TLP: AMBER+STRICT

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY INTELLIGENCE TRENDS SUMMARY

October – December 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 final quarter of 2024, the three-month period between 1 October and 31 December 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.

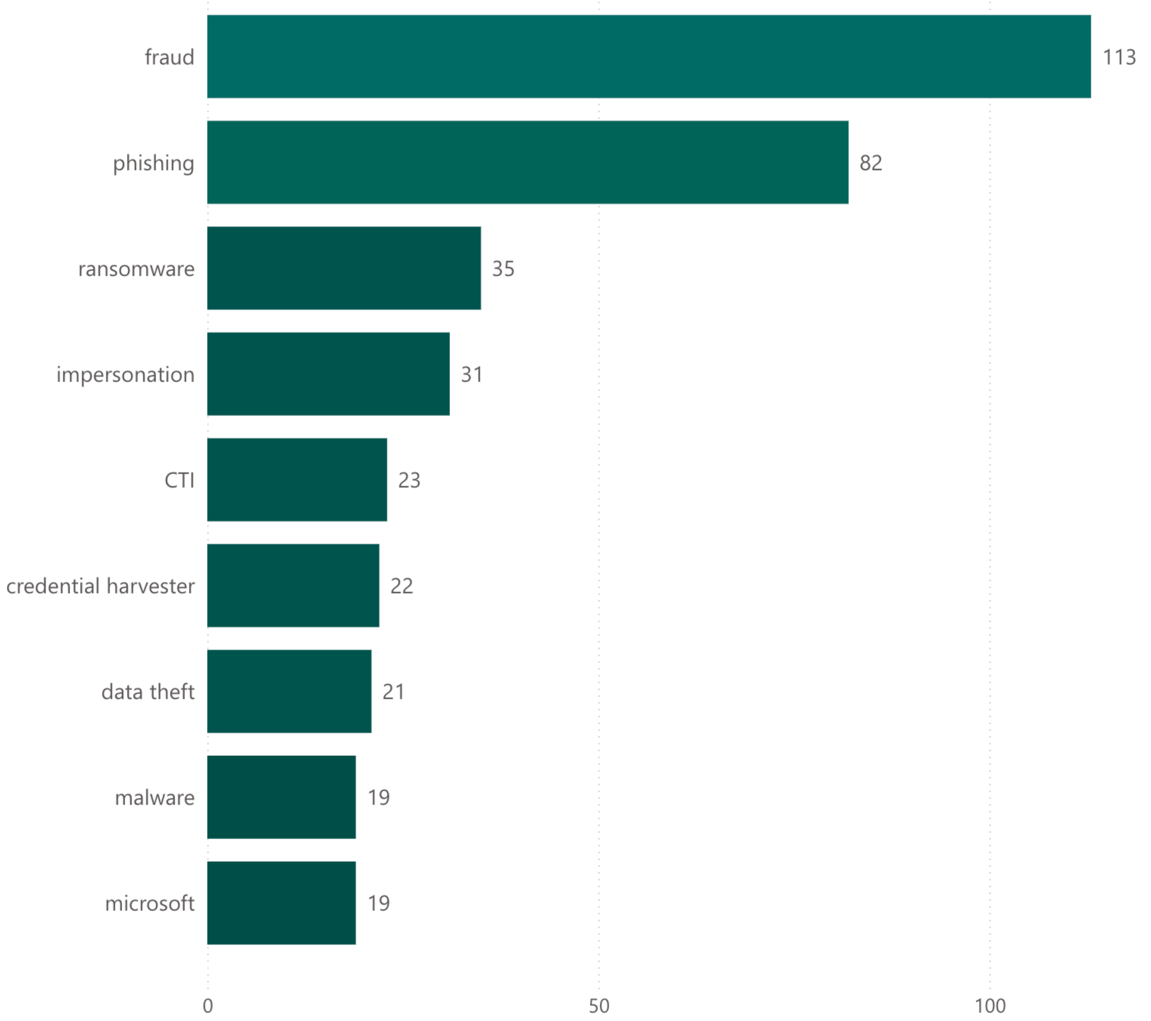
The RH-ISAC Research and Analytics team has also stayed busy supporting the community through the management and distillation of various requests for information (RFIs), surveys, and curating communities in Member Exchange. From risk management to loyalty programs to security architecture, members in 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. Crowdstrike discussion fell off entirely as the effects of the summer outage eased, replaced by a focus on fraud, social engineering, malware, data theft, and threat actor tracking.

THREAT LANDSCAPE: Trends

Top Sharing Trends

This graph 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 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.

For comparison, In the third quarter of 2024, members shared information related to the July 2024 Crowdstrike outage at a higher prevalence than other more established threat trends such as phishing and fraud, both of which remained prevalent. Crowdstrike reporting fell off entirely in the final quarter of 2024. Ransomware reporting fell significantly back to levels seen in the first quarter of 2024, falling from 33 to 19 instances. Imposter sites and brand impersonation remained prevalent, just behind fraud.

