TLP: CLEAR

RETAIL & HOSPITALITY ISAC

RETAIL & HOSPITALITY INTELLIGENCE TRENDS SUMMARY

July – September 2024

Introduction

In this installment of the the Retail & Hospitality Information Sharing and Analysis Center (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 third quarter of 2024, the three-month period between 1 July and 30 September 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.

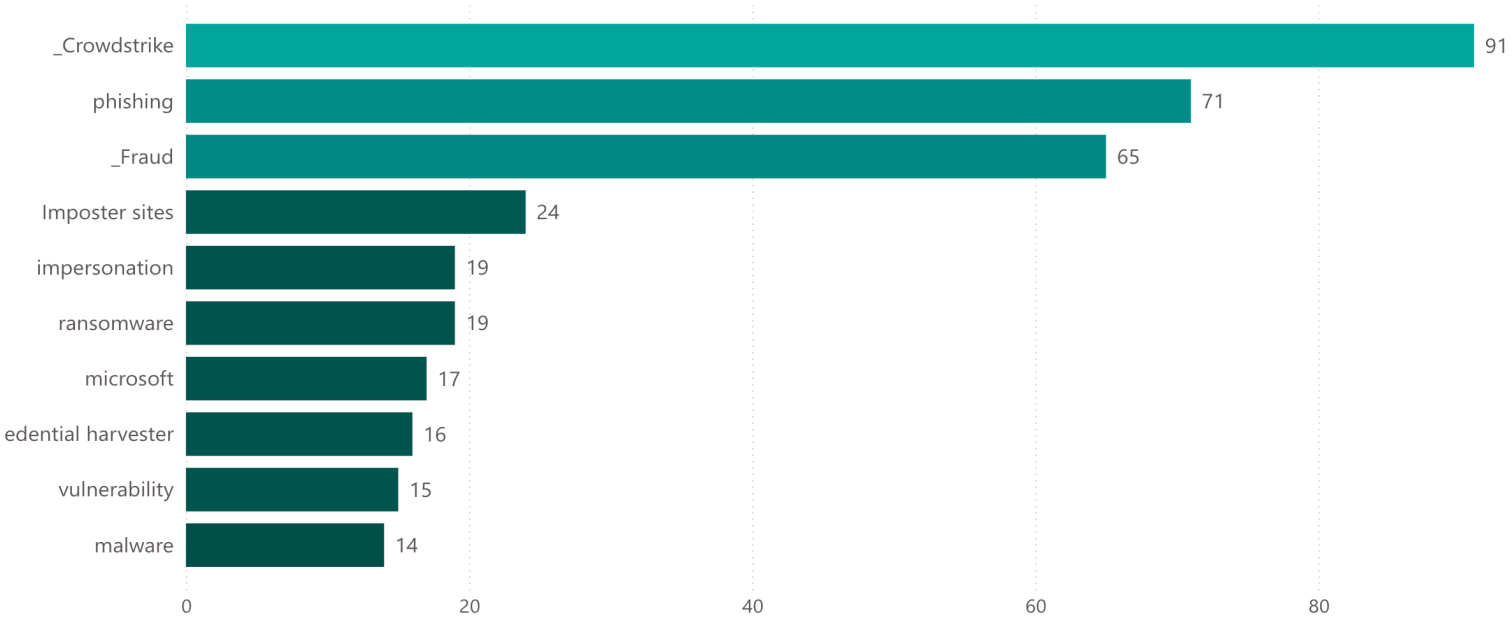
The RH-ISAC Research and Analytics team has also stayed busy supporting the community through the management and distillation of various requests for information (RFIs), surveys, and curating communities in Member Exchange. From risk management to loyalty programs to security architecture, members in 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. While reporting on the Crowdstrike outage of July 2024 leads reporting for the third quarter of 2024, phishing and fraud remained the second most prevalent threats reported by the community, with social engineering and ransomware threats remaining prevalent.

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 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. 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.

For comparison, 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 repoting 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.

