TLP: WHITE

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY INTELLIGENCE TRENDS SUMMARY

May – August 2022

Introduction

In this installment of the Retail & Hospitality ISAC (RH-ISAC) Intelligence Trends Summary, we highlight where intelligence sharing, requests for information (RFIs), surveys, and a wide variety of other engagements continued to add value to RH-ISAC membership. This report looks back at the RH-ISAC community's intelligence sharing output for the four-month period between May 1 and August 31, 2022. We shed light on the top threats and malware families reported by the community and try to extract trends and insights to help member analysts understand and detect shifts in the retail, hospitality, and travel threat landscape.

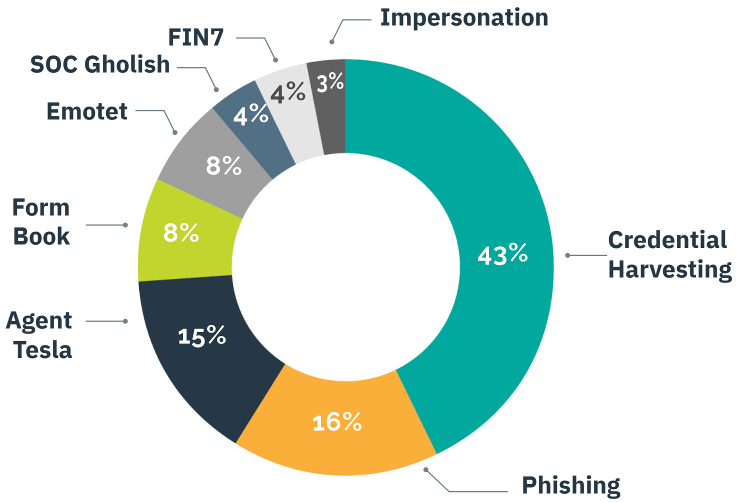
The RH-ISAC Research and Analytics team has also stayed busy supporting the community through the management and distillation of various requests for information (RFIs), surveys, and the management of the Chief Information Security Officer (CISO) and Analyst Communities in Member Exchange. From risk management to loyalty programs to security architecture, members in both communities engaged in enriching exchanges and produced practical and actionable content.

Analysis of the intelligence sharing for this period showed that the top reported threats by volume continued to reflect the steady reliance by cybercriminals on tried and tested threat vectors like credential harvesting and phishing. Log4j has now taken a back seat to new emerging trends, such as the resurgence of Emotet. As familiar threats continue to shape the threat landscape for the retail, hospitality, and travel sectors, emerging trends shift the nuances and demands on resources for cyber defenders.

THREAT LANDSCAPE: Trends

Top Sharing Trends

This graph illustrates the shared threat trends for the current period, which can be described as the frequency that threat types were shared through Member Exchange, Slack, and the Core Member Listserv. For the May to August period, credential harvesting remained the most common threat shared by members at 43%, falling noticeably from the Jan-April period's 48%.

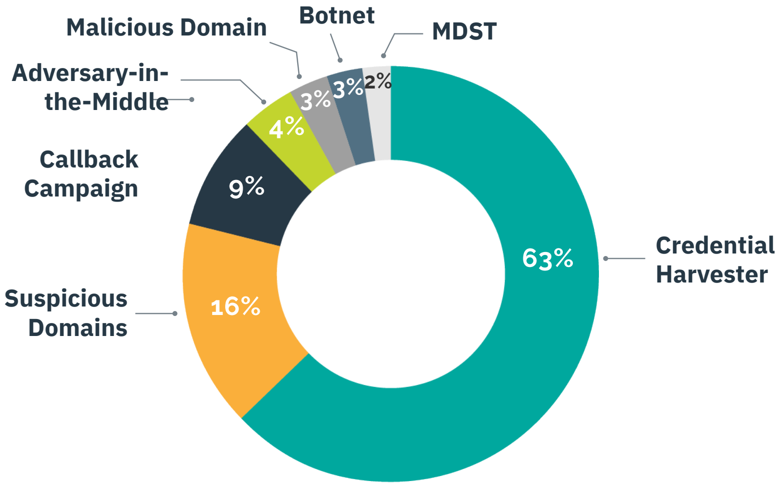


Phishing emerged as the second-most prominent threat at 16%, up from 10% in the previous period. In the first months of 2022, Members reported a general increase in phishing attempts, noting especially novel methods.

