TLP: CLEAR

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY INTELLIGENCE TRENDS SUMMARY

January – March 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 first quarter of 2024, the three-month period between January 1 and March 31, 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. Ransomware fell significantly in prominence to sixth place after being the most prominent threat for the prior reporting period. The most prevalent trend for the current reporting period was phishing, up slightly from second place for September-December 2023.The prevalence of fraud reporting rose significantly in the first quarter of 2023, from sixth place last period to second for the current quarter. Additional social engineering tactics such as spearphishing impersonation also proved to be prominent trends for the first quarter of 2024.

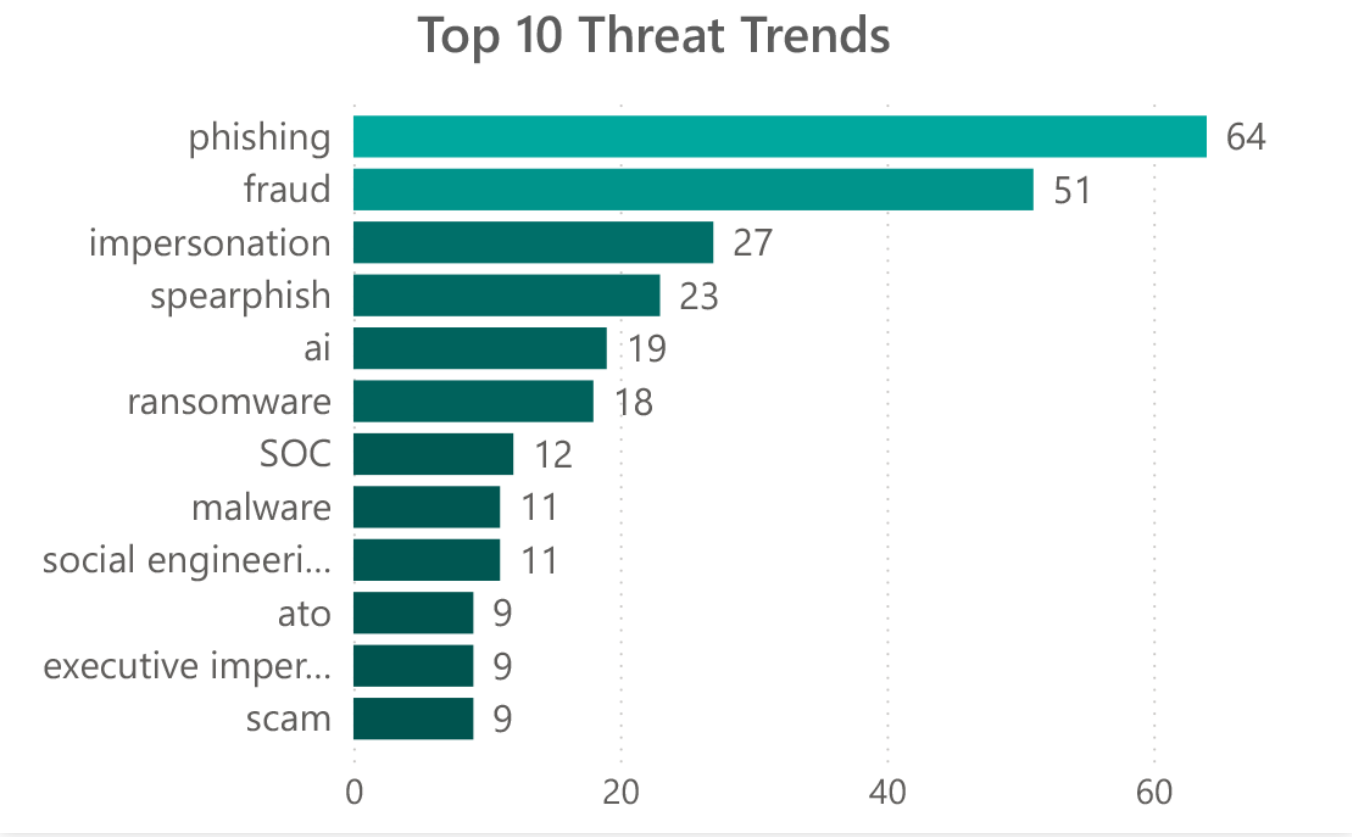
Top Sharing Trends

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).

For comparison, the top reported threats for the September-December 2023 period, by total count of instances, were:

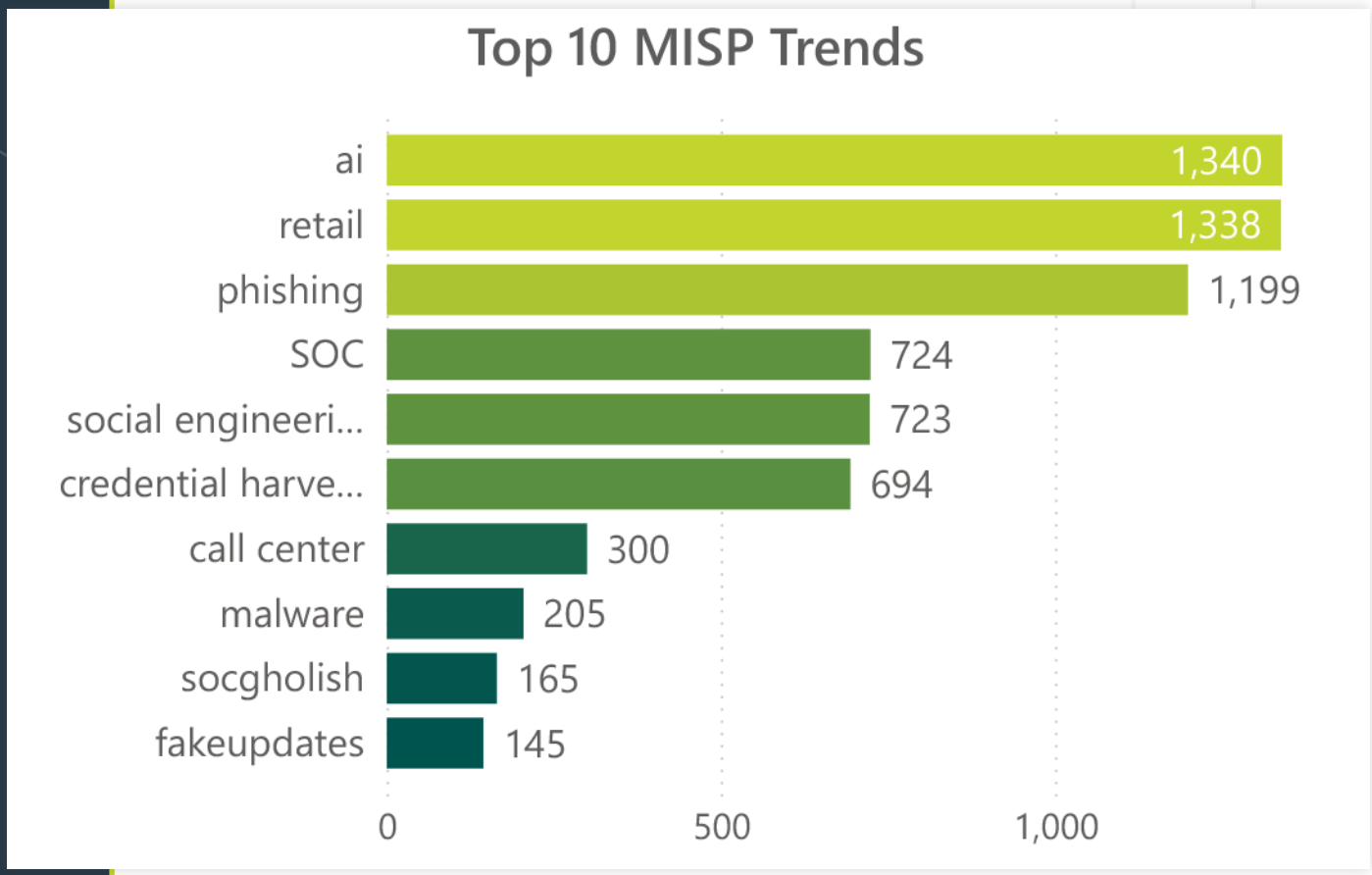
- Ransomware – 26%, up significantly from 13% from the prior reporting period
- Phishing – 15%, down slightly from 16% from the prior reporting period
- Microsoft-related threats – 7%, down from 16% from the previous reporting
- General vulnerabilities –14%
- General malware – 11%
- Fraud – 5%

Interestingly, generalized credential harvesting remained off the list entirely after it fell off the list in the second half of 2023. 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.



