

# INTELLIGENCE TRENDS SUMMARY

## October - December 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 continue to provide insights into the major security concerns and challenges facing the retail hospitality, and travel sectors. This report looks back at the RH-ISAC community's intelligence-sharing output for the fourth quarter of 2025, the three-month period between 1 October and 31 December 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 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.

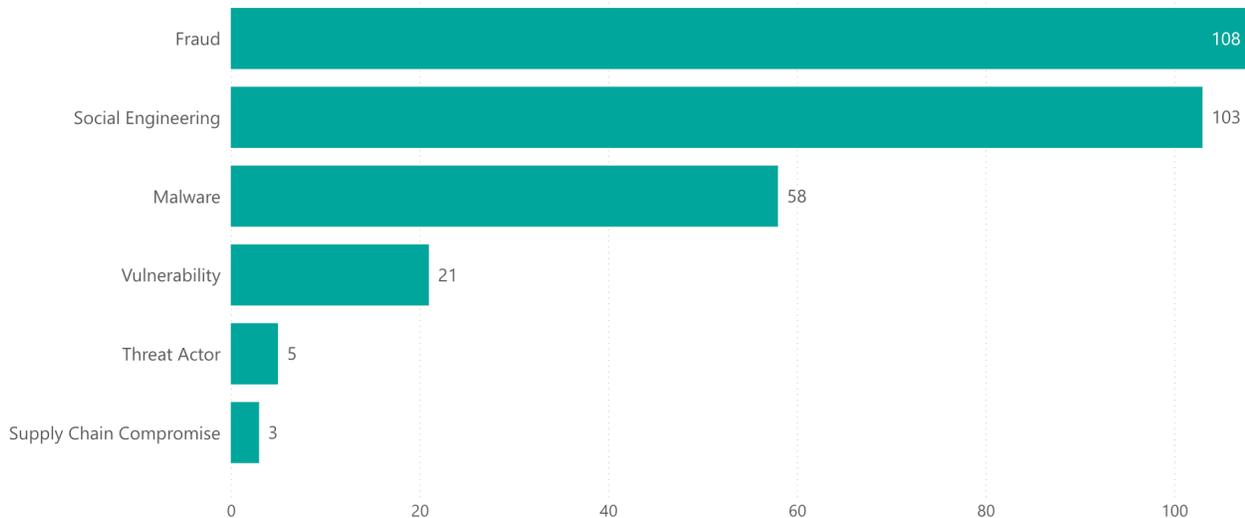
Analysis of the intelligence sharing for this period showed that the top reported threats by volume continued to reflect the steady reliance by cybercriminals on tried and tested threat vectors like fraud, social engineering, and malware. Member reporting heavily focused on IT and helpdesk impersonation calls, activity from The Com threat cluster, novel supply chain attacks targeting developers, fraud methodologies and fraud-as-a-service operations, and ransomware group claims.

# THREAT LANDSCAPE

## Top Sharing Trends

This graph illustrates the shared threat topics for the current period, which can be described as the frequency with which threat discussions were shared through Member Exchange and Slack.

For contrast, in the third quarter of 2025, threat trend reporting from RH-ISAC Core showed: phishing, impersonation (both of brands and executives), and Scattered Spider remained the top threat topics of discussion, with fraud remaining prevalent as well.

