categories of technical intelligence shared by members) by total count of instances were:



Top Holiday Season Attack Trends

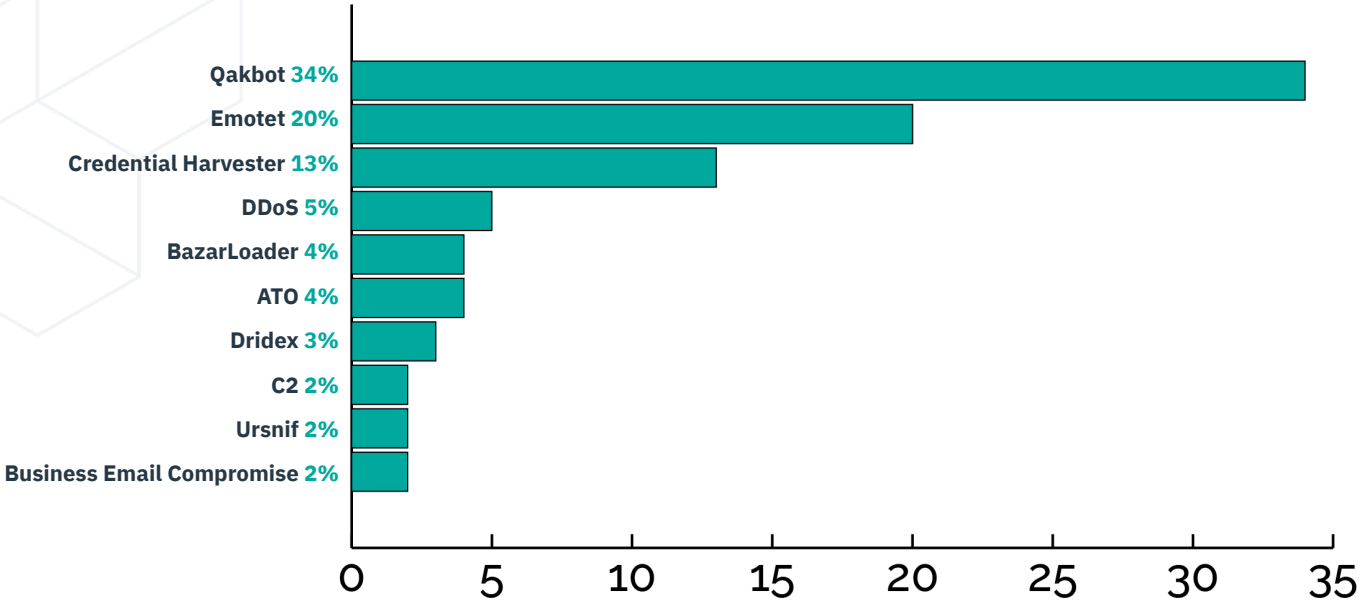
This graph illustrates the total instances of threat indicators reported by members during the 2021 holiday period (October 1-December 31). Whereas the Top Shared Trends graphs outlined the frequency of sharing regarding a threat topic, the Top Reported Threats graphs show the volume of threat indicators shared related to a given topic. The top attack trends shared by RH-ISAC member analysts for the 2021 Holiday period were:

2021



The top attack trends shared by RH-ISAC member analysts for the 2020 holiday period were:

2020



Threat Landscape Trend Analysis

Between the holiday seasons in 2022 and 2021, there were four key trends:

- Credential harvesting held first place and rose from 37% of reporting in 2021 to 53% or reporting in 2022.
- Phishing rose from fourth place with 16% in 2021 to second place with 31% in 2022.
- Agent Tesla fell from third place in 2021 with 16% to fourth place in 2022 with 4%.
- Imposter Domains held steady, falling only one point from 2% to 1%.

Between the holiday seasons in 2020 and 2021, there were six key 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.

The 2022 holiday period saw some trends, such as credential harvesting and phishing, increase in prevalence, while others, such as malware families like Agent Tesla and Formbook, fell. Additionally, RH-ISAC enhancements to MISP allowed a more granular look at threat trends reported by members, showing:

- Agent Tesla and Cobalt strike emerged as top identified malware by members.
- APT32 and FIN6 emerged as the top threat actors identified by members.
- Spearphishing links and attachments emerged as the most prevalent MITRE techniques.
- Email addresses and Domains were the most prevalent attribute (indicator) types reported.