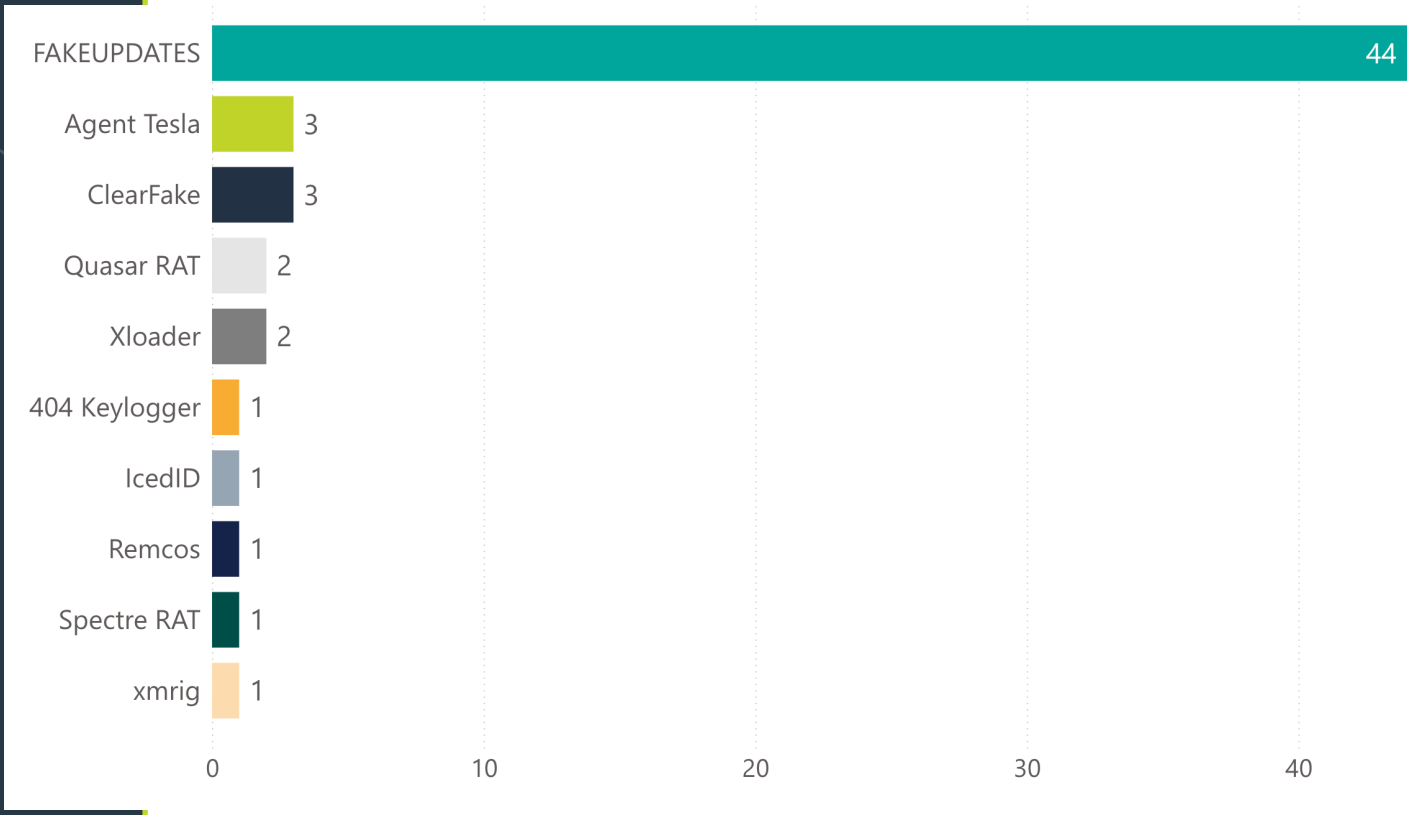
Top MISP Trends

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



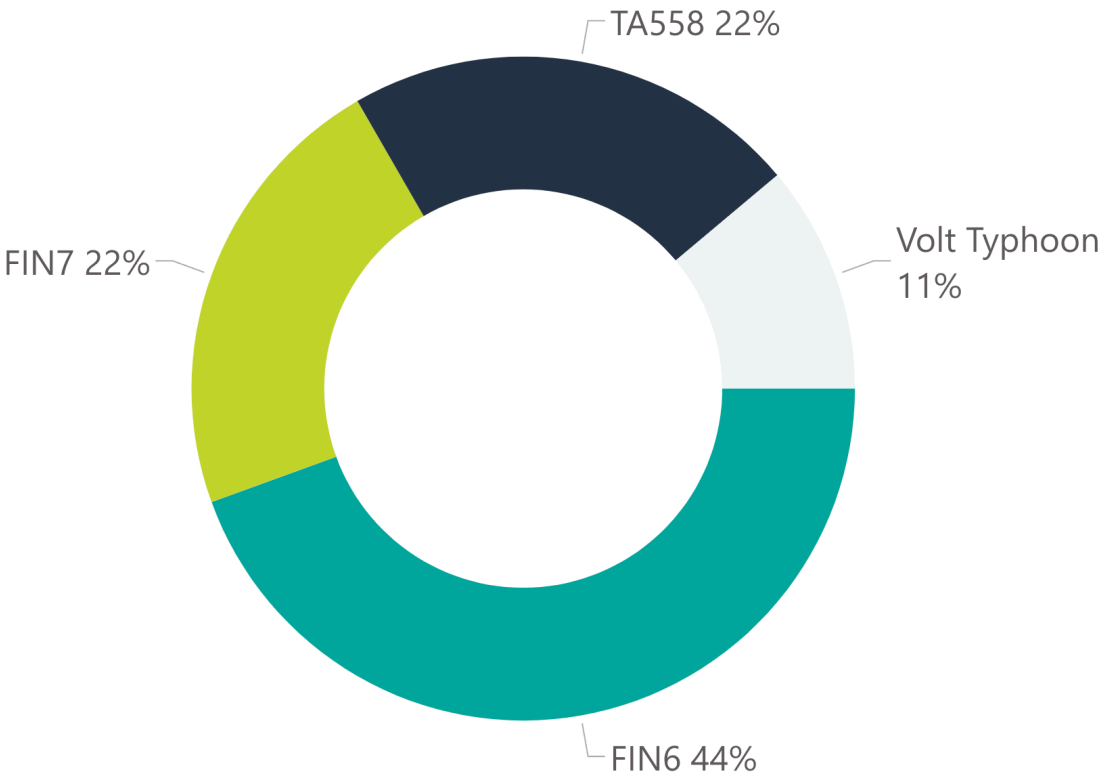
For comparison, the top reported malware (MITRE ATT&CK-defined software) for the second quarter of 2024, by total count of instances, were:

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

Top Reported Threat Actors

The top reported threat actors for the period of 1 July - 30 September 2024 by total count of instances were:

- FIN6 (4)
- FIN7 (2)
- TA558 (2)
- Volt Typhoon (1)



