TLP: CLEAR

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY INTELLIGENCE TRENDS SUMMARY

April – June 2025

Introduction

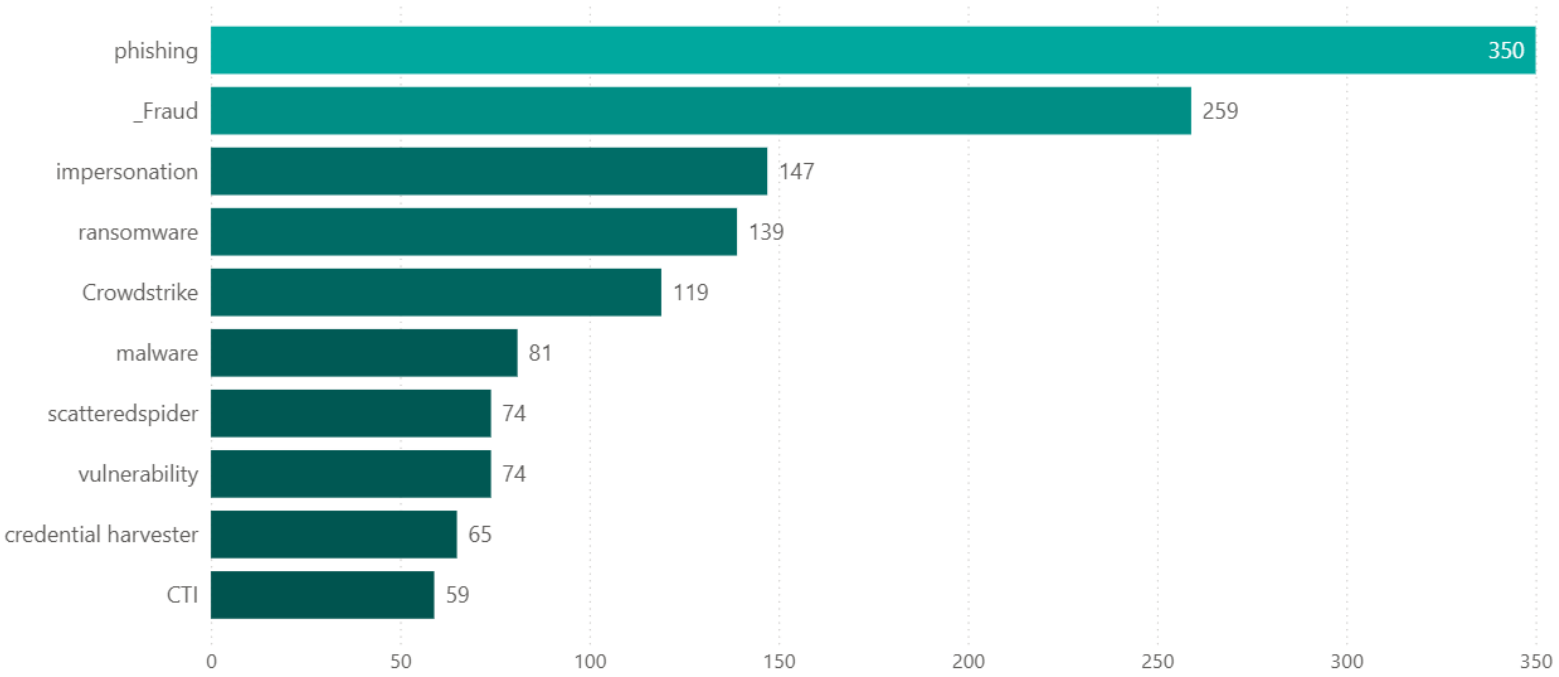
In this installment of the RH-ISAC Intelligence Trends Summary, we highlight where intelligence sharing, requests for information (RFIs), surveys, and a wide variety of other engagements which continued to provide insights into the major security concerns and challenges facing the community. This report reviews the RH-ISAC community's intelligence-sharing output for the second quarter of 2025, the three-month period between 1 April and 30 June 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 fraud. Members heavily reported on Scattered Spider activity, 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 graph above illustrates the 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.

In the second quarter of 2025, threat trend reporting from RH-ISAC Core Members showed interesting developments. Most notably, call center social engineering fell off the list after appearing in the previous period. Phishing, fraud, and impersonation remained top threats, and Scattered Spider discussion remained prevalent.

In the first quarter of 2025, 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.