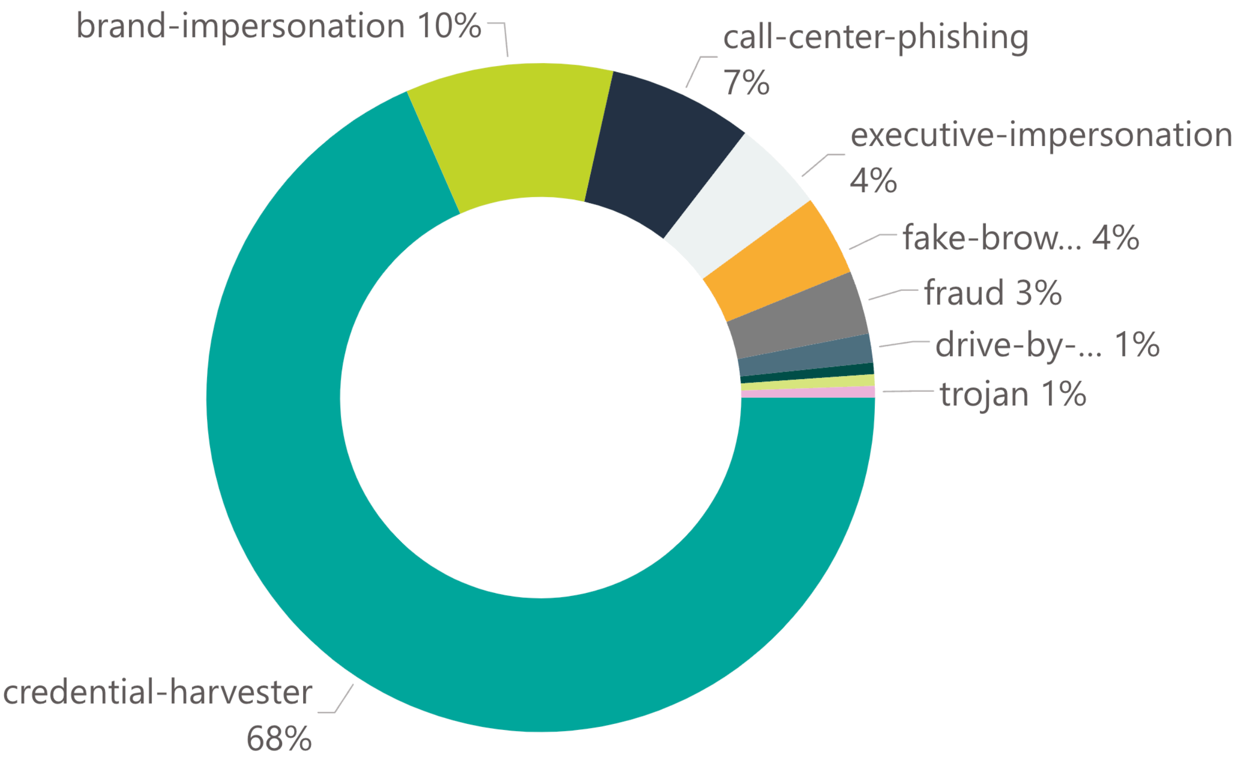
Top MISP Trends

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 Types of Threats

Due to enhanced tracking, we are adding a new category of sharing reank for the Intelligence Trends Summary: the top reported types of threats by members for the current period by total count of instances were:

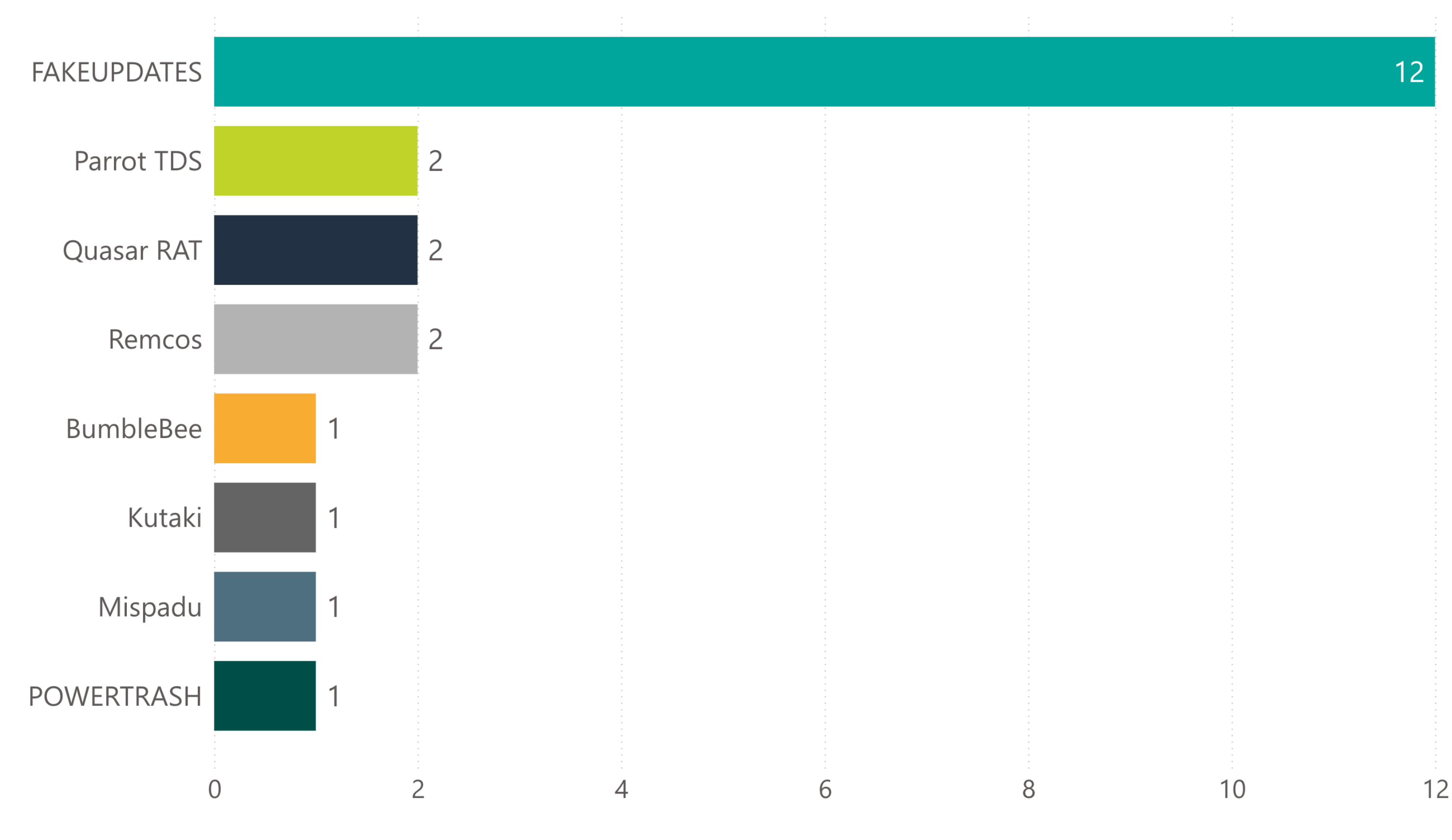
- credential-harvester (245)
- brand-impersonation (36)
- call-center-phishing (25)
- executive-impersonation (16)
- fake-browser-update (14)
- fraud (11)
- drive-by-phishing (5)
- loader-malware (2)
- trojan (2)
- malware-delivery (2)



Top Reported Malware

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

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



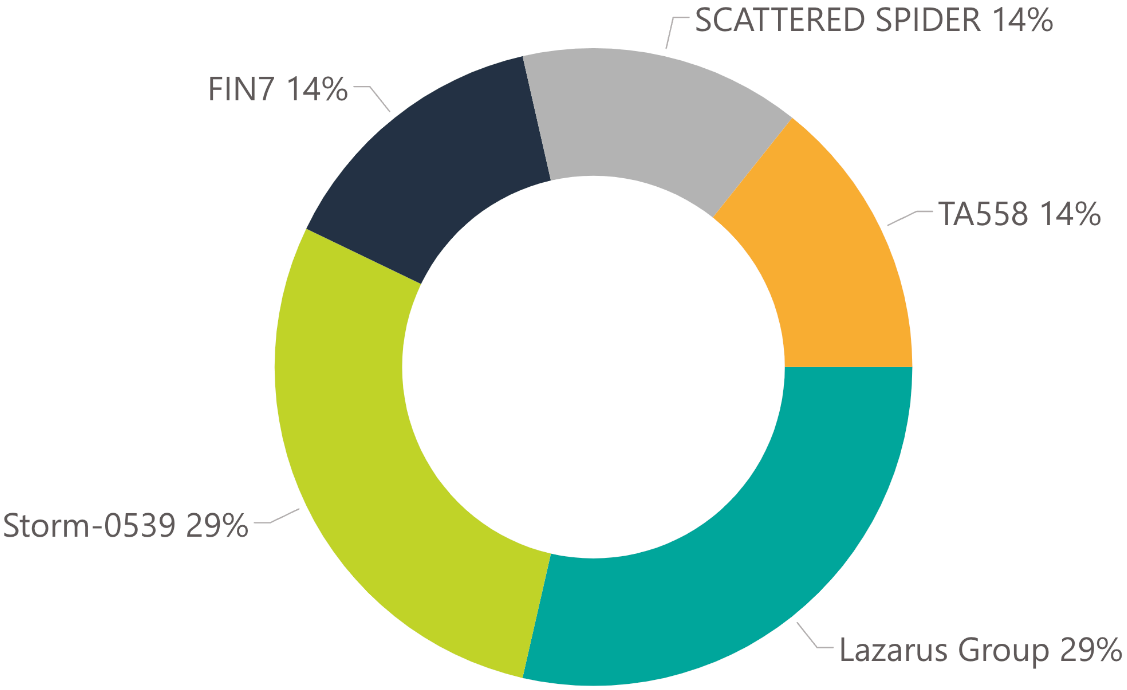
For comparison, the top reported malware (MITRE ATT&CK-defined software) for the third quarter of 2024, by total count of instances, were:

- FAKEUPDATES (44)
- Agent Tesla (3)
- ClearFake (3)
- Quasar RAT (2)
- Xloader (2)
- 404 Keylogger (1)
- Xmrig (1)
- Remcos (1)
- Spectre RAT (1)
- IcedID (1)

Top Reported Threat Actors

The top reported threat actors for the current period by total count of instances were:

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



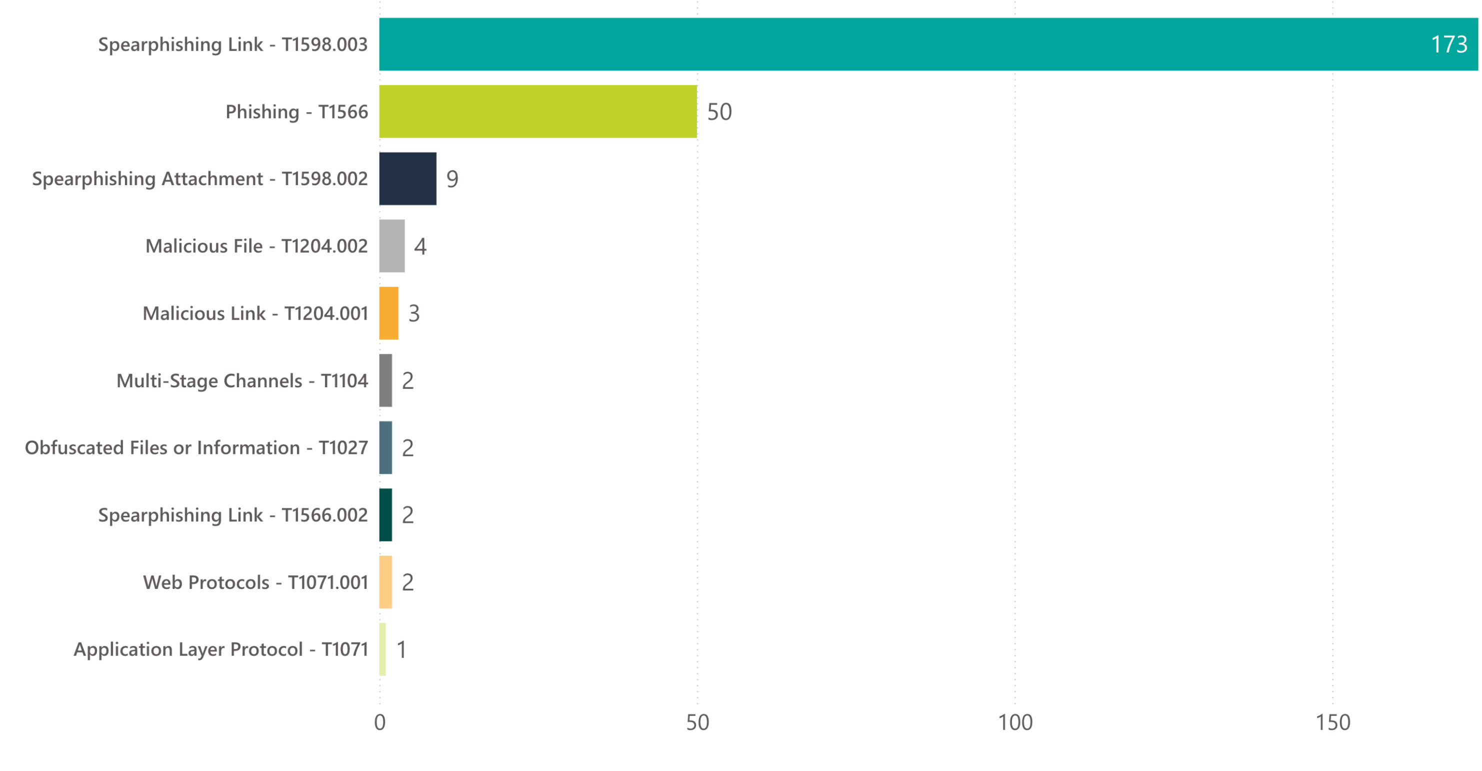
For comparison, the top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) for the third quarter of 2024 by total count of instances were:

- FIN6 (4)
- FIN7 (2)
- TA558 (2)
- Volt Typhoon (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
- 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