In third and fourth place are Agent Tesla, at 15%, and Formbook, at 8%. RH-ISAC members have seen a decrease in Agent Tesla since the previous reporting period, where the malware came in at 17%. Formbook previously held fifth place with 8%. In fifth place for the current period is Emotet at 7%, as compared to fourth place at 10% during the previous period. While Emotet reemerged in significant volume in late April 2022, the group has become a stable threat in RH-ISAC member reporting for the current period.

Top Reported Trends

This graph illustrates the total instances of threat indicators reported by members. Whereas the previous graph, Top Shared Trends, outlined the frequency of sharing regarding a threat topic, the Top Reported Trends graph shows the volume of threat indicators shared related to a given topic.



For total volume, credential harvesting was by far the most prevalent reported threat at 63%, down from the last supporting period, where credential harvesting ranked first with 67%. The remaining reported threats were split between well-known, established trends such as malicious domains (3%) and more recent developments such as AiTM attacks with 4%.

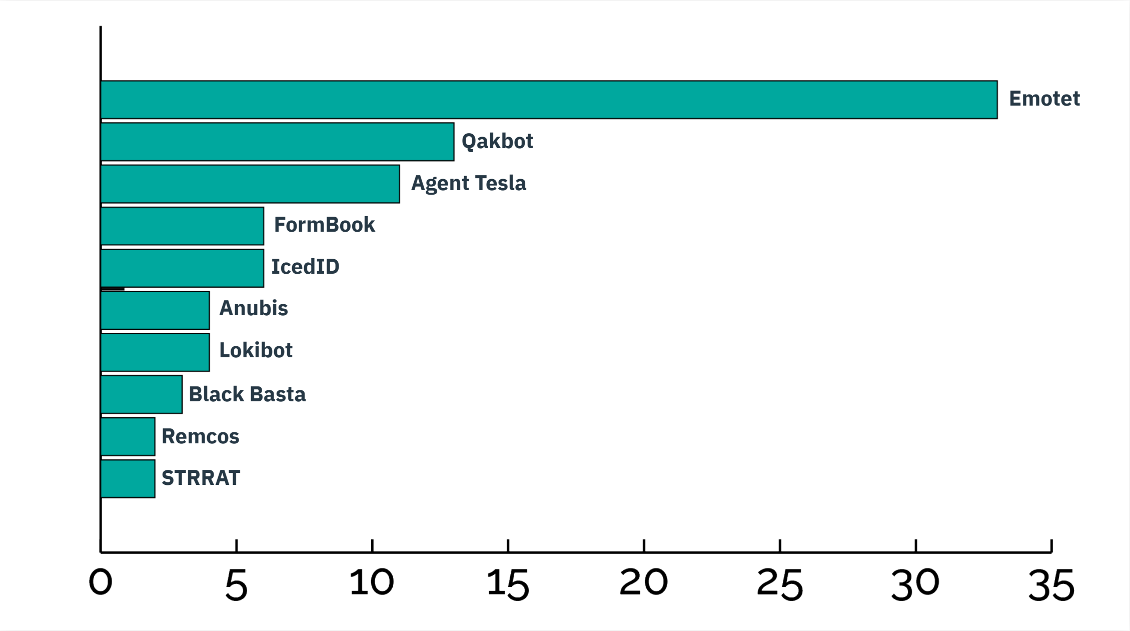
Top Reported Malware

The top ten malware threats from May-August 2022 make up 81% of the total reports the RH-ISAC tracked during this period. Emotet was by far the most prevalent malware for the period, a continuing trend from the first period of 2022. Emotet reporting came in at 33%, down from 47% of total reported malware instances during the previous period. During the first period of 2022, the prevalence of Emotet by itself at 47% outweighed the remaining nine top malware threats, which together totaled 42%. At the time, RH-ISAC assessed that it was not clear whether the drastic increase in Emotet reporting was a result of a massive increase in Emotet activity, a pivot of members to focus on Emotet defense, or some combination thereof. While it is still not possible to make a definitive judgment, the sustained Emotet activity reporting over a five-month period could suggest that Emotet activity is once again steady after the group's reemergence earlier this year.

