TLP: CLEAR

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY INTELLIGENCE TRENDS SUMMARY

January – March 2025

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 reviews the RH-ISAC community's intelligence-sharing output for the first quarter of 2025, the three-month period between 1 January and 31 March 2025. 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.

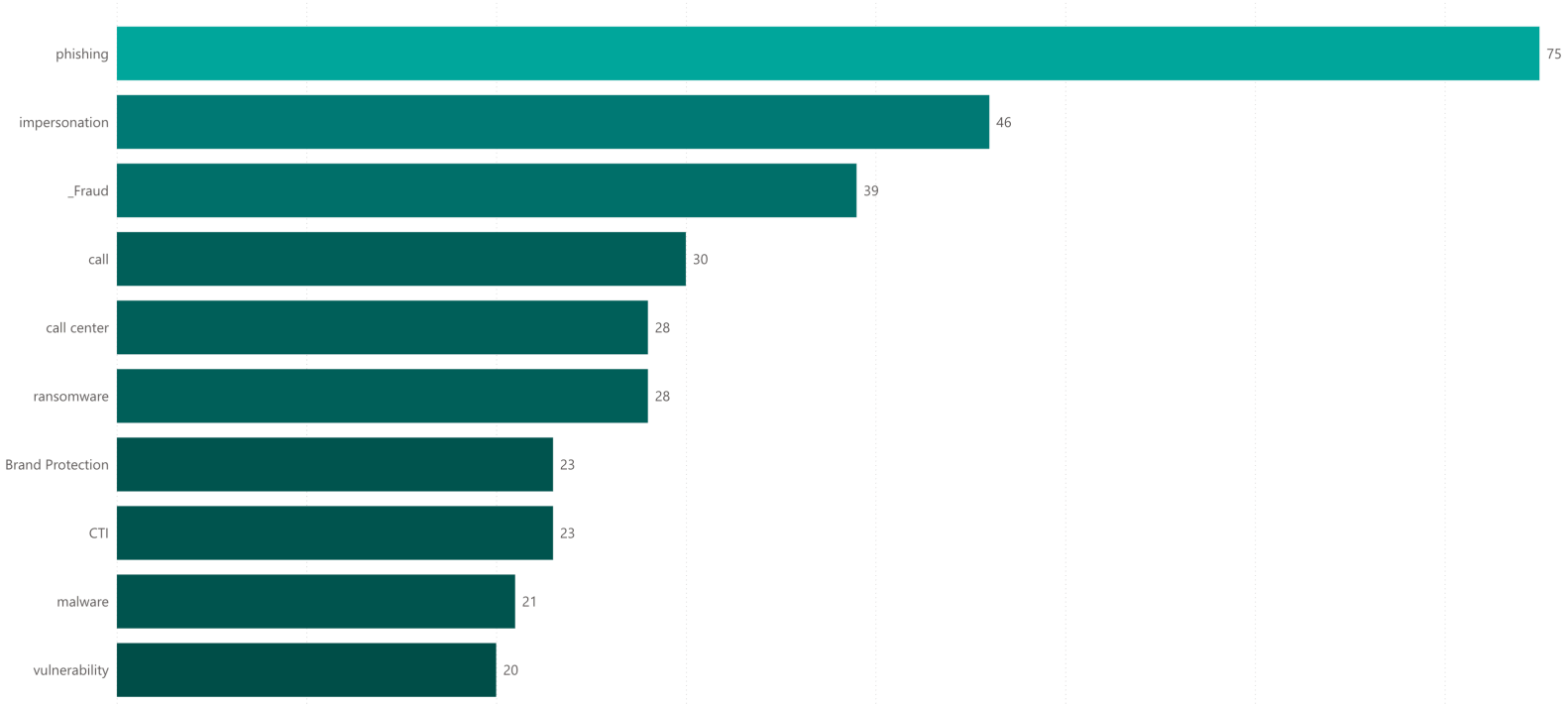
Analysis of the intelligence sharing for this period showed that the top reported threats by volume continued to reflect the steady reliance by cybercriminals on tried and tested threat vectors phishing, social engineering, and vulnerabilities. Members heavily reported increases in call center social engineering, the continuing prevalence of fraud activity, the steady presence of ransomware (even as the ransomware landscape changes with new groups and law enforcement actions), and impersonation of both brands and prominent leaders for fraud purposes.

THREAT LANDSCAPE: Trends

Top Threat Trends

The top shared threat trends for the current period, which can be described as the frequency with which threat types were shared through Member Exchange and Slack were:

- phishing (75)
- impersonation (46)
- fraud (39)
- call (30)
- call center (28)
- ransomware (28)
- brand protection (23)
- CTI (23)
- malware (21)
- vulnerability (20)



In the first quarter of 2025, threat trend reporting from RH-ISAC Core Members shifted: fraud dropped from first to third most prevalent threat topic, phishing rose to first, impersonation rose to second, and notably, call center social engineering emerged in the top threats for the first time.

In the final quarter of 2024, members shared a plethora of fraud intelligence, covering loyalty, gift card, refund, and call center fraud activities, among others. Additional topics of interest included social engineering, vendor vulnerabilities, data and credential theft, malware, and sophisticated threat actors.