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

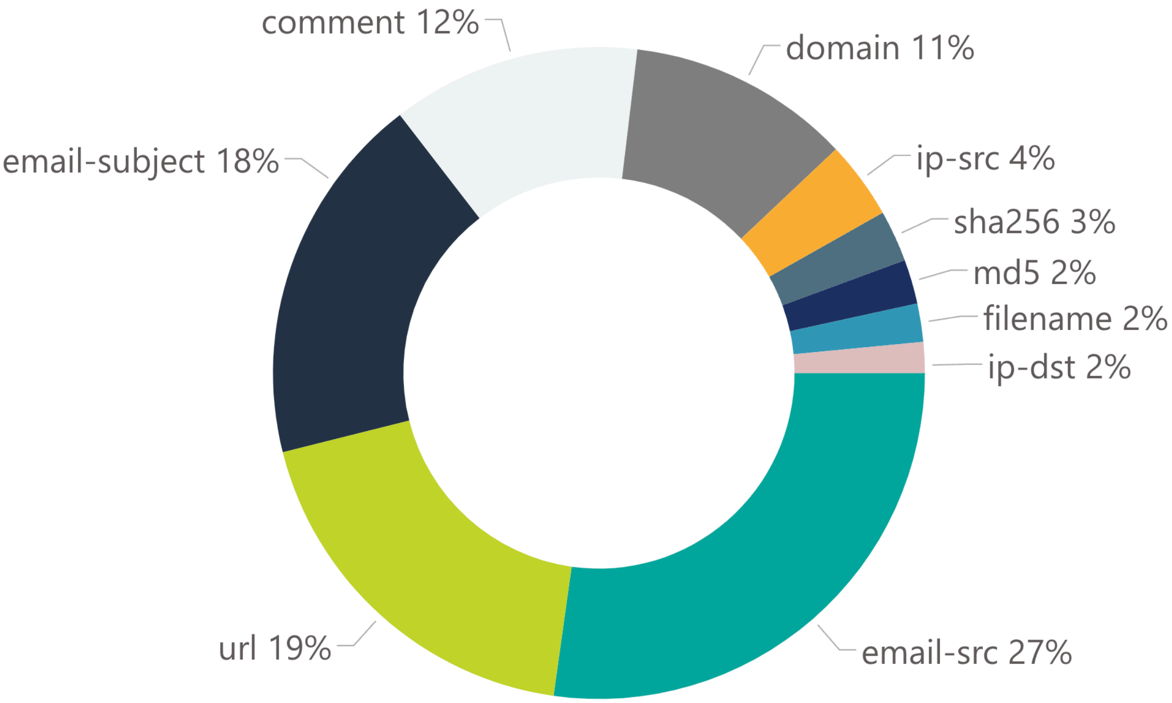
- Spearphishing Link - T1598.003 (240)
- Phishing - T1566 (27)
- Malicious File - T1204.002 (7)
- Spearphishing Attachment - T1566.001 (6)
- Command Obfuscation - T1027.010 (5)
- PowerShell - T1059.001 (5)
- Ingress Tool Transfer - T1105 (4)
- Multi-Stage Channels - T1104 (4)
- Encrypted/Encoded File - T1027.013 (3)
- Obfuscated Files or Information - T1027 (3)