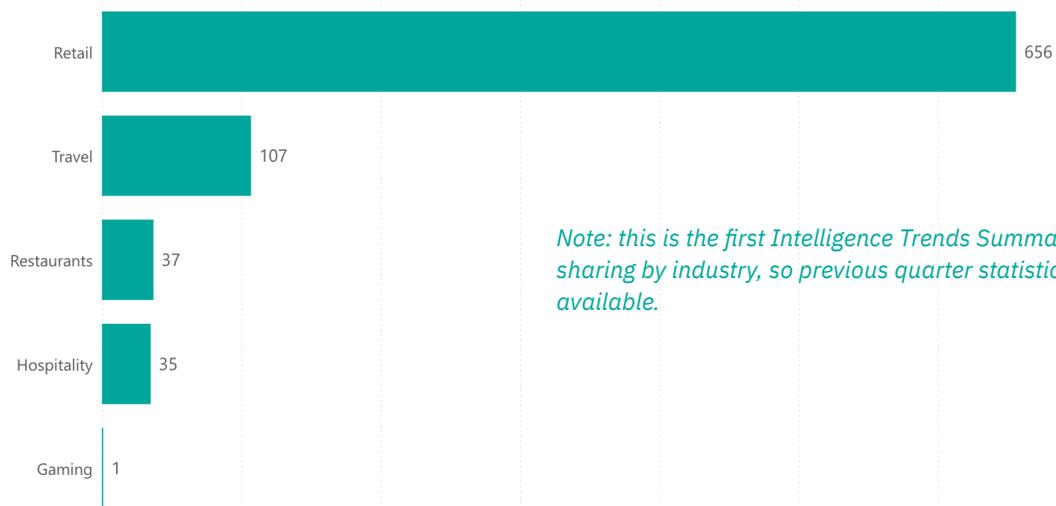


## Top MISP Trends

Tracked data on member-reported threat trends from the RH-ISAC Malware Information Sharing Platform (MISP) includes prevalent malware, threat actors, intrusion sets, MITRE ATT&CK Techniques, and attribute types.

## Industries

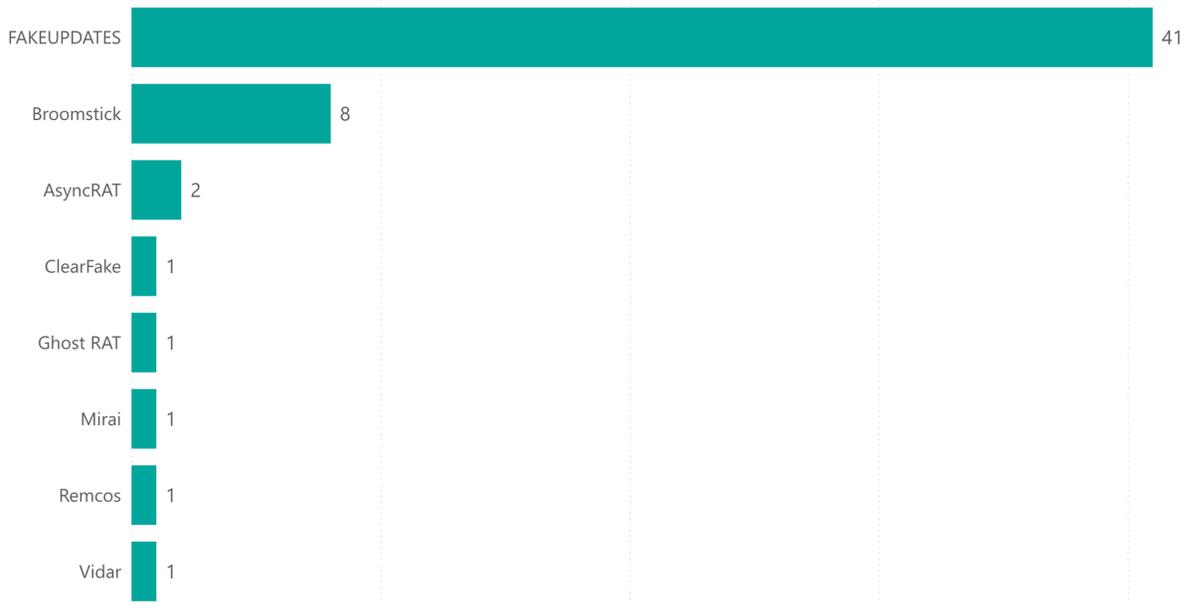
The top industries sharing intelligence with the RH-ISAC membership by total count of instances were:



*Note: this is the first Intelligence Trends Summary tracking sharing by industry, so previous quarter statistics are not yet available.*

