TLP: CLEAR

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY INTELLIGENCE TRENDS SUMMARY

April – June 2024

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 second quarter of 2024, the three-month period between 1 April and 30 June 2024. 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. Phishing and fraud remained the key threats reported by the community, with social engineering and ransomware threats remaining prevalent. Reporting on specific attribution of threat activity increased significantly, and third-party/supply chain risks remained a key concern in the second quarter of 2024.

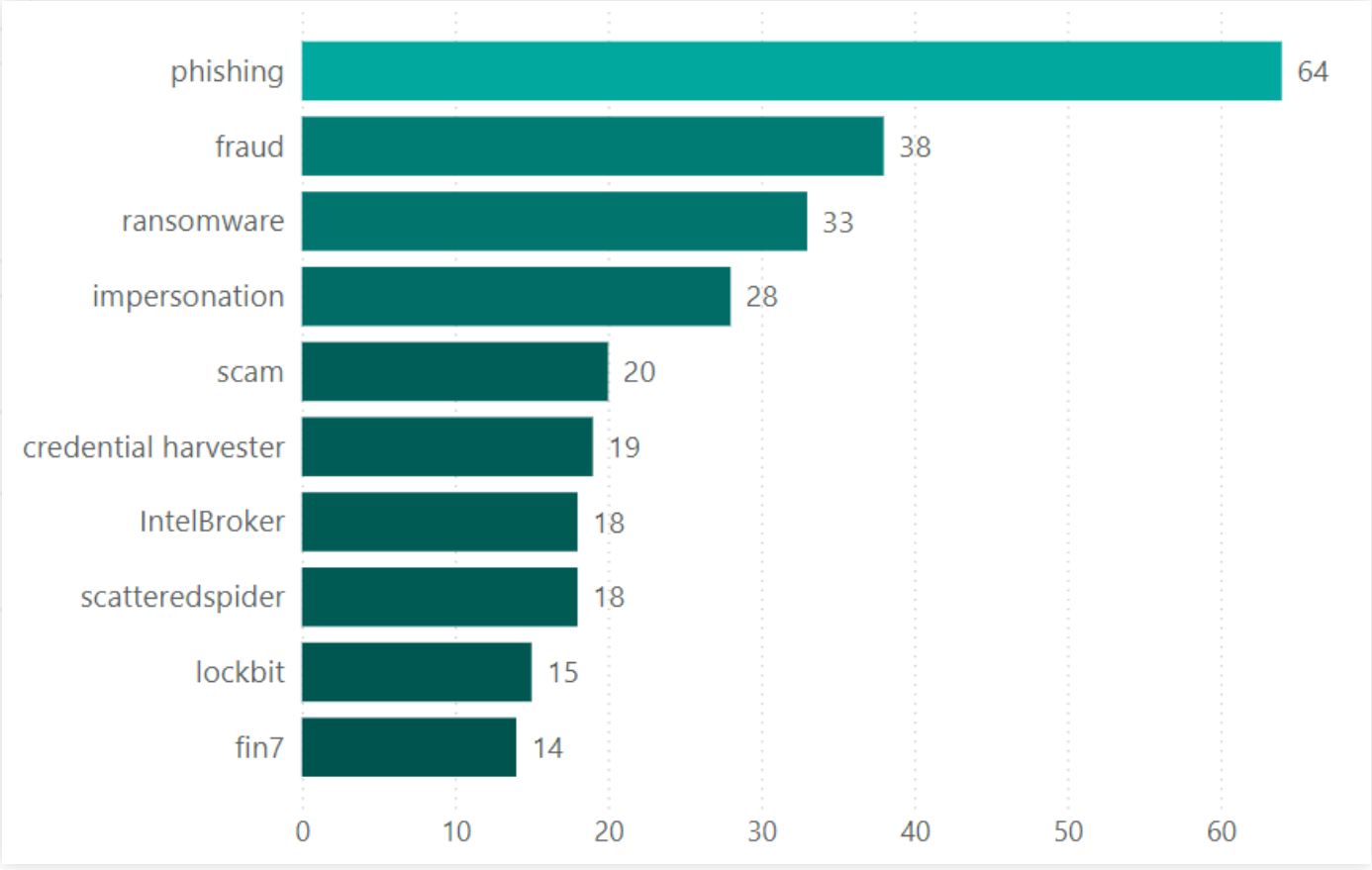
THREAT LANDSCAPE: Trends

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 RH-ISAC Malware Information Sharing Platform (MISP). Note: fraud appears

The top threat trends reported by the RH-ISAC community remained relatively static between the first and second quarters of 2024, with only minor changes:

- Ransomware reporting rose slightly from 18 to 33 instances to become the third most reported threat.
- Scam reporting nearly doubled to become the fifth most reported trend.
- Credential harvesting reemerged as a top threat after several reporting periods of low reporting prevalence.
- Reporting on individual threat actor groups became prevalent enough to make the top threat list: Intel Broker, Scattered Spider, LockBit, and FIN7.