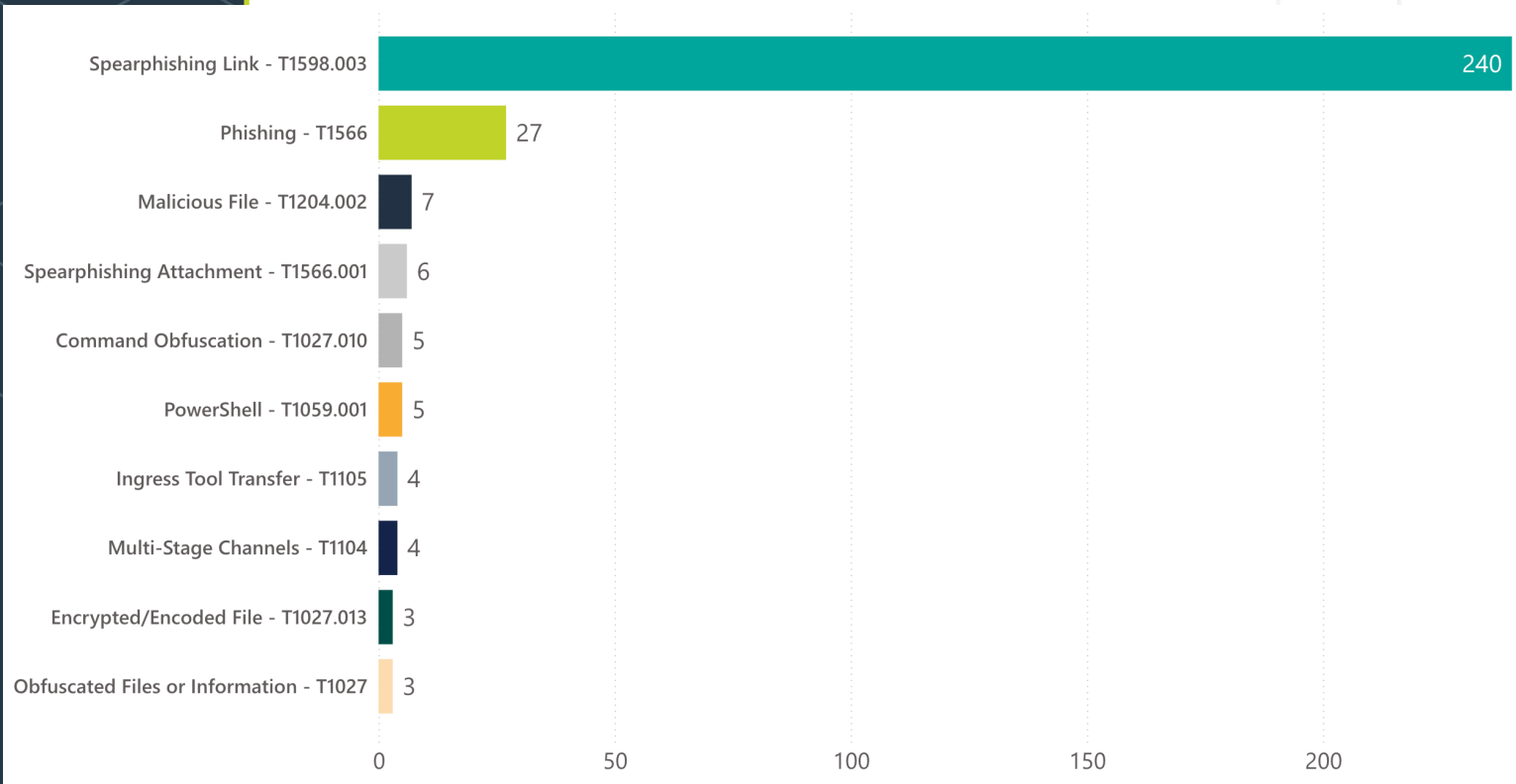
For comparison, the top reported threat actors (characteristic clusters of malicious actors representing a cyber threat) for the second quarter of 2024 by total count of instances were:

- FIN7 (12)
- FIN6 (4)
- TA558 (3)
- FIN8 - G0061 (2)
- Black Basta (2)
- Carbanak - APT-C-11 (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 (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)