As predicted in the 2022 Holiday Threat Trends Report, Log4J did not emerge as a leading trend for the period. Former top threats such as Lokibot and Emotet also fell off the list, to be replaced by new top malware threats such as SocGholish, in third place for 2022 with 4% of total reporting. Notably, Business Email Compromises and Account Takeover (ATO) also did not rank as a top threat in 2022, a divergence from previous years.

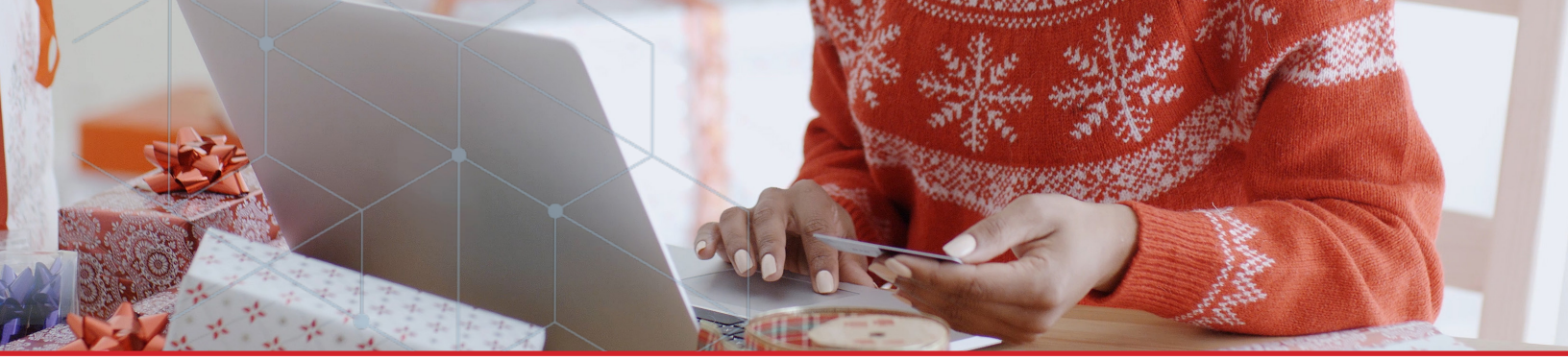
For the 2023 period, credential harvesting, phishing, and imposter domains are likely to remain key threats to members if the previous holiday period and current trends, as identified in the May-September 2023 Intelligence Trends Summary hold steady. Malware trends may fluctuate slightly, and major zero-day vulnerabilities that emerged throughout 2023 (and those that have yet to emerge) are also likely to rank among key threats to member holiday operations.