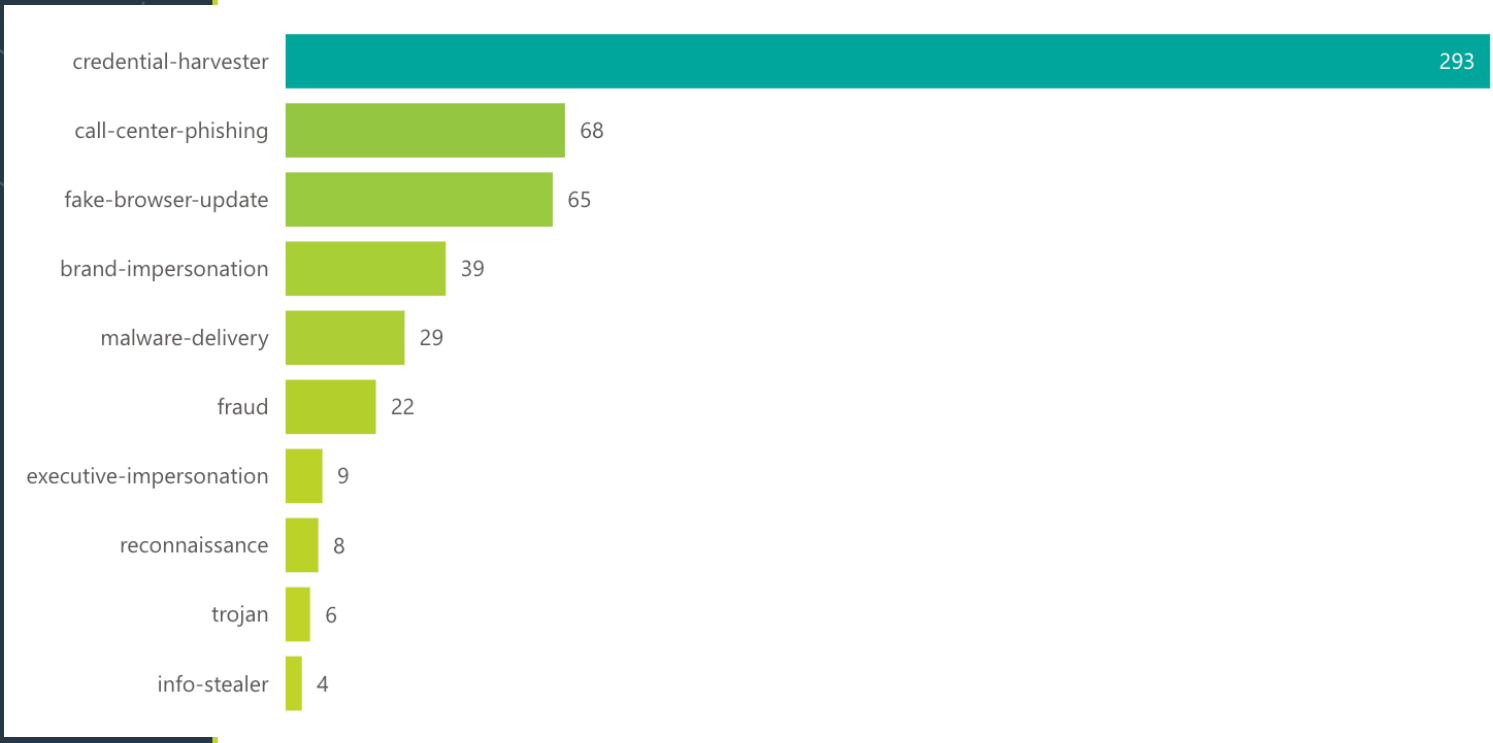
Top MISP Trends

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 Threat Types

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

- credential-harvester (293)
- call-center-phishing (68)
- fake-browser-update (65)
- brand-impersonation (39)
- malware-delivery (29)
- fraud (22)
- executive-impersonation (9)
- reconnaissance (8)
- trojan (6)
- info-stealer (4)