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



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

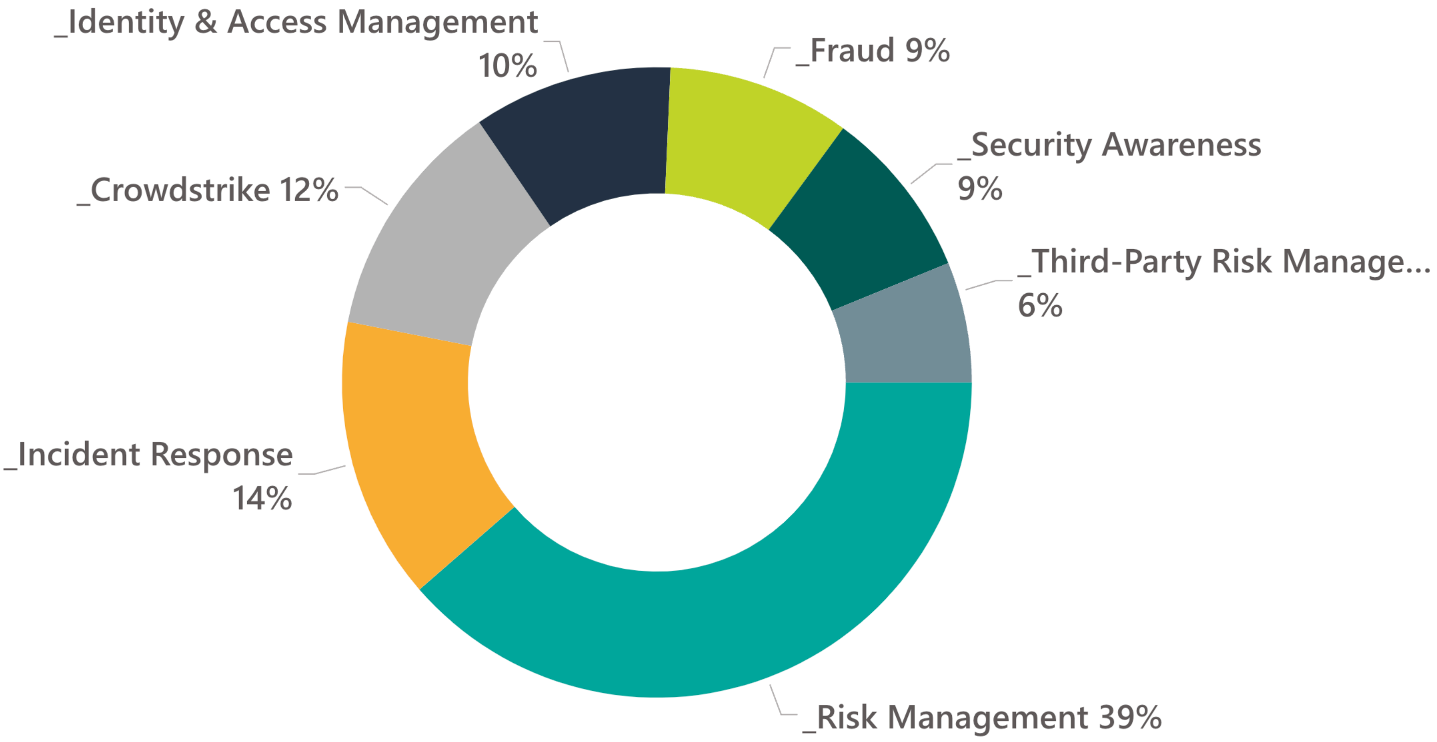
- email-src (925)
- url (695)
- email-subject (669)
- domain (540)
- comment (352)
- ip-src (304)
- link (301)
- email-src-display-name (95)
- text (66)
- other (36)

Requests for Information

The RH-ISAC Intelligence Team actively tracks Requests for Information (RFIs) and surveys to understand our members' interests, spanning both analyst perspectives and those of CISOs. From October to December 2024, 161 unique members, or 54% of our total membership, participated in RFIs, with a total of 175 RFIs submitted, generating 429 responses. In comparison, during the same period in 2023, RH-ISAC received 97 RFIs, resulting in 223 responses. This year, the continued focus on engagement and enhanced offerings led to a substantial increase in community interaction, with RFIs rising by 80% and responses increasing by 92%.

Overall RFI Domains for October - December 2024

175 RFIs | 429 Responses



Summary of RFI Publications

Justifying Financial Costs of PAM Solutions

an RH-ISAC member posted an RFI in the CISO Community seeking feedback on the challenges of implementing Privileged Access Management (PAM) solutions. The organization is exploring options like CyberArk, BeyondTrust, and Okta to meet a cyber insurance requirement but is concerned about the high implementation costs, which could be three to five times higher than the licensing fees.

Level 1 PCI Compliance QSA Services

An RH-ISAC member posted an RFI in the CISO community asking for assistance with achieving or maintaining Level 1 PCI compliance for organizations handling large volumes of payment card transactions and finding Qualified Security Assessor (QSA) services to aid in the transition to or maintenance of that status. The question is focused on gathering practical advice and reliable service providers to manage the complexities of PCI compliance for large scale businesses. This RFI summary is a compilation of discussion responses that generated eight individual responses.

Surveys & Best Practices Reports

In addition, the RH-ISAC has produced best practices summary reports and two comprehensive survey reports:

Implementing DLP To Mitigate Security Risks

This report provides a comprehensive overview of how DLP can be used to reduce risks both for customers and internally. It includes a list of Indicators of Compromise (IOCs), as well as recommended best practices and mitigation strategies.

Data Loss Prevention (DLP) Survey Report

In September 2024, RH-ISAC conducted a Data Loss Prevention (DLP) survey, gathering insights from 26 unique member companies. This report provides an in-depth analysis of maturity levels, key performance indicators (KPIs), tools, challenges, and solutions related to DLP.