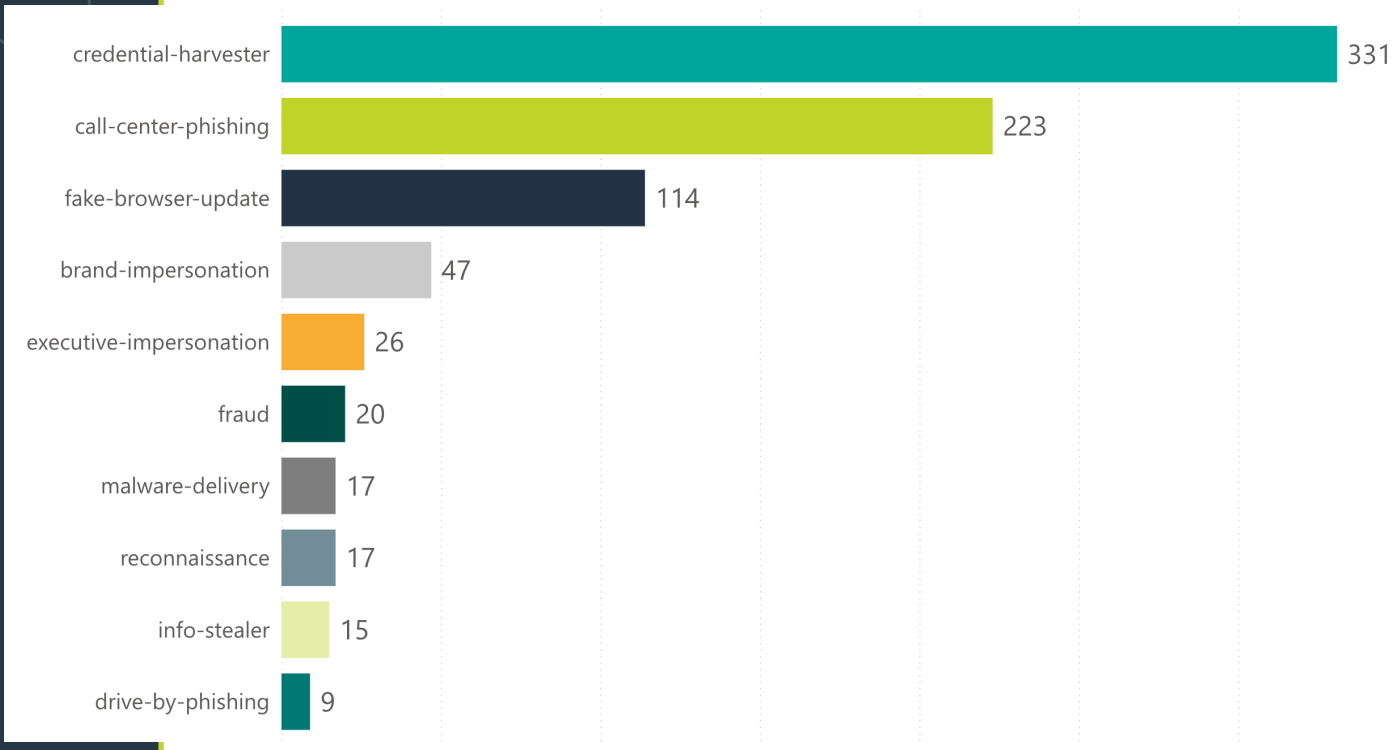
Top MISP Trends

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, attribute types. Due to enhancements in how we track, tag, and curate data shared by members in MISP, for the final quarter of 2024, we added the top reported types of threats as a tracking category for the Intelligence Trends Summary, and are adding a new category for the current period: industry share of reporting.

Top Reported Threat Types

The top reported types of threats by members for the current period by total count of instances were:

- credential-harvester (331)
- call-center-phishing (223)
- fake-browser-update (114)
- brand-impersonation (47)
- executive-impersonation (26)
- fraud (20)
- reconnaissance (17)
- malware-delivery (17)
- info-stealer (15)
- drive-by-phishing (9)