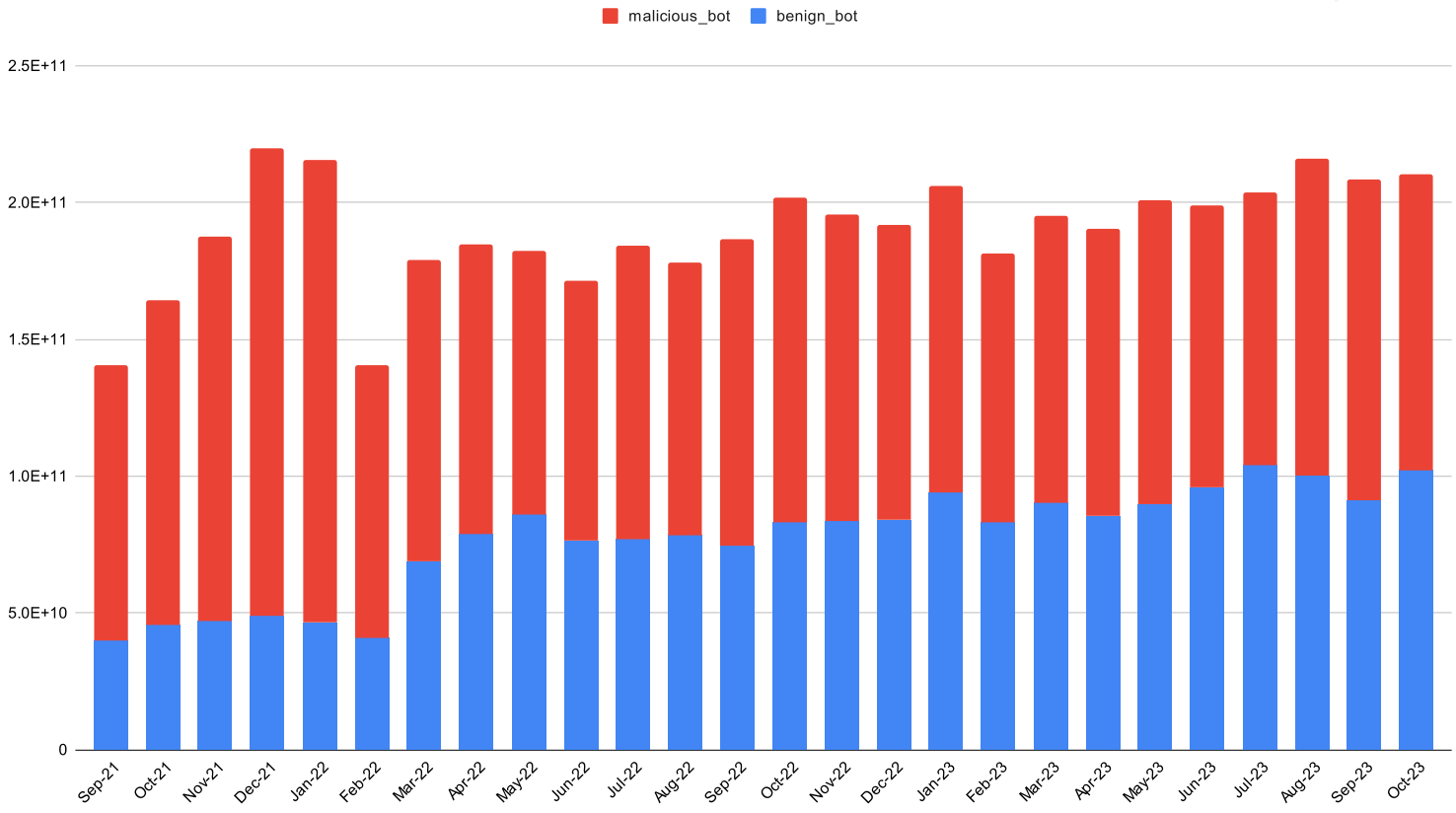
ASSOCIATE MEMBER ANALYSIS

Associate Member Akamai provided the following analysis for the 2023 Holiday season.

About Akamai

Akamai provides comprehensive security coverage across application workloads and APIs to application infrastructure for the world's largest enterprises and brands. Each day Akamai analyzes over 691 terabytes of data and secures 11 trillion DNS queries daily. Our deep visibility across the global internet provides insights into a variety of attack trends and abuse including bot, OWASP Top 10, OWASP API Top 10, API business logic abuse, DDoS (Infra, DNS, and AppDos), and ClientSide (formjacking, web skimming) among other types of threats.