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

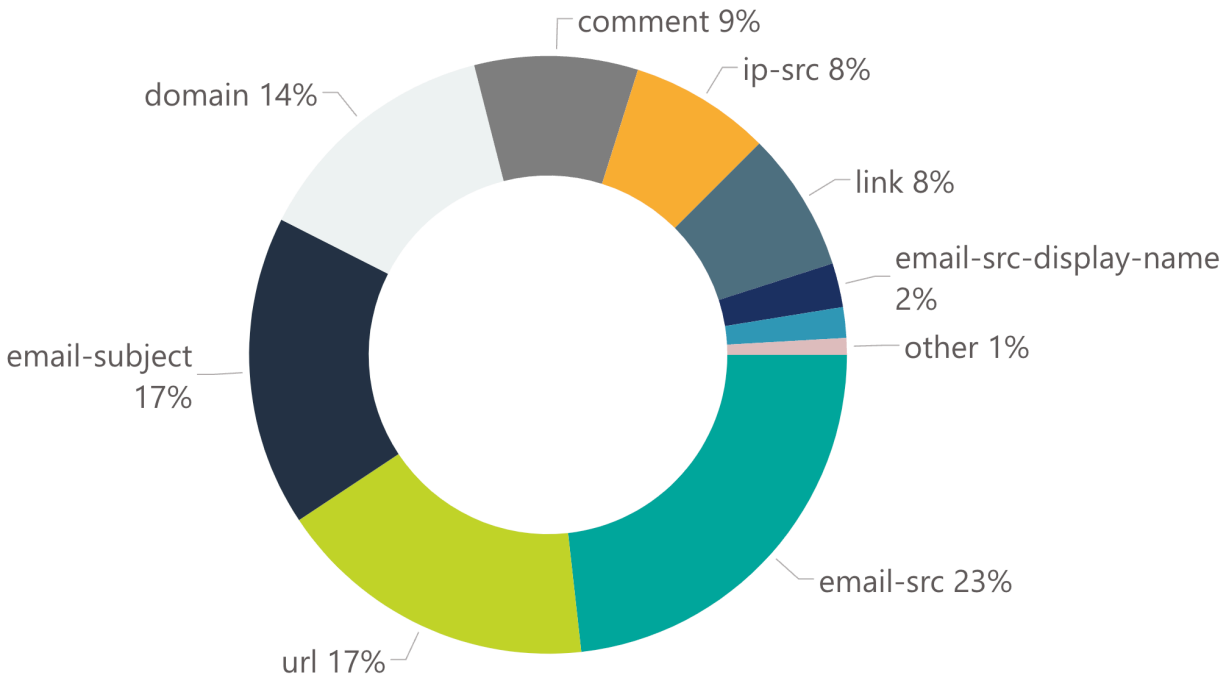
- Spearphishing Link - T1598.003 (313)
- Phishing - T1566 (34)
- Spearphishing Attachment - T1566.001 (19)
- Process Injection - T1055 (12)
- Malicious File - T1204.002 (11)
- Deobfuscate/Decode Files or Information - T1140 (8)
- Ingress Tool Transfer - T1105 (8)
- Malicious Link - T1204.001 (7)
- Obfuscated Files or Information - T1027 (6)
- Scheduled Task - T1053.005 (6)