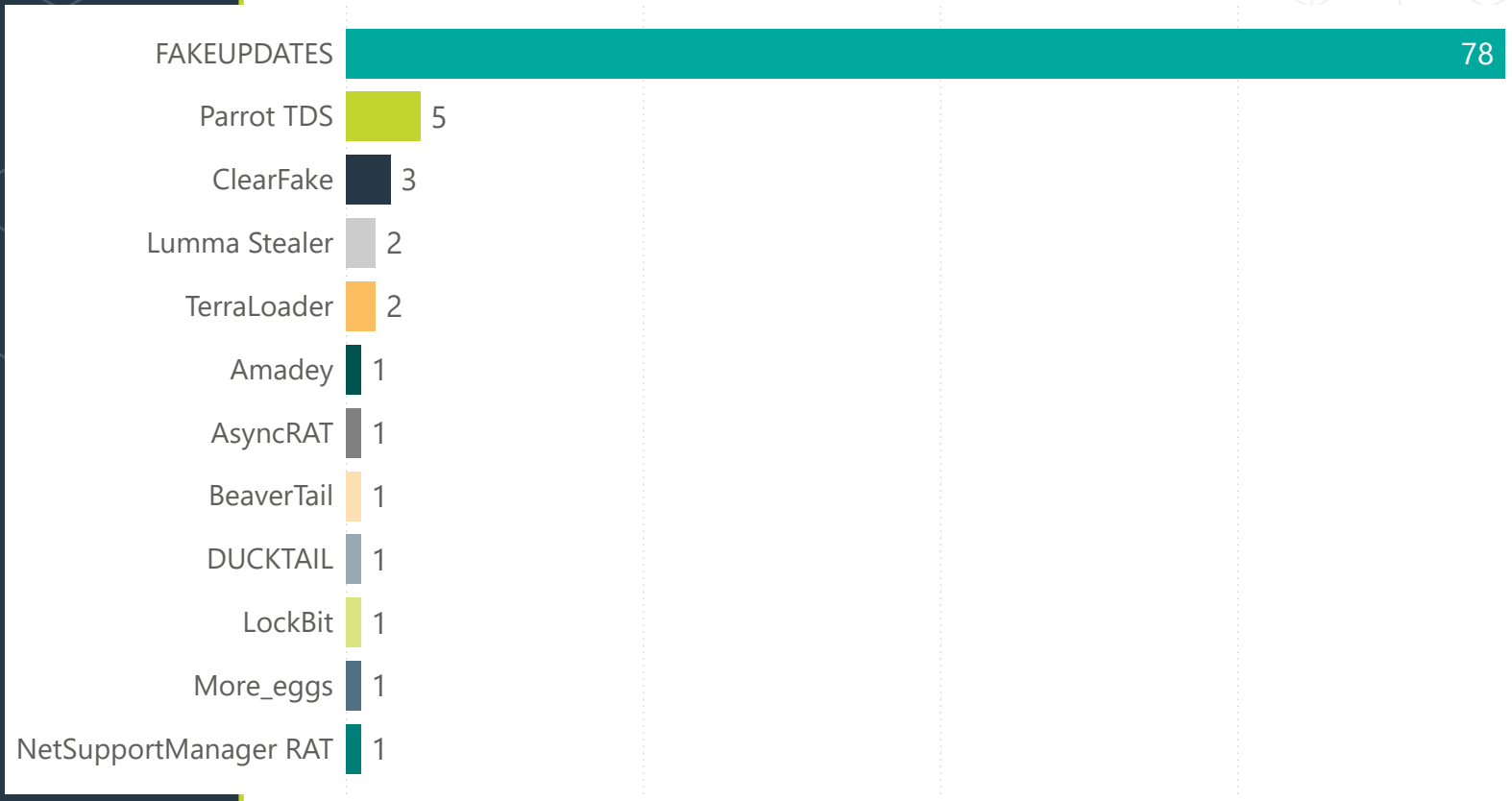
The top reported types of threats by members for the previous period by total count of instances were:

- credential-harvester (245)
- brand-impersonation (36)
- call-center-phishing (25)
- executive-impersonation (16)
- fake-browser-update (14)
- fraud (11)
- drive-by-phishing (5)
- loader-malware (2)
- trojan (2)
- malware-delivery (2)

Top Reported Malware

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

- FAKEUPDATES (78)
- Parrot TDS (5)
- ClearFake (3)
- Lumma Stealer (2)
- TerraLoader (2)
- Amadey (1)
- AsyncRAT (1)
- BeaverTail (1)
- DUCKTAIL (1)
- LockBit (1)
- More_eggs (1)
- NetSupportManager RAT (1)



For comparison, the top reported malware (MITRE ATT&CK-defined software) for the final quarter of 2024 by total count of instances, were:

