TLP: CLEAR

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY INTELLIGENCE TRENDS SUMMARY

September - December 2023

Introduction

In this installment of the RH-ISAC Intelligence Trends Summary, we highlight where intelligence sharing, requests for information (RFIs), surveys, and a wide variety of other engagements continued to provide insights into the major security concerns and challenges facing the community. This report looks back at the RH-ISAC community's intelligence-sharing output for the four-month period between September 1 and December 31, 2023. 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.

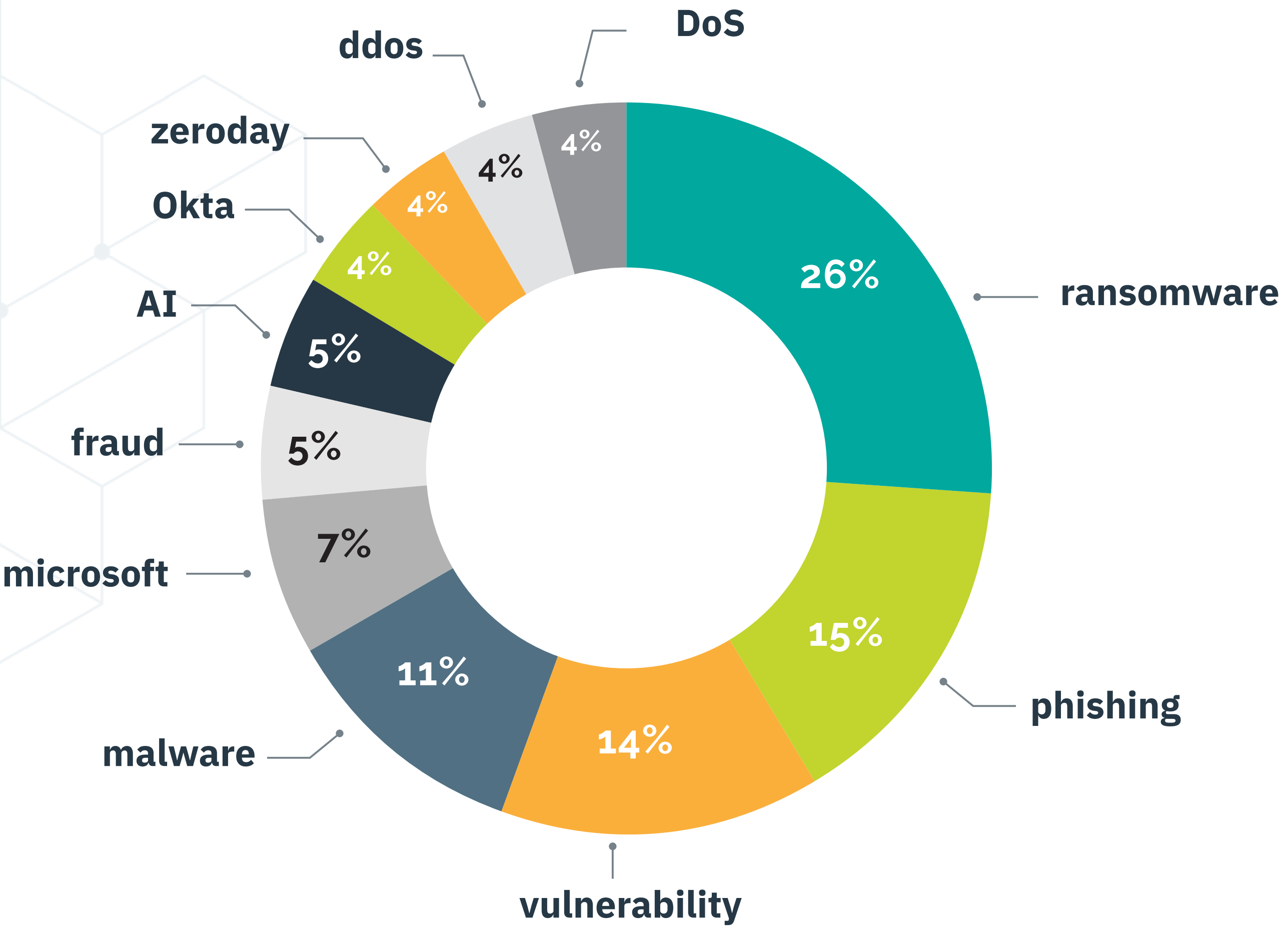
The RH-ISAC Research and Analytics team has also stayed busy supporting the community through the management and distillation of various requests for information (RFIs), surveys, and curating Communities in Member Exchange. From risk management to loyalty programs to security architecture, members in the Analyst and CISO 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 phishing. While phishing remained the second most prevalent threat, the community saw a huge spike in ransomware reporting, coinciding with a global surge in activity, bringing it to the most prevalent reported threat by members. Reporting trends for the period focused on critical threats to member operations, including Cl0p Ransomware activity, BlackCat (AlphV) ransomware activity, and Okta related vulnerabilities and activity. 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.