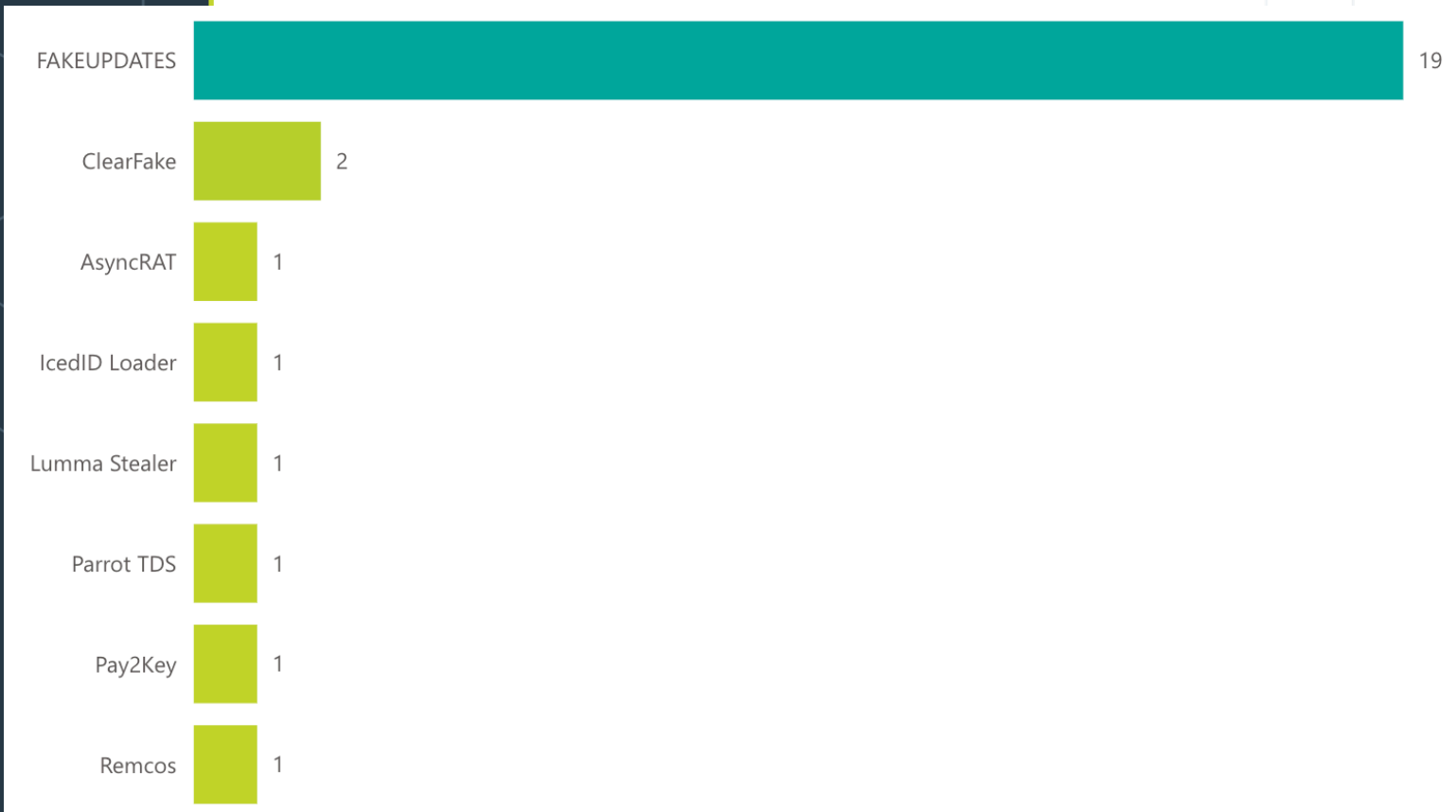
The top reported types of threats by members for the previous period by total count of instances were:

- 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)

Top Reported Malware

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

- FAKEUPDATES (19)
- ClearFake (2)
- AsyncRAT (1)
- Lumma Stealer (1)
- Parrot TDS (1)
- Pay2Key (1)
- Remcos (1)
- IcedID Loader (1)