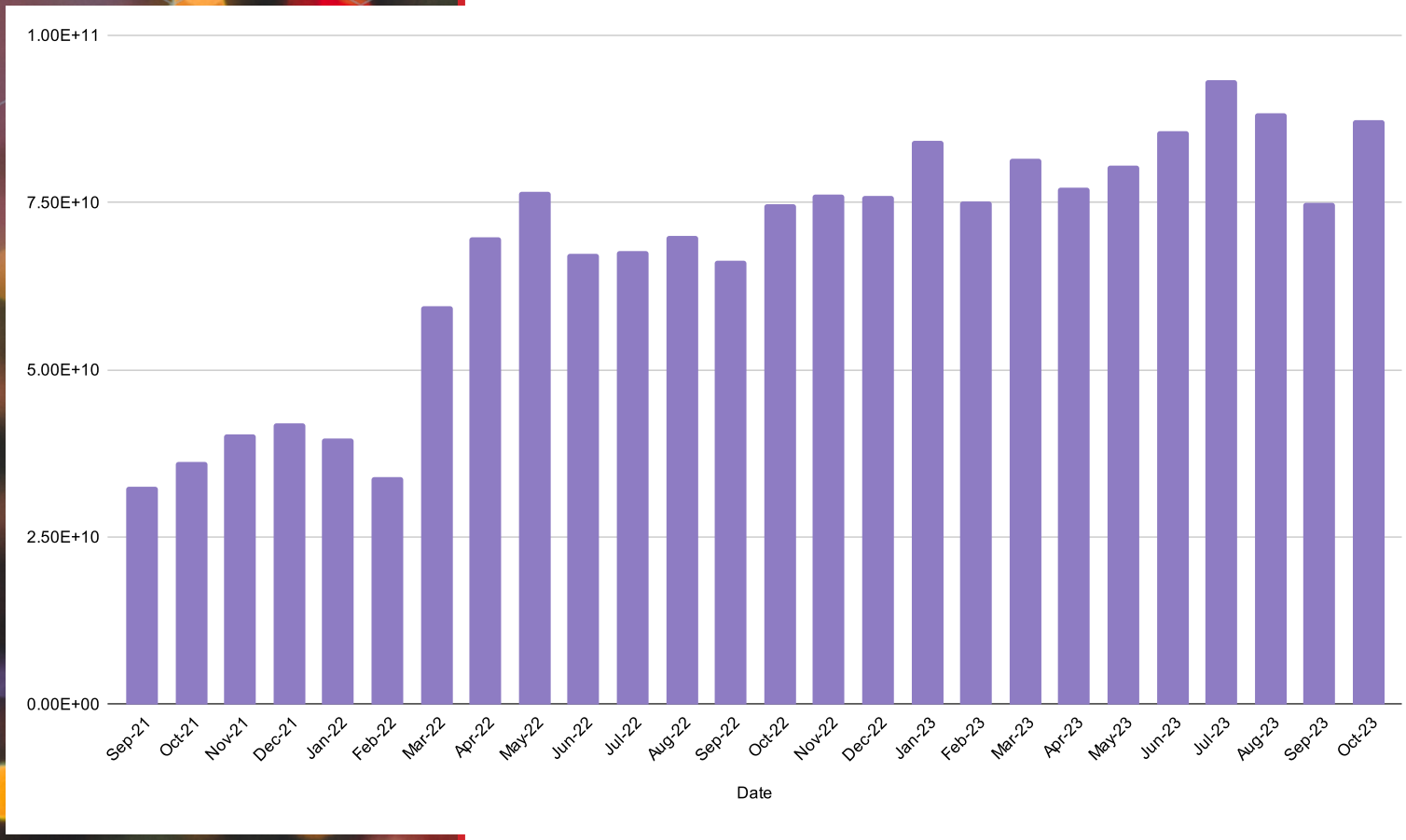




Benign Bot Traffic Patterns

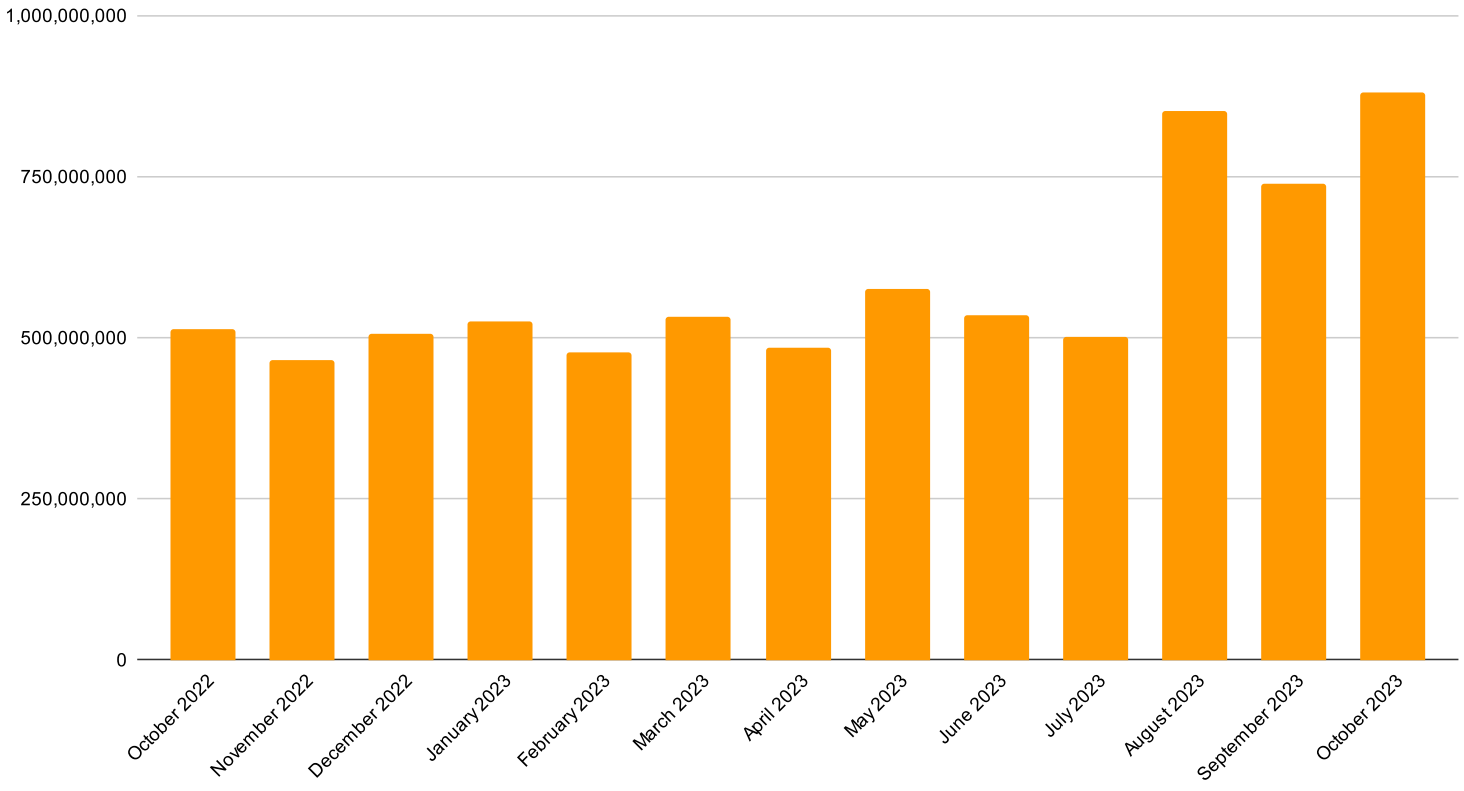
Bot management and mitigation will be top of mind again this holiday season as Akamai has observed steady growth of both malicious and "benign" bot traffic patterns within the Retail sub-vertical. Similar to last year, a hyper-competitive retail environment will attract scraper bots looking to aggregate pricing, product availability, and competitive information as retailers battle for the shopper's share of wallet. Given the increase in benign bot traffic, it's