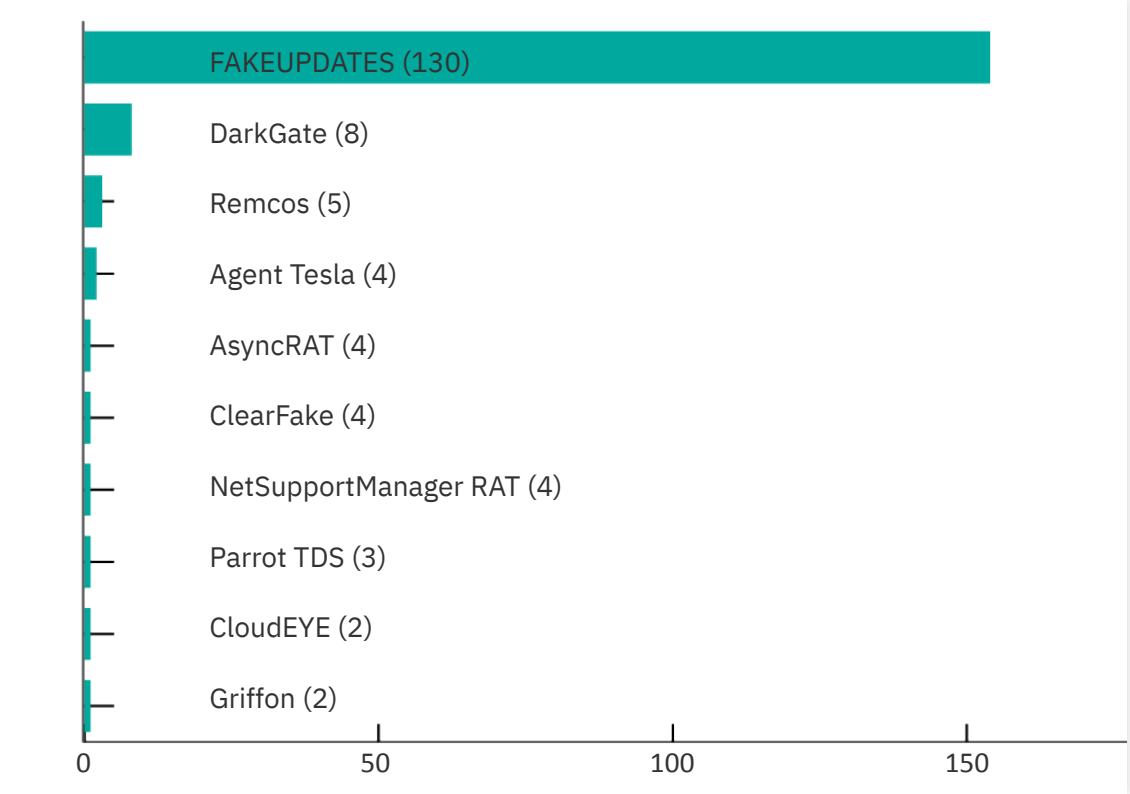
Top MISP Trends

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 current period by total count of instances were:

- FAKEUPDATES (130)
- DarkGate (8)
- Remcos (5)
- Agent Tesla (4)
- AsyncRAT (4)
- ClearFake (4)
- NetSupportManager RAT (4)
- Parrot TDS (3)
- CloudEYE (2)
- Griffon (2)