Top MISP Trends

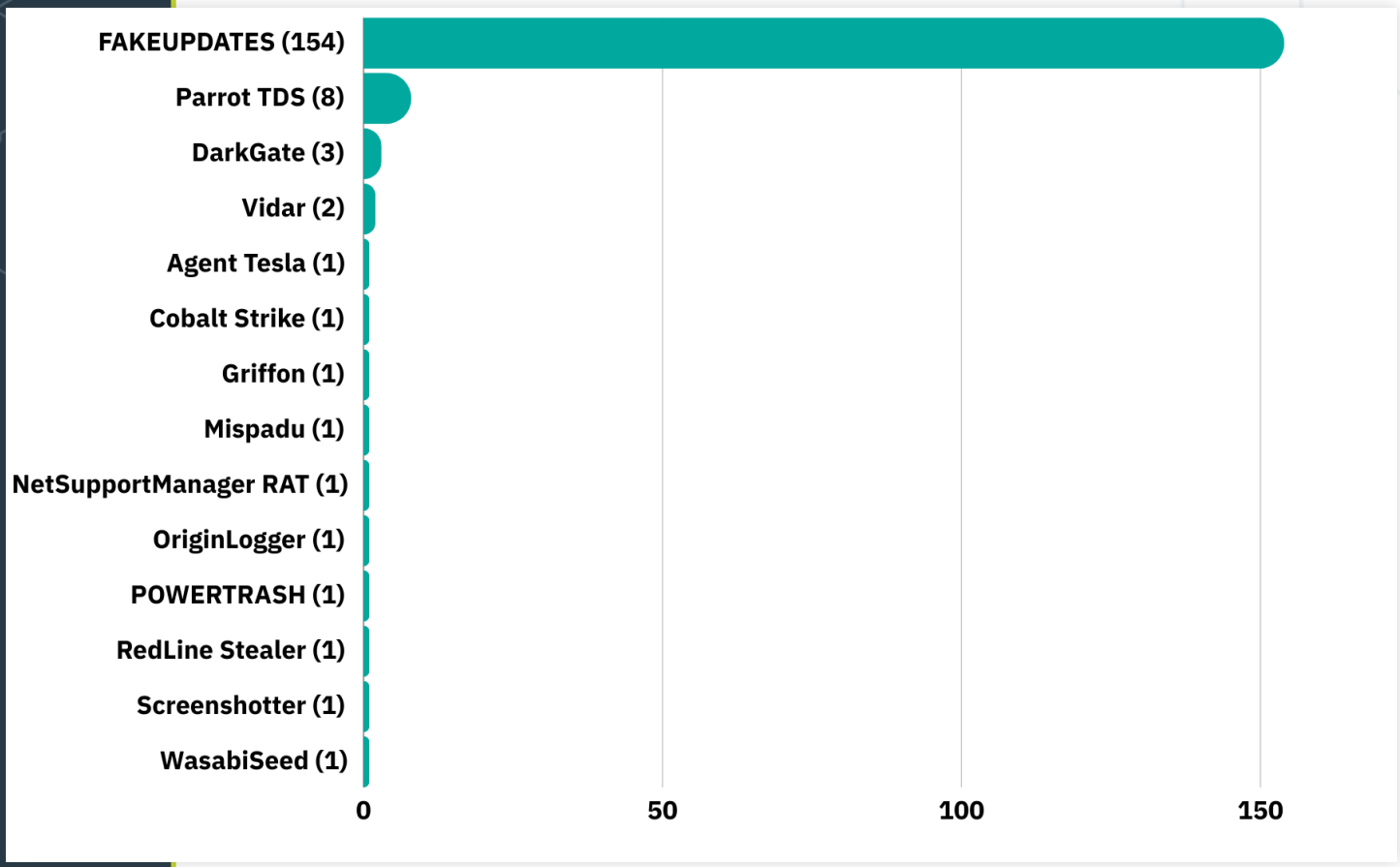
After the launch of MISP by RH-ISAC, threat trends are tracked via the RH-ISAC MISP instance, which changed the way data is presented for threat trends in the Intelligence Trends Summary, beginning in January 2023. Tracked data on member-reported threat trends includes prevalent malware, threat actors, 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 (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)



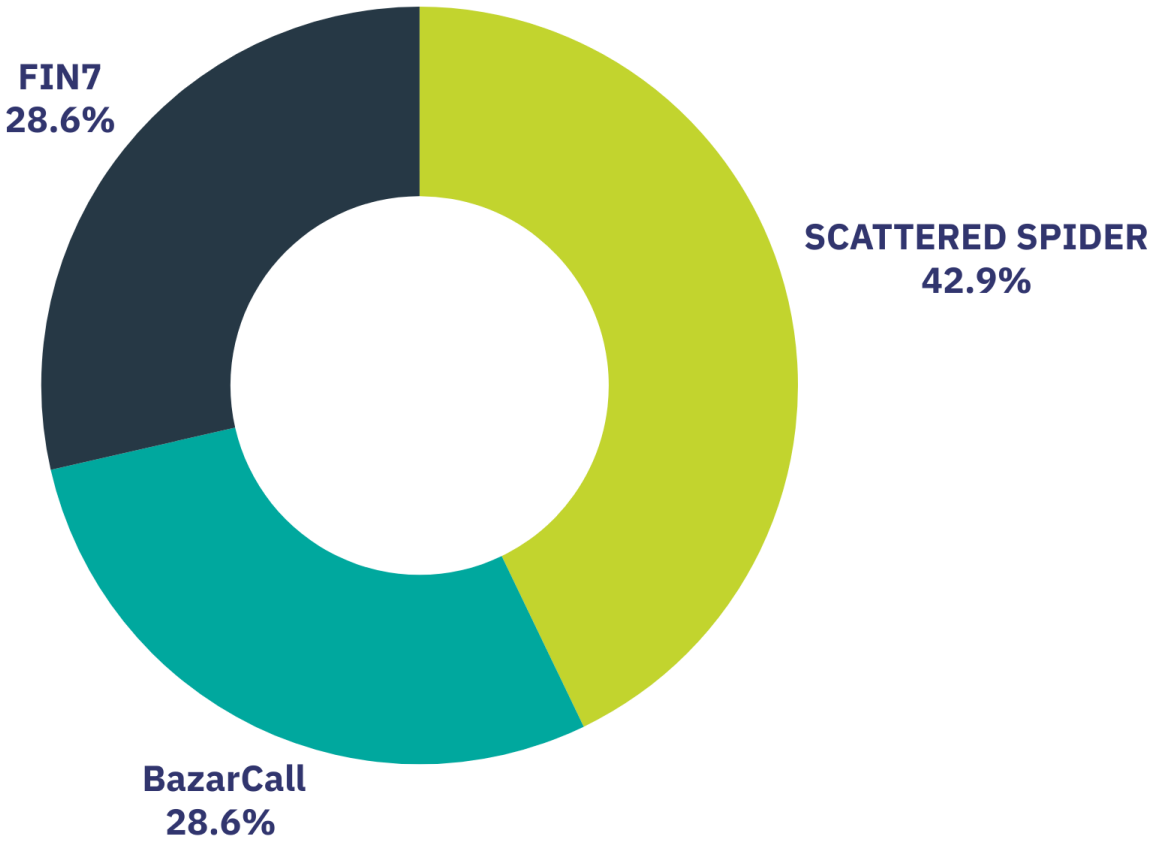
For comparison, the top reported malware (MITRE ATT&CK-defined software) for the September-December 2023 period, by total count of instances, were:

- 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)

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 (3)
- BazarCall (2)
- FIN7 (2)



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:

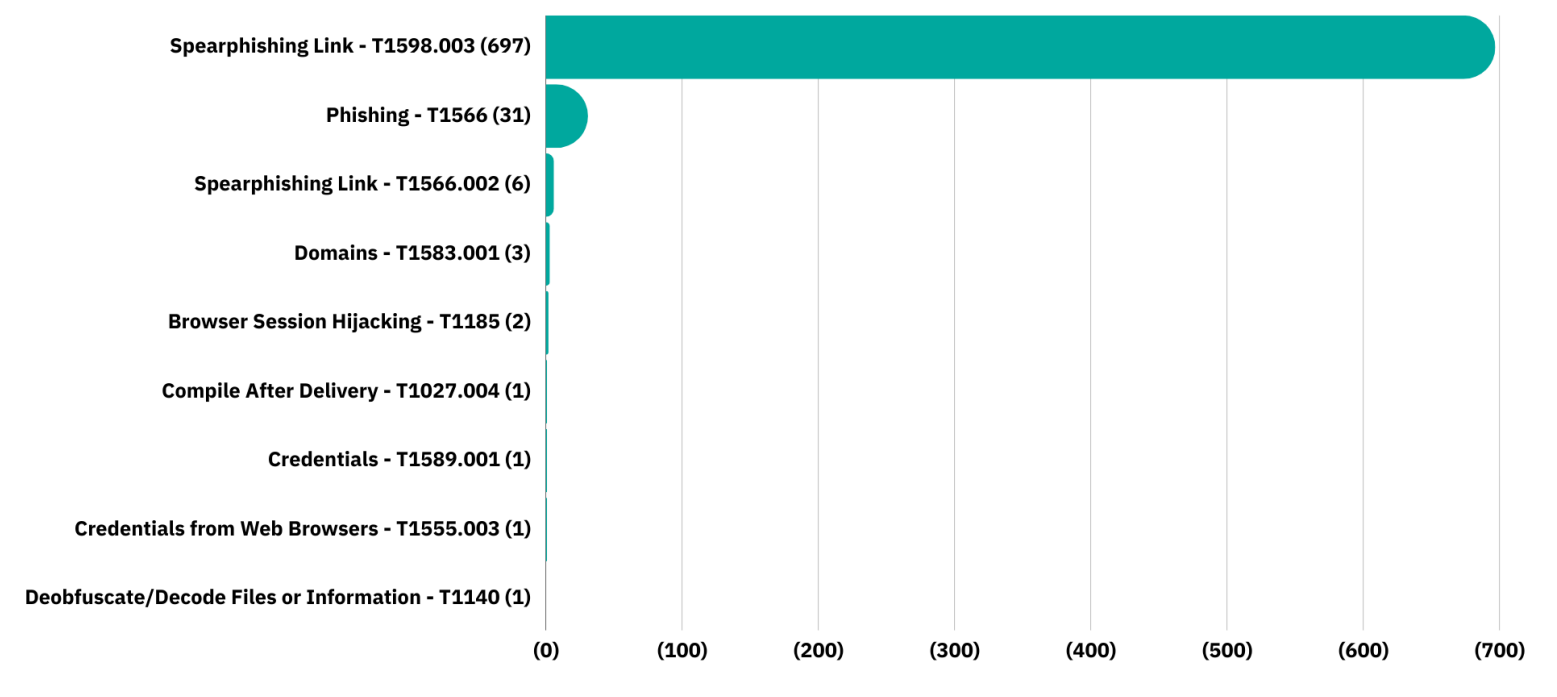
- SCATTERED SPIDER (29)
- FIN6 (8)
- APT38 (1)
- Carbanak (1)
- FIN7 (1)
- GOLD PRELUDE (1)

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).

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 (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.