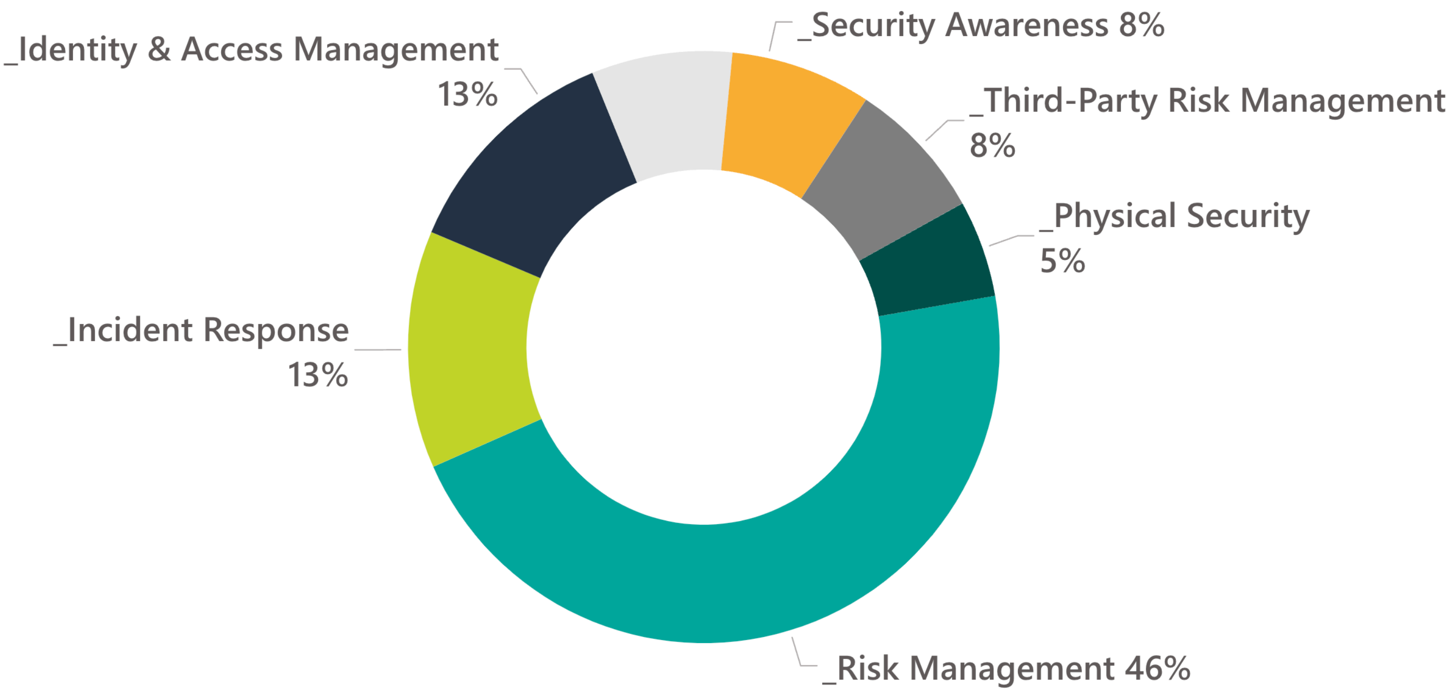
Gift Card Fraud Survey Report

In October 2024, RH-ISAC conducted a Gift Card Fraud survey, gathering insights from nine unique member companies. This report provides an in-depth analysis of tampering trends, partnerships with internal departments, gift card providers, and law enforcement, as well as strategies for packaging, in-store security, and enhancing the customer experience.

CISO Community Overview

In the CISO Community, from October to December 2024, a total of 59 RFIs were submitted, resulting in 191 responses. During this period, 46% of the RFIs came from the Risk Management Domain with greater interest in Policy and Architecture and Governance, Risk, and Compliance. Incident Response was responsible for 13% of CISO RFIs with sub-domain topics of Best Practices and Tabletop Exercises. Identity and Access Management was responsible for 13% of CISO RFIs with sub-domain topics Privileged Access Management. The figure below shows a total breakdown of the RFIs submitted to the CISO Community.