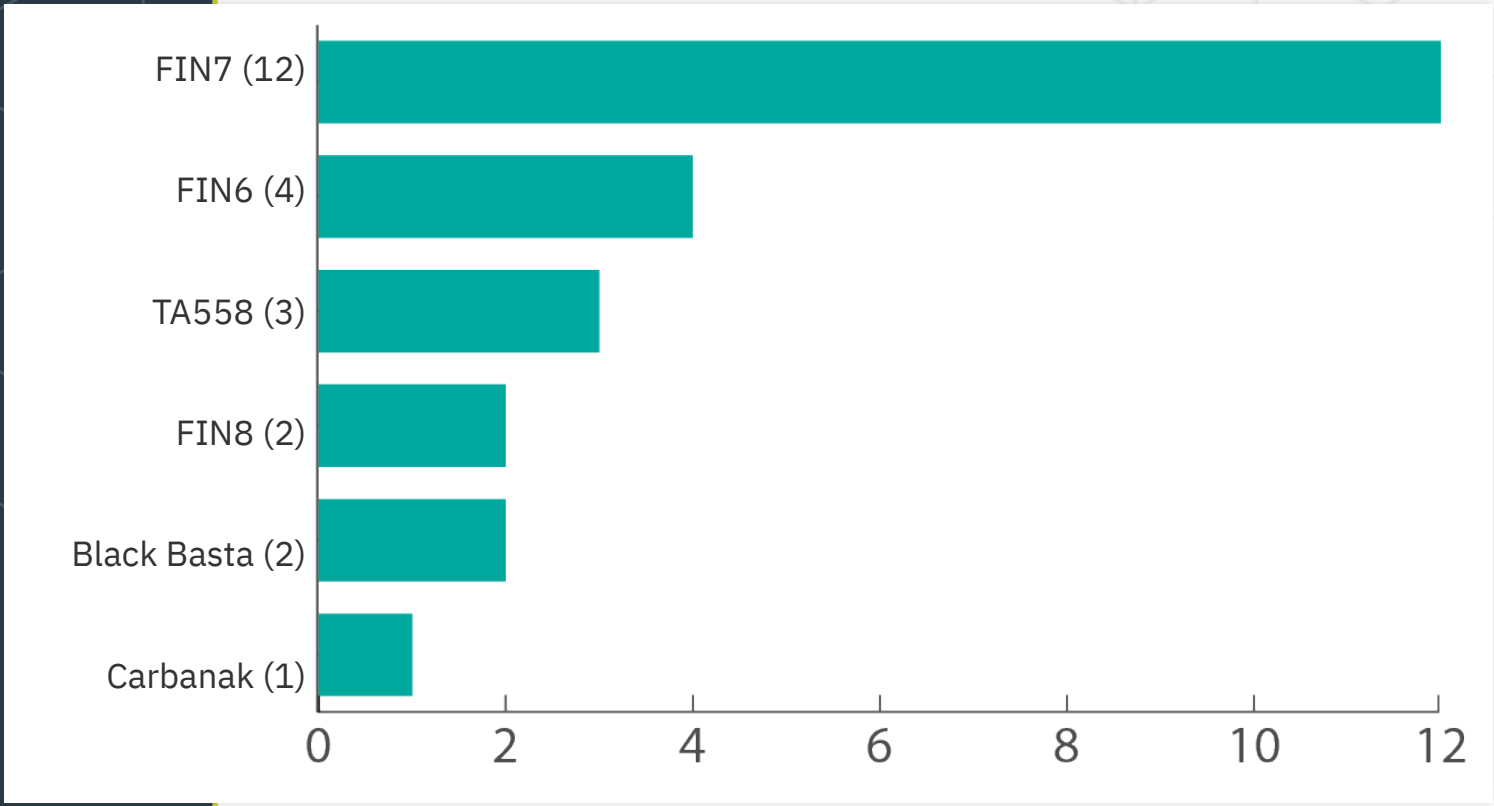
For comparison, the top reported malware (MITRE ATT&CK-defined software) for the January-March 2024 period, by total count of instances, were:

- FAKEUPDATES (154)
- Parrot TDS (8)
- DarkGate (3)
- Vidar (2)
- Agent Tesla (1)
- Cobalt Strike (1)
- Griffon (1)
- Mispadu (1)
- NetSupportManager RAT (1)
- OriginLogger (1)
- POWERTRASH (1)
- RedLine Stealer (1)
- Screenshotter (1)
- WasabiSeed (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:

- FIN7 (12)
- FIN6 (4)
- TA558 (3)
- FIN8 (2)
- Black Basta (2)
- Carbanak (1)