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 RH-ISAC Malware Information Sharing Platform (MISP). In the current period, ransomware emerged as the most common 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.



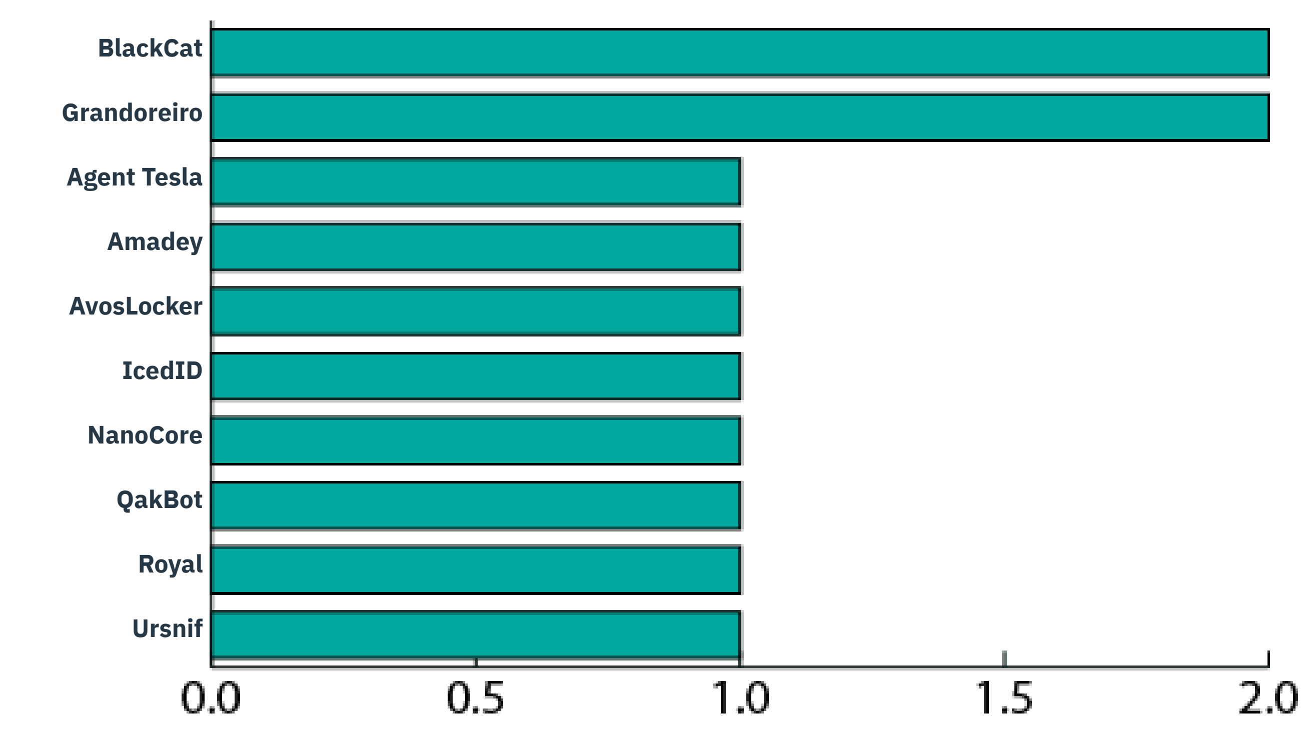
Top MISP Trends

After the launch of MISP by RH-ISAC, threat trends are tracked via the RH-ISAC MISP instance, which changed the way data is presented for threat trends in the Intelligence Trends Summary, beginning in January 2023. Tracked data on member-reported threat trends includes prevalent malware, threat actors, intrusion sets, MITRE ATT&CK Techniques, and attribute types.

Top Reported Malware

The top reported malware (MITRE ATT&CK-defined software) for the September-December 2023 period, by total count of instances, were:

- Cobalt Strike - S0154 (114)
- BlackCat - S1068 (2)
- Grandoreiro - S0531 (2)
- Agent Tesla - S0331 (1)
- Amadey - S1025 (1)
- AvosLocker - S1053 (1)
- IcedID - S0483 (1)
- NanoCore - S0336 (1)
- QakBot - S0650 (1)
- Royal - S1073 (1)
- Ursnif - S0386 (1)



Note: Nearly all Cobalt Strike reporting is from a single source, and is thus not included in the above graph to avoid skewing the perception of the data.