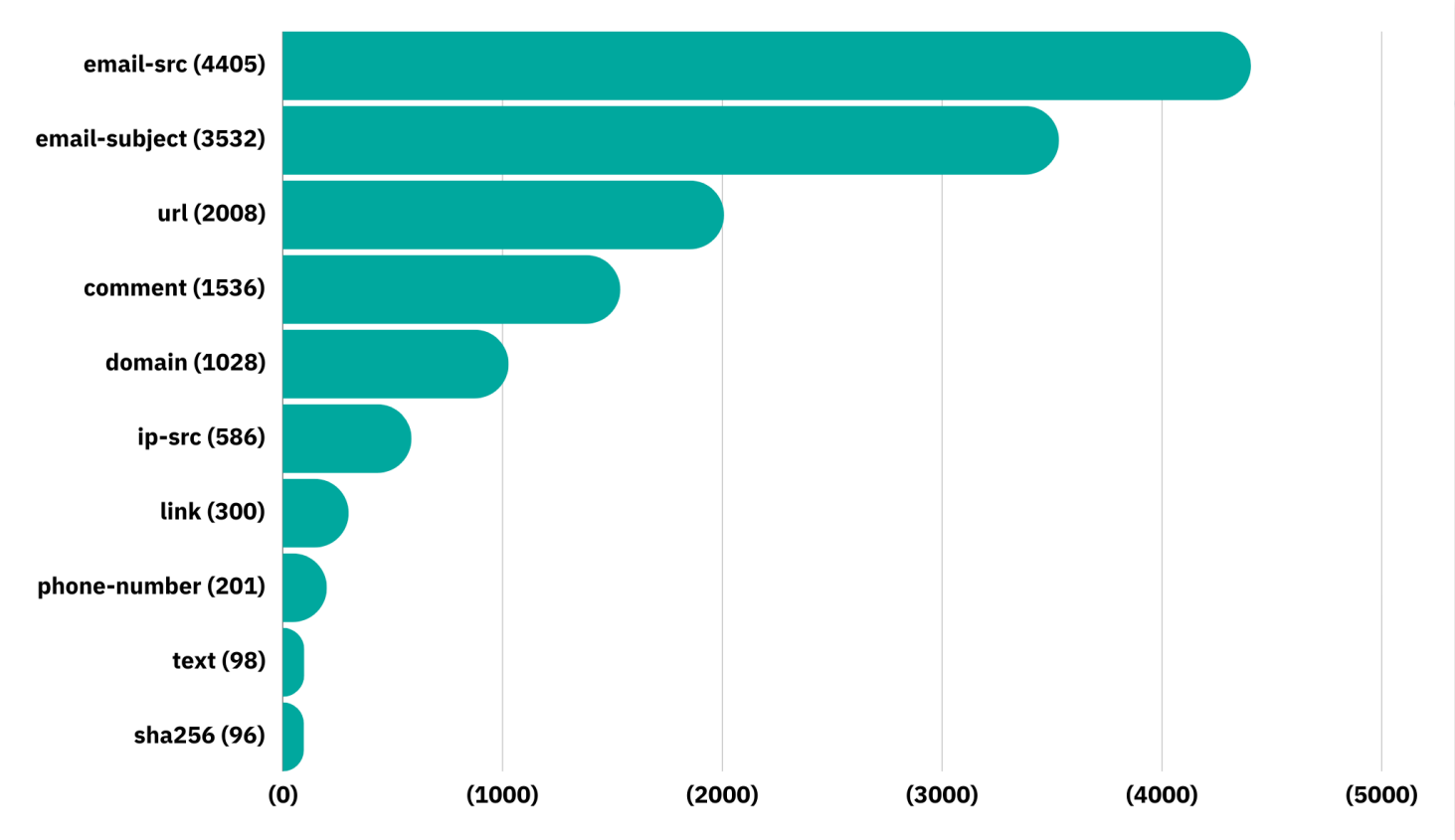
For comparison, the previous period's top reported MITRE ATT&CK techniques by total count of instances were:

- 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)

Top 10 Attribute Types

The 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)