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

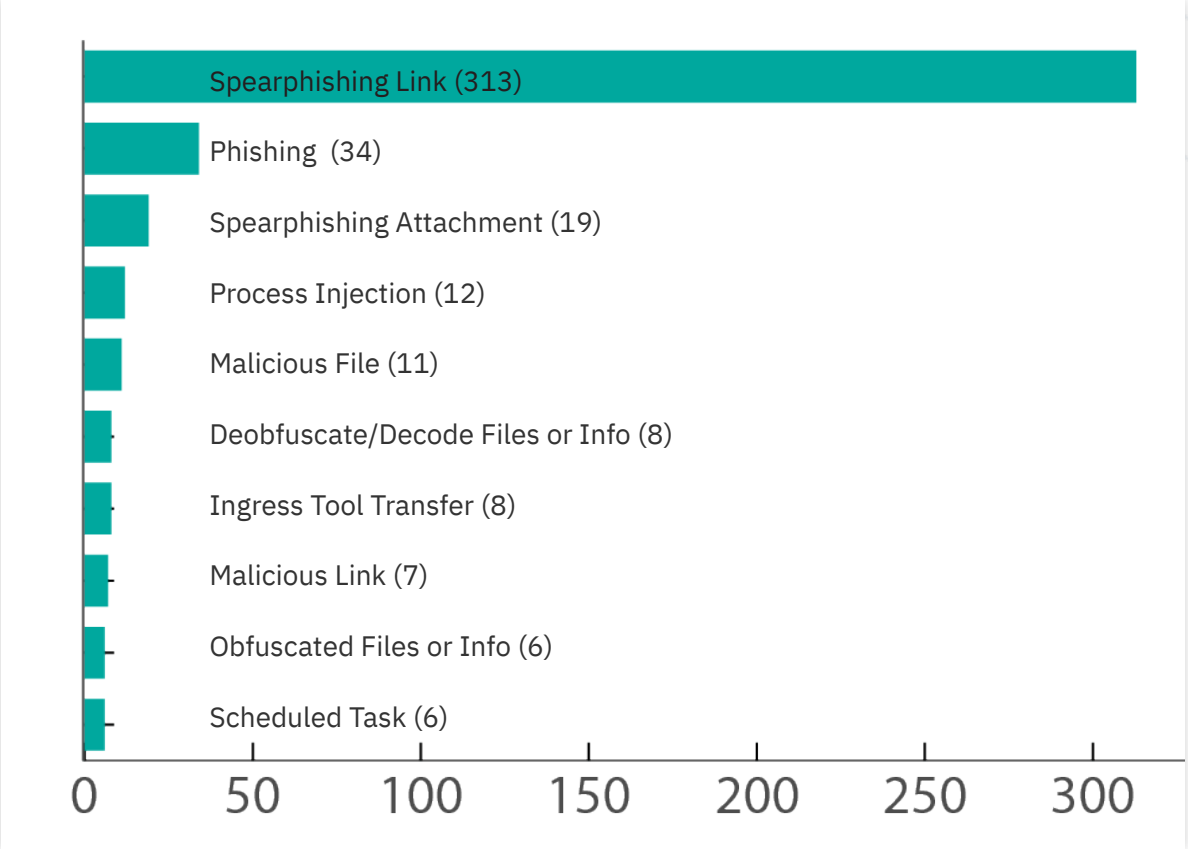
- SCATTERED SPIDER (3)
- BazarCall (2)
- FIN7 (2)

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).

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 (313)
- Phishing - T1566 (34)
- Spearphishing Attachment - T1566.001 (19)
- Process Injection - T1055 (12)
- Malicious File - T1204.002 (11)
- Deobfuscate/Decode Files or Information - T1140 (8)
- Ingress Tool Transfer - T1105 (8)
- Malicious Link - T1204.001 (7)
- Obfuscated Files or Information - T1027 (6)
- Scheduled Task - T1053.005 (6)