# Malware

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

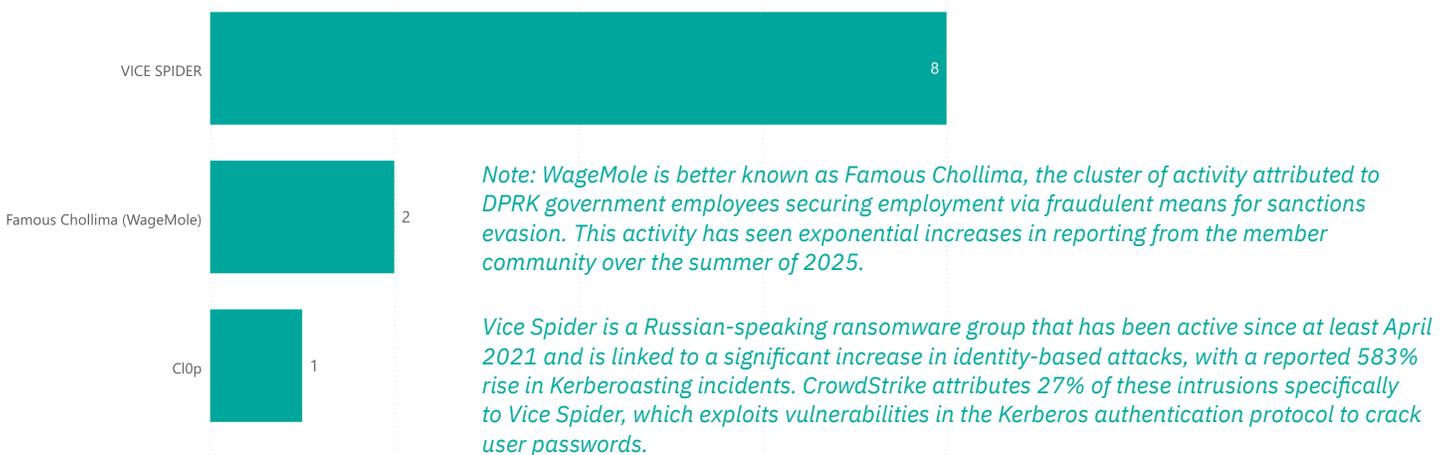


For comparison, the top reported malware (MITRE ATT&CK-defined software) for the third quarter of 2025 by total count of instances, were:

- |                         |                   |              |                  |
|-------------------------|-------------------|--------------|------------------|
| FAKEUPDATES (17)        | ClearFake (2)     | Amadey (1)   | DarkComet (1)    |
| Broomstick (Oyster) (5) | Lumma Stealer (2) | DUCKTAIL (1) | HijackLoader (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:



For comparison, the top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) for the third quarter of 2025 by total count of instances were:

- |                                      |   |                               |
|--------------------------------------|---|-------------------------------|
| Famous Chollima (WageMole)<br>(1392) | SCATTERED SPIDER (4)<br>VICE SPIDER (4) | Akira (1)<br>ShinyHunters (1) |
|--------------------------------------|---|-------------------------------|

# MITRE ATT&CK Techniques

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

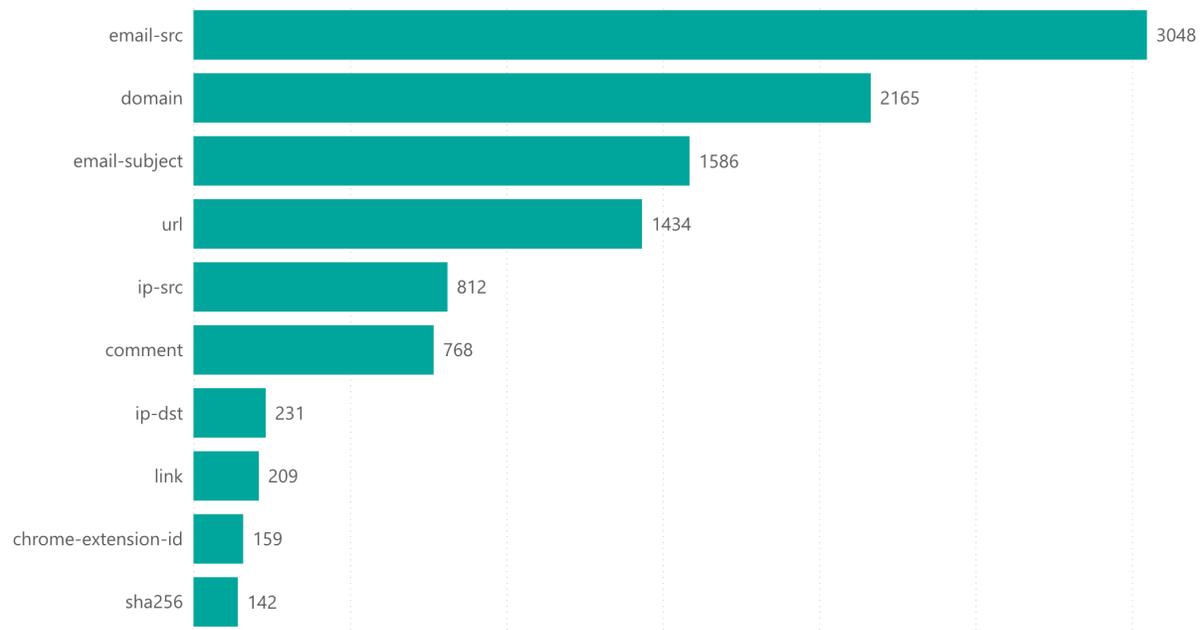


For comparison, the previous period's top reported MITRE ATT&CK techniques by total count of instances were:

- |                                      |  |                                     |
|--------------------------------------|--|-------------------------------------|
| Spearphishing Link - T1598.003 (223) | Spearphishing Attachment - T1598.002 (3) | Cloud Service Dashboard - T1538 (1) |
| Phishing - T1566 (18)                | Spearphishing Link - T1192 (3)           | Cloud Service Discovery - T1526 (1) |
| Spearphishing Link - T1566.002 (10)  | Spearphishing Attachment - T1193 (2)     |                                     |
| Credentials - T1589.001 (7)          | Account Discovery - T1087 (1)            |                                     |

# Attribute Types

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



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 (2437) | hostname (664) | email-subject (529) | ip-src (293) | ip-dst (249) |
| domain (1548)    | url (650)      | comment (435)       | md5 (282)    | sha256 (138) |

# RESEARCH & EDUCATION

## Requests for Information

RH-ISAC actively tracks requests for information (RFIs) and surveys to understand our members' interests, spanning both analyst and CISO perspectives. From October to December 2025, 136 unique members, or 41% of our total membership, participated in RFIs, and a total of 122 RFIs were submitted, generating 286 responses. In comparison, during the same period in 2024, RH-ISAC received 174 RFIs, resulting in 429 responses. While overall engagement declined slightly this quarter, Requests for Information (RFIs) related to Identity and Access Management (IAM) have doubled compared to last year.

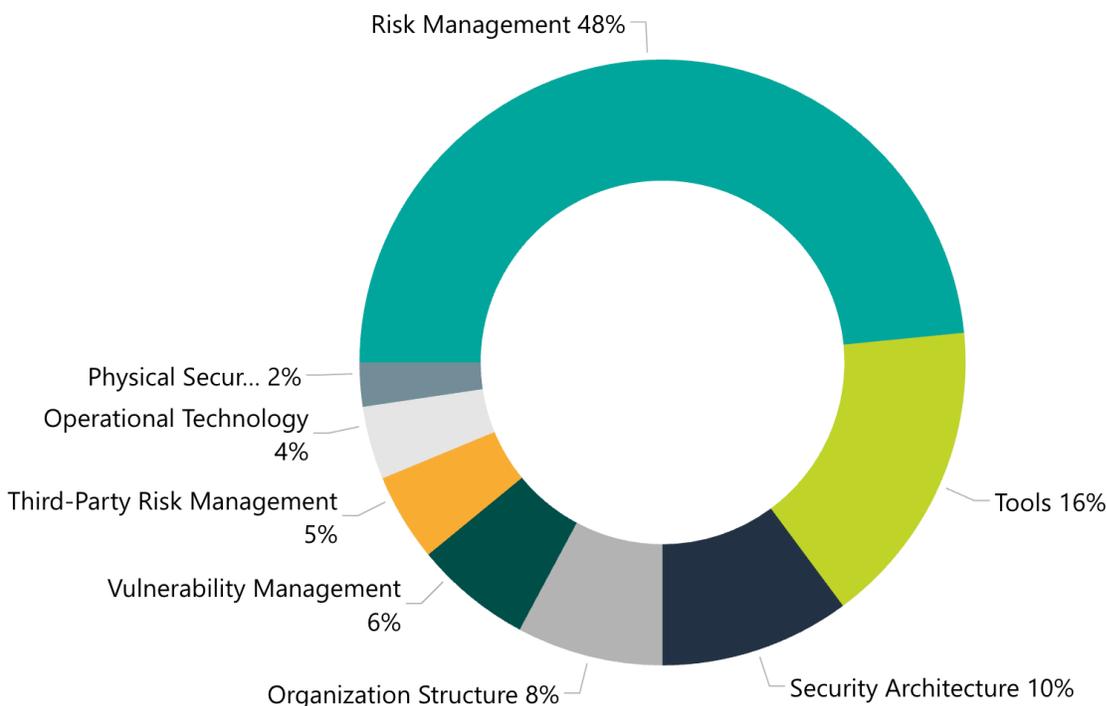
## Summary of RFI Publications

### CIAM Ownership

In October 2025, a member from the CISO community submitted an RFI asking where Customer Identity and Access Management (CIAM) lives within member organizations. Responses highlighted varied ownership models based on organizational structure and strategic focus. While more than half of respondents indicated that CIAM is owned by Digital or eCommerce teams, others shared that it sits within Cybersecurity, IAM, Engineering, or IT. Several organizations reported recent transitions or hybrid models involving shared responsibilities between business and technical teams. This summary compiles 14 responses and outlines the range of CIAM ownership approaches currently in place.