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

Requests for Information

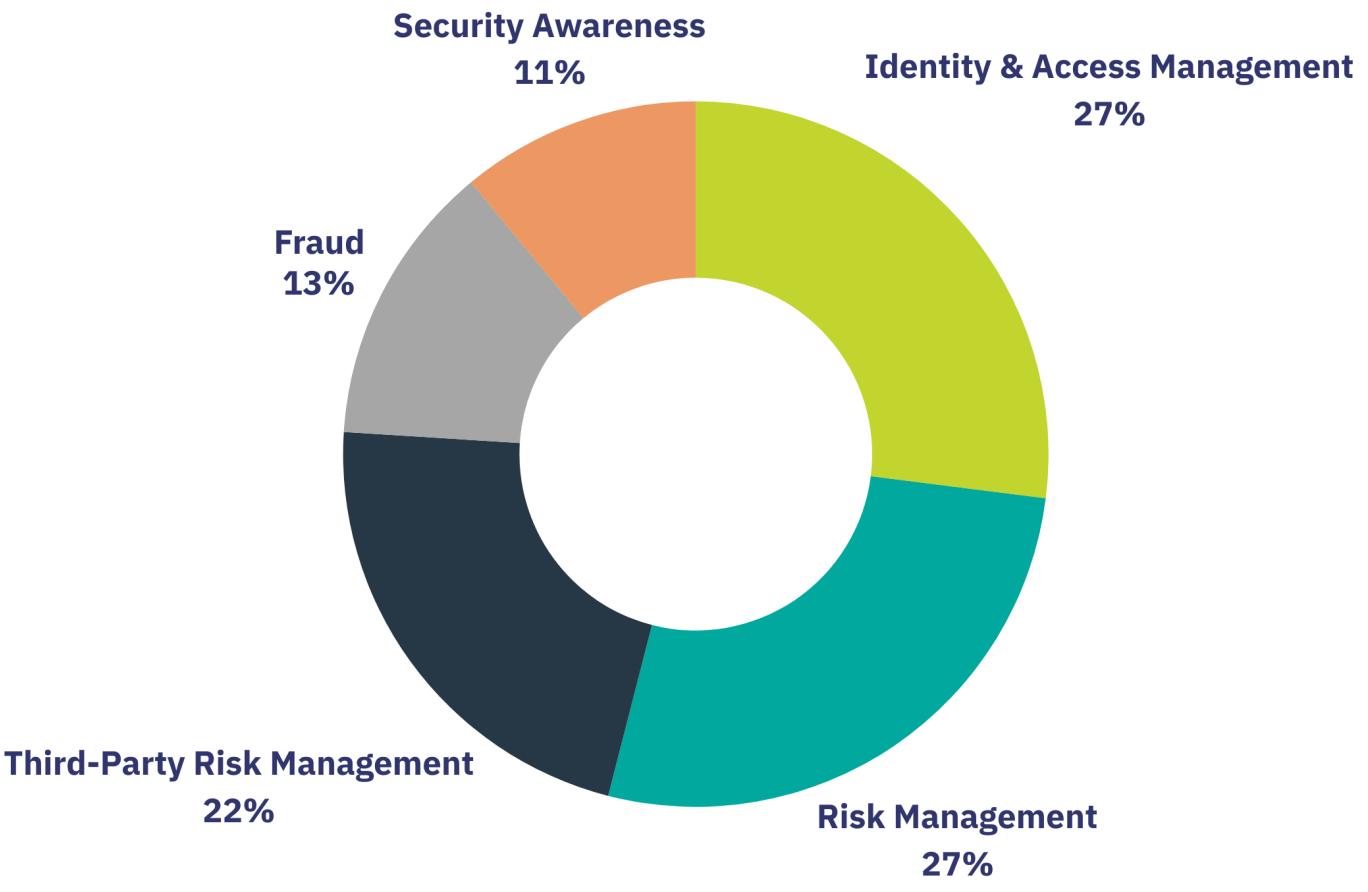
Members continue to leverage the RH-ISAC Request for Information (RFI) process integrated into Member Exchange, enabling our members to post RFIs to their peers with attribution or anonymously.

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 January and March 2024, 137 unique members, or 52% of our total membership, participated in RFIs.

In total, for the timeframe of January to March 2024, 161 RFIs were submitted, with 502 responses. The figure below displays the category of RFIs submitted for January-March 2024.

Overall RFI Domains for January - March 2024

161 RFIs | 502 Responses | Average Responses: 3



Community Engagement Outlook

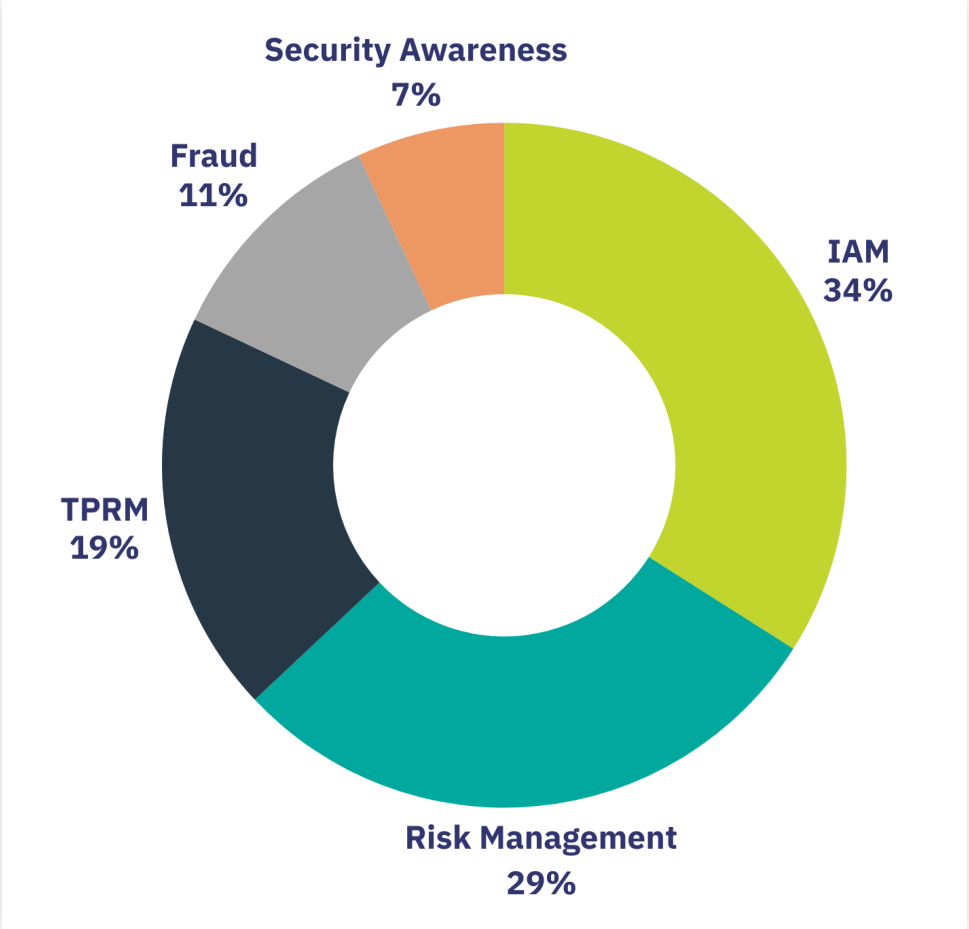
In 2023 for the timeframe of January to March, RH-ISAC received 113 RFIs that generated 274 responses. During 2024 continuous persistence, enhanced offerings, and growth in networking reflected an increase in community engagement with a spike in the numbers of RFIs (43% increase) and responses (83% increase).