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

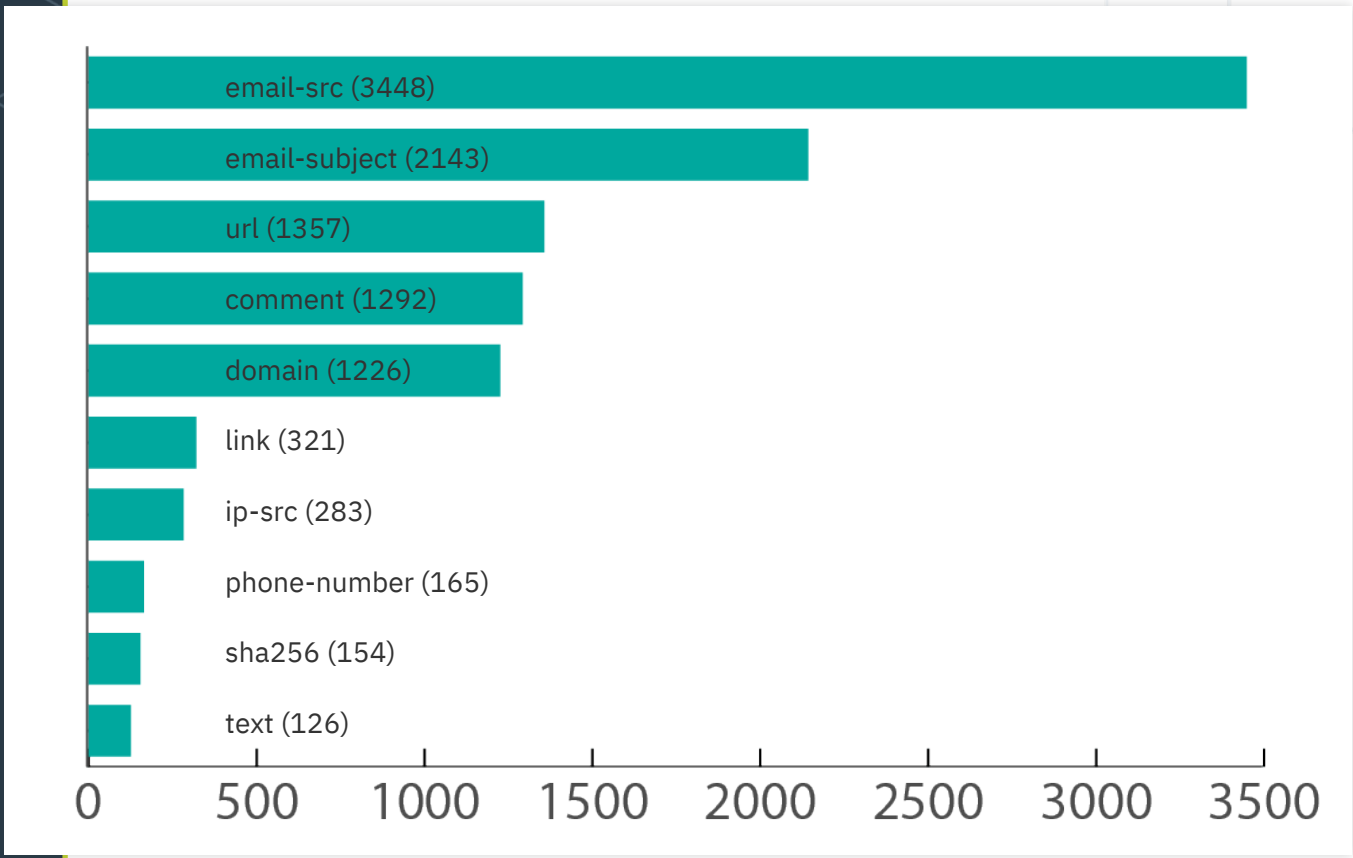
- Spearphishing Link - T1598.003 (697)
- Phishing - T1566 (31)
- Spearphishing Link - T1566.002 (6)
- Domains - T1583.001 (3)
- Browser Session Hijacking - T1185 (2)
- Compile After Delivery - T1027.004 (1)
- Credentials - T1589.001 (1)
- Credentials from Web Browsers - T1555.003 (1)
- Deobfuscate/Decode Files or Information - T1140 (1)

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.

Top 10 Attribute Types

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

- email-src (3448)
- email-subject (2143)
- url (1357)
- comment (1292)
- domain (1226)
- link (321)
- ip-src (283)
- phone-number (165)
- sha256 (154)
- text (126)



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 (4405)
- email-subject (3532)
- url (2008)
- comment (1536)
- domain (1028)
- ip-src (586)
- link (300)
- phone-number (201)
- text (98)
- sha256 (96)