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

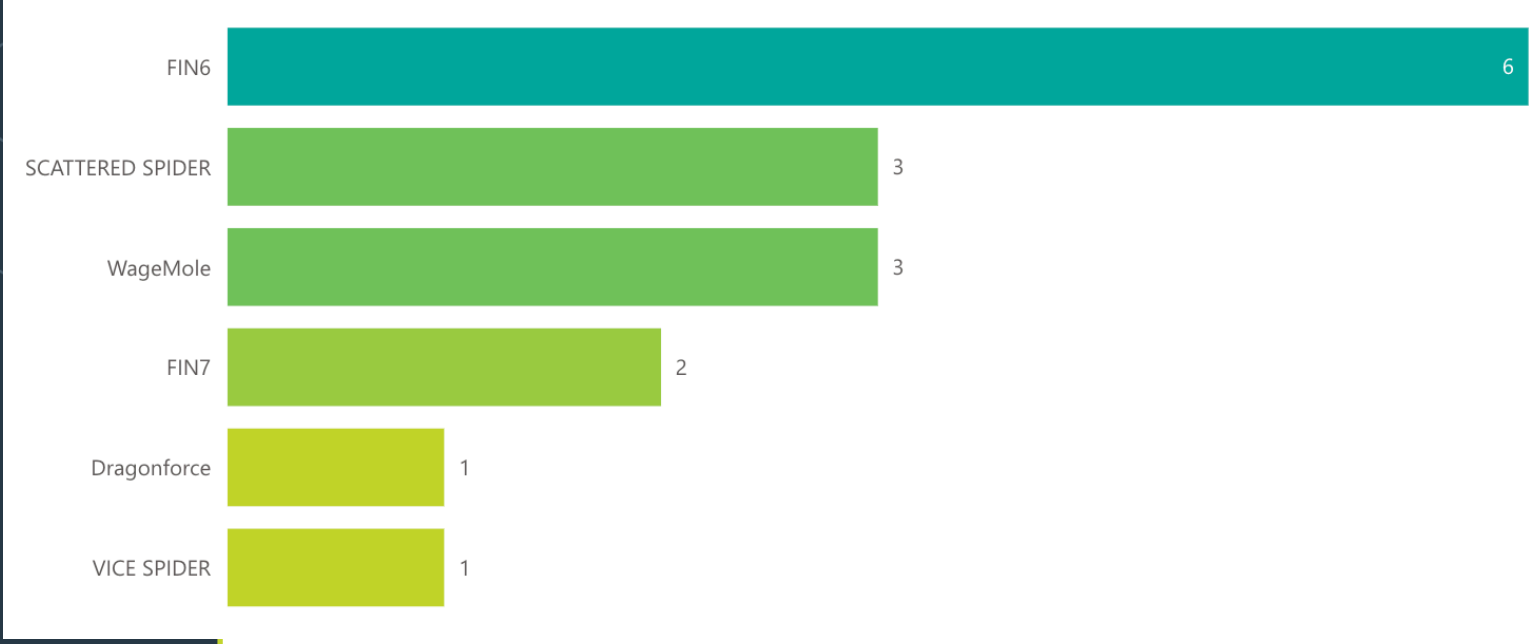
- FAKEUPDATES (78)
- Parrot TDS (5)
- ClearFake (3)
- Lumma Stealer (2)
- TerraLoader (2)
- Amadey (1)
- AsyncRAT (1)
- BeaverTail (1)
- DUCKTAIL (1)
- LockBit (1)
- More_eggs (1)
- NetSupportManager RAT (1)

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 (6)
- WageMole (3)
- SCATTERED SPIDER (3)
- FIN7 (2)
- Dragonforce (1)
- VICE SPIDER (1)

Note: WageMole is better known as Famous Chollima, the cluster of activity attributed to DPRK government employees securing employment via fraudulent means for sanctions evasion.