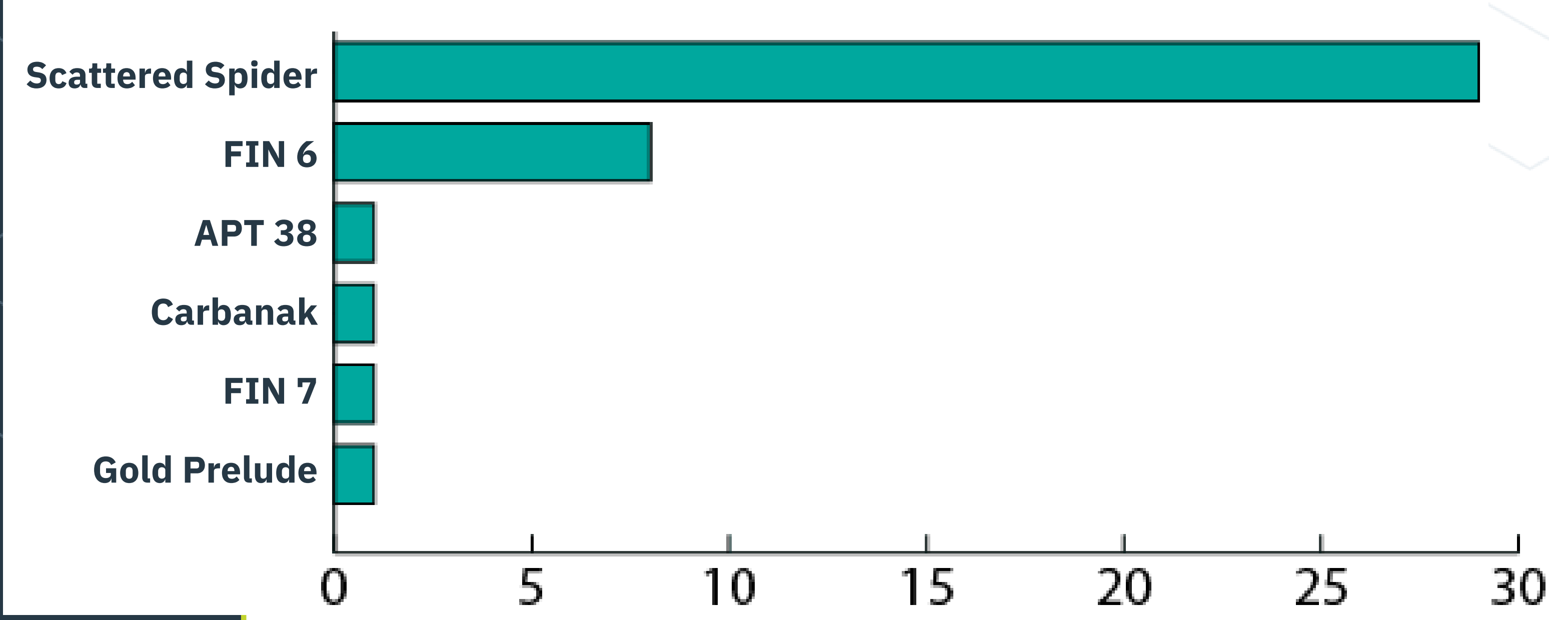
For comparison, the top reported malware (MITRE ATT&CK-defined software) for the May-August 2023 period, by total count of instances, were:

- Cobalt Strike - S0154 (102)
- QakBot - S0650 (6)
- Agent Tesla - S0331 (4)
- Grandoreiro - S0531 (2)
- IcedID - S0483 (2)
- Ursnif - S0386 (2)
- Clop - S0611 (1)
- DarkComet - S0334 (1)
- More_eggs - S0284 (1)

Threat Actors and Intrusion Sets

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

- SCATTERED SPIDER (29)
- FIN6 (8)
- APT38 (1)
- Carbanak (1)
- FIN7 (1)
- GOLD PRELUDE (1)



Note: FIN7 may be linked to the Carbanak Group, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. GOLD PRELUDE is a financially motivated cybercriminal threat group that operates the SocGholish (aka FAKEUPDATES) malware distribution network. GOLD PRELUDE operates a large global network of compromised websites, frequently running vulnerable content management systems (CMS), that redirect into a malicious traffic distribution system (TDS).