CISO Community Overview

In the CISO Community, for January to March 2024, 58 RFIs were submitted, with 232 responses. During this period, 34% of the RFIs came from the Identity and Access Management Domain with greater interest in sub-domains Access controls and Privileged Access Management.

Risk Management was responsible for 29% of CISO RFIs with sub-domain topics of Governance, Risk and Compliance, Cloud Governance Practices, Policy and Architecture, and Cyber Insurance. Similarly, Third-Party Risk Management was responsible for 19% of CISO RFIs with sub-domain topics of Vendor best practices and Implement mitigating security controls.

CISO RFI Domains for January - March 2024
58 RFIs | 232 Responses | Average Responses: 4



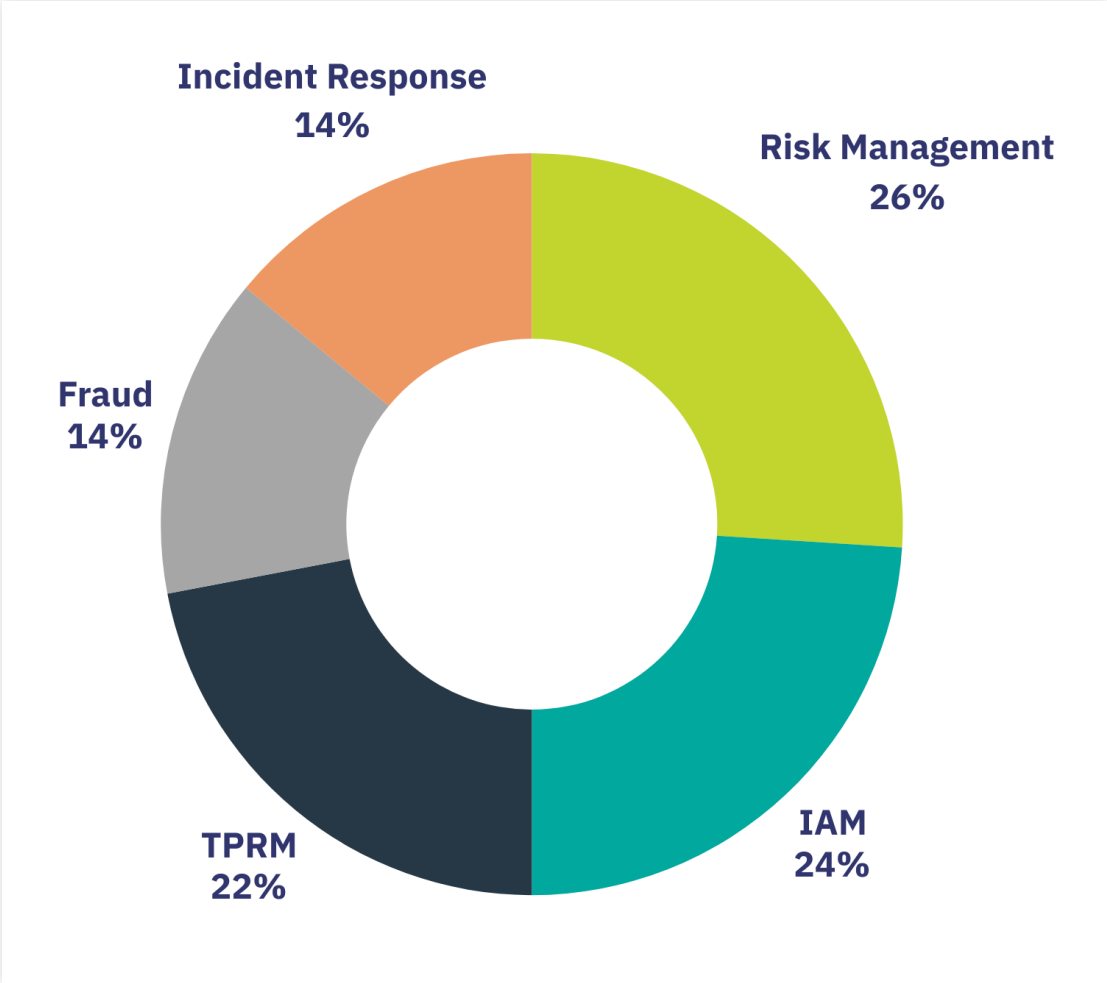
Analyst Community Overview

In the Analyst Community, for January to March 2024, 51 RFIs were submitted, with 142 responses. During this period, Risk Management, Identity & Access Management, Third-Party Risk Management, Fraud, and Incident Response were key discussion topics among the analyst community.