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



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

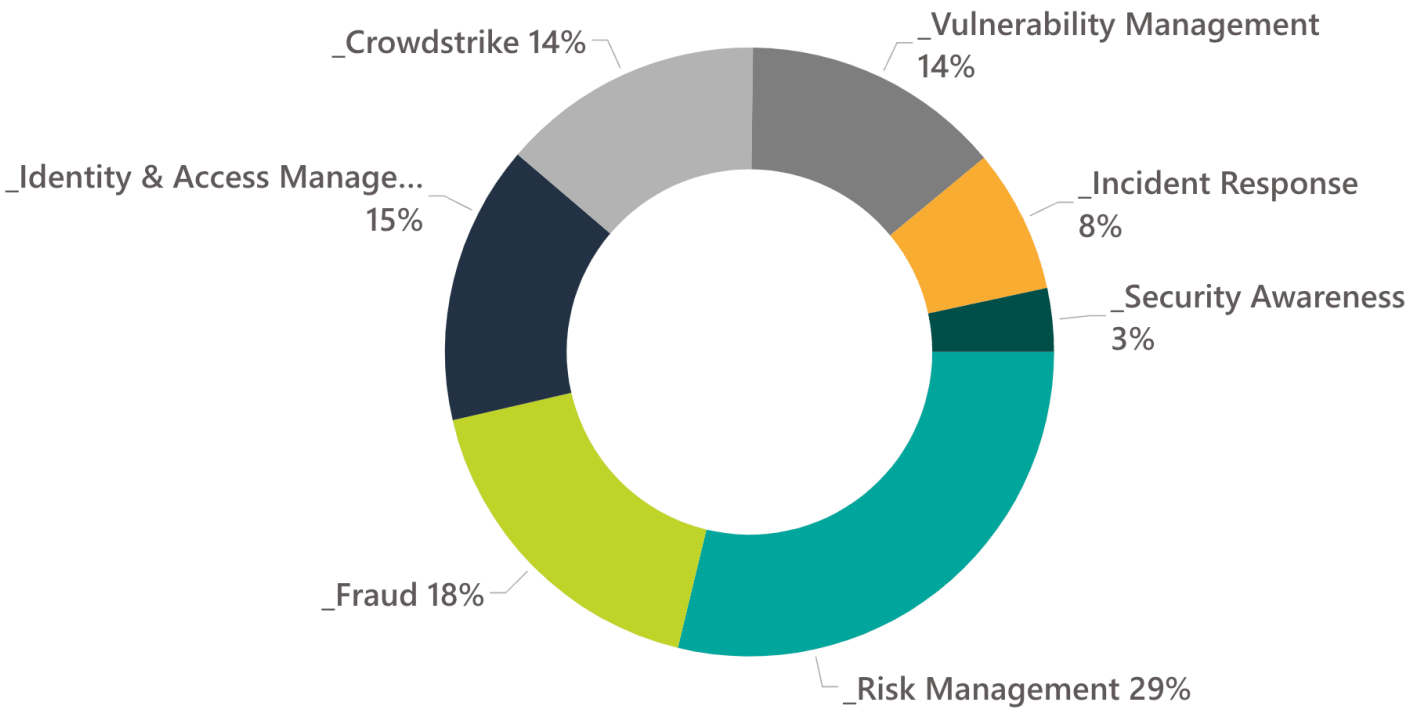
- email-src (3448)
- email-subject (2143)
- url (1357)
- comment (1292)
- domain (1226)
- link (321)
- ip-src (283)
- phone-number (165)
- sha256 (154)
- text (126)