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

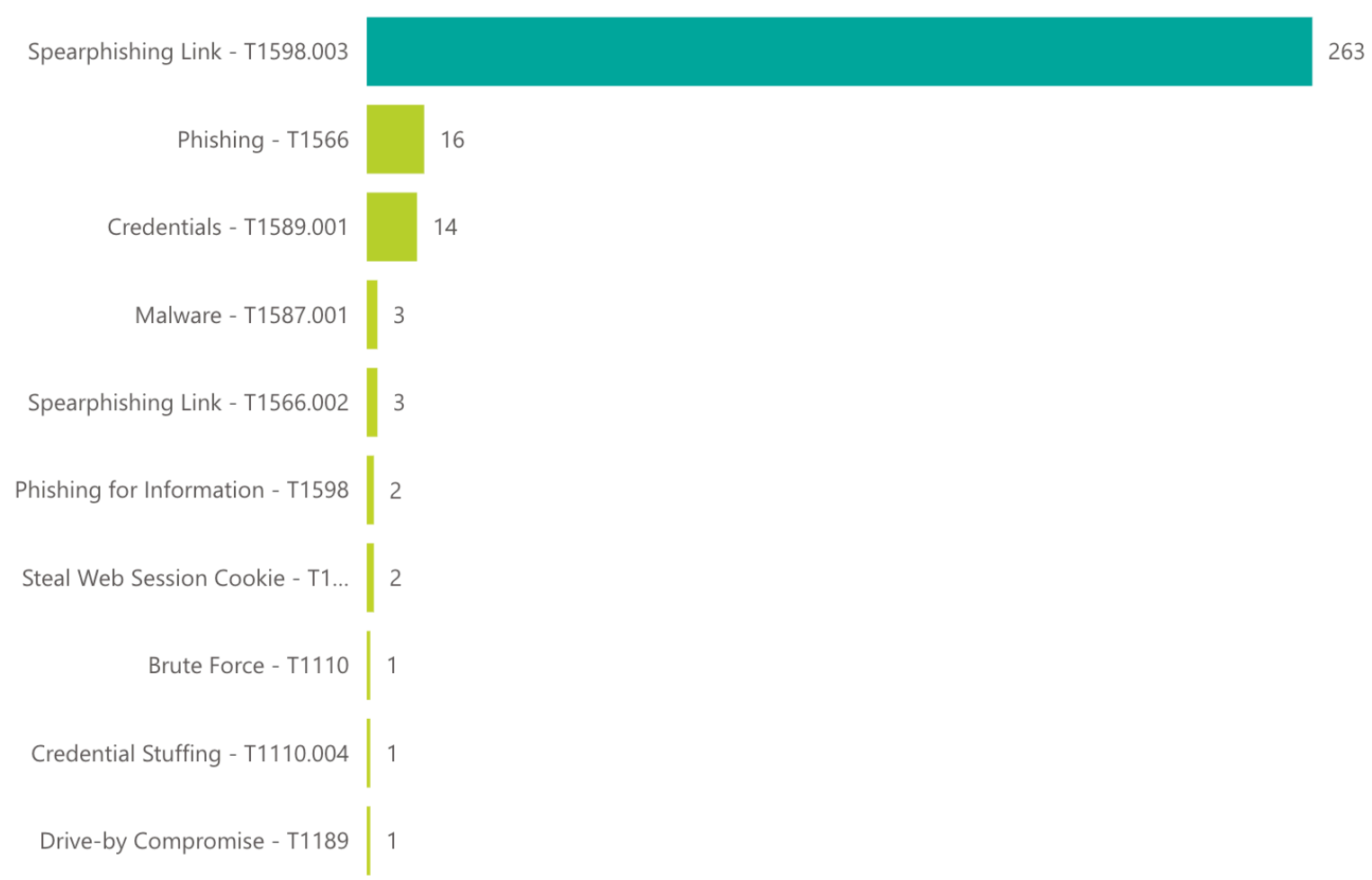
- FIN6 (4)
- TA505 (1)
- VICE SPIDER (1)

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.

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 (263)
- Phishing - T1566 (16)
- Credentials - T1589.001 (14)
- Malware - T1587.001 (3)
- Spearphishing Link - T1566.002 (3)
- Phishing for Information - T1598 (2)
- Steal Web Session Cookie - T1539 (4)
- Brute Force - T1110 (1)
- Credential Stuffing - T1110.004 (1)
- Drive-by Compromise - T1189 (1)