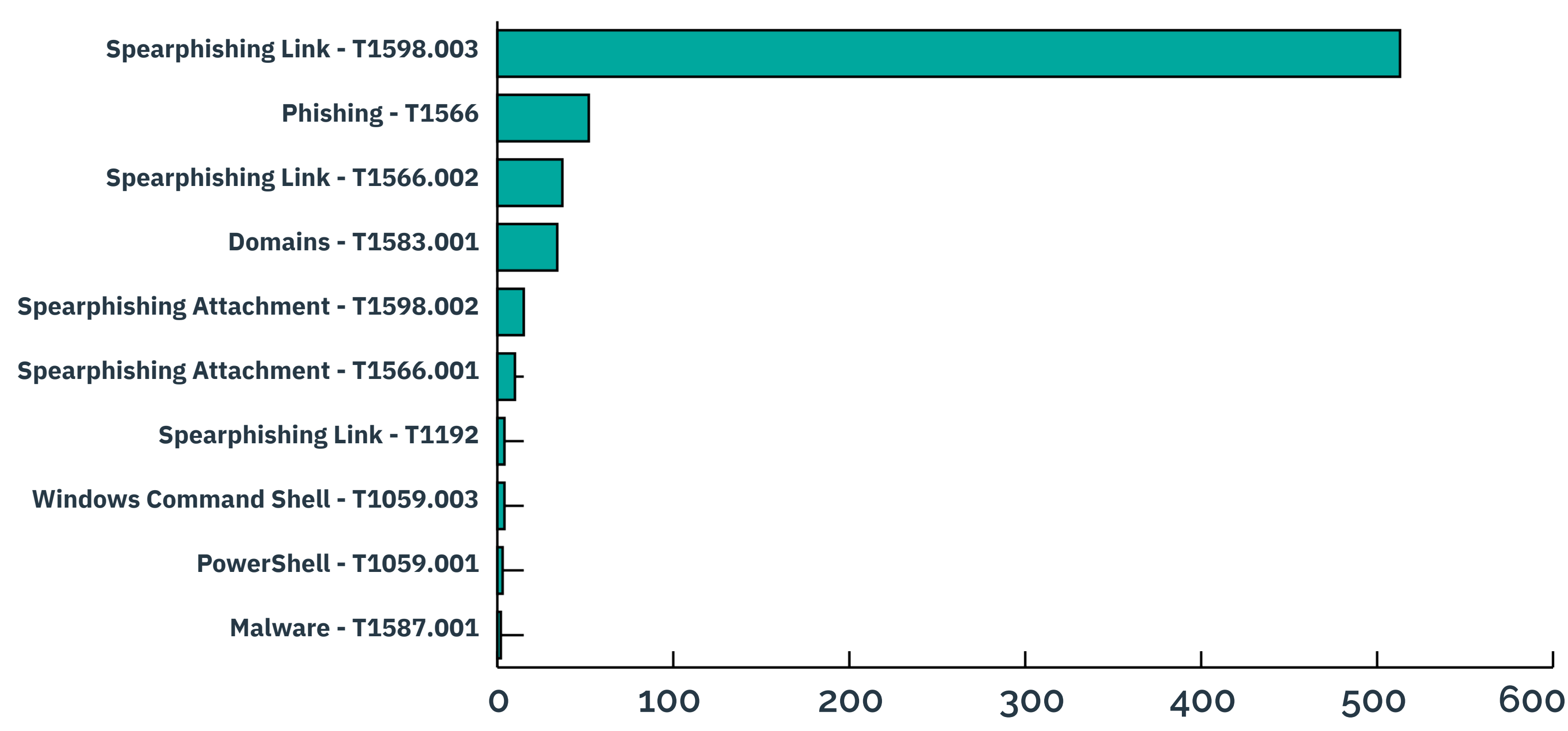
For comparison, the previous period's top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) by total count of instances were:

- FIN6 (10)
- APT32 (3)
- SCATTERED SPIDER (2)
- TA2541 (2)
- APT38 (1)
- TA505 (1)
- Volt Typhoon (1)

Top 10 MITRE ATT&CK Techniques

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

- Spearphishing Link - T1598.003 (513)
- Phishing - T1566 (52)
- Spearphishing Link - T1566.002 (37)
- Domains - T1583.001 (34)
- Spearphishing Attachment - T1598.002 (15)
- Spearphishing Attachment - T1566.001 (10)
- Spearphishing Link - T1192 (4)
- Windows Command Shell - T1059.003 (4)
- PowerShell - T1059.001 (3)
- Malware - T1587.001 (2)



Note: Spearphishing Link and Spearphishing Attachment are presented twice because they represent identical MITRE TTPs that occur at different stages of the killchain and are thus tracked separately and designated by different numerical identifiers.