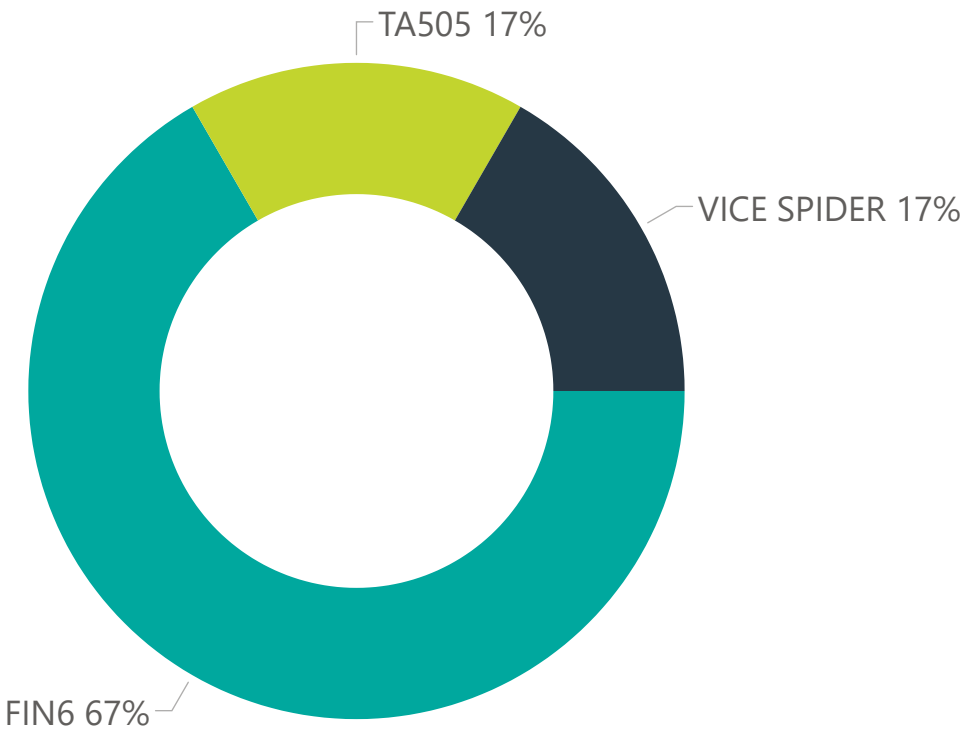
- FAKEUPDATES (12)
- Parrot TDS (2)
- Remcos (2)
- BumbleBee (1)
- Kutaki (1)
- Mispadu (1)
- POWERTRASH (1)
- Quasar RAT (1)

Top Reported Threat Actors

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

- FIN6 (4)
- TA505 (1)
- VICE SPIDER (1)

Note: Vice Spider is a Russian-speaking ransomware group that has been active since at least April 2021 and is linked to a significant increase in identity-based attacks, with a reported 583% rise in Kerberoasting incidents. CrowdStrike attributes 27% of these intrusions specifically to Vice Spider, which exploits vulnerabilities in the Kerberos authentication protocol to crack user passwords.



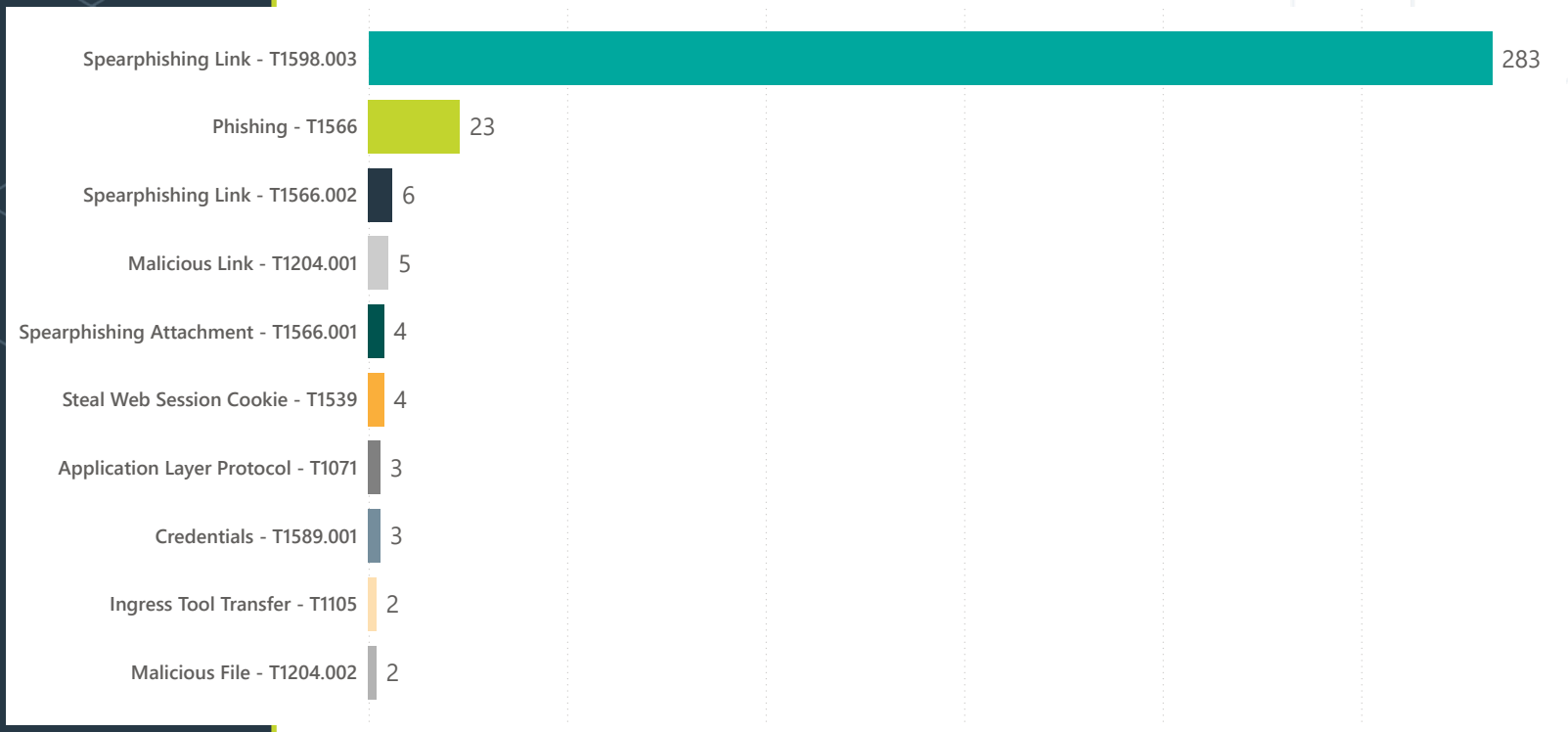
For comparison, the top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) for the fourth quarter of 2024 by total count of instances were:

- Lazarus Group (2)
- Storm-0539 (2)
- TA558 (1)
- FIN7 (1)
- SCATTERED SPIDER (1)

Top 10 MITRE ATT&CK Techniques

The top reported MITRE ATT&CK techniques for the current period by total count of instances were:

- Spearphishing Link - T1598.003 (283)
- Phishing - T1566 (23)
- Spearphishing Link - T1566.002 (6)
- Malicious Link - T1204.001 (5)
- Spearphishing Attachment - T1566.001 (4)
- Steal Web Session Cookie - T1539 (4)
- Application Layer Protocol - T1071 (3)
- Credentials - T1589.001 (3)
- Ingress Tool Transfer - T1105 (2)
- Malicious File - T1204.002 (2)



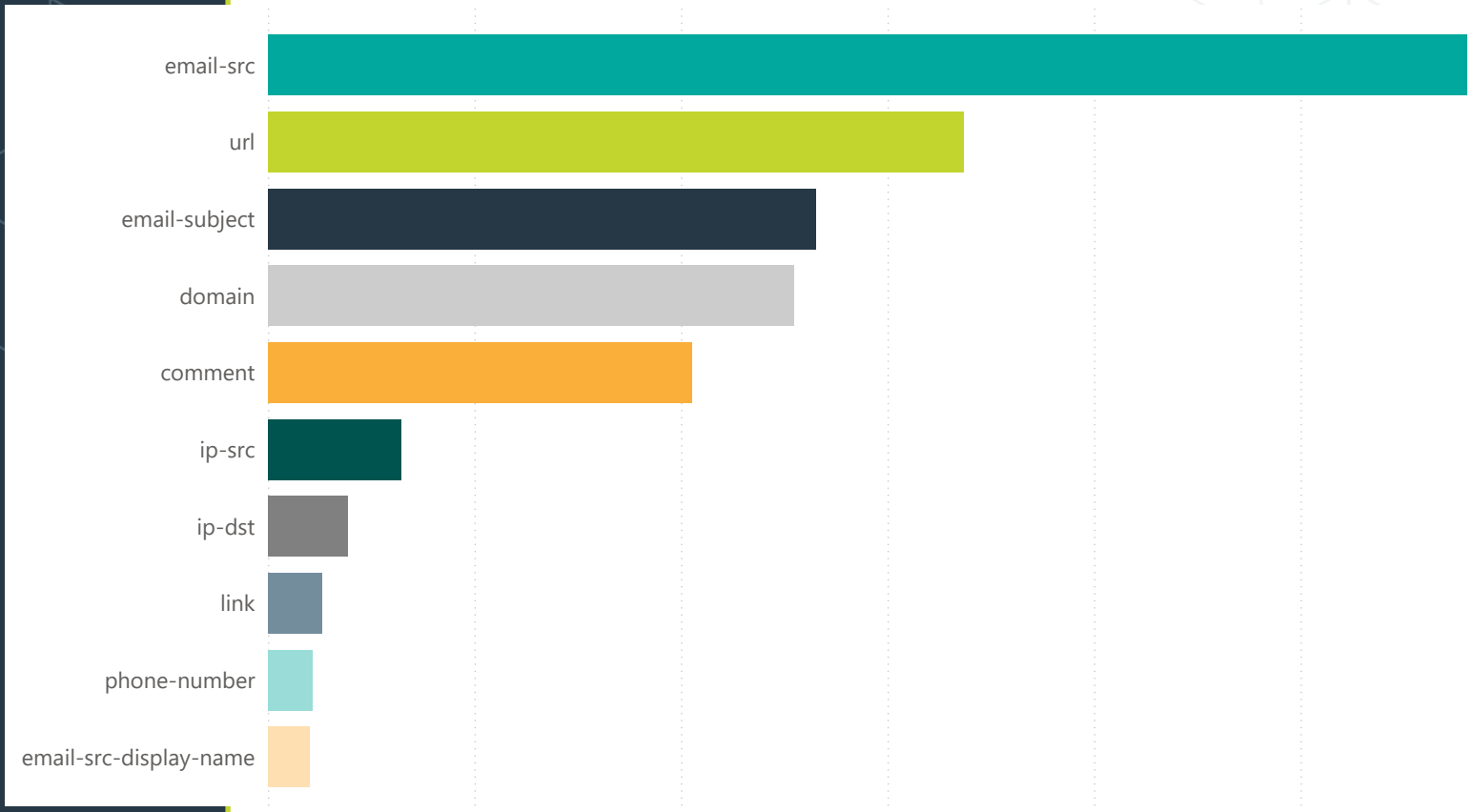
For comparison, the previous period's top reported MITRE ATT&CK techniques by total count of instances were:

- Spearphishing Link - T1598.003
- Phishing - T1566
- Spearphishing Attachment - T1598.002
- Malicious File - T1204.002
- Malicious Link - T1204.001
- Multi-Stage Channels - T1104
- Obfuscated Files or Information - T1027
- Spearphishing Link - T1566.002
- Web Protocols - T1071.001

Top 10 Attribute Types

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

- email-src (2902)
- url (1684)
- email-subject (1326)
- domain (1273)
- comment (1026)
- ip-src (322)
- ip-dst (192)
- link (131)
- phone-number (107)
- email-src-display-name (101)



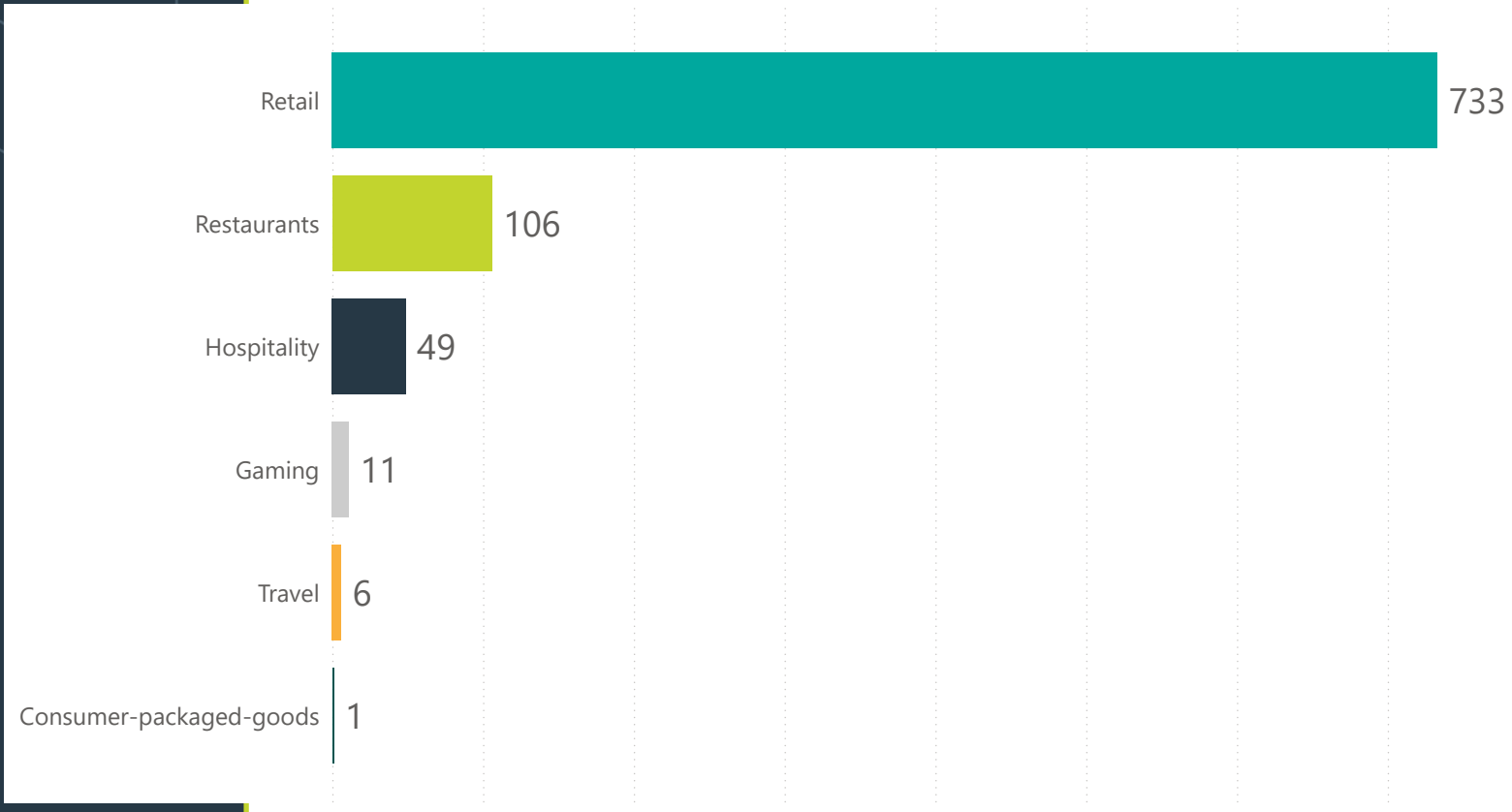
For comparison, the prior period's top reported attribute types (categories of technical intelligence shared by members) by total count of instances were:

- email-src (3601)
- url (2496)
- email-subject (2440)
- comment (1632)
- domain (1464)
- ip-src (511)
- sha256 (338)
- md5 (291)
- filename (251)
- ip-dst (202)

Industry Breakdown

The share of intelligence reporting in MISP by members broken down by industry vertical (by percentage) is as follows:

- Retail (80.9%)
- Restaurants (11.6%)
- Hospitality (5.4%)
- Gaming (1.2%)
- Travel (>1%)
- Consumer Packaged Goods (>1%)

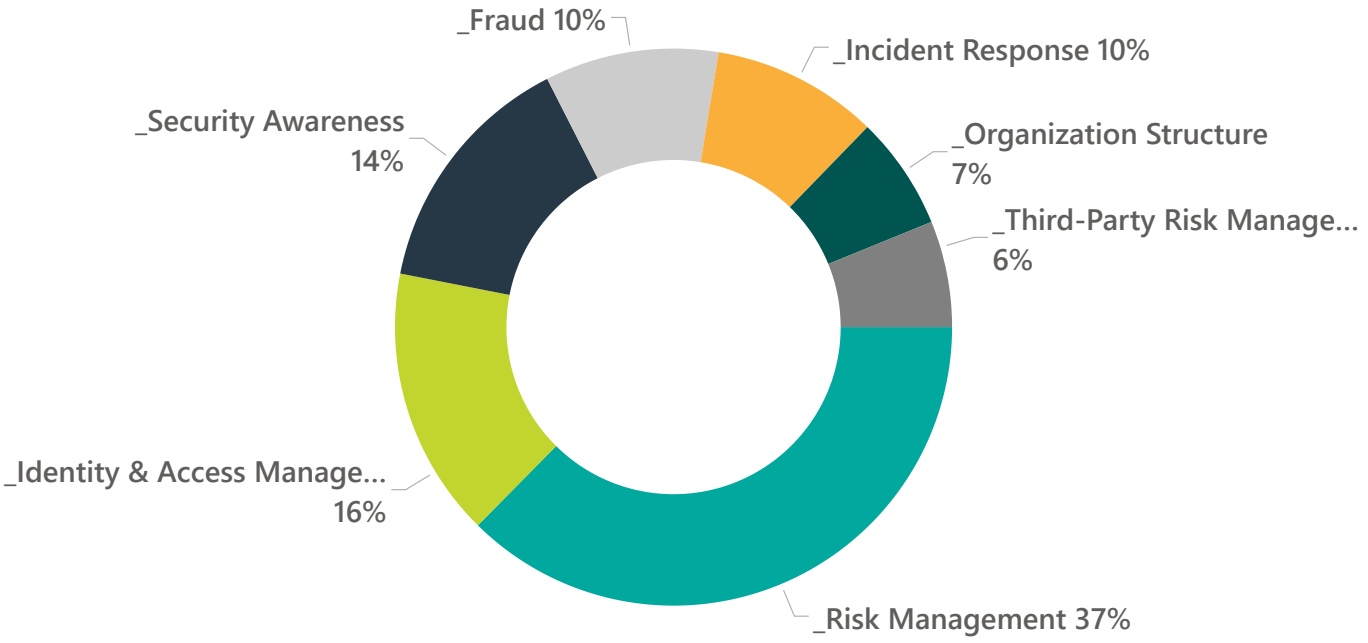


Requests for Information

The RH-ISAC actively tracks Requests for Information (RFIs) and surveys to understand our members' interests, spanning both analyst perspectives and those of CISOs. From January to March 2025, 186 unique members, or 58% of our total membership, participated in RFIs. During this period, a total of 220 RFIs were submitted, generating 702 responses. In comparison, during the same period in 2024, RH-ISAC received 151 RFIs, resulting in 499 responses. This year, the continued focus on engagement and enhanced offerings led to a substantial increase in community interaction, with RFIs rising by 46% and responses increasing by 41%.

Overall RFI Domains for January - March 2025

220 RFIs | 702 Responses



RFI Summary Publications

RH-ISAC produces reports summarizing the key take aways from RFI responses for topics that generate particularly engaging insights from the community.

Email Quarantine

In January 2025, an RH-ISAC member posted an RFI asking how other organizations manage employee access to quarantined emails. The request explored best practices around permissions, including whether employees can view-only, release emails, or require case-by-case approval. It also invited additional methods or suggestions from the community. The summary compiles insights from 15 member responses.

AI Use in The Boardroom

In January 2025, an RH-ISAC member posted an RFI in the CISO community seeking feedback on the use of AI tools for recording and producing meeting minutes, particularly for board meetings. This member expressed concerns about security, confidentiality, and legal compliance, especially around sensitive information. They are looking for recommendations on AI tools that can effectively address these concerns while ensuring data protection. This RFI summary compiles discussion responses that generated nine individual responses.

Survey & Community Recommendations Publications

In addition, the RH-ISAC produced community recommendations summary report and comprehensive survey reports:

Manufacturing Asset Management Trends Report

RH-ISAC conducted a manufacturing asset management trends survey, gathering insights from 10 unique member companies. This report provides an in-depth analysis of how RH-ISAC members manage their manufacturing assets and operations. This report explores the number of internal and outsourced plants, asset management practices, and responses to pressures for internet-based resources.