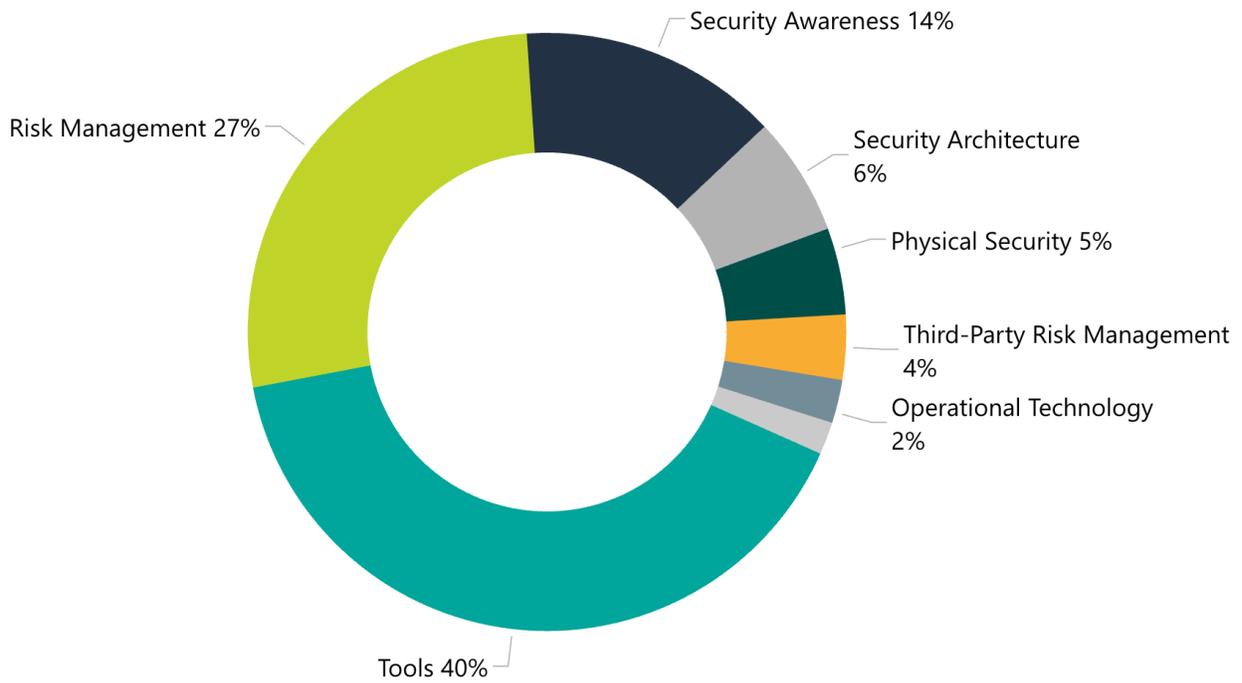
## CISO Community RFIs

In the CISO Community, from October to December 2025, a total of 33 RFIs were submitted, resulting in 128 responses. During this period, 48% of the RFIs came from Risk Management domain and Tools were responsible for 16% of CISO RFIs. The figure below shows a total breakdown of the RFIs submitted to the CISO Community.



## Analyst Community RFIs

In the Analyst Community, from October to December 2025, a total of 89 RFIs were submitted, generating 158 responses. Key discussion topics among the analyst community during this period were Tools, Risk Management, and Security Awareness.



## Surveys

RH-ISAC conducted one survey during this period:

### Risk Register Practices Survey Report

In October 2025, the RH-ISAC conducted a survey to gather insights from member organizations on the use of risk registers. The goal was to understand how risk registers are implemented, managed, and measured across the community—with attention to ownership models, maturity frameworks, technologies used, and the types of risks being tracked. A total of 20 member companies participated in the survey. By sharing their experiences, members helped highlight common practices, identify potential gaps, and inform the development of stronger risk management approaches.