important to keep in mind that benign bots (which include scrapers) also need to be managed as part of a holistic strategy; Organizations should consider the impacts of overall bot volume — both good and bad — on web-facing and mobile applications.

Web Search Engine Bot Volume



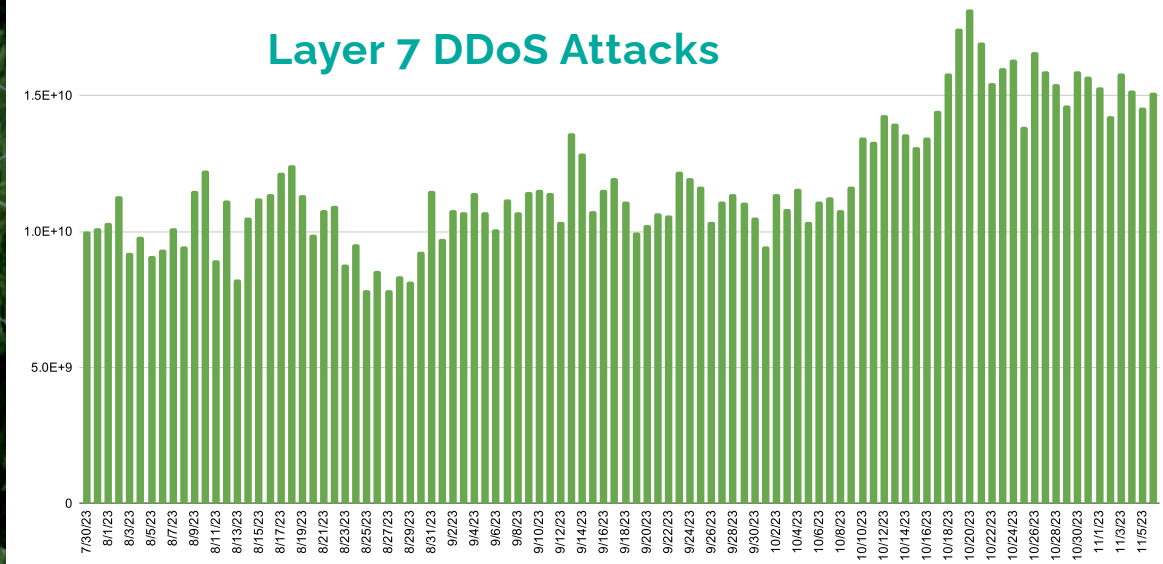
Digging deeper into the benign bot volume, we can see that a significant portion of the activity is driven by the web_search_engines category. This type of bot traffic is typically associated with SEO web-crawler bots surfacing content and indexing information.