Requests for Information

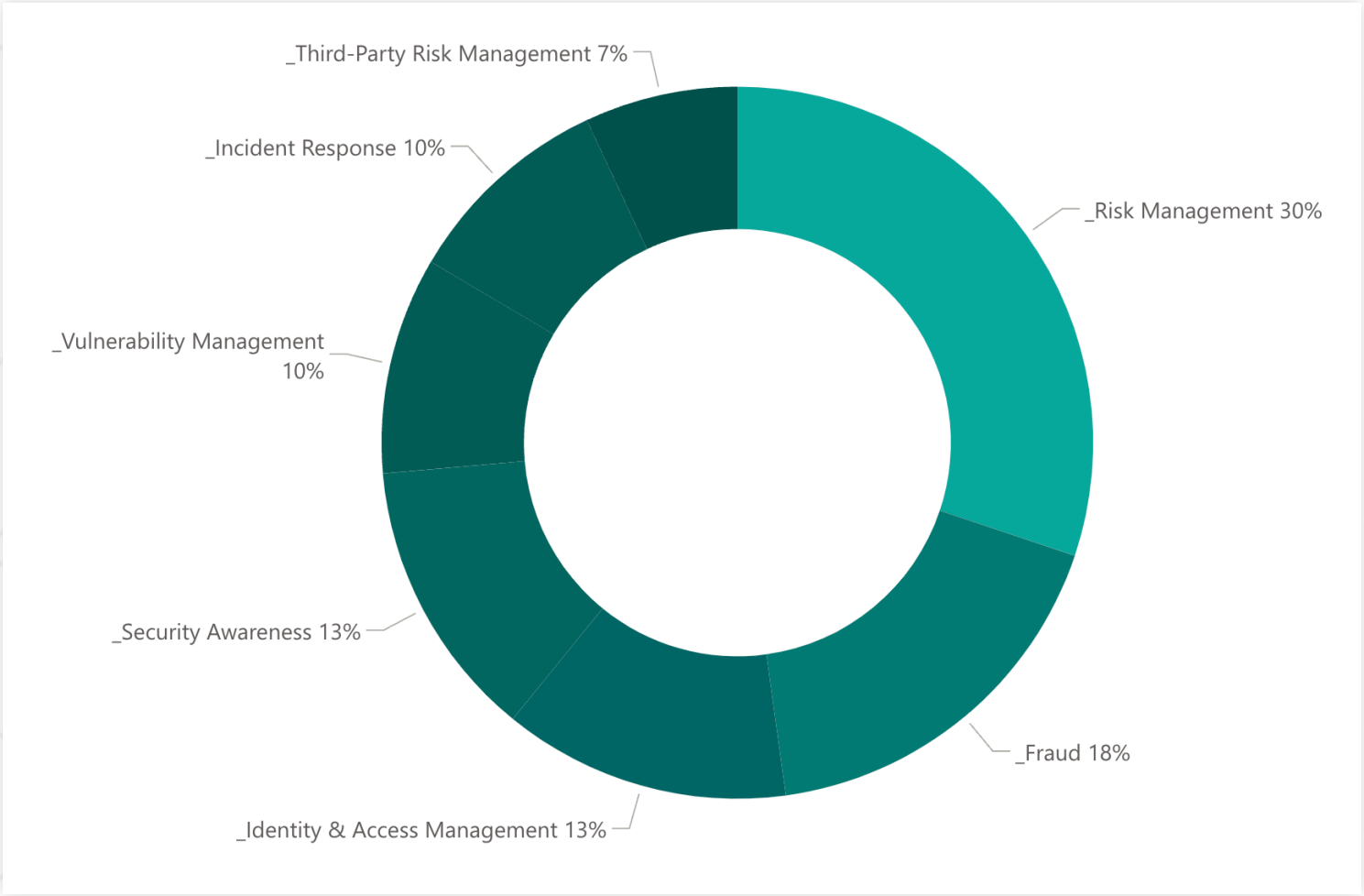
Members continue to leverage the RH-ISAC Request for Information (RFI) process integrated into Member Exchange, enabling our members to post RFIs to their peers with attribution or anonymously.

The RH-ISAC continues 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 April and June 2024, 89 unique members, or 32% of our total membership, participated in RFIs.

In total, for the timeframe of April to June 2024, 174 RFIs were submitted, with 419 responses.