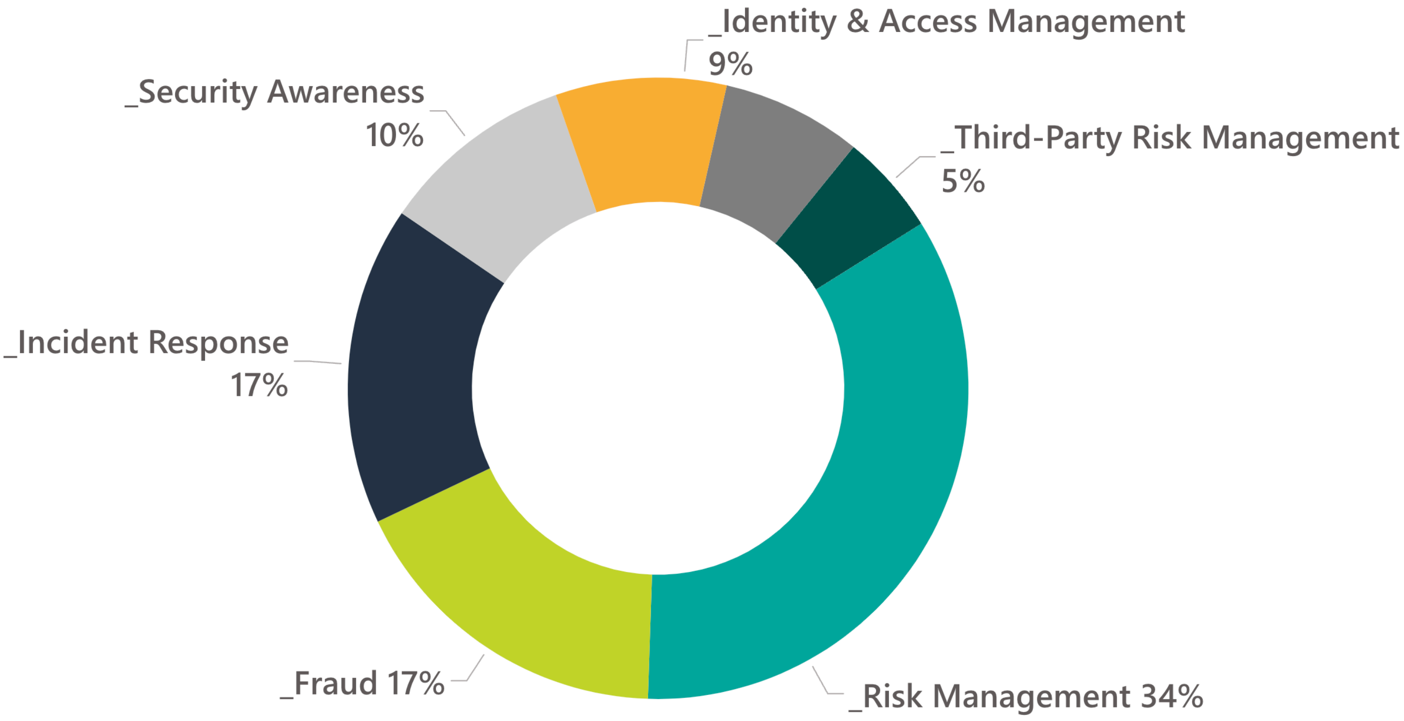
CISO RFI Domains for October - December 2024
59 RFIs | 191 Responses



Analyst Community Overview

In the Analyst Community, from October to December 2024, a total of 116 RFIs were submitted, generating 238 responses. Key discussion topics among the analyst community during this period were Risk Management, Fraud, and Incident Response. The top subdomains across the Analyst community were Policy and Architecture, Best Practices, Governance Risk and Compliance, Data Loss Prevention, Vendor Best Practices, and Brand Protection. The figures below show a total breakdown of the RFIs submitted to the Analyst Community.

Analyst RFI Domains for October - December 2024
116 RFIs | 238 Responses



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 final quarter of 2024, RH-ISAC intelligence reporting focused on critical incidents affecting consumer-facing sectors, third party vulnerabilities, and fraud activity.

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 October - 31 December 2024 included:

- Fortinet Warns of Critical Flaw in Wireless LAN Manager FortiWLM
- Four Chinese APT Groups Target Critical Infrastructure Disruption
- Ivanti Warns of Maximum Severity CSA Auth Bypass Vulnerability
- Horns&Hooves Campaign Delivers RATs to Russian Retail Entities
- Technical Analysis of FPNTX Digital Skimmer Found on eCommerce Site
- Blue Yonder Software Hack Impacting UK Grocery and FMCG Stores
- Financially Motivated Threat Actor, SilkSpecter, Targeting Black Friday Shoppers
- Iranian TA455 Initiates Dream Job Campaign to Target Aviation and Other Critical Industries with Malware
- RH-ISAC Releases Standards and Best Practices Document for Hospitality
- Midnight Blizzard Conducts Large-Scale Spear-Phishing Campaign Utilizing RDP Files
- Infostealer Infection Results in One of the Largest Retail Breach in History
- Chinese Nation-State Hackers APT41 Attack Gambling Sector for Financial Gain
- Intel Broker Claims Cisco Breach, Selling Stolen Data from Major Firms
- 4,000+ Adobe Commerce, Magento Shops Compromised in CosmicSting Attacks
- BitSight Discloses Zero-Day Vulnerabilities in ATG ICS Critical Infrastructure Systems

Leading reporting from the third quarter of 2024 included:

- Netskope Report Details Exponential Increase in Microsoft Sway QR Code Phishing
- FIN7 Found Hosting Malicious Domains Hosted on Tech Internal Infrastructure
- Researchers Exploit Vulnerabilities to Exploit Industrial Remote Access Gateways
- Polyfill Supply Chain Attack Highlights Risks of Third-party Code in Modern Web Applications
- New GoGra Backdoor Deployed Against South Asia Media Organization via Cloud Services in Widespread Cyberespionage Operation
- Threat Actor Abuses Cloudflare Trial Tunnels to Deliver RATs
- Ransomware Operators Exploit Novel ESXi Vulnerability for Attacks
- FrostyGoop Leverages Modbus TCP to Exploit Sensitive OT Systems