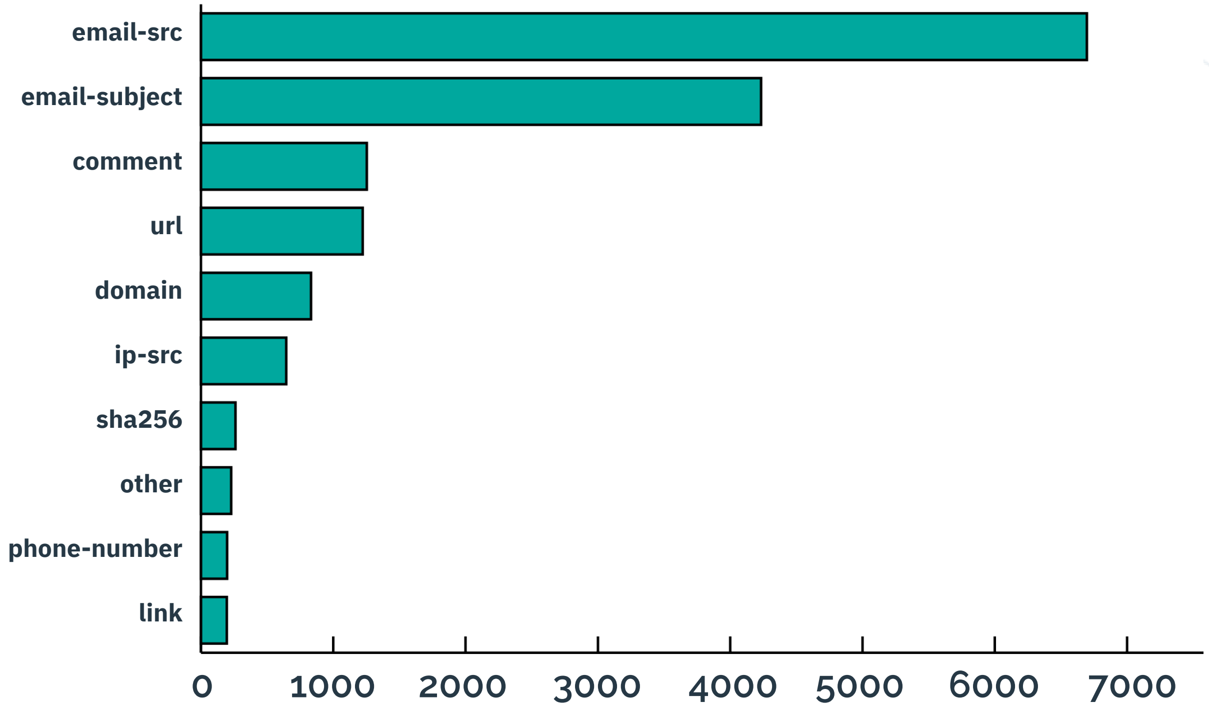
For comparison, the prior period’s top reported attribute types (categories of technical intelligence shared by members) by total count of instances were:

- Spearphishing Link - T1598.003 (219)
- Phishing - T1566 (70)
- Domains - T1583.001 (38)
- Spearphishing Attachment - T1598.002 (36)
- Spearphishing Link - T1566.002 (24)
- Spearphishing Link - T1192 (20)
- Spearphishing Attachment - T1566.001 (15)
- Credentials - T1589.001 (9)
- Spearphishing Attachment - T1193 (5)
- Credential Stuffing - T1110.004 (2)

Top 10 Attribute Types

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

- email-src (6696)
- email-subject (4234)
- comment (1254)
- url (1223)
- domain (832)
- ip-src (645)
- sha256 (261)
- other (228)
- phone-number (197)
- link (195)



For comparison, the previous period's top reported MITRE ATT&CK techniques by total count of instances were:

- email-src- (2289)
- email-subject (2200)
- url (777)
- comment (587)
- sha256 (288)
- ip-dst (266)
- ip-src (250)
- link (248)
- domain (239)
- phone-number (209)