Overall RFI Domains for April - June 2024

174 RFIs | 419 Responses | Average Responses: 3.12



Community Engagement Outlook

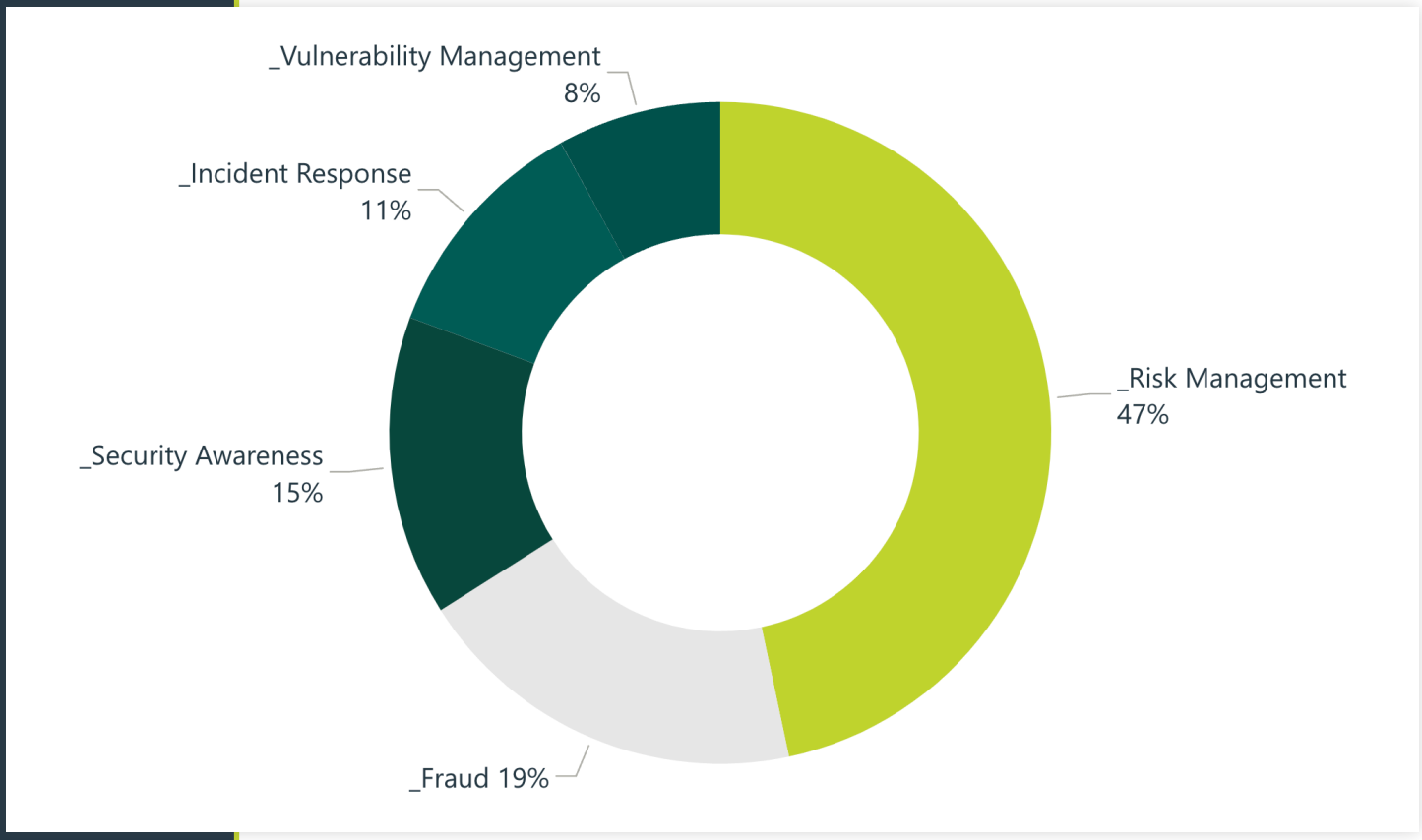
In 2023 for the timeframe of April to June, RH-ISAC received 92 RFIs that generated 245 responses. During 2024, enhanced offerings, and growth in networking reflected an increase in community engagement with a spike in the numbers of RFIs (89% increase) and responses (71% increase).

CISO Community Overview

In the CISO Community, for April to June 2024, 48 RFIs were submitted, with 181 responses. During this period, 47% of the RFIs came from the Risk Management Domain with greater interest in Governance Risk and Compliance and Policy and Architecture. Fraud was responsible for 19% of CISO RFIs with sub-domain topics of Security Controls and Bots. Similarly, Security Awareness was responsible for 15% of CISO RFIs with sub-domain topics security best practices. The figure below shows a total breakdown of the RFIs submitted to the CISO Community.

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

CISO RFI Domains for April - July 2024
48 RFIs | 181 Responses | Average Responses: 4