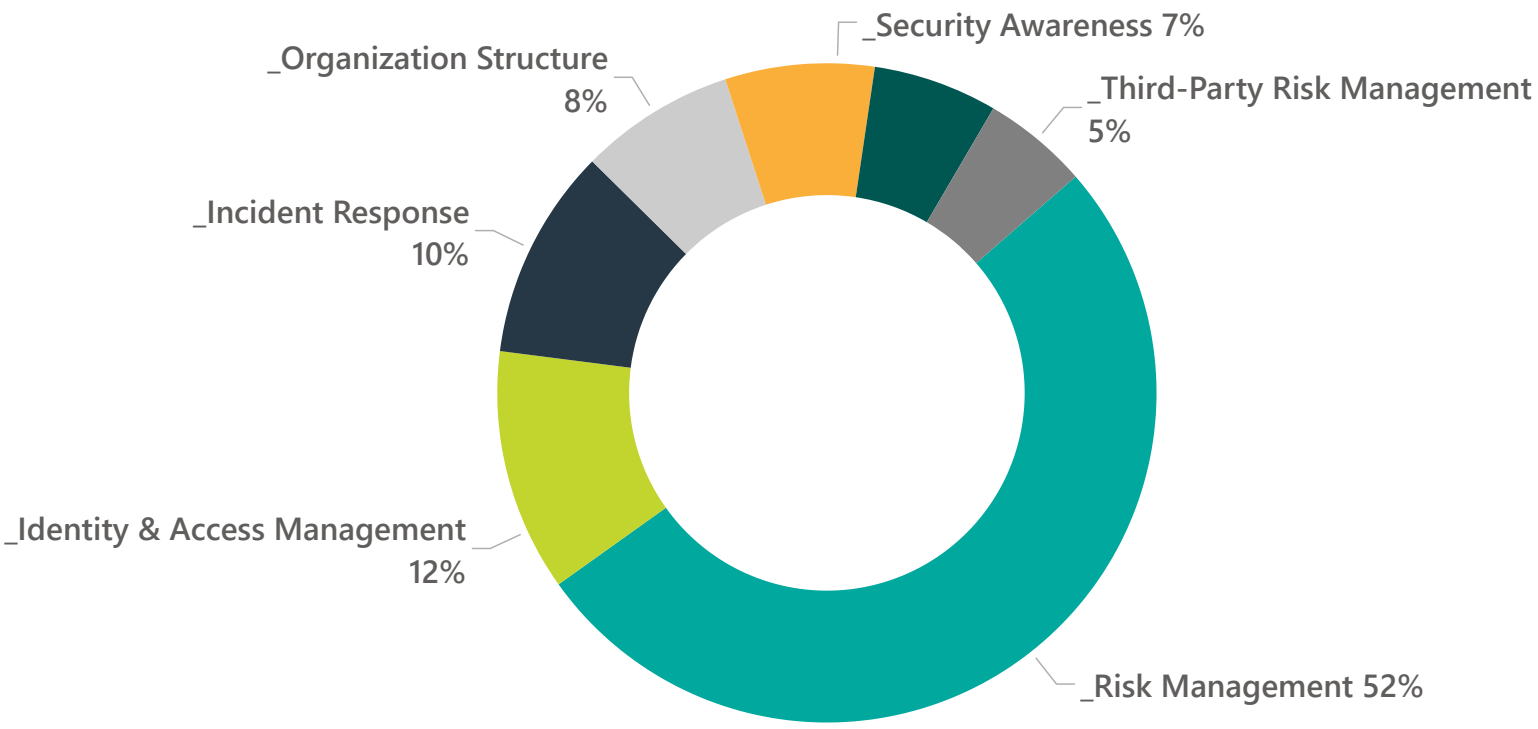
Community Recommendations Report: GenAI

This community recommendations report explores the benefits and risks of Generative AI (GenAI). It highlights how GenAI can enhance customer experience, streamline operations, and improve personalization, while also presenting significant cybersecurity risks such as AI-generated phishing, deepfake scams, and data privacy concerns. The report includes a list of Indicators of Compromise (IOCs), suggested mitigations, and best practices for safe GenAI adoption. It also links to relevant RFIs previously shared by RH-ISAC members for additional context and guidance.

CISO Community Overview

In the CISO Community, from January to March 2025, a total of 63 RFIs were submitted, resulting in 305 responses. During this period, 52% of the RFIs came from the Risk Management Domain with greater interest in Policy and Architecture and Governance, Risk, and Compliance. Identity and Access Management was responsible for 12% of CISO RFIs with sub-domain topics Password Management. The figure below shows a total breakdown of the RFIs submitted to the CISO Community.

CISO RFI Domains for January - March 2025
63 RFIs | 305 Responses



Analyst Community Overview

In the Analyst Community, from January to March 2025, a total of 157 RFIs were submitted, generating 397 responses. Key discussion topics among the analyst community during this period were Risk Management, Security Awareness, and Identity and Access Management. The top subdomains across the Analyst community were Governance Risk and Compliance, Best Practices, Security Awareness Training, and Access Controls. The figure below shows a total breakdown of the RFIs submitted to the Analysit Community.

Analyst RFI Domains for January - March 2025
157 RFIs | 397 Responses