Requests for Information

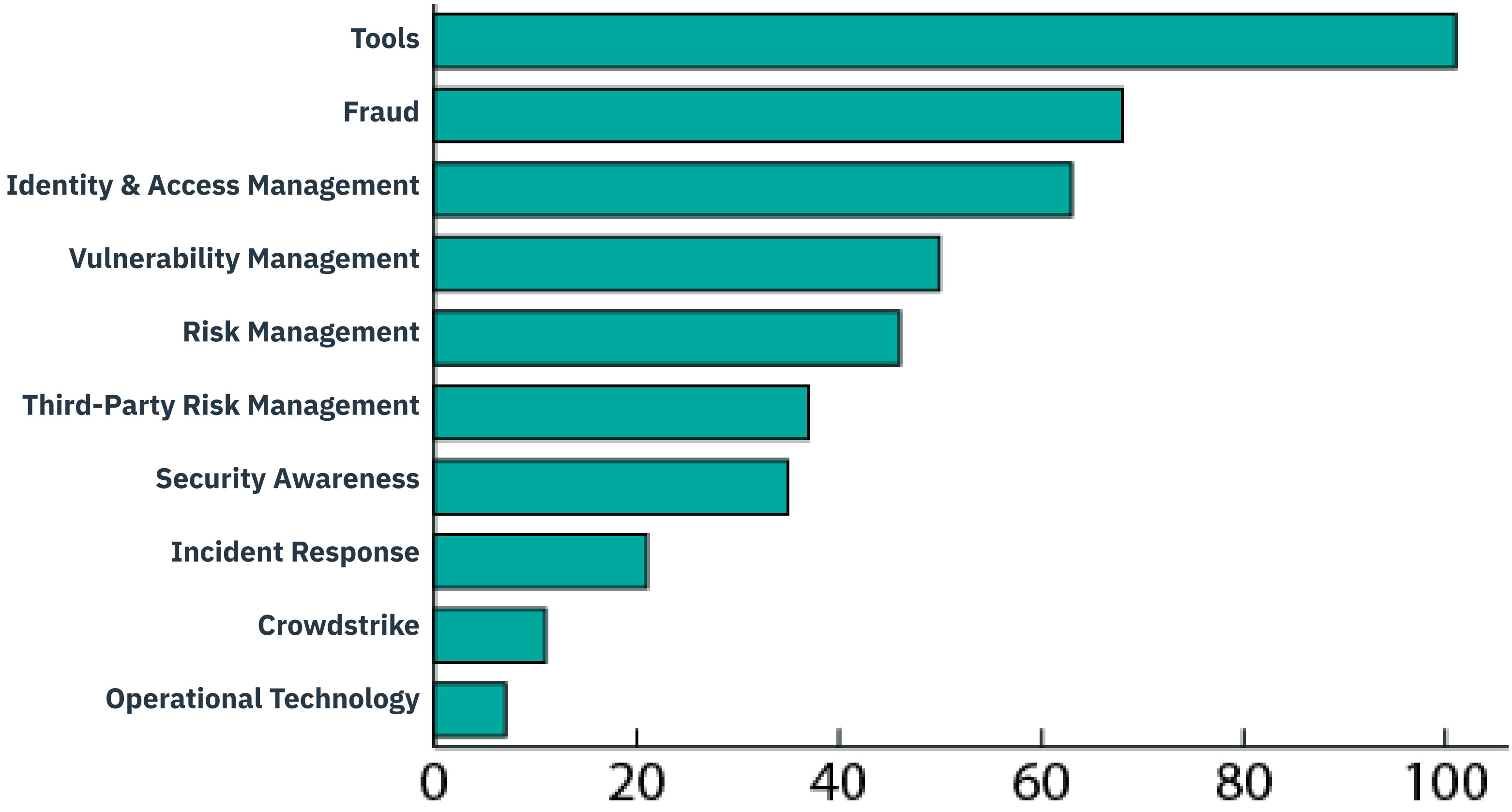
Members continue to leverage the RH-ISAC Request for Information (RFI) process integrated into Member Exchange, enabling our members to post RFIs to their peers with attribution or anonymously.

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. Between September and December 2023, 130 unique members, or 73% of our total membership, participated in RFIs or surveys.

In total, for the timeframe of September to December 2023, 110 RFIs were submitted, with 295 responses. In addition, two benchmark studies were conducted that generated 175 responses.

The figure below displays the category of RFIs, and surveys submitted for September-December 2023.