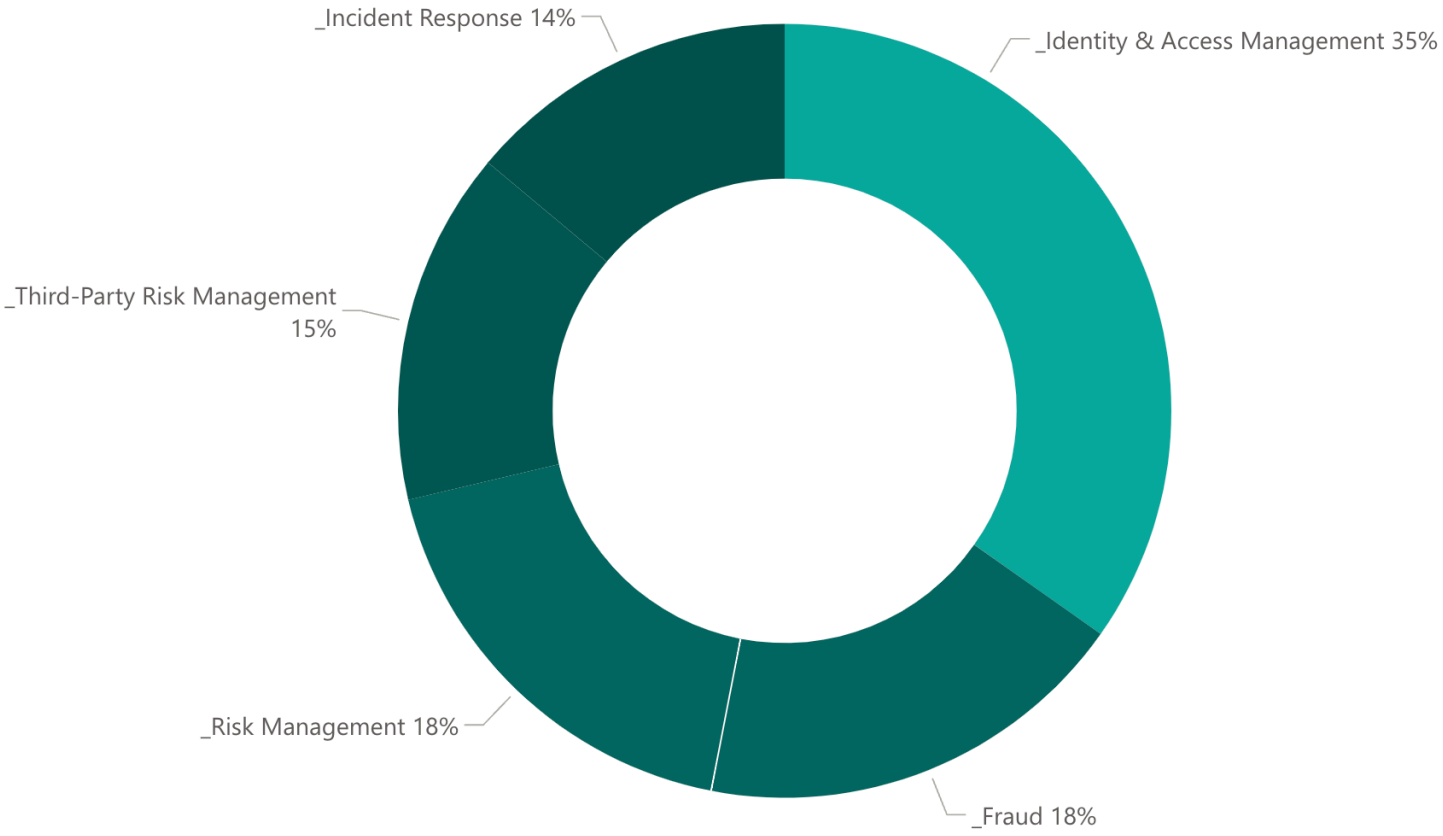


Analyst Community Overview

In the Analyst Community, for April to June 2024, 70 RFIs were submitted, with 154 responses. During this period Identity & Access Management, Fraud, Risk Management, Third-Party Risk Management, and Incident Response were key discussion topics among the analyst community. The top subdomains across the Analyst community were multi-factor authentication, vendor best practices, and Policy and Architecture.

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

Analyst RFI Domains for April - July 2024
70 RFIs | 154 Responses | Average Responses: 2.4



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 to strengthen or renew their prevalence. For the second quarter of 2024, third-party vulnerability disclosures, exploits, and compromises were the primary theme of RH-ISAC intelligence reporting, especially events related to Palo Alto, Sisense, TeamViewer, Snowflake, and Checkpoint.

About RH-ISAC

The Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC) operates as a central hub for sharing sector-specific cybersecurity information and intelligence. The association connects information security teams at the strategic, operational, and tactical levels to work together on issues and challenges, share practices and insights, and benchmark among each other. All with the goal of building better security for the retail, hospitality, and travel industries through collaboration. RH-ISAC currently serves companies in retail, hospitality, gaming, travel, and other consumer-facing entities. For more information, go to www.rhisac.org.