Other top trend shifts included:

- Qakbot rose to second place with 13%, up from 21st place with less than 1% last period
- Agent Tesla fell to third place with 11%, down from second place last period with 12%
- IcedID fell to fifth place with 6%, down from third place last period with 7%
- Formbook held at fourth place with 6%, compared to 5% last period

The remaining 19% of reported malware threats are split between 26 other malware, including but not limited to BazarCall, Maui Ransomware, BlueStealer, CopperStealer, Snake Keylogger, and SocGhoulish.

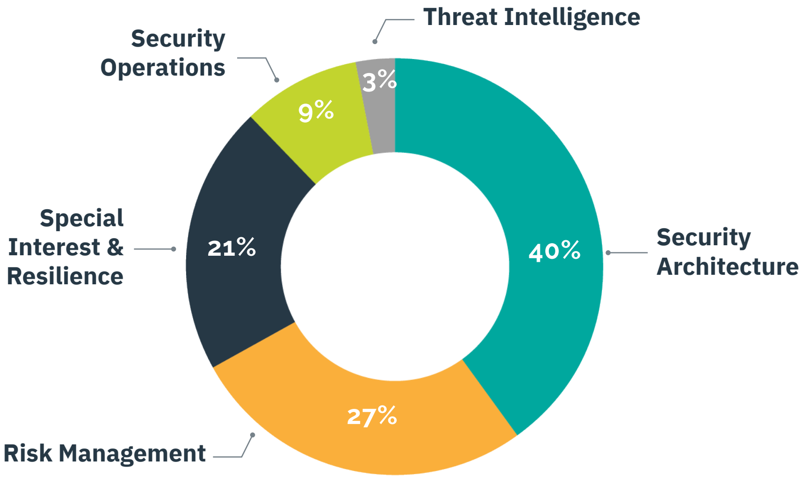


RESEARCH & ANALYTICS

The RH-ISAC has continued to track Requests for Information (RFIs) and surveys to determine what our members are most interested in, from the analyst perspective to the CISOs. Members continue to leverage the RH-ISAC RFI process integrated into Member Exchange, enabling our members to post RFIs to their peers with attribution or anonymously.

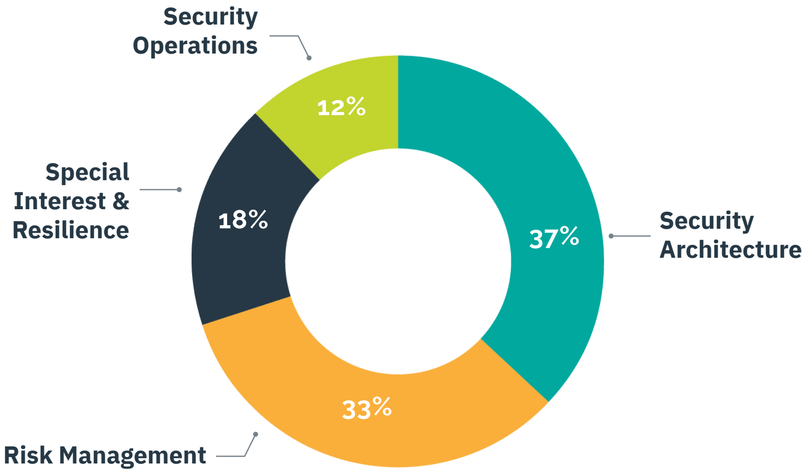
Requests for Information

In total, for the timeframe of May-August 2022, members submitted 70 RFIs, with 170 responses. The figure to the right displays the category of RFIs submitted for May-August 2022.



CISO Community Reports

The Research & Education team published four CISO Community Reports reflective of Core Member CISO viewpoints on ATO, Data retention policies (related to emails and other communication channels such as Slack or Teams), Bug bounty programs, and Splunk tool/capabilities overviews.