110 RFIs | 295 Responses | Average Response: 2.7



Community Engagement Outlook

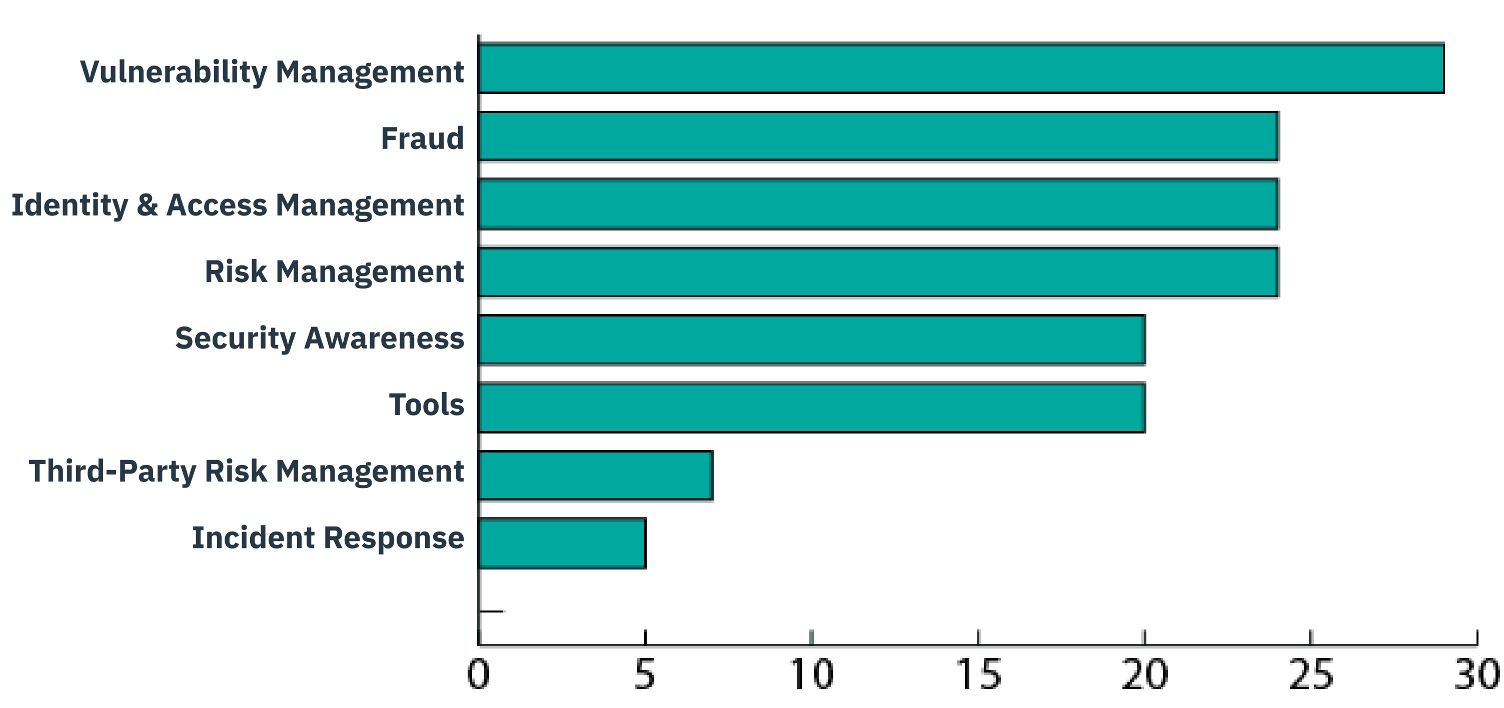
In 2022 for the timeframe of September to December, RH-ISAC received 65 RFIs that generated 245 responses. During the 2023 timeframe, continuous persistence, enhanced offerings, and growth in networking reflected an increase in community engagement with a spike in the numbers of RFIs (72%) and responses (22%).

CISO Community Overview

In the CISO Community for September to December 2023, 35 RFIs were submitted, with 111 responses. During this period, 24% of the RFIs came from the Vulnerability Management Domain with the subdomains of Penetration Testing and SOC. 20% of CISO RFIs were from Identity and Access Management with greater interest in sub-domains Access Controls and Multi-Factor Authentication. Fraud was also responsible for 20% of CISO RFIs with sub-domain topics of Gift Card and Phishing. Risk Management was responsible for 24% of CISO RFIs with sub-domain topics of Governance Risk and Compliances and Cloud Governance Practices.