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 July to September 2024, a total of 209 RFIs were submitted, generating 621 responses and 168 unique members participated, representing 58% of our total membership. In comparison, during the same period in 2023, RH-ISAC received 74 RFIs that resulted in 241 responses. This year, the continuous focus on engagement and enhanced offerings led to a significant increase in community interaction, with RFIs up by 182% and responses by 158%.

Overall RFI Domains for July - September 2024

209 RFIs | 617 Responses



Summary of RFI Publications

Firewall Management Responsibilities

On 6 August 2024, a member published an RFI within the CISO community through RH-ISAC. This inquiry aimed to clarify the responsibilities between the Information Security and Networking departments regarding firewall management.

Vulnerability Management (VM) Board Reporting

On 27 July 2024, a member released an RFI in the CISO Community focusing on how organizations communicate vulnerabilities to their Boards of Directors. The goal was to gather best practices for reporting vulnerabilities and related security issues.

Assessment of Brand Protection and Digital Risk Management Responsibilities

On 11 September 2024, a member published an RFI in the CISO Community on Slack. This inquiry aimed to identify the individuals responsible for Brand Protection and Digital Risk Management within organizations, exploring various management approaches in these critical areas.

Assessing Personal Email Access on Company Devices

On 24 September 2024, member published an RFI in the CISO community. This inquiry sought to assess whether organizations restrict employees from accessing personal email on company devices, examining the pros and cons of such policies.

Surveys & Best Practices Reports

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

Bulk User Account Impact on Return Fraud

This report outlines best practices for managing the influence of bulk user accounts on return fraud, specifically within the retail sector. It highlights key indicators of compromise (IoCs) and effective mitigation strategies to counter common tactics, techniques, and procedures (TTPs) associated with bulk account fraud. Valuable insights from our Associate Member, Kasada, further enrich this document.

2024 RH-ISAC Tools & Technology Report

Conducted in August 2024, this third annual Tools & Technology Benchmark collected insights from 71 distinct member companies. The report offers an overview of the most commonly used tools among members, including Threat Intelligence Platforms (TIP), Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), Endpoint Detection and Response (EDR), and other critical solutions.