Like the CISO community, RFIs from the domain Risk Management with the main subdomain of Governance, Risk, and Compliance.

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

Analyst RFI Domains for January - March 2024
51 RFIs | 142 Responses | Average Responses: 8



Surveys

During January-March 2024, 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.

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.

ANALYSIS & INSIGHTS

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 forst quarter of 2024, third-party vulnerability disclosures and exploits were the primary theme of RH-ISAC intelligence reporting, especially AnyDesk, Invanti, GitHub, Microsoft, and Adobe vulnerabilities.

Reporting Trends

During the current period, a series of high-profile topics and events dominated the cyber threat landscape globally and for the retail, hospitality, and travel sectors specifically. Key reporting for 1 January 2024 - 31 March 2024 included:

- TLP:CLEAR: Firms Potentially Exposed to Supply Chain Compromise Attack via New Class of GitHub CI/CD Attack, PoC Available
- TLP:CLEAR CDN Flaw in GitLab Allows Malware Hosting, Like Recent GitHub Issue
- TLP:CLEAR: Researchers Discover Mass Manipulation of GitHub Search Functionalities to Distribute Malware
- TLP:CLEAR: Ivanti Announces Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN by Suspected Nation State Actors
- TLP:CLEAR: Two Critical Vulnerabilities Patched in GitLab, All Organizations Advised to Update Instances
- TLP:CLEAR: GitHub Rotates Keys After High-Severity Credential-Exposing Vulnerability Discovered
- TLP:AMBER+STRICT: RH-ISAC Members Reporting Significant Surge in Call Center Social Engineering
- TLP:AMBER+STRICT: Recent LockBit Activity Affecting the RH-ISAC Community, TTPs and IOCs
- TLP:AMBER+STRICT Nevada Gaming Control Board Website Taken Offline to Respond to Compromise
- TLP:AMBER+STRICT AnyDesk for Windows Code Signing Certificate Likely Stolen and Being Used to Sign Malware Samples
- TLP:CLEAR: ConnectWise Discloses Two ScreenConnect Critical Vulnerabilities Exploited by Multiple Threat Actors
- TLP:CLEAR: Fortinet Warns of Critical VPN Flaw Likely Under Active Exploitation
- TLP:CLEAR: TeamT5 Releases Latest Developments on Active Exploitation of Adobe ColdFusion Vulnerability
- TLP:CLEAR: Ivanti Discloses 2 New Zero-Day Flaws, One Under Active Exploitation

- TLP:CLEAR: Microsoft Warns of Critical Exchange Server Flaw Under Active Exploitation
- TLP:CLEAR Microsoft Attributes Executive Email Incident to Midnight Blizzard/NOBELIUM
- TLP:CLEAR Chinese Threat Group UNC5274 Reportedly Exploiting F5 BIG-IP and ScreenConnect CVEs
- TLP:CLEAR: Red Hat Warns of Urgent XZ Tools Vulnerability, Impacts Major Linux Distros
- TLP:CLEAR: LockBit Ransomware Operations Significantly Disrupted by Recent Law Enforcement Operations; Decryptor Tool Updated
- TLP:AMBER+STRICT: Recent AlphV Activity, Law Enforcement Actions, and New Mitigation Options
- TLP:CLEAR: BlackCat/ALPH Claims Responsibility for Change Healthcare Ransom; Claims 6TB of Data Stolen
- TLP:CLEAR: Sekoia Releases Latest Findings and Indicators of Compromise Related to Scattered Spider
- TLP:AMBER+STRICT: Current Timeline of Sisense Breach Intelligence and Impact on BigPanda Clients, Including RH-ISAC Core Members
- TLP:AMBER: Health-ISAC Releases Indicators from Recent Change Healthcare Incident
- TLP:AMBER+STRICT: RH-ISAC Members Impacted by Palo Alto Zero Day, Members Advised to Update Immediately

Leading reporting from the previous period included:

- TLP:CLEAR 2023 Holiday Season Cyber Threat Trends Report
- TLP:AMBER+STRICT: Recent AlphV Activity, Law Enforcement Actions, and New Mitigation Options
    - TLP:AMBER+STRICT AlphV Hospitality Activity Timeline and TTPs
- TLP:AMBER+STRICT: Best Practices for Executive Exposure Monitoring and Cyber Defense
- TLP:AMBER+STRICT HR Data Provider Zeroed-In Discloses Data Breach, RH-ISAC Members Potentially Affected
- TLP:AMBER+STRICT RH-ISAC Timeline of Recent Okta Activity
    - TLP:CLEAR Okta Announces Unauthorized Access to Support Case Management System
    - TLP:GREEN Proactive Defense Options Against Recent Activity Targeting Okta Customer Organizations
- TLP:AMBER LockBit 3.0 Aviation Incident Observables and IOCs
- TLP:AMBER+STRICT: On-Going SMS Phishing Campaign (analysis and indicators)