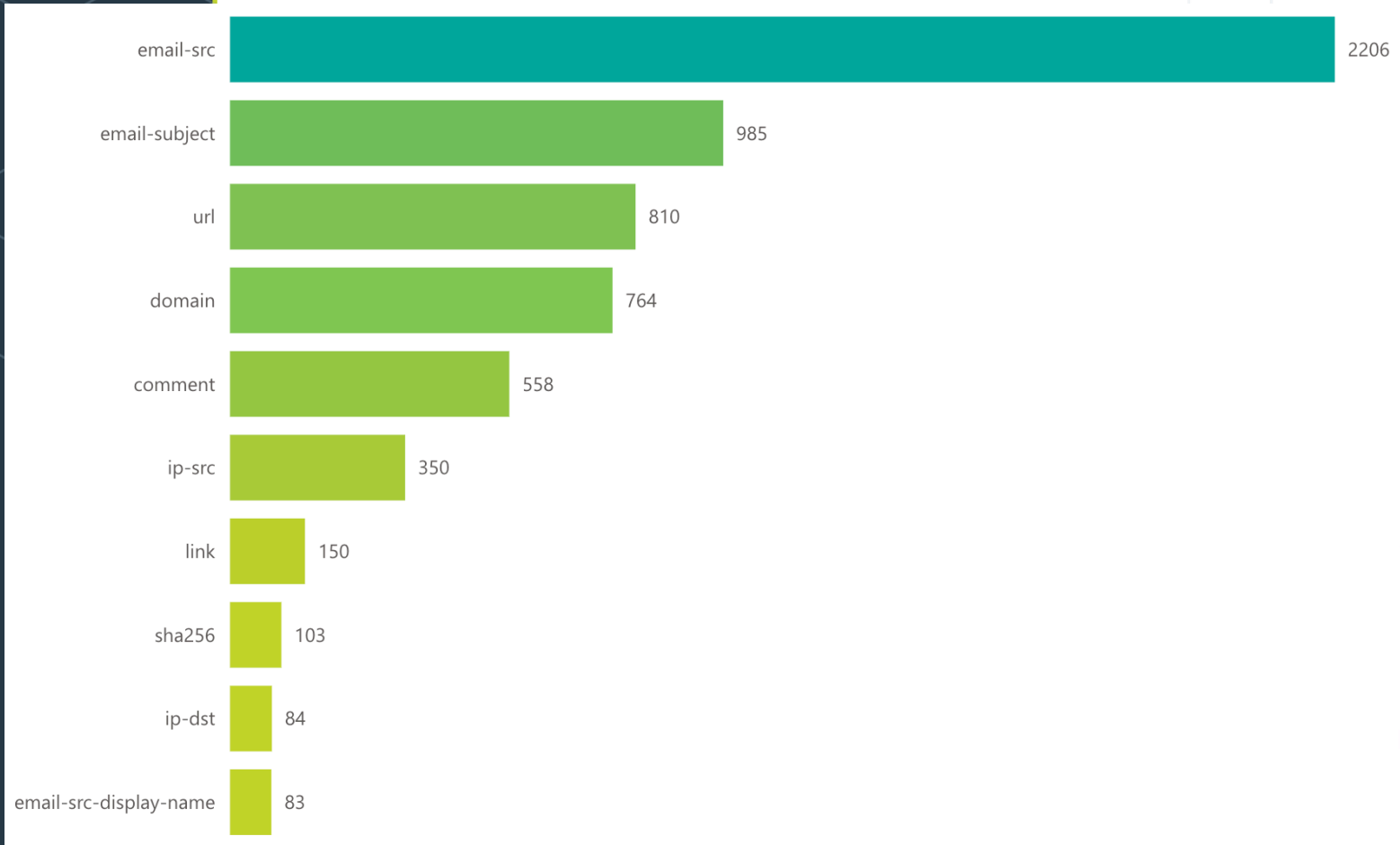
For comparison, the previous period's top reported MITRE ATT&CK techniques by total count of instances were:

- 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)

Top 10 Attribute Types

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

- email-src (2206)
- email-subject (985)
- url (810)
- domain (764)
- comment (558)
- ip-src (350)
- link (150)
- sha256 (103)
- ip-dst (84)
- email-src-display-name (83)



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 (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)

Industry Breakdown

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

- Retail (521)
- Restaurants (43)
- Hospitality (40)
- Travel (12)
- Food Retail (1)
- Gaming (1)

For comparison, the prior period's top reporting industries were:

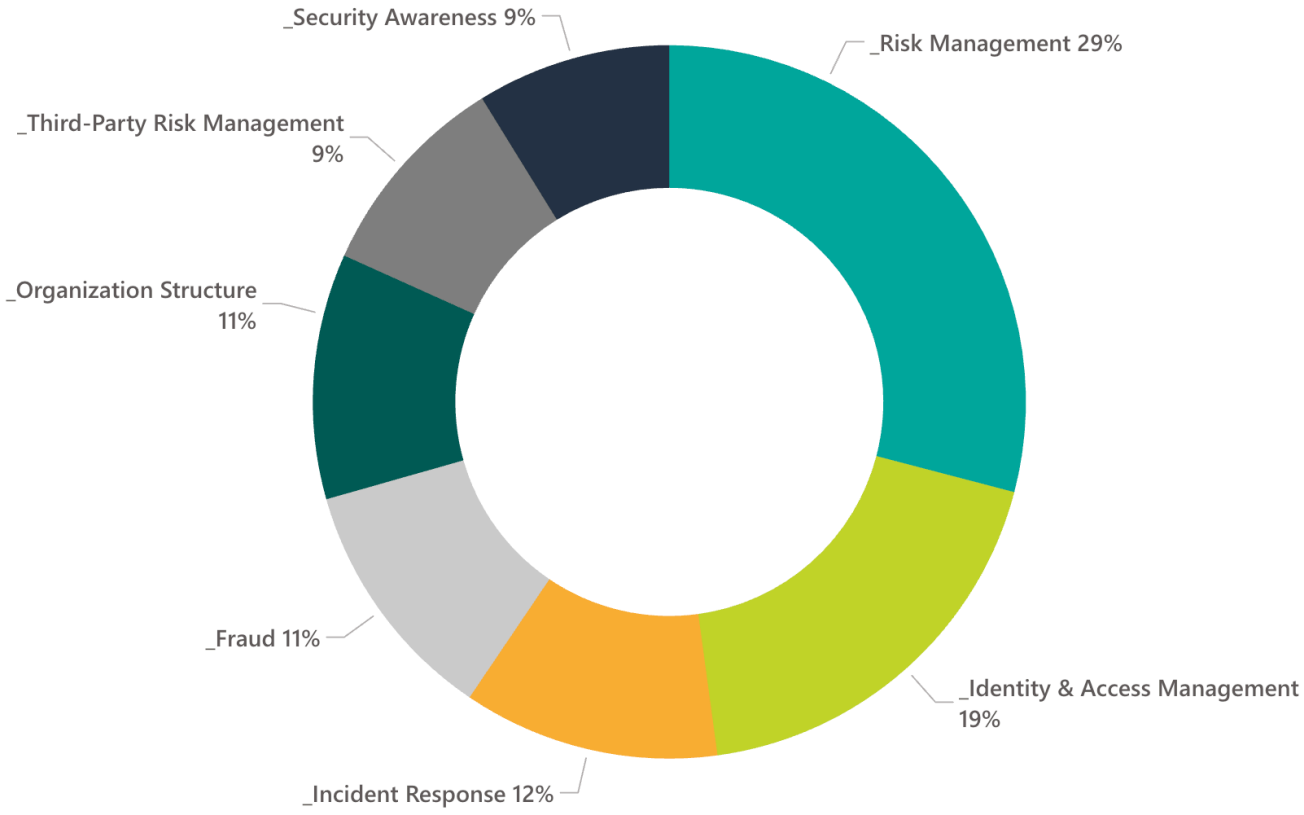
- Retail (733)
- Restaurants (106)
- Hospitality (49)
- Gaming (11)
- Travel (6)
- Consumer Packaged Goods (1)

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 April to June 2025, 174 unique members, or 58% of our total membership, participated in RFIs. During that time period, a total of 215 RFIs were submitted, generating 568 responses. In comparison, during the same period in 2024, RH-ISAC received 170 RFIs, resulting in 420 responses. This year, the continued focus on engagement and enhanced offerings led to a substantial increase in community interaction, with RFIs rising by 26% and responses increasing by 35%.

Overall RFI Domains for April - June 2025

215 RFIs | 568 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.

Password Complexity and Rotations

In April 2025, a member submitted an RFI to the CISO community seeking guidance on extending the password rotation period for non-privileged users from 90 days to once annually. He noted the use of MFA and SSO as compensating controls and asked if others had implemented similar changes. This RFI generated 21 responses, with members sharing current practices around password length, complexity, rotation frequency, and supporting controls. The compiled summary highlights key trends, including widespread MFA use, increased character requirements, and movement toward longer or conditional password lifecycles.

Incident Response Retainers

In June 2025, a member submitted an RFI to the CISO community seeking insight into how organizations structure their incident response retainers. Specifically, he asked whether members rely on third-party forensics firms, utilize services provided by their cyber insurance provider, or have no formal retainer in place. This RFI generated 31 responses, with members sharing their current approaches, preferred vendor models, and lessons learned from past engagements.

Survey Reports

In addition, RH-ISAC produced two comprehensive survey reports:

Cyber Risk Quantification (CRQ) Survey Report

In February 2025, the RH-ISAC conducted a survey on how organizations implement Cyber Risk Quantification (CRQ). The survey focused on aspects such as CRQ maturity, its integration with business risk management, and its prioritization within cybersecurity strategies. This report provides a comprehensive analysis of key practices, challenges, and opportunities for improvement based on insights gathered from 31 member companies, offering valuable guidance for organizations looking to strengthen their CRQ efforts.