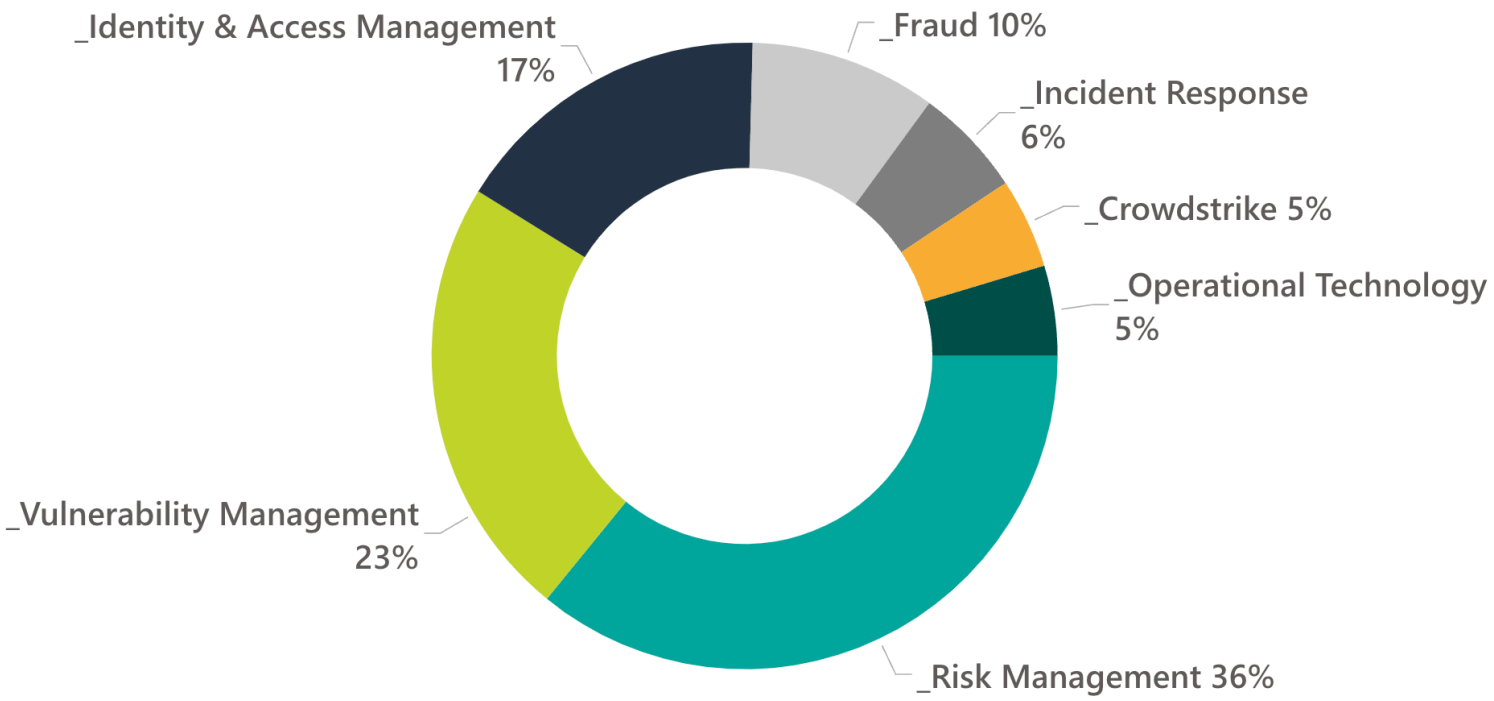
Data Loss Prevention (DLP) Survey Report

In September 2024, the RH-ISAC conducted a DLP survey that gathered 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.

CISO Community Overview

In the CISO Community, from July to September 2024, a total of 34 RFIs were submitted, resulting in 126 responses. During this period, 32% of the RFIs originated from the Risk Management domain, with a notable focus on Policy and Architecture as well as Governance, Risk, and Compliance. Fraud accounted for 18% of the RFIs, primarily addressing sub-domain topics related to Security Controls and Bots. Additionally, Risk Management constituted 36% of the RFIs, highlighting key areas such as Policy and Architecture, Governance, Risk and Compliance, and Risk Mitigation. The figures below provide a detailed breakdown of the RFIs submitted to the CISO Community.