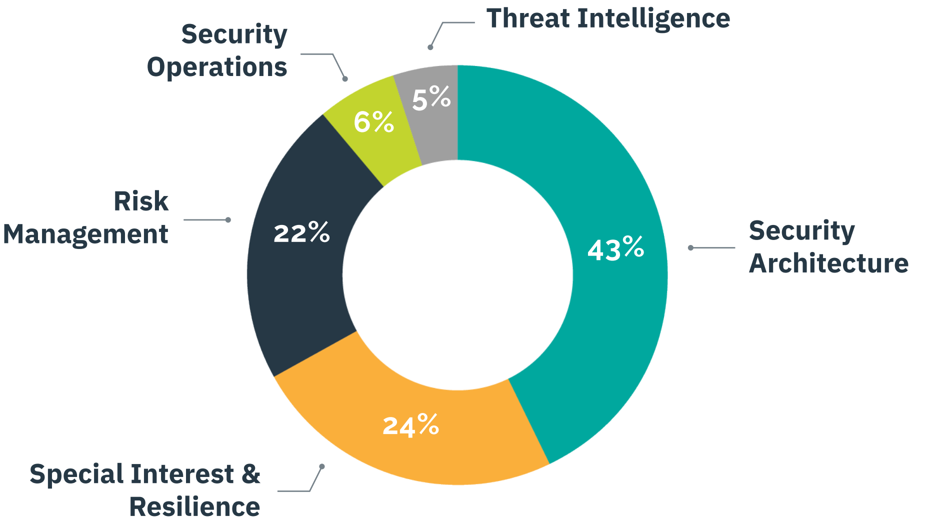
Analyst Community Reports

In the Analyst Community, security architecture is of primary interest to the audience as it relates to security engineering (tool Integrations & use cases) and identity and access management (IAM). This is a shift in trend when compared to the first period (Jan–April), where risk management was the most common trend, covering security awareness and third-party risk management topics.

This period's most discussed topics include tool-related questions related to Splunk, MDR providers, container runtime protection tools, as well as IAM topics covering MFA, cloud orchestration, and overall CIAM strategy.

Another key topic trending in the Analyst Community is special interest and resilience, which includes RFIs related to ATO, Fraud, and Ransomware. Members inquired if other members were seeing an uptick in ATO, BOT/ATO attacks, and Fraud sites.

The figure below shows a total breakdown of the RFIs submitted to the Analyst Community.



Surveys

During May–August 2022, RH-ISAC conducted one survey in partnership with Alfahive, an Associate Member that specializes in cyber risk quantification. The survey will help the RH-ISAC to better understand how relevant risk is to different parts of member organizations: online sales, store sales, supply chain, human resources (HR) & finance, and IT & software infrastructure.

A potential outcome of this survey is a three-month Cyber Risk Quantification working group dedicated to exploring the likelihood and financial impact of ransomware, bot fraud risk, and personally identifiable information (PII) theft, or a scenario of particular interest to participants as it relates to their business operations.

The RH-ISAC Sectors Threat Landscape

Key issues in the cyber threat landscape facing the retail, hospitality, and travel sectors remain complex and rapidly shifting. While new CVEs and threat actors emerge, old threat groups and tried-and-true TTPs continue strong or renew their prevalence.

In their 2022 Phishing Report, Zscaler noted several interesting changes in the phishing threat landscape, including a reported 436% increase in phishing attacks targeting the retail and wholesale industries and a rapid increase in smishing over traditional email phishing. Both of these points track with member-reported activity in the RH-ISAC community in the first half of 2022 and across the first and second periods.

Reporting Trends

During the second period, a series of high-profile topics and events dominated the cyber threat landscape both globally and in the retail, hospitality, and travel sectors specifically. RH-ISAC tracked these topics for the community, which included:

- From July through August, RH-ISAC reported a significant increase in connected adversary-in-the-middle (AiTM) campaigns targeting members and other global organizations.
- Throughout August, the Twilio breach began to affect the community through a series of connected breaches, such as Okta and DoorDash.
- Beginning in May, and continuing from now on, RH-ISAC began providing community and sector-specific context and analysis for major cybersecurity industry reports, including the 2022 Verizon Data Breach Investigation Report and the Flashpoint Mid-Year Data Breach Report.

Leading reporting trends from the previous period included:

- In late February, Russia invaded Ukraine, and multiple related cyberattacks emerged in open-source reporting against Ukrainian, Russian, and European targets.
- Throughout March, the Lapsus$ cybercriminal group compromised multiple high-profile organizations before international law enforcement arrested the group's leadership.
- In late March, the Spring4Shell vulnerability in the Spring web framework for Java was disclosed, and eventually, researchers determined the vulnerability was not as critical or widespread as initial reports indicated.

ASSOCIATE MEMBER ANALYSIS

For the May-August 2022 edition of the Intelligence Trends Summary, RH-ISAC invited associate member Nisos to provide analysis of a major trend they observed during the same period. Nisos is a security vendor that provides security, intelligence, and trust and safety services. Below is their analysis.