Known Scraping Tools Bot Volume



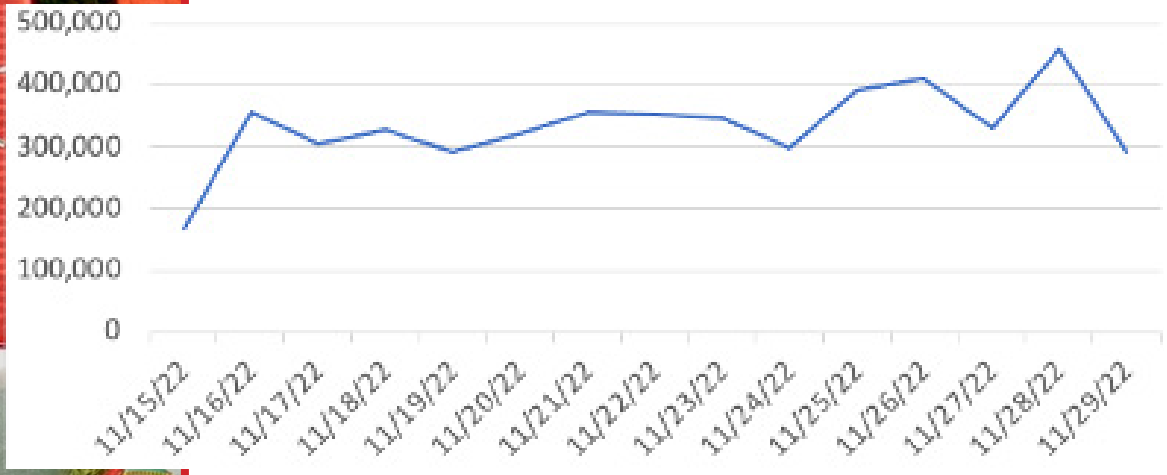
On the other hand, the known_scraping_tools category would include those like coupon and price comparison bots that gather pricing, inventory, product descriptions, and other data, which certain types of commerce organizations may want to prevent. Over the last three months on a rolling average, we have observed a ~53% increase in this type of bot activity driven by back-to-school promotions in August as well as retailers starting 2023 holiday season promotions in October. Note that evasive scrapers, the dangerous ones that are trying to grab your content for purposes like creating an imposter site, fake storefront, or phishing campaign, are not included in this category, they are part of the nefarious bots (the blue bar in our first graphic.)

Layer 7 DDoS Attacks



Since the beginning of August, Akamai has observed a ~50% increase in Layer 7 DDoS attacks against U.S. customers within the Retail sub-vertical. With the approaching holiday season, we expect to see a continued increase in application layer DDoS activity through the new year.

Audience Hijacking Sessions



With inflationary pressures driving consumers to look for the best online deals, expect audience hijacking tactics to increase for the 2023 holiday season. According to Akamai research, up to 15% or more of eCommerce site sessions are impacted by audience hijacking, which occurs when unauthorized advertisements or pop-ups divert site visitors away from an online store to competing and sometimes malicious phishing websites. These diversions are a result of third-party JavaScript being injected into the eCommerce site through browser extensions and plug-ins that can lead to increased cart abandonment, affiliate fraud, and revenue loss. Last year, sessions impacted by coupon and price comparison extensions increased between 25-30% during Cyberweek 2022 and peaked on Cyber Monday.

Background on the Continued Rise in Sophisticated Magecart-style Web Skimming Attacks

Online retailers continue to fall victim to Magecart-style web skimming attacks, which aim to steal sensitive end-user information, including payment card data, through malicious JavaScript code injection during the eCommerce checkout process. By exploiting first-party code vulnerabilities or compromising a website's supply chain of third-party JavaScript dependencies, an attacker is able to skim and exfiltrate an online shopper's sensitive data to a controlled domain. These attacks can have devastating business consequences, including revenue loss, harm to brand reputation, and regulatory fines.