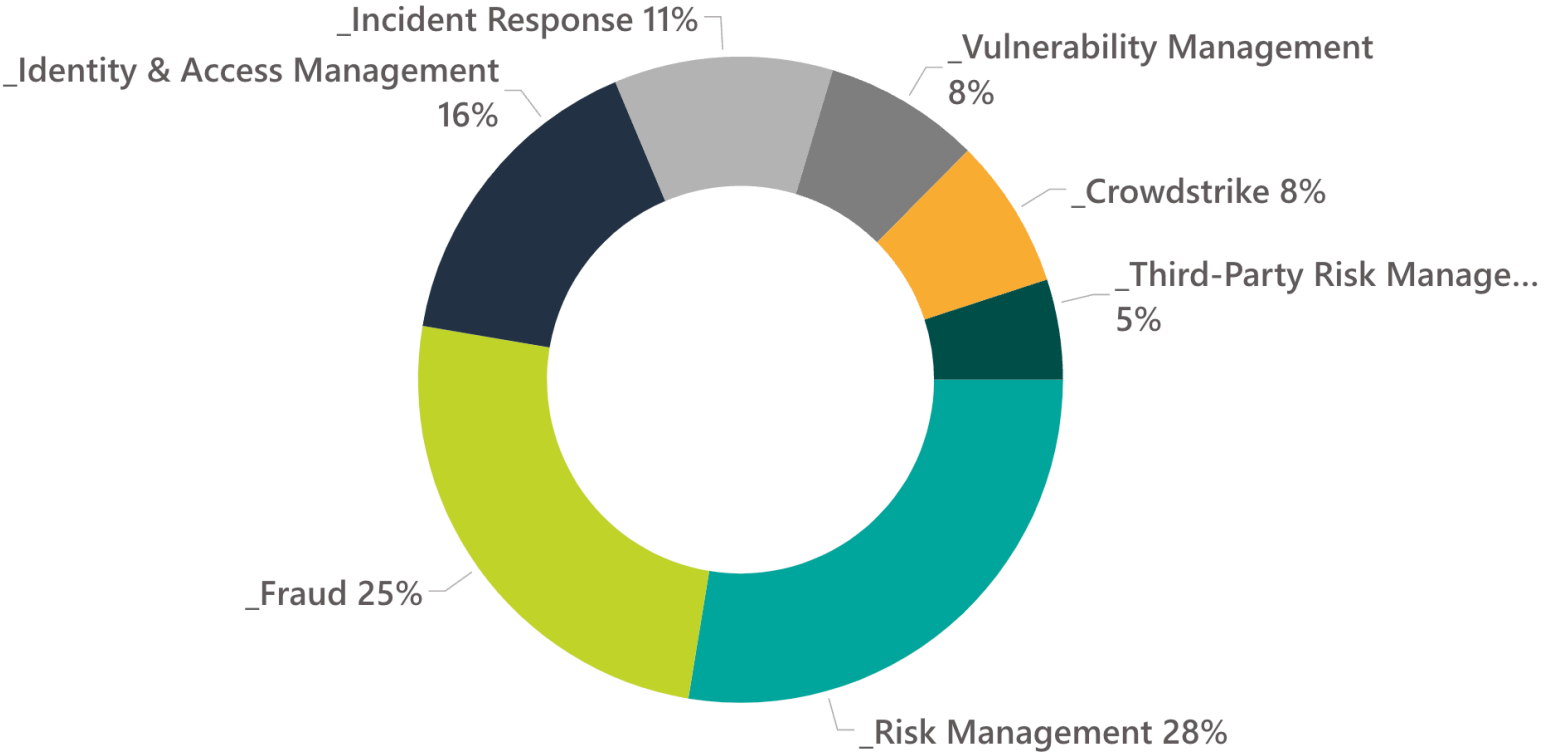
CISO RFI Domains for July - September 2024
34 RFIs | 126 Responses



Analyst Community Overview

In the Analyst Community, from July to September 2024, a total of 104 RFIs were submitted, generating 309 responses. Key discussion topics during this period included Risk Management, Fraud, Identity and Access Management, Incident Response, and Vulnerability Management. The most prominent subdomains within the Analyst Community were Policy and Architecture, Bots, Governance, Risk and Compliance, Access Controls, and Multi-Factor Authentication. The figures below show a total breakdown of the RFIs submitted to the Analyst Community.

Analyst RFI Domains for July - September 2024
104 RFIs | 309 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 third quarter of 2024, third-party outages, vulnerability disclosures, exploits, and compromises continued to be the primary theme of RH-ISAC intelligence reporting, especially events related to Crowdstrike, payroll tools, Magento, and Chrome. Additionally, fraud efforts targeting enterprises and consumers emerged as prevalent themes.

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 July - 30 September 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

Leading reporting from the second quarter of 2024 included:

- GitLab Pipeline Vulnerability Affects Community and Enterprise Versions; Patch Available
- SolarWinds Serv-U Vulnerability Under Active Attack; Patch Available
- CDK Global Cyberattack Impacts Thousands of US Car Dealerships
- PHP Fixes Critical RCE Flaw Impacting All Windows Versions
- Ariane Check-In Terminals Used by Thousands Vulnerable to Info Leak
- CheckPoint Releases New Methodologies for Malicious NSIS-Based Packages for AgentTesla, Remcos, and XLoader Malware
- Cisco Talos Sees New Brand Impersonation Methodologies from Malicious Actors
- HijackLoader Updated with New Evasion Techniques
- Novel Botnet Exploiting High Severity Vulnerability in D-Link Devices
- Widespread Adware targeting macOS “Adload” Adapting to Evade Apple XProtect Signatures