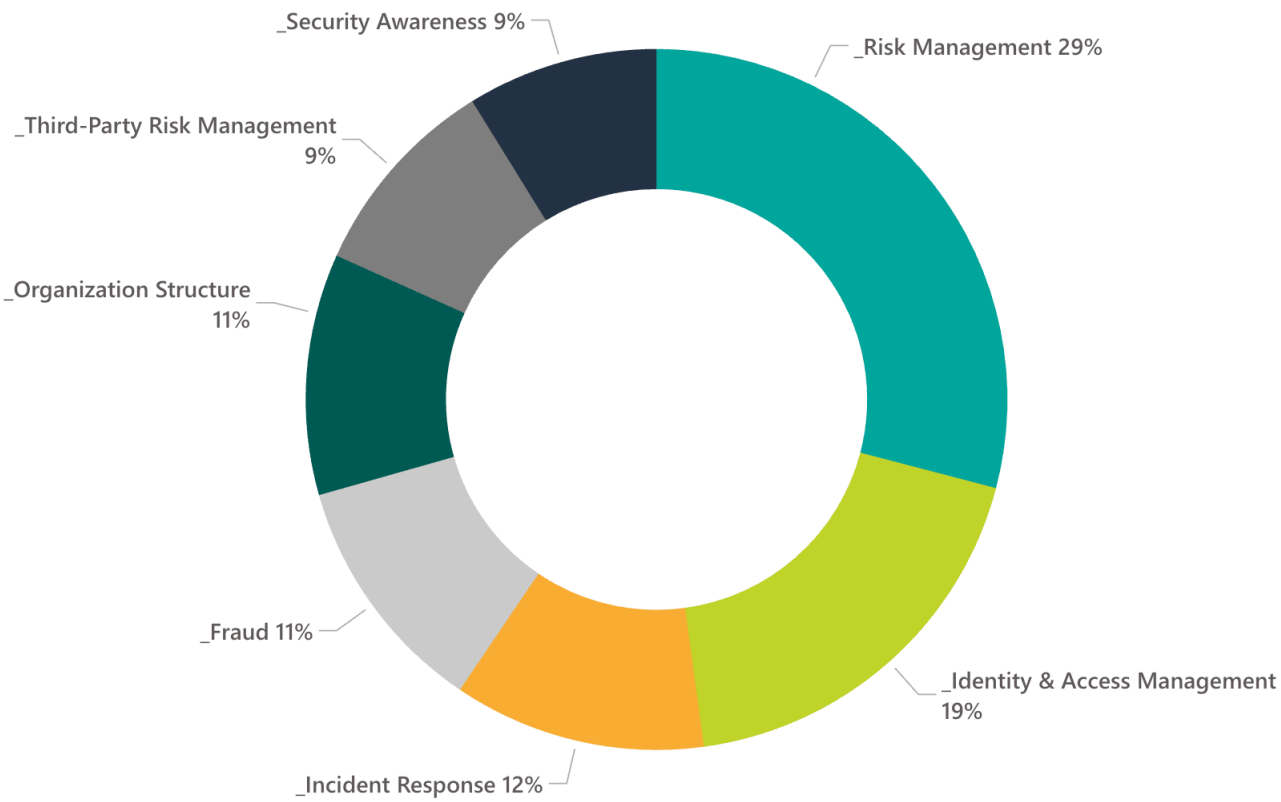
Generative AI (GenAI) Survey Report

In April 2025, the RH-ISAC conducted a survey to better understand how member organizations are managing Generative AI (GenAI) governance. The survey explored governance structures, legal and security considerations, risk management practices, and the maturity of GenAI solution usage. This report offers a comprehensive analysis of key trends, challenges, and emerging practices based on insights from 27 member companies, providing valuable guidance for organizations working to strengthen their GenAI oversight and implementation.

CISO Community Overview

In the CISO Community, from April to June 2025, a total of 58 RFIs were submitted, resulting in 269 responses. During this period, 33% of the RFIs came from the Risk Management Domain and Identity and Access Management was responsible for 20% of CISO RFIs. The figure below shows a total breakdown of the RFIs submitted to the CISO Community.

CISO RFI Domains for April - June 2025
58 RFIs | 269 Responses



Analyst Community Overview

In the Analyst Community, from April to June 2025, a total of 159 RFIs were submitted, generating 303 responses. Key discussion topics among the analyst community during this period were Risk Management, Security Awareness, Identity and Access Management and Organizational Structure.

Analyst RFI Domains for April - June 2025
159 RFIs | 303 Responses