Throughout 2023, Akamai Threat Research discovered a number of new Magecart variants across recent Magecart campaigns targeting thousands of eCommerce sites across the globe, and we can expect these attacks to grow in popularity during the holiday season. Our latest research also uncovered that half of the JavaScript used by online retailers come from third-party vendors, leaving the commerce vertical increasingly vulnerable to the threat of these attacks. To ensure payment card data is protected by client-side threats, the latest PCI DSS standard, v4, introduces new JavaScript security requirements organizations must be in compliance with by 2025.

This year's research on Magecart-style web skimming attacks include:

- At the beginning of the year, Akamai analyzed the attack on Canada's largest liquor retailer, LCBO, and revealed techniques used in the campaign which included abusing a known third-party vendor, Google Tag Manager

- In June, Akamai researchers discovered a new Magecart-style campaign that was abusing legitimate websites to attack others and victimizing two websites. This included the legitimate sites hijacked for hosting, which act as attacker-controlled servers, and the vulnerable commerce sites attacked with client-side web skimming. Some of the victims in this campaign are estimated to handle hundreds of thousands of visitors per month, potentially putting tens of thousands of shoppers' sensitive data at risk of being stolen.

- In August, Akamai researchers discovered another new Magento campaign with a hidden server-side template injection exploiting digital commerce sites to extract pay statistics. This campaign mixed both server-side injection with simple JavaScript-based skimmers.

- Our latest Magecart blog post uncovers a new JavaScript obfuscation technique in which attackers are manipulating a website's default 404 error page to disguise malicious JavaScript code. Akamai researchers found this new campaign consists of two additional sophisticated concealment techniques, revealing how attackers are developing tactics to lengthen the attack chain and further avoid detection.

2022-2023 RH-ISAC RANSOMWARE THREAT LANDSCAPE COMPARISON

Context

Between January and September of 2023, the RH-ISAC community experienced a massive increase in ransomware targeting the hospitality, retail, and travel sectors, and began reporting ransomware-related intelligence at a drastically higher rate than in 2022. This report only covers ransomware activity directly reported by membership, and does not include ransomware activity reported in the Daily Dark Web Summary reports, which have a nexus to the community but do not affect members directly.

Trends in Member Reporting

In 2022, members discussed a total of 7 individual ransomware families, whereas, in 2023, members reported a total of 12 separate ransomware families, indicating both increased reporting and more diversity in ransomware operations targeting the RH-ISAC community.

In 2022, members shared intelligence related to ransomware a total of 200 times, whereas from January to September alone in 2023, members shared intelligence on ransomware 419 times. This is a 109.5% increase in reporting. *(Note: sharing intelligence on ransomware does not indicate or preclude an attempted compromise.)*

TOP SHARED RANSOMWARE FAMILIES

2022	2023
1. Lockbit	1. Cl0p
2. Lapsus$	2. Lockbit
3. Blackcat/AlphV	3. Blackcat/AlphV/ Scattered Spider
4. Blackbasta	4. Akira
5. Stormous	5. BianLian
6. Royal	6. Royal
7. Quantum	7. Blackbyte
	8. Stormous
	9. Blackbasta
	10. Lapsus$
	11. Conti

Community Response

The RH-ISAC community response falls into several categories:

RH-ISAC Disclosure Policy

The RH-ISAC does not discuss events directly affecting members publicly or in sharing channels, but does reach out directly to affected members to offer support and explore sharing opportunities.

Monitoring and Alerting

The RH-ISAC intelligence team, assisted by member subject matter experts, monitors a variety of open and closed source feeds for information regarding potential targeting of members, including Dark Web sources. The RH-ISAC intelligence team also notifies members of potentially vulnerable publicly exposed infrastructure via Shodan and other alert sources.

Dark Web Summary

The RH-ISAC intelligence team produced a daily collection of Dark Web posts and claims by ransomware threat actors that are relevant to the community. Most of these posts do not impact members directly but offer visibility on the increasing number of compromised third-party vendors and service providers.

Mitigation Recommendations

When threat vectors are known, the RH-ISAC intelligence team will report major defensive recommendations and security controls in regular Member Exchange reporting.

Executive Collaboration

While the RH-ISAC intelligence team reports on the tactical and technical intelligence related to ransomware events, the leadership team coordinates closed-door discussions at the executive level between member organization leaders to facilitate defensive collaboration and sharing.

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