In the reporting period between May-August 2022, Nisos investigated 12 instances of extortion involving the retail and travel industry. Numerous extortion actors were identified, ranging from insider threats to ransomware groups and opportunistic individuals. The actor, TTPs, financial impact, and result of these instances are outlined in the table on the next page.

Nisos Observations and Analysis

- Extortion actors will extend conversations with their victims if they believe their actions will result in a payout.
- Extortion actors are human and often make mistakes revealing who they are if given the opportunity, allowing for attribution.
- Not all extortion actors are ransomware actors, and almost half were insiders with access to sensitive intellectual property and PII.
- Extortionists make outlandish claims and expect the individual that they are emailing to be less informed on technology than themselves.
- Excluding insider threat cases, initial access vectors from external actors varied from data brokers, Microsoft Exchange vulnerabilities, misconfigurations to remote and cloud services, and email attachments with macros.
- Insider threat extortion demands were significantly higher when the actor assumed the victim organization would pay, when the size of the enterprise indicated a larger potential loss, or when executive exit packages were at stake. “Poor cultural fits” and “financial difficulties” were often cited as the motivations behind the insider threats.

Reacting to Extortion Events

When navigating incidents involving extortion attempts, organizations were able to minimize damage when:

- They were able to account for different types of extortion, including lockup data extortion, data theft and exfiltration, double extortion, and insider threat extortion.
- Quickly evaluate the impact of paying by ascertaining the status of backups, determining if the adversary still has access, and verifying whether the actor exfiltrated data.
- Determine if payment is reasonable based on insurance coverage, incident response team effectiveness, ability to negotiate, quickly identify the type of extortion, can attribute actors (to a group or individual), understand past behavior, and common TTPs.
- Leadership is prepared for internal communications while minimizing use of email, external communications to customers or guests, necessary documentation or FBI engagement, and coordination with HR.

Extortion Instances Investigated by Nisos, May-August 2022

Extortion Group *(if known)*	TTP and Access Vector *(if known)*	Dollar Amount Initially Requested	Result
Insider	Insider Extortion (money theft): Sent email extorting Bitcoin claiming access to PII	$300,000	Attribution and law enforcement referral
Insider	Insider Extortion (sabotage): Sabotage ERP systems after poorly managed acquisition	$1,000,000 in damages only	Attribution and law enforcement referral
Insider	Insider Extortion (Sabotage): Sabotage application and stole sensitive customer data; suspected competitor	$900,000	Law enforcement referral and continual recovery effort
Blackcat	Double extortion; access through unpatched Exchange servers	$70,000	Law enforcement referral and continual recovery effort
Two U.S.-based criminals	Data theft and exfiltrate: Pilfered millions of records from misconfigured cloud server; sent extortion email	$100,000	Attribution and law enforcement referral
Blackcat	Double extortion: access through third-party data brokers via RDP	$45,000	Law enforcement referral and continual recovery effort
Two India-based criminals	Data theft and exfiltrate: Actor bought access of third-party contractor (who had access to client), used credentials to RDP to subsidiary; pilfered data and sent email; intermediary was related to a third-party contractor; data sold in Telegram channel	$75,000	Attribution and law enforcement referral
Insider	Potential Double Extortion: Human-enabled gang member tried to pay someone with access to steal data	$500,000	Attribution and law enforcement referral before they could execute extortion
Karakurt	Data theft and exfiltrate: Access vector was malicious macros within email attachments; provided copies of stolen file data likely bought from another ransomware gang; did not lock up drives and files	$35,000	Law enforcement referral and continual recovery effort
Elbie	Double extortion: access following a breach of MSSP hit in July; Used neshta and wiped drives with Recuva	$7,000	Law enforcement referral and continual recovery effort
Insider	Insider Extortion: Threatening to release sensitive emails unless buyout was initiated	$1,500,000	Law enforcement referral and continual recovery effort
Previous Insider	Insider Extortion: Email indicating a vulnerability in their products; originated from former employee from one of their foreign factories who retained access	$20,000	Attribution and law enforcement referral

About RH-ISAC

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, to share practices and insights, and to benchmark among each other – all with the goal of building better security for consumer-facing industries through collaboration. RH-ISAC serves businesses including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products, and other consumer-facing companies. For more information, visit www.rhisac.org.