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

35 RFIs | 111 Responses | Average Responses: 3.2

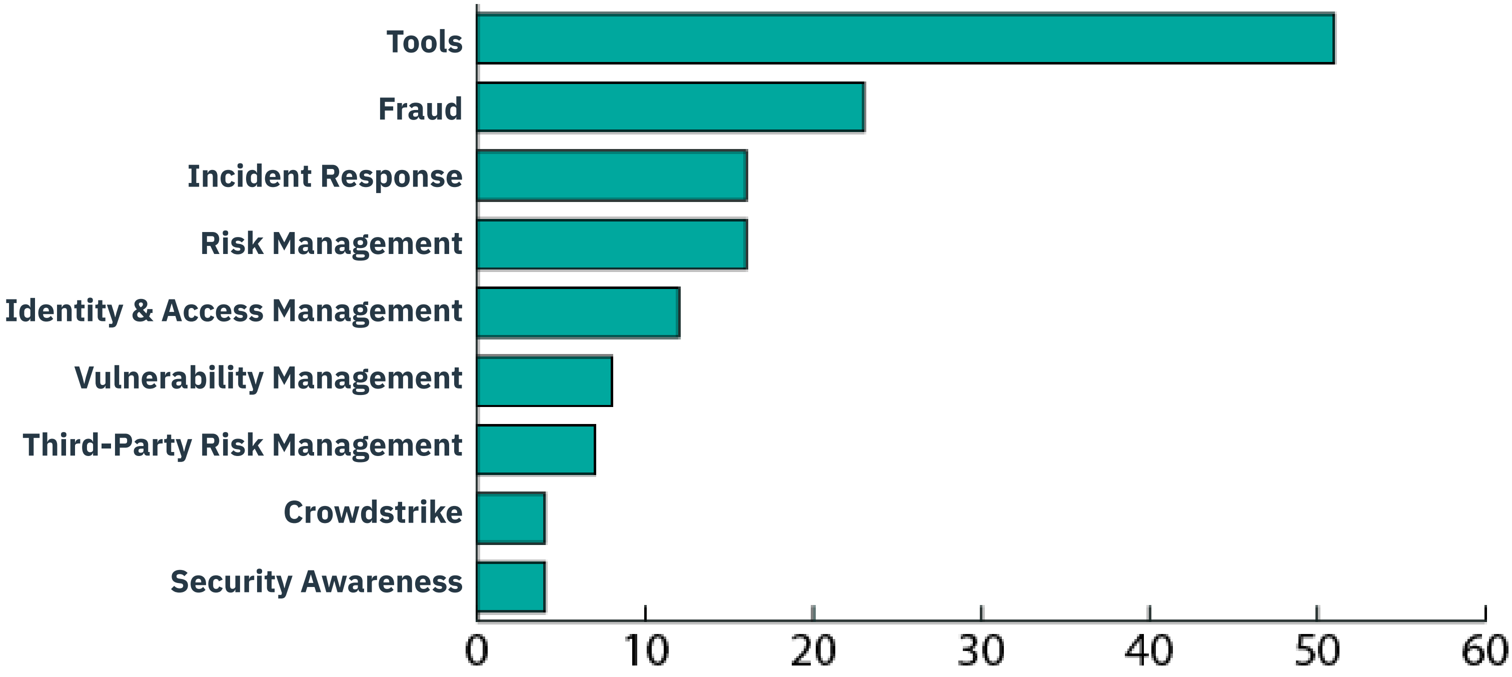


Analyst Community Overview

In the Analyst Community, for September to December 2023, 48 RFIs were submitted, with 117 responses. During this period, Identity and Access Management, Fraud, Risk Management, and Incident Response were key discussion topics among the analyst community, together contributing 53% of overall RFIs. The top subdomains from the Analyst Community were Multi-Factor Authentication, Imposter sites, IR Protocol: Notification/Communication, and Privileged Access Management.

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

48 RFIs | 117 Responses | Average Responses: 2.4



Surveys

During September-December 2023, RH-ISAC conducted one survey:

RH-ISAC Survey Report: Phishing Programs

In October 2023, the RH-ISAC conducted a survey on phishing programs for the Security Awareness WG to better understand how member companies are developing their phishing programs. This survey covered four key sections: Program Structure, Campaigns, Metrics, and Additional Training. We received 34 total responses.

Benchmarks

During this period we also collected data for two critical benchmark reports, both of which were published in February 2024:

Organizational Chart Benchmark

We collected org charts to better understand how information security teams are structured in terms of capabilities and reporting. Analysis includes where functions like cloud security and fraud align, and what shared budget and resources might be considered; and breakdowns data according to sector and revenue group. We received 38 total responses.

CISO Benchmark

Our signature CISO Benchmark Report helps members understand the diversity of the RH-ISAC community, as well as their place in it. Whether it is by industry, annual revenue, or budget, you will learn what responsibilities are most common among CISOs, the collective challenges you face as decision makers, and how different peer groups prioritize and allocate resources. We received 133 total responses.

RH-ISAC Fraud Galaxy in MISP

On November 2, 2023, the RH-ISAC intelligence and engineering team published the RH-ISAC Fraud Galaxy in MISP for the community to contribute to and leverage.

Purpose

The purpose of the RH-ISAC Fraud MISP galaxy is to provide a knowledge base for the numerous fraud types that affect RH-ISAC members. This enables members, regardless of team size or budget, to combat fraud more effectively.

Goal

Elicit collaboration from core members to identify, classify, and describe the different fraud types to indicate what member industry the fraud type affects, how they can be detected, and how they can be mitigated.

Deliverable

- MISP galaxy with clusters for each fraud type to provide a knowledge base on fraud.
- Each galaxy cluster contains relationships to TTPs, tools used to facilitate fraud, detections, and/or mitigations for its specific type of fraud.
- The galaxy clusters can be used to tag and attribute intel to certain fraud types so members can then search or filter by the fraud categories.

Scope

- Fraud types that have an impact on the RH-ISAC member organization rather than impacting the customers.
- TTPs associated with the fraud types.
- Tools/technology/processes that can be used to detect or mitigate the fraud types.

Value

- Ability to understand TTPs associated with different fraud types.
- Ability to identify what indicators for a fraud type look like.
- Ability to share and tag fraud type indicators.
- Tools/technology/processes that can be implemented to detect and/or mitigate fraud types.

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